Аппаратное резервирование

Резервирование является практически единственным и широкое используемым методом кардинального повышения надежности систем автоматизации. Оно позволяет создавать системы аварийной сигнализации, противоаварийной защиты, автоматического пожаротушения, контроля и управления взрывоопасными технологическими блоками [Денисенко] и другие, относящиеся к уровням безопасности SIL1...SIL3 по стандарту МЭК 61508-5 [МЭК], а также системы, в которых даже короткий простой ведет к большим финансовым потерям (системы распределения электроэнергии, непрерывные технологические процессы). Резервирование позволяет создавать высоконадежные системы из типовых изделий широкого применения.

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

Большая доля отказов в системах автоматизации приходится на программное обеспечение. Однако этой теме посвящено множество специализированных книг и журнальных статей (см., например [Черкесов]), поэтому мы ее касаться не будем.

1. Основные понятия и определения

Основные определения понятий теории надежности и надежности, связанной с функциональной безопасностью, даны в ГОСТ 27.002-89 [ГОСТ] и МЭК 61508 [МЭК - МЭК]. Ниже приводится ряд определений, которые потребуются нам для дальнейшего изложения.

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, но неисправным, если этот канал не используется.

Дефектом называется каждое отдельное несоответствие объекта установленным требованиям (ГОСТ 15467-79) [ГОСТ].

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. Отказы возникают вследствие применения ненадежных схемотехнических решений на стадии проектирования контроллеров, электронных компонентов, изготовленных с нарушением техпроцесса, применения некачественных материалов, нарушения технологических режимов пайки, неточной установки компонентов на печатную плату, старения материалов, некачественного технологического оборудования, низкой культуры производства, отсутствия надежных методов контроля, работы компонентов в предельных электрических режимах, нарушений условий эксплуатации и т. п.

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*, в отличие от средней наработки до отказа.

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

Живучесть - свойство объекта сохранять *ограниченную* работоспособность при неисправностях или отказе некоторых компонентов. Этот термин наиболее близок международному термину "fault-tolerance" (дословно - "допустимость неисправностей"), который часто переводят как "отказоустойчивость". Термин "отказоустойчивость" в ГОСТ 27.002-89 используется, но его значения стандартом не определено. Мы будем использовать его в сочетании "*отказоустойчивая система*" как более компактный синоним понятия "система, обладающая свойством безотказности после отказа отдельных элементов".

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 (ГОСТ Р 51840-2001 [ГОСТ]).

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.

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.

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.

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*" [Смит, МЭК].

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 $n(t)-n(t+\Delta t)$ становятся неисправными через время Δt в результате отказа. Интенсивность отказа определяется пределом

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

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 $t=0$, $n(t)$ - число исправных элементов в момент времени t. При конечном числе испытуемых элементов вместо вероятности получают ее точечную статистическую оценку.

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 в (6.1) на $n(0)$, получим

$$\lambda(t) = -\frac{1}{P(t)}\frac{dP(t)}{dt}. \qquad (2)$$

Выражение для функции распределения длительности безотказной работы $P(t)$ можно получить, решая дифференциальное уравнение (2) при начальном условии $P(0)=1$:

$$P(t) = \exp\left(-\int_0^t \lambda(t)dt\right). \qquad (3)$$

Вероятность отказа $Q(t)$, по определению, равна

$$Q(t) = 1 - P(t). \qquad (4)$$

Интенсивность отказов $\lambda(t)$ обычно быстро уменьшается в начале эксплуатации изделия (период приработки), затем длительное время остается постоянной ($\lambda(t) = \lambda = const$) и после исчерпания срока службы резко возрастает.

Поскольку для средств промышленной автоматизации как правило, указывают значение $\lambda = const$, выражение (3) в этом случае упрощается:

$$P(t) = e^{-\lambda t}. \qquad (5)$$

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. Эта вероятность не зависит от того, как долго устройство проработало до начала отсчета времени [Черкесов, Александровская], т.е. не играет роли, используется бывшее в употреблении устройство, или новое. Это кажущееся парадоксальным утверждение справедливо только для экспоненциального распределения и объясняется тем, что выражение (5) получено в предположении, что снижение ресурса изделия с течением времени не происходит, а причины отказов распределены во времени в соответствии с моделью белого шума.

