Г.П.Аншаков, Ю.Г.Антонов, Я.А.Мостовой

# ТОЛЕРАНТНЫЙ ПОДХОД ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВСТРОЕННЫХ УПРАВЛЯЮЩИХ ЦВМ

Программное обеспечение (ПО) встроенных в систему управления управляющих ЦВМ (ВУЦВМ) становится одним из наиболее трудоемких и важных продуктов, производимых в процессе разработки систем управления сложных технических систем.

В связи с этим возрастает "цена" ошибки ПО ВУЦВМ и требования к его надежности - способности выполнять требуемые функции в заданных условиях и диапазонах исходных данных в течении заданного времени эксплуатации.

Объективно в сложных комплексах программ для ВУЦВМ, по опыту их эксплуатации, имеются невыявленные ошибки. Ошибки ПО являются следствием сложности логики системы управления и ПО, ограниченных возможностей человека, большой размерности решаемых задач.

Потребности технологического времени для абсолютно достоверной отладки таких комплексов ПО во много раз превышают отведенные директивные сроки их разработки. Поэтому отладка сложного комплекса программ - всегда разумный компромисс между технологическими возможностями и полным количеством вариантов отладки, определяемых структурой программного комплекса, числом межпрограммных связей, числом локальных переменных, наложением работы программных модулей во времени.

Поэтому для ПО ВУЦВМ наряду с эффективной технологией разработки, основные моменты которой в настоящий момент общеприняты /2/, и тщательным планированием процесса отладки, позволяющим достичь наибольшей "отлаженности" доступным количеством вариантов, необходимо применение ряда конструктивных мероприятий, позволяющих обеспечить выполнение задачи системой при возникновении (проявлении) ошибки в ПО, т.е. обеспечить толерантность к ошибкам по ВУЦВМ.

Классические методы временного и функционального резервирования, применимы и для ПО ВУЦВМ /3,2/, но требуют больших ресурсов ВУЦВМ по памяти и времени процессора.

В настоящей статье предполагается и рассматривается другой подход обеспечения толерантности, связанный с приданием ПО свойств ремонтопригодности, доказавший свою эффективность при разработке ряда сложных систем управления с ВУЦВМ.

При таком подходе наряду с вероятностью безотказной работы необходимо рассматривать еще одну меру надежности ПО ВУЦВМ - коэффициент готовности: вероятность того, что ПО находится в работоспособном состоянии в момент времени t при условии, что ПО было полностью работоспособно в момент t=0.

При этом характеристики ремонтопригодности ПО (время необходимое для обнаружения ошибки, локализации ее, принятия решения о необходимости корректирующего воздействия, время необходимое для составления и применения корректирующего воздействия) оказывают существенное влияние на эксплуатационные характеристики системы управления - коэффициент готовности ПО.

Важным элементом системы управления, обеспечивающим реализацию данного подхода - "ремонт" ПО ВУЦВМ, является распределенная система контроля, обнаруживающая ошибки ПО в процессе его функционирования.

Достоверное и быстрое обнаружение ошибок ПО обеспечивается, если такой контроль осуществляется на нескольких уровнях:

1) на аппаратном уровне ВУЦВМ - средствами ВУЦВМ;
2) на уровне встроенной операционной системы ВУЦВМ;
3) на уровне специального ПО ВУЦВМ;
4) на уровне аппаратуры системы управления;
5) внешними по отношению к ВУЦВМ "дежурными" сигналами.

Во всех случаях обнаружения ошибки автоматическим контролем необходима определенная последовательность действий системы управления по ее парированию.

Эта последовательность действий должна начаться с автономных проверок работоспособности ВУЦВМ (тестирования) и связана, как правило, с прекращением нормального функционирования системы управления.

Прекращение нормального функционирования в зависимости от условий проявления ошибки может быть различной "глубины": от перевода системы управления в пассивный режим "ожидания решения" до выполнения действий по продолжению решения задач. При выборе уровня этой "глубины" следует иметь в виду необходимость разделения аппаратурной ошибки от программной, что вследствии двойственного характера работы ВУЦВМ требует определенного времени и дополнительной информации.

Так же при выборе уровня этой "глубины" следует иметь в виду возможность искажения в случае программной ошибки данных в оперативном запоминающем устройстве ЦВМ не только в зонах, часто обновляемых с датчиков, но и в зонах долговременного хранения информации.

