Основы обеспечения отказоустойчивости программных компонентов

Основные определения

Отказоустойчивость программного средства (Fault tolerance) по ГОСТ 28806-90

Совокупность свойств программного средства, характеризующая его способность поддерживать необходимый уровень пригодности при проявлении дефектов программного средства или нарушении установленных интерфейсов.
Примечание - Необходимый уровень пригодности включает в себя способность к безопасному функционированию при отказах, к минимизации возможных потерь данных и исключению опасных действий при внезапном нарушении условий функционирования [из п. 2.2 Прил. 2 ГОСТ 28806-90]

Введение *отказоустойчивости* требует избыточного аппаратного и программного обеспечения. Направления, связанные с предотвращением неисправностей и с *отказоустойчивостью*, - основные для обеспечения *надежности*.

В настоящее время эти два понятия - *надежности* и *отказоустойчивости* - при описании компьютерных систем часто смешивают. Во многом это объяснятся тем, что пользователя (не обязательно индивидуального) интересует главное: *вычислительная система* должна работать необходимое время и предоставлять определенный набор услуг.

К неправильному функционированию компьютерных систем приводят ошибки в программном обеспечении (ПО) или отказ аппаратуры.

Надежность - свойство объекта сохранять во времени в установленных пределах значения всех параметров в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортирования.

Между определениями надежности для аппаратных средств и ПО имеется принципиальные различия. Программа в большинстве случаев не может отказать случайно. Ошибки в ПО, допущенные при его создании, зависят от технологии, организации и квалификации исполнителей и в принципе не являются функцией времени. Причиной отказов, возникающих из-за этих ошибок и фиксируемых как случайный процесс, является не время функционирования системы, а набор входных данных, сложившихся к моменту отказа.

Надежность является одной из важных характеристик качества объекта - совокупности свойств, определяющих пригодность использования его по назначению. В отличии от других характеристик качества надежность обладает следующей специфической особенностью. Обычные характеристики качества объекта, такие как быстродействие, производительность, емкость памяти и т.д. измеряются для некоторого момента времени («точечные» характеристики качества). Надежность характеризует зависимость «точечных» характеристик качества либо от времени использования, либо от наработки объекта. Надежность характеристика временная. Она может быть ориентированна либо на прошедшее время (в этом случае говорят: изделие до данного момента проработало такое-то количество часов, поэтому они обладали такими-то показателями надежности), либо в будущее время (в этом случае говорят: данные изделия, если они будут использоваться в предложенных условиях, будут обладать такой-то надежностью).

Объект - техническое изделие определенного целевого назначения, рассматриваемое в периоды проектирования, производства, испытаний и эксплуатации.

Объектами могут быть различные системы и их элементы.

Различают пять основных видов технического состояния объектов.

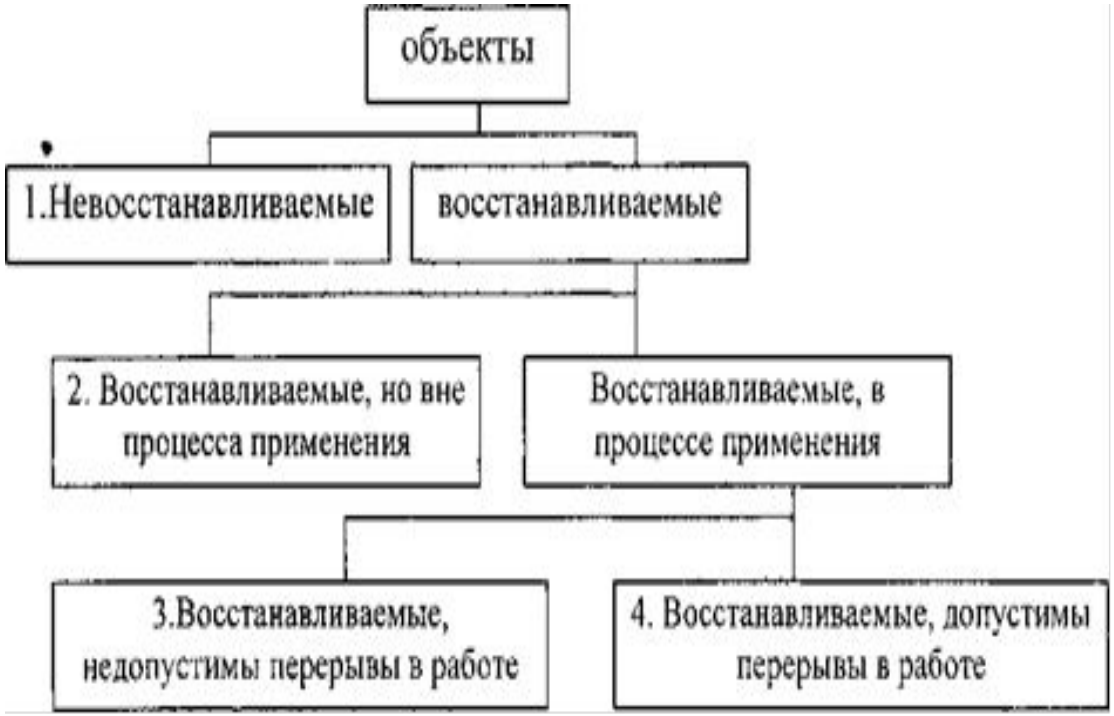
Исправное состояние. Состояние объекта, при котором он соответствует всем требованиям нормативно-технической и (или) конструкторской (проектной) документации (НТиКПД).