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

$$f(t) = \frac{dF(t)}{dt} = \frac{d[1 - P(t)]}{dt} \qquad (6)$$

и для экспоненциальной функции распределения (5) равна

$$f(t) = \lambda e^{-\lambda t}. \qquad (7)$$

Зная плотность распределения (7), можно найти среднюю наработку до первого отказа T_{cp}, которая, по определению, является математическим ожиданием случайной величины - длительности безотказной работы t, т.е.

$$T_{cp} = \int_0^\infty t f(t) dt = \lambda \int_0^\infty t e^{-\lambda t} dt = \frac{1}{\lambda}. \qquad (8)$$

Интегрирование в (8.8) выполняется по частям.

Наработка до отказа T_{cp} является основным параметром, который указывается в эксплуатационной документации на электронные средства промышленной автоматизации. Поскольку при $t = T_{cp}$ из (5) получается $P(T_{cp}) = 1/e = 0{,}37$, то наработку на отказ можно интерпретировать следующим образом: если в системе автоматизации имеется 100 модулей ввода-вывода, то через время T_{cp} 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" (подробнее см. раздел "Функциональная безопасность"), т. е. вероятность отказа при наличии необходимости быть в состоянии готовности. Например, если рассматривается система охраны нефтебазы, то 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.

В системах, связанных с безопасностью, наработка до отказа рассматривается отдельно для опасных и безопасных отказов. Безопасным считается отказ, не вызывающий опасную ситуацию на объекте. Рассмотрим, например, систему *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. Однако отказ такого же источника питания 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. Предположим, например, что 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. Во всех приведенных примерах существует сильная корреляция между случайными величинами, вызывающими отказ основного и резервного элемента.

Для уменьшения коэффициента корреляции (снижения влияния общих причин отказов) нужно по возможности выбирать элементы системы от разных производителей, выполненные на разных физических принципах, с применением различных материалов, различных технологических процессов и с разным программным обеспечением. Основное и резервное оборудование, включая кабели, датчики и исполнительные механизмы желательно разносить территориально, а монтаж основной и резервной системы должны выполнять разные люди или разные монтажные организации, чтобы исключить появление одинаковых ошибок монтажа и одинаково ошибочную интерпретацию руководства по эксплуатации монтируемого изделия.

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

2. Резервирование ПЛК и устройств ввода-вывода

Несмотря на существование большого разнообразия методов резервирования, в промышленной автоматизации получили распространение только два из них: горячее резервирование замещением (hot standby) и метод голосования (2oo3 voting, 1oo2 voting и др.). Реже используется теплый резерв (warm standby).

Целью резервирования может быть обеспечение безотказности или обеспечение безопасности. Методы резервирования, используемые для достижения этих двух целей, существенно различаются. Основное различие состоит в том, что для обеспечения безопасности достаточно снизить вероятность только опасных отказов, в то время как для обеспечения безотказности требуется обеспечить работоспособность системы при всевозможных отказах. Поэтому системы, связанные с безопасностью, получаются проще, чем отказоустойчивые системы при условии одинаковой наработки до отказа.

2.1. Общие принципы резервирования

В основе метода резервирования лежит очевидная идея замены отказавшего элемента исправным, находящемся в резерве. Однако реализация этой идеи часто становится достаточно сложной, если необходимо обеспечить минимальное время перехода на резерв и минимальную стоимость оборудования при заданной вероятности безотказной работы в течение определенного времени (наработки).

Для замены отказавшего элемента достаточно иметь резервный (запасной) элемент на складе. Однако продолжительность ручной замены составляет единицы часов, что для многих систем автоматизации недопустимо долго. Сократить время вынужденного простоя позволяет применение контроллеров и модулей ввода-вывода с разъемными клеммными соединителями и с возможностью "горячей замены" [Боломытцев] при условии наличия развитой системы диагностики неисправности. Для обеспечения возможности "горячей замены" необходимо предусмотреть следующее:

- защиту от статического электричества, которое может возникать на теле оператора, выполняющего замену устройства;
- необходимую последовательность подачи напряжений питания и внешних сигналов. Для этого используют, например, разъемы с контактами разной длины и секвенсоры внутри устройства;
- защиту системы от броска тока, вызванного зарядом емкостей подключаемого устройства, например, с помощью токоограничительных резисторов или отдельного источника питания;
- защиту устройства от перенапряжения, короткого замыкания, переполюсовки, превышения напряжения питания, от ошибочного подключения;
- программируемые устройства должны быть заранее запрограммированы, в сетевые устройства должен быть записан правильный адрес и предусмотрена подсистема автоматической регистрации нового и исключения старого устройства из сети;
- в алгоритмах автоматического регулирования должен быть предусмотрен "безударный" режим смены контроллера или модулей ввода-вывода [Денисенко].