Поскольку в общем случае нормальное функционирование ПО ВУЦВМ при проявлении в нем ошибки может оказаться невозможным до момента ее устранения, ремонтопригодное ПО и система управления в целом должны обладать рядом характерных свойств.

Во-первых, ПО ВУЦВМ должно быть построено таким образом, что даже в случае проявления ошибки ПО остается функционировать некоторое "ядро", на которое передается управление, обеспечивающее решение "дежурных" задач системы управления и задач, связанных с реализацией упомянутой последовательности действий по диагностике ошибки, задач "выживаемости", восстановления правильной информации в ОЗУ БВС.

Если ошибка ПО затрагивает и это "ядро", то в ПО должны быть фрагменты, переводящие (по возможности организованно) систему управления в пассивное состояние с передачей информации об этом в систему более высокого ранга, что обеспечивает прекращение развития катастрофических последствий ошибки ПО.

Методы "ремонта" программ, 'зашитых" в ПЗУ ВУЦВМ и вследствие этого недоступных для прямого изменения, базируются на трех основных способах.

Первый из них связан с исполнением в ОЗУ ВУЦВМ специальной корректирующей программы (ПрОЗУ), которая работает "параллельно" с неверно работающей штатной программой ПО и закладывается при этом в ОЗУ по линии оперативной связи до момента выдачи ошибочных результатов из штатного ПО ПрОЗУ подменяет неверный результат на правильный, полученный в результате ее работы.

Данный подход требует определенной организации вычислительного процесса, реализуемого бортовой операционной системой и допускающей параллельное исполнение корректирующей ПрОЗУ и штатного ПО.

Второй способ связан с организацией в ПО ВУЦВМ возможности замены фрагментов (модулей или программ целиком) ПО прошитых в ПЗУ на фрагменты ПО аналогичного назначения, размещаемых в ОЗУ.

При этом в штатном ПО создается система блоков анализа признаков наличия ПрОЗУ. Признак наличия ПрОЗУ засылается по линии связи в определенную зону ОЗУ, вместе с самой ПрОЗУ, которая также заносится по определенным адресам ОЗУ ВУЦВМ.

При инициализации программа или ее фрагмент проверяет наличие ПрОЗУ для своей работы. Если такой признак имеется, то управление передается программой на ПрОЗУ и таким образом осуществляется замещение-обход "дефектного" места ПО. По завершении работы ПрОЗУ осущест-

вляется возврат в программу из ПЗУ.

Данный способ требует довольно большого дополнительного расхода памяти и поддержки со стороны операционной системы.

Третий способ реализуется путем исполнения всех программ ПО из ОЗУ, в которое они загружаются из ПЗУ при включении в работу ВУЦВМ. В этом случае имеется возможность загрузить в ОЗУ ВУЦВМ по линии связи уже исправленную программу.

Исполнение всех программ ПО из ОЗУ предъявляет повышенные требования к защищенности информации в ОЗУ, что требует дополнительных аппаратных и программных затрат.

Для традиционных ВУЦВМ, в которых программы исполняются из ПЗУ, наиболее рациональным является сочетание первого и второго способа.

Для оценки численных характеристик надежности - ремонтопригодности ПО в рассматриваемом смысле можно использовать аппарат марковских процессов с непрерывным временем и дискретными состояниями.

Поток ошибок бортового ПО, а также поток ремонтных воздействий можно принять пуассоновским вследствие выполнения условий ординарности и отсутствия последействия, а также учитывая предельные свойства пуассоновских потоков.

Рассмотрим возможные состояния ПО в зависимости от наличия ошибок в нем:

1) система исправна, то есть ошибки не проявляются - $S_0$.

2) в системе проявилась ошибка, обнаруженная автономной системой контроля, и система управления в результате прекратила выполнение задачи и переведена в пассивное состояние, предотвращающее развитие катастрофической ситуации - $S_1$. Обозначим $\lambda_{01}$ интенсивность перехода системы из состояния $S_0$ в состояние $S_1$. Эта интенсивность переменна во времени, но в течении времени эксплуатации одного-двух экземпляров системы управления ее можно принять постоянной.

3) из состояния $S_1$ система может перейти в состояние $S_0$ (с интенсивностью $\mu_{10}$), когда в результате анализа обнаруживаются неправильные данные, введенные в ВУЦВМ в процессе эксплуатации, неправильные управляющие действия эксплуатационников или ошибки в ПО, корректирующие действия на которые известны и не требуют составления новых ПрОЗУ.

