**Надежность технических средств**

**Введение**

Одна из основных причин широкого применения РВС в АСУ производством – их высокая надежность. При делении системы на ряд автономно работающих ЛВС сбой в одной машине не влечет за собой отказ всей системы. Для того чтобы система функционировала непрерывно, необходимо иметь не только резервные средства обработки, но и обеспечить надежность всей системы в целом – от датчиков до исполнительных органов, поскольку ЭВМ, получающая неверную информацию от датчиков, даже при ее полной исправности может принести больший ущерб, чем просто неисправная ЭВМ. Поэтому главная цель мероприятий по повышению надежности - обеспечение непрерывной работы системы, на которую не должны влиять ни ошибки, ни сбои.

**1. Жизнеспособность вычислительного комплекса**

Практика внедрения информационных, управляющих и других систем реального времени показывает, что недооценка жизнеспособности системы на стадии ее проектирования ведет порой к катастрофическим результатам - провалу всего проекта.

В отличие от систем пакетной обработки, рассматривавшихся ранее, к комплексам технических систем реального времени (СРВ) предъявляются дополнительные требования, связанные с особенностью данных систем, а именно: комплексы программ, работающие в реальном масштабе времени, обмениваются данными многими различными способами как в одной ЭВМ, так и по линиям связи, образуя сложные интерфейсы; сообщения поступают в систему независимо друг от друга и в случайные моменты времени; нарушение связи между программными модулями или ошибка в данных даже в одной ЭВМ могут вызвать непоправимые нарушения и не только в работе остальных входящих в вычислительную систему ЭВМ и периферийного оборудования, но и в деятельности всего предприятия или даже объединения, эксплуатирующего данную систему управления. Тем не менее, при всей очевидной важности проблемы обеспечения жизнеспособности комплекса технических средств при проектировании и создании АСУ различного профиля, данный вопрос редко когда решается более серьезно, чем простым резервированием некоторых наиболее "ненадежных", с точки зрения разработчиков, технических средств.

Рассмотрим компоненты, определяющие жизнеспособность вычислительной системы.

Жизнеспособность является интегральной мерой возможностей системы, которая количественно связывает три следующих фактора: надежность, ремонтопригодность и технические возможности оборудования.

Надежность в приложении к ВС часто количественно определяют средним временем между отказами (СВМО) или наработкой на отказ, т.е. как ожидаемое время между ближайшими последовательными сочетаниями событий, приводящих к отказу.

Ремонтопригодность статистически выражается средним временем восстановления (СВВ), которое необходимо для того, чтобы устранить те причины, которые привели к возникновению отказа.

Технические возможности системы определяются как степень удовлетворения системой требований со стороны задач, для решения которых она предназначена.

В основе высокой жизнеспособности КТС лежит его способность "деградировать" постепенно, т.е. способность продолжать свое хотя бы частичное функционирование, несмотря на то, что со временем технические параметры устройств ухудшаются, до тех пор, пока не перестанет работать его основное ядро.

**2. Среднее время между отказами**

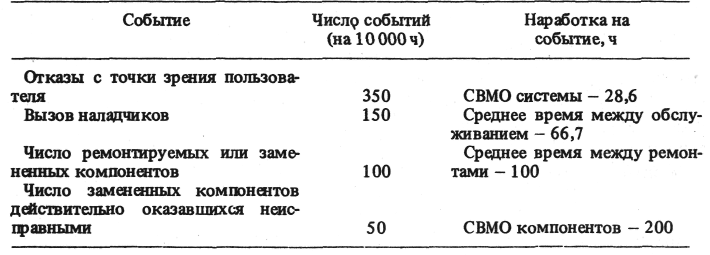
Используя СВМО, можно характеризовать надежность от отдельных элементов до системы в целом. При этом для оценки СВМО используют перечень приводящих к отказу событий и функцию, описывающую вероятность наступления таких событий. Надежность выражается СВМО, измеряемым в часах или его обратной величиной – частотой отказов.

По мере сборки блоков из элементов вплоть до устройства в целом все сложнее становится идентификация событий, составляющих отказ. Тем не менее в большинстве случаев можно применить эффективные меры для выяснения того, произошел отказ в системе или нет. Такие меры составляют важную часть технических условий на систему.