Если резервный элемент входит в состав системы, то она относится к резервированным системам с ручным замещением отказавшего элемента.

Системы с голосованием

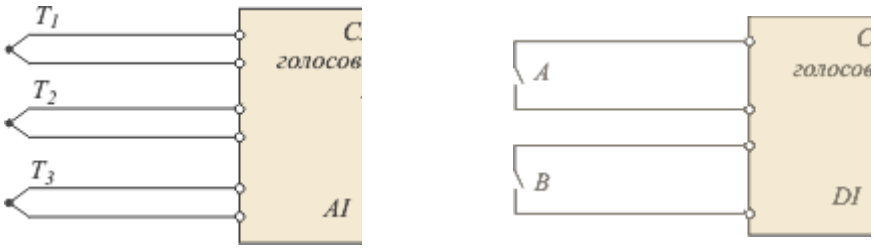
Основным отличительным признаком систем резервирования с голосованием является невозможность выделения в системе основных элементов и резервных, поскольку все они равноправны, работают одновременно и выполняют одну и ту же функцию. Выбор одного сигнала из нескольких осуществляется схемой голосования, которая в частном случае нечетного числа голосов называется мажоритарной схемой.

Системы с голосованием не требуют контроля работоспособности элементов для своего функционирования, но используют подсистему диагностики для сокращения времени восстановления отказавших элементов. Наличие системы диагностики снижает также вероятность накопления скрытых неисправностей, которые со временем могут явиться причиной отказа.

Принцип работы схемы голосования рассмотрим на примере резервирования датчиков (см. рис. 1-а). В такой системе вместо одного датчика используются три (например, три термопары), которые подсоединены к одному модулю ввода. В схему голосования поступают, соответственно, три значения измеряемой величины (например, три значения температуры T_1, T_2, T_3), из которых необходимо выбрать одно. Значения температуры располагаются в порядке возрастания: $T_1 < T_2 < T_3$, а на выход схемы голосования поступает значение, расположенное между двумя крайними (но не среднее арифметическое!). Например, если в результате измерения получены значения (0,12; 39,5; 39,4)°С, то используется только значение 39,4, остальные игнорируются.

Резервирование элементов с дискретными сигналами выполняется аналогично рассмотренному выше. Поскольку значениями дискретных сигналов являются логические "0" или "1", то в результате мажоритарного голосования выбирается то значение, которое принимают большинство сигналов. Например, при логических сигналах A="1", B="1", C="0" результатом голосования будет значение Y="1". Блок мажоритарного голосования реализует логическую функцию Y = AB + BC + CA.

Очевидно, что для работы мажоритарной схемы число "голосов" должно быть нечетным. Однако *в системах безопасности* возможно применение любого числа "голосов". Вместо недостающего голоса используется условие, что система считается работоспособной, если отказ является безопасным. Это позволяет использовать системы, в которых выбирается один голос из двух и такие системы по стандарту МЭК 61508 [МЭК] обозначаются как 1oo2 (1 Out Of 2). Используются также системы 2oo2 - (два голоса из двух), 2oo3 (два голоса из трех), 2oo4 (два голоса из четырех), 3 oo4 (три голоса из четырех). Нерезервированные системы обозначаются как 1oo1. Если в резервированной системе имеется развитая подсистема диагностики неисправностей, то к обозначению добавляется буква "D", например, 1oo2D .



а) б)

Рис. 1. Устройства с голосованием по схеме 2oo3 (а) и по схеме 1oo2 (б)

Примером системы с голосованием вида 1oo2 может служить система охранной сигнализации двери, в которой используются два датчика A и B с целью взаимного резервирования (рис. 1, б). При отказе одного из датчиков (например, датчика B, когда вместо A=1, B=1 получаем A=1, B=0) система, пользуясь правилом большинства голосов, не может принять решение. Однако, если учесть, что ложное срабатывание охранной системы не приводит к опасной ситуации, а несрабатывание системы при наличии нарушителя является опасным отказом, очевидно, схема голосования должна считать, что достаточно одного голоса из двух, чтобы принять решение о подаче аварийного сигнала. Если сигналом срабатывания сигнализации является логическое значение "1", а сигналом отсутствия нарушителя является значение "0", то блок голосования реализует логическую функцию Y = A + B.

Если входными данными для голосования являются два аналоговых сигнала, то пользователь при программировании должен установить, какой сигнал из двух должен быть выбран системой в случае их несовпадения. Такой подход возможен только в системах безопасности.