Из состояния $S_1$ система может также перейти с интенсивностью $\lambda_{12}$ в состояние $S_2$ - состояние, требующее разработки ПрОЗУ.

4) из состояния $S_2$ система после составления и применения корректирующей ПрОЗУ переходит в исправное состояние $S_0$. Интенсивность

перехода в состояние - $\mu_{20}$.

Сказанное отражается графом (Рис.)

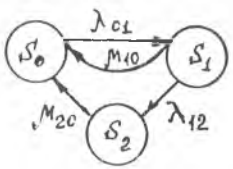


Рис.

Составим уравнение Колмогорова для этого случая

$$\begin{aligned}
\frac{dP_0}{dt} &= \mu_{10}P_1 + \mu_{20}P_2 - \lambda_{01}P_0,\\
\frac{dP_1}{dt} &= \lambda_{01}P_0 - \mu_{10}P_1 - \lambda_{12}P_1, \qquad (1)\\
\frac{dP_2}{dt} &= \lambda_{12}P_1 - \mu_{20}P_2,\\
P_0 &+ P_1 + P_2 = 1.
\end{aligned}$$

Тогда в установившемся состоянии вероятность нахождения ПО в "исправном состоянии" $S_0$ - коэффициент готовности равен:

$$P_0 = \frac{\mu_{20}(\mu_{10}+\lambda_{12})}{\lambda_{01}(\lambda_{12}+\mu_{20})+\mu_{20}(\mu_{10}+\lambda_{12})} = \frac{1}{\frac{\lambda_{01}}{\mu_{20}}\cdot\frac{1+\mu_{20}/\lambda_{12}}{1+\mu_{10}/\lambda_{12}} + 1}.$$

Предложенные в данной статье подходы к обеспечению и оценке надежности ПО ВУЦЕМ реализованы при создании сложных комплексов ПО реального времени и позволяют рассчитывать надежность ПО и системы управления в целом как на этапе эксплуатации систем, так и в процессе их проектирования.

Ошибки ПО ВУЦЕМ даже при принятии мер, предотвращающих их катастрофические последствия, в практически реализуемом диапазоне значений $\lambda_{01}/\mu_{20}$, $\mu_{10}$, $\lambda_{12}$ приводят к заметному снижению эффективности систем управления. Поэтому весьма актуальны дальнейшие усилия по совершенствованию технологии разработки и отладки ПО, что также повысит эффективность от придания ПО свойств "ремонтопригодности" ( за счет уменьшения $\mu_{10}$, $\mu_{20}$).

Список литературы

1. Димон Б., Сингх Ч. Инженерные методы обеспечения надежности систем. – М.:Мир, 1984. – 317 с.

2. Липаев В.В. Тестирование программ. М.:Мир, 1986.– 293с.

3. Шураков В.В. Надежность программного обеспечения систем отработки данных. – М.:Финансы и статистика, 1987. – 271 с.

УДК 531.383

Г.П.Аншаков, С.Н.Егоров

## ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕОРИИ ЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ОРИЕНТАЦИИ КА ДЗЗ

В практике проектирования высокоточных активных систем ориентации КА дистанционного зондирования Земли (ДЗЗ) широко используется принцип декомпозиции вращательного движения КА на программное и возмущенное движения, что позволяет исследовать эти движения раздельно. При разработке алгоритмов программного управления в общем случае должны применяться полные нелинейные уравнения вращательного движения КА, но допустимо пренебрегать влиянием малых факторов, вызванных неполнотой априорной и измерительной информации об уравнениях движения и параметрах состояния. При проектировании подсистемы управления возмущенным вращательным движением КА существенным является учет малых, обычно случайных или неизвестных, возмущений, не учтенных при синтезе программного управления. Высокая точность активных систем ориентации позволяет эффективно линеаризовать уравнения вращения КА, исполнительных органов и измерителей в окрестности программного движения. Поэтому для исследования возмущенного движения КА целесообразно применять методы теории линейных динамических систем управления с учетом неопределенности возмущающих воздействий и ошибок измерений.

В системе ориентации КА динамический наблюдатель теории линейных систем соответствует подсистеме определения параметров ориентации, а закон управления – подсистеме управления возмущенным вращательным