Основная трудность, с которой сталкивается проектировщик АСУ при определении надежности технических средств, заключается в том, что расчетные данные достоверны лишь в той степени, в какой достоверны принятые исходные значения частоты отказов элементов. Серийно выпускаемые в настоящее время элементы вычислительных систем и средств автоматизации имеют достаточно высокую надежность (например, частота отказов интегральных микросхем составляет от 0,01 до 0,4 отказа на миллион часов работы). В силу этого достоверные данные по надежности отдельных устройств и системы могут быть получены только после длительных испытаний.

Кроме того, само понятие отказа вычислительной системы нуждается в уточнении. Различают отказы элементов системы и отказы системы с точки зрения пользователя. Данные об отказах первого типа, как было отмечено, содержатся в паспортных данных. Отказы второго типа не всегда вызываются отказами компонентов системы. Причинами системных отказов, с точки зрения пользователя, могут быть не только перемежающиеся отказы и сбои в работе компонентов, но также отказы программного обеспечения. Поэтому не всегда верна трактовка отказа системы, заключающаяся в том, что дефектный компонент дает всего один отказ, приводящий к системному, после чего он заменяется. Ниже приведен пример ситуации (табл. 1), когда 50 дефектных компонентов привели к 150 случаям вызова наладчиков и инженерного персонала пользователями системы, кроме того, к 50 случаям бесполезного поиска неисправных компонентов и 100 случаям замены компонентов, половина из которых на самом деле исправны.

Таблица 1



Значение СВМО системы зависит в определенной мере от пользователей; некоторые из них при отказе перезапускают ее процедурами рестарта, в то время как другие прибегают к помощи наладчиков и требуют поиска неисправностей. В результате, с точки зрения пользователя, СВМО системы окажется отличным от рассчитанного разработчиком и указанного в технической документации.

**3. Ремонтопригодность системы**

Статистически ремонтопригодность выражается средним временем восстановления системы, которое зависит от контекста еще в большей степени, чем средняя наработка на отказ.

Среднее время восстановления само по себе является величиной, определяемой средними временами выполнения следующих основных операций: обнаружения факта появления отказа; выделения отказавшего элемента; удаления отказавшего элемента; получения, замены или ремонта данного элемента; монтажа заменяемого элемента; проверки работы после замены; инициализации ВС; возобновления работы программного обеспечения эксплуатируемой системы.

Все эти операции, кажущиеся простыми, на самом деле взаимосвязаны. Например, замена отказавшего элемента может привести к отказу другого; на поиск отказа в ВС может уйти непредсказуемо долгое время, особенно если этот отказ не выявлен сразу, а повлек за собой серию лавинообразных изменений в системе программного обеспечения; выявление отказавшего элемента вызывает побочные действия, приводящие к отказу уже не одного блока, а всей вычислительной системы в целом. В частности, отключение питания на отказавшем устройстве в случае отсутствия отдельного разъема может привести к необходимости отключения стойки, в которой находится ряд исправных и не подлежащих выключению устройств; проверка работоспособности отремонтированного блока вне системы не является гарантией того, что блок является исправным; успешная инициализация системы после ремонта одного из ее блоков может подчас говорить не об успешном включении данного блока в работу всей ВС, а лишь о слабой его загрузке и т д.

Поэтому ремонтоспособность системы зависит в первую очередь от следующих "неизмеряемых" факторов: организации обслуживания на месте, средств обслуживания, квалификации обслуживающего персонала, места расположения неисправного блока, его окружения, удобства замены блока. Все эти факторы могут вызвать заметное отклонение от ^среднего времени восстановления системы. Игнорировать эти кажущиеся "мелочи" проектировщик систем реального времени не имеет права.

В вычислительной системе можно довести детализацию любого из ее блоков до элементов, с которыми не происходит постепенной "деградации". Такой элемент находится всегда в одном из двух альтернативных состояний - ВКЛ или ВЫКЛ. Вероятность того, что элемент находится в состоянии ВКЛ называется готовностью элемента. Аналогичный параметр ВС называется готовностью системы.