Противоположная ситуация используется при голосовании вида 2 oo2. Примером может быть система контроля герметичности люка при погружении подводной лодки. Если люк имеет два датчика, то сигнал готовности к погружению может появиться только при наличии подтверждения (A="1", B="1") от обоих датчиков одновременно (двух из двух). Выход из строя одного датчика не должен позволить системе выработать сигнал готовности к погружению, чтобы опасная ситуация не возникла. Такой блок реализует логическую функцию Y = AB.

Несмотря на высокую эффективность схем голосования с четным числом голосов, они имеют недостаток, состоящий в возможности ложного срабатывания. Хотя этот тип отказов и не является опасным, в некоторых случаях он приводит к значительному материальному ущербу. Для исключения ложного срабатывания можно использовать более дорогие системы с нечетным количеством голосов, которые снижают вероятность отказов обоих типов. Выбор наилучшей системы осуществляется на основании результатов экономических расчетов.

При отказе одного из элементов резервированной системы безопасности 2oo3 ее уровень безопасности понижается и она может начать функционировать как система 1oo2. Если замена неисправного элемента не произведена и произошел второй отказ, то система переходит в режим без резервирования 1oo1, однако в этом режиме система не может находиться долго по требованиям безопасности. Очередность перехода от одной схемы резервирования к другой называется схемой деградации.

Система безопасности 2oo3 может иметь второй вариант схемы деградации: 2oo3 - 2oo2 - 1oo1 - 0. Здесь "0" обозначает состояние, когда система перестает функционировать (останавливается). Перед остановкой система должна перевести все свои выходы в безопасные состояния. Понятие безопасного состояния для каждой системы определяется при ее проектировании. Например, для систем аварийного отключения безопасными являются обесточенные состояния исполнительных механизмов, а для систем автоматического пожаротушения или аварийной вентиляции - наоборот, состояния, при которых на исполнительные устройства подана энергия.

Схемы голосования широко используются в системах противоаварийной защиты и сигнализации, где они имеют большое разнообразие. В системах же, не связанных с безопасностью, обычно нельзя применить иные схемы голосования, кроме 2oo3, которые являются достаточно дорогими. Однако их уникальным свойством является непрерывность функционирования во время перехода на резерв и это свойство является определяющим при принятии решения о выборе метода резервирования.

Резервирование замещением

Другой класс резервированных систем составляют системы с горячим резервированием замещением (Hot Standby) (рис. 2). Их отличительной чертой является принципиальная необходимость в подсистеме контроля работоспособности как основного, так и резервного элементов, наличие блока переключения на резерв (обычно переключение выполняется программно), а также шины для синхронизации между процессорами (последнее относится только к резервированию процессоров). Основным параметром систем с резервированием замещением является время переключения на резерв. Переход на резерв выполняется в пределах одного или нескольких контроллерных циклов и занимает время от единиц миллисекунд до долей секунды.

Системы с более медленным переключением на резерв (от долей до единиц секунд) относят к системам с теплым резервом (Warm Standby). Конструктивное отличие теплого резервирования контроллеров от горячего заключается в отсутствии высокоскоростного канала синхронизации между процессорами, вместо него используется стандартная низкоскоростная промышленная сеть или другой последовательный канал обмена.

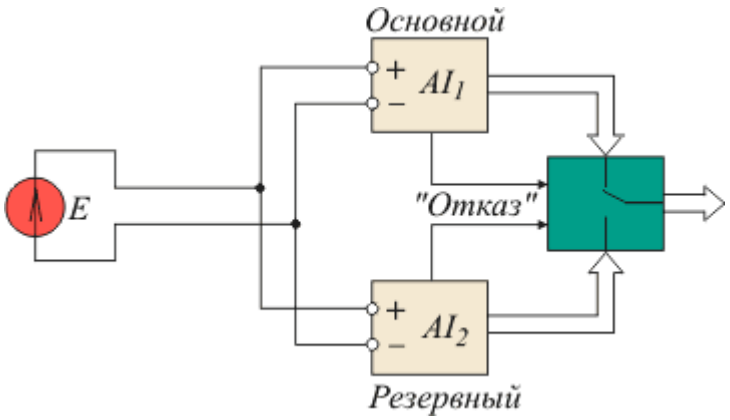


Рис. 2. Дублирование модуля ввода методом замещения

Для контроля работоспособности используются такие параметры и события, как, например, обрыв линии связи, короткое замыкание (к. з.), величина напряжения и тока питания, отсутствие связи, перегрев выходных каскадов модулей вывода, перегрузка

по току, отсутствие нагрузки, выход сигналов за границы динамического диапазона, срабатывание предохранителя, срабатывание блокировок и защит, целостность линий связи с модулями ввода-вывода, ошибка контрольной суммы, ошибка памяти, "зависание" процессора и т. п. Перечень процедур контроля ПЛК приведен в ГОСТ Р 51841 [ГОСТ]. Диагностическая информация должна выводиться на пульт оператора и одновременно может использоваться для переключения на резерв.

