Аппаратное резервирование

Резервирование является практически единственным и широкое используемым методом кардинального повышения надежности систем автоматизации.

Оно позволяет создавать высоконадёжные системы:

- аварийной сигнализации;
- противоаварийной защиты;
- автоматического пожаротушения;
- контроля и управления взрывоопасными технологическими блоками
- и др. системы, относящиеся к уровням безопасности SIL1...SIL3.

Также этот метод широко используется в системах, в которых даже короткий простой ведет к большим финансовым потерям (системы распределения электроэнергии, электроснабжения, непрерывные технологические процессы).

Резервирование позволяет создавать высоконадежные системы из типовых изделий широкого применения.

Составной и очень важной частью систем с резервированием является подсистема автоматического контроля работоспособности и диагностики неисправностей.

Если проанализировать причины отказа систем, то можно выделить как минимум четыре, а то и более групп:

- наибольшая группа отказов в системах автоматизации отказ программного обеспечения;
- отказ технических средств (не уступает по многочисленности первой);
- человеческий фактор;
- природные явления и связанные сними последствия.

Аппаратное резервирование

Каждая группа отказов имеет свои способы устранения, а также способы повышения отказоустойчивости.

Рассмотрим вопросы повышения отказоустойчивости технических средств.

Основные определения темы

Неисправностью называется состояние объекта, при котором он не соответствует хотя бы одному своему параметру, указанному в эксплуатационной документации.

Неработоспособностью называется состояние объекта, при котором он не способен выполнять хотя бы одну из своих функций, описанных в эксплуатационной документации. Например, контроллер, у которого отказал один из каналов ввода, является работоспособным, если этот канал не используется, но неисправным.

Дефектом называется каждое отдельное несоответствие объекта установленным требованиям.

Отказом называется событие, заключающееся в нарушении работоспособности объекта. Факт отказа устанавливается на основании некоторых критериев отказа, т.е. признаков, позволяющих судить о нарушении работоспособности. В результате отказа объект становится **неисправным**.

Причины отказов самые различные: от ненадежных схемотехнических решений на стадии проектирования до низкой культуры производства, отсутствия надежных методов контроля, работы компонентов в предельных электрических режимах, нарушений условий эксплуатации и т. п.

Аппаратное резервирование

Наработкой называется продолжительность работы объекта, выражаемая в единицах времени или в количестве циклов (например, циклов срабатывания реле). Различают **наработку до отказа** (от начала эксплуатации до первого отказа) и наработку **между отказами** (от начала работы после ремонта до очередного отказа). Используют также средние значения этих величин.

Среднюю наработку между отказами называют **наработкой на отказ**.

Безотказность - свойство объекта непрерывно сохранять работоспособность в течение некоторого времени или наработки.

Живучесть - свойство объекта сохранять *ограниченную* работоспособность при неисправностях или отказе некоторых компонентов.

Вероятность безотказной работы - вероятность того, что в пределах заданной наработки отказ не возникнет.

Коэффициент готовности - вероятность того, что объект окажется работоспособным в произвольный момент времени, кроме запланированных периодов, в течение которых его работа по назначению не предусматривается. Высокая готовность системы обеспечивается избыточностью, допустимостью сбоев, автоматическим контролем ошибок и диагностированием.

Резервирование может быть **общим**, когда резервируется система в целом, и **раздельным** (поэлементным), когда резервируются отдельные элементы системы. В случае, когда в системе много однотипных элементов (например, модулей ввода сигналов термопар), число резервных элементов может быть в несколько раз меньше, чем резервируемых.

Аппаратное резервирование

Кратность резерва - отношение числа резервных элементов к числу резервируемых, которое выражается несокращаемой дробью. В частности, в соответствии с ГОСТ 27.002-89, кратность резерва 3:2 нельзя представлять как 1,5 и иногда используемый термин "полуторное резервирование" не соответствует стандарту.

При сокращении дроби исчезает важная информация об общем количестве элементов в системе.

Дублированием называют резервирование с кратностью резерва один к одному.

Постоянное резервирование (к нему относится мажоритарное резервирование и метод голосования) - резервирование с нагруженным резервом, при котором все N элементов в резервированной системе выполняют одну и ту функцию и являются равноправными, а выбор одного из N сигналов на их выходе выполняется схемой "голосования", без переключений. Постоянное резервирование позволяет получить системы с самым высоким коэффициентом готовности.

Резервирование замещением - резервирование, при котором функции основного элемента передаются резервному только после отказа основного элемента. Резервирование замещением может быть с холодным, теплым или горячим резервом. Его недостатком является зависимость от надежности переключающих устройств.