Неисправное состояние. Состояние объекта, при котором он не соответствует хотя бы одному из требований (НТиКПД).

Работоспособное состояние. Состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям (НТиКПД).

Неработоспособное состояние. Состояние объекта, при котором значения хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям (НТиКПД).

Предельное состояние. Состояние объекта, при котором его дальнейшая эксплуатация недопустима или нецелесообразна, либо восстановление его работоспособного состояния невозможно или нецелесообразно.


объекты
1.Невосстанавливаемые
восстанавливаемые
2. Восстанавливаемые, но вне процесса применения
Восстанавливаемые, в процессе применения
3.Восстанавливаемые, недопустимы перерывы в работе
4. Восстанавливаемые, допустимы перерывы в работе

Переход объекта (изделия) из одного вышестоящего технического состояния в нижестоящее обычно происходит вследствие событий: ***повреждений*** или ***отказов.***

Согласно ГОСТ 27.002-89 ***отказ -*** это событие, заключающееся в нарушении работоспособного состояния объекта.

Повреждение - событие, заключающееся в нарушении исправного состояния объекта при сохранении работоспособного состояния.

Переход объекта из исправного состояния в неисправное не связан с отказом.

В ГОСТ 15467-79 введено еще одно понятие, отражающее состояние объекта - дефект. Дефектом называется каждое отдельное несоответствие объекта установленным нормам или требованиям. Дефект отражает состояние отличное от отказа.

Классификация и характеристики отказов

- По типу отказы подразделяются на отказы функционирования и отказы параметрические;
- По своей природе отказы могут быть: случайные и систематические;
- По характеру возникновения: внезапный отказ и постепенный отказ;
- Причина возникновения: конструкционный отказ, производственный отказ, эксплуатационный отказ;
- характер устранения: перемежающийся, средний, тяжелый отказы;
- Дальнейшее использование объектов: полные и частичные отказы;
- Легкость обнаружения: очевидные и скрытые;
- Время возникновения: приработочные отказы, отказы при нормальной эксплуатации, износовые отказы.

Стороны надежности

- **Безотказность** - свойство объекта непрерывно сохранять работоспособность в течение некоторого времени или некоторой наработки. Количественные показатели безотказности: вероятность безотказной работы, интенсивность отказов, средняя наработка до отказа.
- **Ремонтопригодность** - свойство объекта, заключающееся в приспособленности объекта к предупреждению и обнаружению отказов и восстановлению работоспособности объекта либо путем проведения ремонта, либо путем замены отказавших комплектующих элементов. Количественные показатели ремонтопригодности: вероятность восстановления в заданное время, среднее время восстановления, удельная трудоемкость и стоимость восстановительных работ.

- **Долговечность** - свойство объекта сохранять работоспособность до наступления предельного состояния. Количественные показатели долговечности: средний срок службы объекта, средний срок службы объекта до первого отказа.

Технический ресурс - наработка объекта от начала его эксплуатации или возобновления эксплуатации после ремонта до наступления предельного состояния.

Назначенный ресурс - суммарная наработка объекта, при достижении которой эксплуатация должна быть прекращена независимо от его состояния.

Срок службы - календарная продолжительность эксплуатации (в том числе, хранение, ремонт и т. п.) от ее начала до наступления предельного состояния.

- **Сохраняемость** - свойство объекта сохранять работоспособность в течение (и после) его хранения и (или) транспортирования.

- **Живучесть** - свойство объекта сохранять работоспособность (полностью или частично) в условиях неблагоприятных воздействий, не предусмотренных нормальными условиями эксплуатации.
- **Достоверность** - это свойство объекта производить безошибочные преобразования, хранение и передачу информации.

Факторы, влияющие на надежность систем

1. Технические факторы:
   - структура объекта и рабочие режимы
   - резервирование
   - контроль и восстановление
   - характеристики комплектующих элементов
   - защищенность от неблагоприятных воздействий
   - степень приспособленности аппаратуры для ее эксплуатации

2. программные факторы:
- точность математической формализации на этапе разработки программ
- полнота и обоснованность требований при выдаче задания на разработку ПО
- степень безошибочности выполнения заданных требований
- степень отлаженности программ
- качество структуры общего алгоритма и степень согласованности отдельных программ в общем комплексе

3. В процессе эксплуатации возникает ряд факторов, влияющих на надежность, к ним относятся:
- качество организации и проведения обслуживания объекта, в т.ч. и профилактического
- своевременность и полнота восстановления работоспособности объекта при его отказах.