Для исключения ошибочного перехода на резерв по причине сбоя в системе контроля используют временной фильтр, который разрешает переключение только при условии, что состояние неисправности длится не менее установленного времени (например, 1...100 мс).

Общее и поэлементное резервирование

Резервированными могут быть отдельные элементы системы, их группы и вся система в целом. Поэлементное резервирование позволяет повысить отказоустойчивость в первую очередь наиболее важных или наименее надежных элементов, выбрать различную кратность резервирования для разных элементов системы и тем самым достичь максимального отношения надежности к цене.

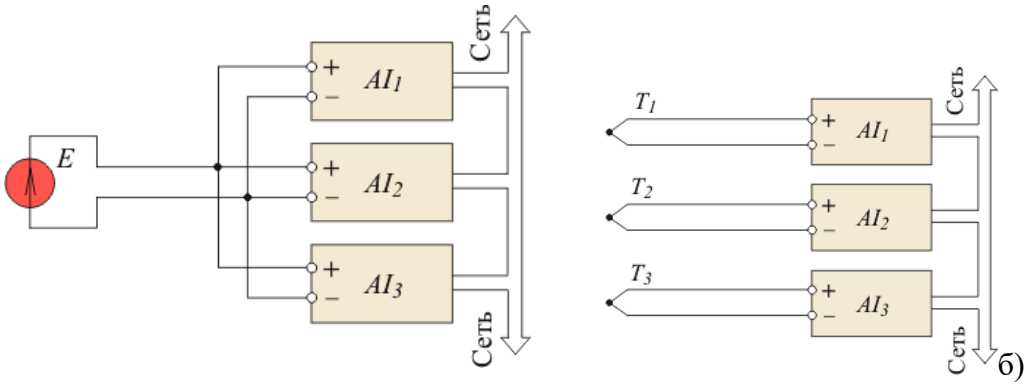
Общее резервирование не требует анализа соотношений между надежностью отдельных элементов системы, исключает ошибки при расчете надежности и выборе различных схем резервирования, а также ошибки, вызванные плохой наглядностью архитектуры системы при поэлементном резервировании.

В случае общего резервирования достаточно двух отказов для отказа всей системы, если один из элементов расположен в основной системе, второй - в резервной. При поэлементном резервировании вероятность такого отказа существенно ниже, поскольку для его реализации необходимо, чтобы один из отказавших элементов был основным, второй - его резервом, что крайне маловероятно.

2.2. Модули ввода и датчики

Типичными отказами при вводе сигналов в ПЛК является обрыв или короткое замыкание линии связи. На долю отказов линий связи, датчиков и исполнительных устройств в системах автоматизации приходится 85% всех отказов [SIMATIC]. Линии связи могут повреждаться в результате стихии (обмерзание проводов), земляных работ, неправильного монтажа, злонамеренных действий и т. п., поэтому их надежность часто не связана напрямую с надежностью кабеля.

Резервирование аналоговых модулей ввода и датчиков



а)

Рис. 3. Резервирование модулей ввода (а) и датчиков с модулями (б)