Готовность элемента определяется формулой Рвкл = СВМО/ (СВМО + СВВ). Данная формула является приближенной, тем не менее она является весьма эффективной при оценке жизнеспособности системы. Вероятность того, что элемент находится в состоянии ВЫКЛ, определяется формулой

Рвыкл = 1 - Рвкл = СВВ/ (СВМО + СВВ).

Для работоспособности системы нет никакой разницы между отключением элемента из-за его выхода из строя или отключения в профилактических целях. Следовательно, СВМО и СВВ должны отражать организацию профилактических работ, предусмотренных для данной системы. Если эти времена существенно зависят от профилактических работ (например, для лентопротяжных механизмов), имеет смысл оценить это влияние. Пусть система состоит из п элементов. Так как каждый из них может находиться в одном из двух состояний (ВКЛ или ВЫКЛ), то имеется 2n возможных или конфигурационных состояний системы и с каждым состоянием связана вероятность нахождения ВС в этом состоянии. Для подсистемы i получим:

Piвкл = СВМОi/(СВМОi + СВВi), а Piвыкл = СВВi(СВМОi + + СВВi).

Вероятность данного состояния системы РS определяется для независимых подсистем как произведение вероятностей для подсистем, отвечающих данному состоянию:



где



Предположим, что для каждого конфигурационного состояния системы, т.е. для каждого интересующего нас параметра технических возможностей, его величина, определяемая в числовом виде, имеет особое значение. Тогда анализ жизнеспособности ВС будет состоять из следующих шагов:

1) разработка модели конфигурационного состояния ВС;

2) определение на основе элементов СВМО и СВВ коэффициента готовности для каждого конфигурационного состояния.

**4. Функция ограничения возможностей системы**

Предположим, что нас интересуют k параметров, определяющих технические возможности ВС. С каждым конфигурационным состоянием Sx связана определенная величина каждого из рассматриваемых параметров Аkх, с которым в свою очередь связана функция ограничения (Fогр), определяющая относительную важность соответствующего параметра. Эта функция

Fогр = f {Sх; Akx, τx},

где τх - длительность нахождения системы в данном состоянии. Задержка выполнения функции обработки может оказаться не столь важной, пока не достигнет пороговой величины. Повышение (относительно расчетных) технических возможностей никак не учитывается, тогда как уменьшение их ниже допустимого предела резко ограничивает возможности ВС. Например, для нормального функционирования операционной системы UNIX на ЭВМ класса СМ-4 требуется объем оперативной памяти – 1 Мбайт, в случае уменьшения ее до 256 Кбайт возможности данной ОС резко падают и она практически теряет все преимущества перед другими ОС, значительно более слабыми (RSX - 11 М).

На рис. 1 приведен вид некоторых типичных функций ограничения, где по оси X откладывается значение параметра (в нормализованном от некоторого заданного уровня виде), а по оси Y – значение параметра, определенное функцией ограничения.

На рис. 1, а приведена функция ограничения параметра, для которого превышение технических возможностей игнорируется по каждому их уровню вплоть до максимума, которому присваивается полный вес. Например, дисковая память емкостью ?9 Мбайт не дает никаких практических преимуществ, если для создания базы данных системы со всеми словарями необходимо 10 Мбайт.

На рис. 1, б приведена функция ограничения для нежелательного параметра. Номинальному значению соответствует полное отсутствие данного фактора. Примером такого параметра является время реакции в системе, которое в идеальном случае должно выражаться несколькими миллисекундами. В случае его увеличения до величины, вызывающей у пользователя нежелание работать с предлагаемой ему системой, дальнейшее снижение значения функций ограничения приостанавливается.

На рис. 1, в приведена функция ограничения параметра, который получает положительную оценку лишь по достижении определенной минимальной величины (например, система сервоуправления, где для обеспечения стабильности каждую секунду необходимо выполнять минимальное число итераций).

На рис. 1, г приведен параметр с функцией ограничения типа "окно". Примером может служить устройство построчной печати, при уменьшении скорости печати которого до некоторой минимальной величины его полезность равна нулю, поскольку для этой скорости печати существуют знакосинтезирующие устройства, значительно более дешевые. Если же устройство печатает с очень большой скоростью все время, то это также не имеет смысла, поскольку гору бумаги, которую в состоянии напечатать современное устройство печати даже за 1 ч непрерывной работы, невозможно просмотреть в приемлемое время ни одному пользователю.