Аппаратное резервирование

Нагруженный резерв ("горячий резерв") - резервный элемент, который находится в таком же режиме, как и основой. Недостатком горячего резерва является уменьшение ресурса с течением времени. В системах автоматизации с горячим резервом переход на резерв может занимать время от нескольких миллисекунд до единиц секунд.

Облегченный резерв ("теплый резерв") - резервный элемент, находящийся в менее нагруженном состоянии, чем основной. Например, резервный компьютер в "спящем" режиме является облегченным резервом.

Ненагруженный резерв ("холодный резерв") - резервный элемент, находящийся в ненагруженном режиме до начала его использования вместо основного элемента. Ненагруженный резерв позволяет получить системы с самой высокой надежностью, но с низким коэффициентов готовности. Они эффективны в случае, когда система некритична к времени простоя величиной в несколько минут.

Основное отличие между "горячим", "холодным" и "теплым" резервом состоит в длительности периода переключения на резерв.

При горячем резервировании контроллеров время переключения составляет от единиц миллисекунд до долей секунды, при теплом - секунды, холодном - минуты. Поэтому время переключения на резерв иногда рассматривают как основной признак при классификации резервирования замещением.

Аппаратное резервирование

Надежность - это **свойство** объекта сохранять во времени значения всех параметров и выполнять требуемые функции в заданных условиях применения. Надежность является составным понятием. Оно может включать в себя понятия безотказности, долговечности, ремонтопригодности, сохраняемости. В промышленной автоматизации для количественной оценки надежности чаще всего используется параметр «наработка на отказ» или «интенсивность отказов», а в системах безопасности – «вероятность отказа при наличии запроса»

Интенсивностью отказов называется условная плотность вероятности возникновения отказа объекта, определяемая при условии, что до рассматриваемого момента времени отказ не возник. При испытаниях на надежность количество исправных элементов *n(t)* с течением времени *t* уменьшается за счет того, что часть из них *n(t)-n(t+dt)* становятся неисправными через время *dt* в результате отказа. Интенсивность отказа определяется пределом

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{1}{n(t)} \frac{n(t) - n(t + \Delta t)}{\Delta t} = -\frac{1}{n(t)} \frac{dn(t)}{dt}$$

Длительность *t* безотказной работы элемента (от момента включения *t=0* до *t*) является случайной величиной, поэтому ее можно характеризовать вероятностью

$$P(t) = \frac{n(t)}{n(0)},$$

где $n(0) \to \infty$ - число исправных элементов в момент времени *t=0* (все исправны);

n(t) - число исправных элементов в момент времени *t*.

При конечном числе испытуемых элементов вместо вероятности получают ее точечную статистическую оценку.

Аппаратное резервирование

Вероятность безотказной работы можно интерпретировать следующим образом: если в системе автоматизации используется 100 модулей ввода-вывода, каждый из которых имеет вероятность безотказной работы *P(t)* =0,99 в течение времени *t*=1 год, то через год после начала эксплуатации в среднем один из модулей станет неработоспособен.

Поделив числитель и знаменатель предыдущего выражения на *n(0)* , получим

$$\lambda(t) = -\frac{1}{n(t)}\frac{dn(t)}{dt} = -\frac{1}{P(t)}\frac{dP(t)}{dt}$$

Выражение для функции распределения длительности безотказной работы *P(t)* можно получить, решив дифференциальное уравнение с начальными условиями *P(0)=1:*

$$P(t) = \exp\left(-\int_0^t \lambda(t)dt\right),$$

Вероятность отказа соответственно

$$F(t) = 1 - P(t),$$

Если проанализировать величину интенсивности отказов, то можно выделить три этапа её поведения:

- первый этап - быстрое уменьшение в начале эксплуатации изделия (период приработки);
- второй этап – постоянство
- третий этап – резкое увеличение после окончания срока службы.

Аппаратное резервирование

Для средств промышленной автоматизации указывают значение постоянной интенсивности отказов, то выражение для функции распределения упрощается до следующего

$$P(t) = \exp^{-\lambda t},$$

Таким образом, вероятность безотказной работы устройства на интервале времени от *t=0* до *t* экспоненциально уменьшается с течением времени, если устройство прошло этап приработки и не выработало свой ресурс.