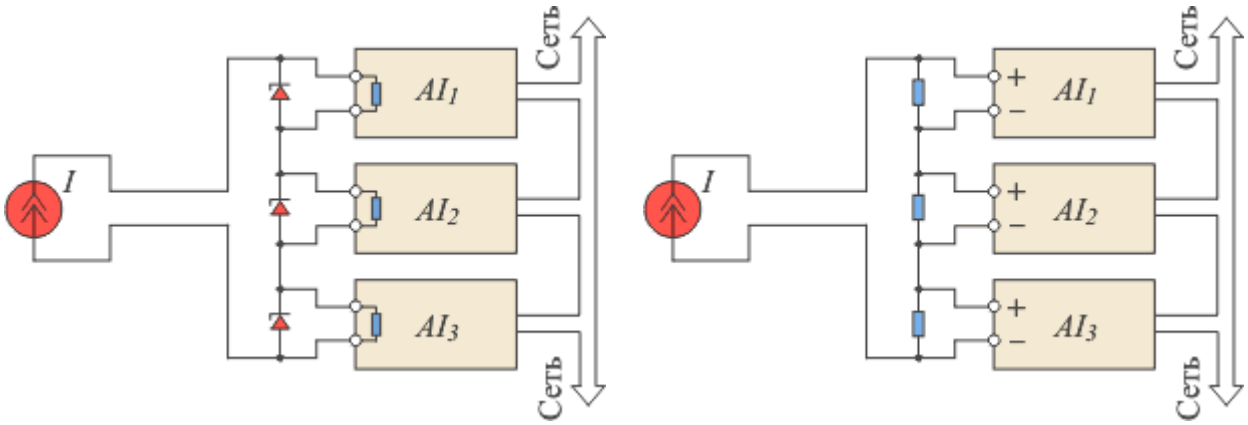
Схемы голосования могут применяться для резервирования датчиков при использовании одного модуля ввода (рис. 1), для резервирования модулей ввода при наличии одного датчика (рис. 3-а) или датчиков и модулей ввода одновременно. В последнем случае потенциальные входы модулей соединяются параллельно (рис. 3-а), а токовые - последовательно (рис. 4). Поскольку при последовательном соединении отключение одного из модулей (например, для выполнения замены) приводит к разрыву всей цепи, то для устранения этого эффекта используют стабилитроны (рис. 4-а). При использовании источника тока с большим внутренним сопротивлением (например, стандартного источника 4...20 мА) ток I не зависит от сопротивления нагрузки, поэтому появление стабилитрона в контуре с током при удалении одного из модулей не вносит погрешность в результат измерения. Ток утечки стабилитрона должен быть мал по сравнению с допустимой абсолютной погрешностью измерения тока, а напряжение стабилизации - больше максимального падения напряжения на измерительном резисторе.

Тот же эффект достигается, если использовать внешние измерительные резисторы (рис. 4-б), которые обеспечивают замкнутый путь для тока при удалении одного из модулей. При этом используются модули с потенциальным входом, а измерение тока выполняется косвенным методом (по падению напряжения на сопротивлении).

Схемы голосования в рассмотренных примерах и количество элементов в резервированной системе могут быть произвольными; алгоритм голосования реализуется программно в ПЛК.

Принцип работы системы, резервированной методом замещения, иллюстрируется рис. 2. В системе выделяется основной модуль, резервный и блок выбора модуля после отказа. До отказа на выход системы поступают данные только из основного модуля. Блок выбора постоянно контролирует состояние работоспособности модулей и после наступления отказа автоматически переключает выходной канал системы на исправный модуль. Одновременно на пульт оператора и в журнал ошибок посылается диагностическое сообщение о вышедшем из строя элементе. Переключение выполняться, как правило, программно.

Аналогично работают системы с несколькими резервными элементами. Переключение на один из них выполняется по заранее определенному алгоритму.



а) б)

Рис. 4. Резервирование модулей ввода тока с измерительными резисторами внутри модулей (а) и снаружи (б)

Основной проблемой в системах, резервированных методом замещения, является автоматический контроль исправности.

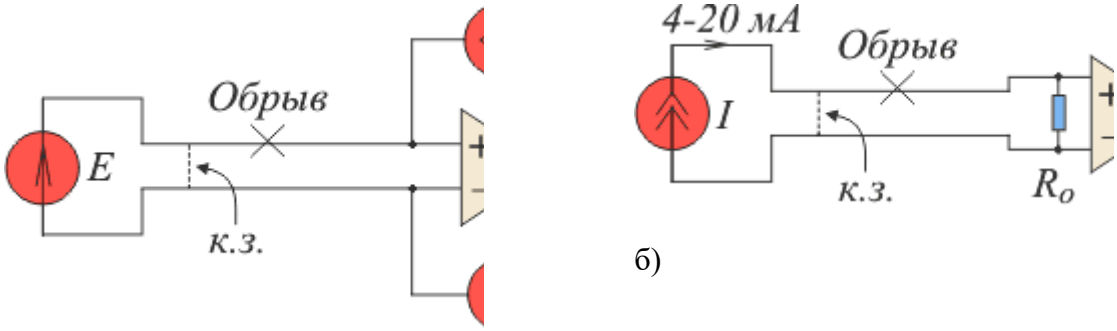
Для контроля исправности аналоговых модулей ввода могут быть использованы следующие величины и события:

- среднеквадратическое значение напряжения или тока шума;
- напряжение смещения нуля;
- температура внутри корпуса модуля;
- погрешность (оценивается с помощью встроенного источника опорного напряжения);
- зависание процессора (диагностируется с помощью сторожевого таймера);
- напряжение питания процессора;
- ошибка контрольной суммы;
- ошибка в ответе на команду.