На рис. 1, д приведена двоичная функция ограничения, которая характеризуется тем, что, как только рассматриваемый параметр превзойдет заданный минимальный уровень, функция ограничения сразу приобретет максимальное значение. Пример такой системы – синхронная передача данных: при стыковке дисплея с ЭВМ совершенно неважно, что линия может работать со скоростью в несколько млн. бод, поскольку дисплейный интерфейс работает со значительно меньшей скоростью (9600 бод), а на любой другой скорости передачи данных возникают искажения.

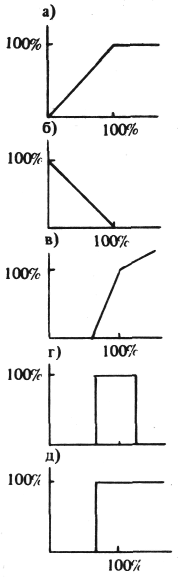


Рис. 1

Приведенные примеры не описывают весь возможный диапазон функций ограничения, которая может быть непрерывной, дискретной, разрывной, нелинейной и т.д. Кроме того, Fогр может меняться с течением жизни вычислительной системы или программного обеспечения, реализованного на данной ВС.

**5. Распределение уровней технической возможности КТС**

Поскольку каждому конфигурационному состоянию системы ставится в соответствие некоторая вероятность, а каждому параметру технических возможностей – некоторая величина, то вероятность достижения любого заданного уровня технической возможности определяется как сумма вероятностей пребывания в каждом из состояний с таким уровнем. Как правило, состояний, в которых достигается данный уровень некоторой технической возможности, достаточно много.



Рис. 2

Суммируя вероятности, относящиеся к каждому уровню параметра технических возможностей, можно построить функцию распределения вероятностей, подобную изображенной на рис. 2. Практически такая функция не может быть непрерывной, однако в таком виде ею значительно легче пользоваться.

Для каждого параметра технических возможностей имеется по одному такому распределению. Система, у которой отсутствует постепенная "деградация", на таком графике будет представлена двумя точками. Система более общего вида характеризуется подобной кривой, и именно это распределение описывает жизнеспособность системы.

Математическое ожидание распределения выражает ожидаемое значение рассматриваемого параметра, получаемое усреднением по всей совокупности возможных состояний. Отношение среднего значения параметра к максимальному называется эффективной жизнеспособностью ВС. Второй момент этого распределения характеризует спорадичность поведения системы, третий – показывает, насколько может ухудшиться положение перед окончательным выходом ВС из строя.

Показанное на рис. 2 распределение типично для системы с хорошей жизнеспособностью. Чем больше μ, тем меньше σ, и чем меньше пик при нулевом уровне рассматриваемого параметра, тем лучше качество системы. Подъем вблизи нуля показывает, что ВС имеет больше состояний, в которых она не работоспособна, чем это определяется уровнем технических возможностей.

Еще более удобный способ представления данных о жизнеспособности системы - построение кривых распределения интегральной вероятности различных параметров технических возможностей. В результате получим кривые, показанные на рис. 3. Кривая А типична для систем с постепенной деградацией; В – отражает более высокий уровень жизнеспособности; кривая D характерна для ВС, в которой высокая надежность отдельных блоков сочетается с малой собственной жизнеспособностью; Е – отражает работу системы в режиме двоичного отказа при нахождении точки разрыва далеко от начала, такая система близка к идеальной; кривая F является иллюстрацией получения высокой жизнеспособности за счет большого запаса надежности.



Рис. 3

Необходимая в каждом случае форма кривой зависит от характера применения ВС, что должно быть оговорено в технических условиях на нее. Следует задавать, по крайней мере, два уровня каждого параметра технических возможностей, а также значение вероятности для каждого из этих уровней.

В настоящее время эффективное значение жизнеспособности, равное 0,99, в случае достаточно больших систем обеспечивается при условии минимальной избыточности (20-30%) при весьма скромных требованиях к среднему времени между отказами в сотни часов и среднему времени восстановления, составляющему десятки минут. Надо обратить внимание на то, что СВМО в данном случае рассматривается при довольно высоком (90%) уровне достоверности, что не часто бывает на практике.