Вероятность отказа за время *t*, равна $F(t) = 1 - P(t)$, а плотность распределения (частота отказов) *f(t)* равна производной от функции распределения:

$$f(t) = \frac{dF(t)}{dt} = \frac{d\left(1 - P(t)\right)}{dt}.$$

Для экспоненциальной функции распределения

$$f(t) = \lambda e^{-\lambda t}.$$

Зная плотность распределения f(t), найдём среднюю наработку до первого отказа $T_{ср}$, которая является математическим ожиданием случайной величины – длительности безотказной работы *t*

$$T_{ср} = \int_0^\infty t f(t) dt = \lambda \int_0^\infty t e^{-\lambda t} dt = \frac{1}{\lambda},$$

Аппаратное резервирование

Наработка до отказа $T_{ср}$ является основным параметром, который указывается в эксплуатационной документации на электронные средства промышленной автоматизации.

Поскольку при $t = T_{ср}$ получается

$$P(T_{ср}) = \frac{1}{e} = 0{,}37,$$

то наработку на отказ интерпретируют следующим образом:

если в системе автоматизации имеется 100 модулей ввода-вывода, то через время после начала эксплуатации останется в среднем 37 работоспособных и 63 отказавших модулей.

Иногда наработку на отказ неправильно интерпретируют как время, в течение которого устройство почти наверняка будет работоспособно, и только после истечения этого времени наступит отказ.

При анализе надежности систем, **связанных с безопасностью**, вместо вероятности отказа используется понятие «вероятность отказа при наличии запроса», т. е. вероятность отказа при наличии необходимости быть в состоянии готовности.

Пример

Система охраны нефтебазы. Нужно учитывать вероятность отказа системы во время попытки проникновения нарушителей на базу, а не в то время, когда их нет. Отсюда следует вывод, что с точки зрения надежности охраны нужно рассматривать вероятность несрабатывания датчика охранной сигнализации на интервале времени, в течение которого может появиться нарушитель, и не нужно учитывать вероятность ложного срабатывания системы, поскольку она не влияет на выполнение функции охраны.

Классическая же теория надежности учитывает оба вида отказов.

Аппаратное резервирование

В системах, связанных с безопасностью, наработка до отказа $T_{ср}$ рассматривается отдельно для **опасных** и **безопасных** отказов.

Безопасным считается отказ, не вызывающий опасную ситуацию на объекте.

Пример 1.

Система *аварийного отключения*, в которой исчезновение питания приводит к обесточиванию обмотки реле и поэтому реле отключает нагрузку, переводя ее тем самым в безопасное состояние. В такой системе отказ источника питания обмотки реле является безопасным отказом и поэтому не учитывается при расчете вероятности отказа при наличии запроса.

Пример 2.

Если такой отказ произошёл в системе автоматического пожаротушения, когда необходимо, наоборот, *подать напряжение* на насосы, рассматривается как опасный отказ.

Поэтому **средняя вероятность отказа при наличии запроса** в двух рассмотренных системах будет различной несмотря на применение блока питания с одним и тем же значением наработки до отказа.

Учет обычной наработки до отказа при проектировании систем безопасности может привести к неоправданно заниженным показателям надежности и невозможности достижения требуемого уровня безопасности.

Фактические значения наработки до отказа систем с резервированием оказываются гораздо ниже расчетных. Это связано с существованием так называемых отказов по общей причине (ООП), которые происходят одновременно у основного элемента и резервного и которые составляют основную долю отказов в системах автоматизации.

Аппаратное резервирование

Пример.

Резервированная система находится в помещении, которое оказалось затопленным водой или охваченным пожаром. Отказ основного элемента и резерва при этом наступит одновременно.

Другим примером может быть одновременный обрыв основного и резервного кабеля в результате земляных работ.

Третьим примером может быть применение двух контроллеров с процессорами из одной и той же партии, которая была изготовлена с применением просроченной паяльной пасты. Следующим примером может быть применение двух датчиков давления одной и той же конструкции, от одного и того же производителя, которые окислились и разгерметизировались одновременно.

Электромагнитный импульс молнии или импульс в сети электропитания может явиться причиной отказа основного и резервного оборудования одновременно.

Приведённые примеры не из области фантастики, а вполне реальные жизненные ситуации

Аппаратное резервирование

Как быть в этих ситуациях? Как снизить возможный ущерб?

Способов достаточно много:

- выбирать элементы системы от разных производителей;
- элементы системы выполненные на разных физических принципах;
- с применением различных материалов и технологий изготовления;
- с разным программным обеспечением.
- основное и резервное оборудование, включая кабели, датчики и исполнительные механизмы желательно разносить территориально;
- монтаж основной и резервной системы выполнять разными людьми или разными монтажными организациями, чтобы исключить появление одинаковых ошибок монтажа и одинаково ошибочную интерпретацию руководства по эксплуатации монтируемого изделия и т. д.

Общие факторы, влияющие на всю систему, учитываются в моделях отказа как последовательно включенное звено со своей наработкой на отказ.