Для диагностики обрыва во входных цепях аналоговых модулей используются следующие методы:

- контроль выхода переменной за границы динамического диапазона или границы ее изменения;
- применение тестирующих источников тока (рис. 5).

Типовым методом обнаружения к. з. является измерение сопротивления входной цепи с помощью источников тока I, подключенных как показано на рис. 5-а). Величина тока выбирается достаточно малой, чтобы падение напряжения на линии связи и внутреннем сопротивлении датчика не вносило погрешность в результат измерений. Например, в модуле NL-8TI фирмы НИЛ АП используется ток величиной 2 мкА. При обрыве во входной цепи напряжение между входами модуля выходит за границы динамического диапазона, что является диагностическим признаком обрыва.



а) б)

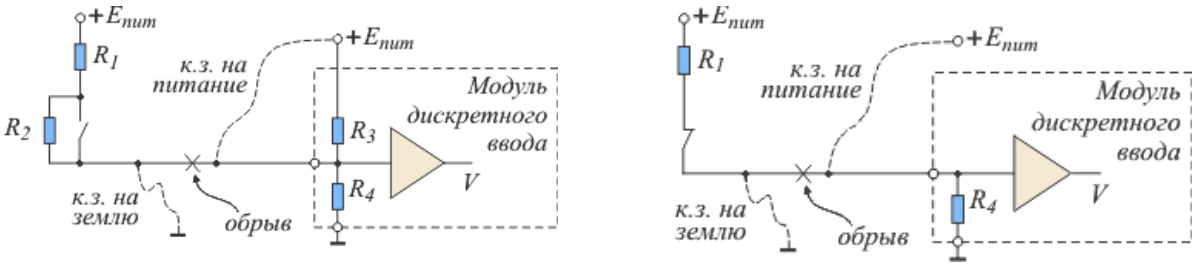
Рис. 5. Обнаружение обрыва и к.з. в линии связи или датчике, когда носителем сигнала является напряжение (а) или ток (б)

При к. з. во входной цепи напряжение между входами модуля становится равным нулю, что является диагностическим признаком короткого замыкания. Для того, чтобы к. з. можно было отличить от полезного сигнала нулевой величины, диапазон изменения сигнала датчика искусственно сдвигают от нулевого уровня. Такой подход использован в стандарте 4...20 мА, где вся информация о сигнале содержится в диапазоне токов от 4 мА до 20 мА (см. рис. 5-б). В этом случае появление нулевого напряжения на входе приемника сигнала однозначно говорит о нарушении линии связи. Однако отличить обрыв от к. з. и в этом случае невозможно, поскольку оба отказа обнаруживаются по нулевой величине принимаемого тока.

Резервирование датчиков и модулей ввода дискретных сигналов

При вводе дискретных сигналов используются методы голосования и резервирования замещением, описанные в разделе "Резервирование ПЛК и устройств ввода-вывода".

Схемы подключения датчика типа "сухой контакт", которые обеспечивают диагностику обрыва, к. з. на землю и на шину питания, показаны на рис. 6 и рис. 7. При обрыве линии на входе модуля появляется сигнал, величина которого определяется делителем напряжения $\frac{R_4}{R_3+R_4}E_{пит}$ (см. рис. 6-а). В случае короткого замыкания на шину питания напряжение на входе модуля равно напряжению питания. При к. з. на землю напряжение на входе равно нулю. При разомкнутом состоянии датчика напряжение равно $\frac{R_4}{R_4+R_3\|(R_1+R_2)}E_{пит}$, при замкнутом - $\frac{R_4}{R_4+R_3\|R_1}E_{пит}$.



а) б)

Рис. 6. Схема обнаружения обрыва и к.з. в цепи датчика: с пятью различимыми состояниями (а) и с тремя (б)

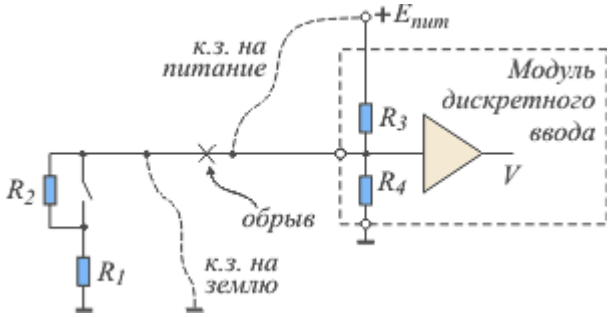
Таким образом, на входе модуля дискретного ввода могут быть пять различных уровней напряжения, которые с помощью АЦП преобразуются в пять различных событий: "0", "1", "к. з. на землю", к. з. на питание", "Обрыв". Переключение на резерв происходит, если в блок выбора модуля (см. рис. 2) поступает информация о неисправности. Тип неисправности выдается на пульт оператора системы автоматизации и заносится в журнал ошибок.

В ряде случаев достаточно иметь упрощенную схему диагностики. Например, если на рис. 6-а убрать резисторы R_2 и R_3 (см. рис. 6-б), то при замкнутом датчике получим напряжение на входе модуля, равное $\frac{R_4}{R_4 + R_1} E_{пит}$; при открытом состоянии датчика, при обрыве линии и при к. з. на землю - одно и то же напряжение, равное нулю; при к. з. на шину питания - $E_{пит}$. Таким образом, вместо пяти состояний на входе получаем только три.

Предположим, что датчик используется в системе охраны и его нормальным состоянием является открытое. Тогда обрыв линии связи и к. з. на землю останутся незамеченными, поскольку их невозможно отличить от нормального состояния датчика. Предположим теперь, что нормальным состоянием датчика является замкнутое, как показано на рис. 6-б. Тогда при любом из перечисленных отказов линии связи сигнализация сработает, т.е. отказа, приводящего к несрабатыванию функции безопасности, произойти не может. Поэтому такая упрощенная схема контроля может быть использована в системах безопасности только с датчиками, у которых нормальным состоянием считается замкнутое.

При выборе упрощенных схем диагностики следует учитывать, что в правильно спроектированной системе безопасности срабатывание датчика не должно быть блокировано неисправностями линии связи, а если такая блокировка возможна, то она должна быть обнаружена системой контроля.

Для обнаружения неисправностей модуля ввода может использоваться автоматическое тестирование во время кратковременного отключения источников сигнала и нагрузок путем подачи на вход тестовых комбинаций логических уровней (см. выше).



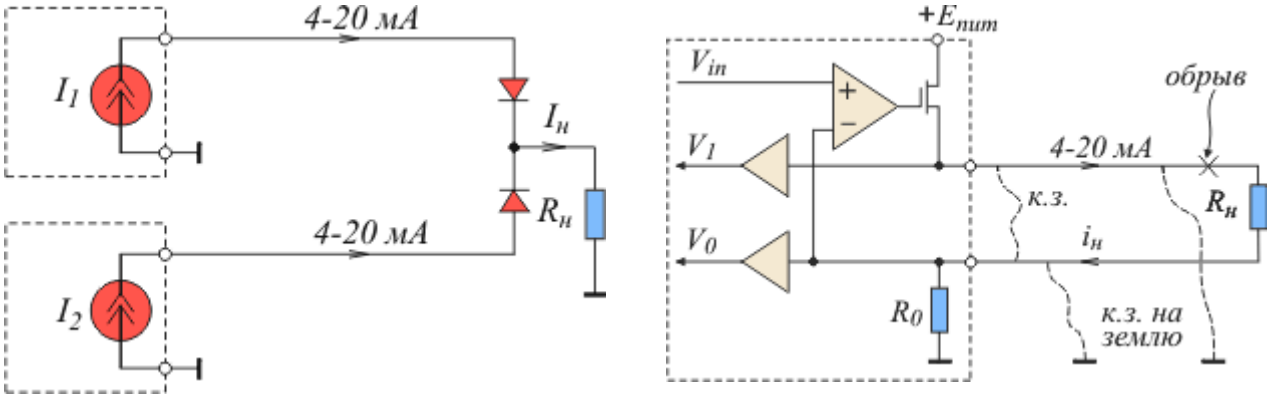
б)

Рис. 7. Схема обнаружения обрыва и к. з. в цепи датчика

2.3. Резервирование модулей вывода

Резервирование модулей вывода принципиально отличается от резервирования модулей ввода тем, что устройства вывода в большинстве случаев являются источниками энергии, в то время как устройства ввода являются приемниками информации (сигналов). Поэтому если для переключения на резерв в модулях ввода достаточно программно перенаправить поток принимаемой информации, то в модулях вывода необходимо переключить поток энергии, что невозможно сделать только программными средствами.

Резервирование аналоговых модулей вывода



а) б)

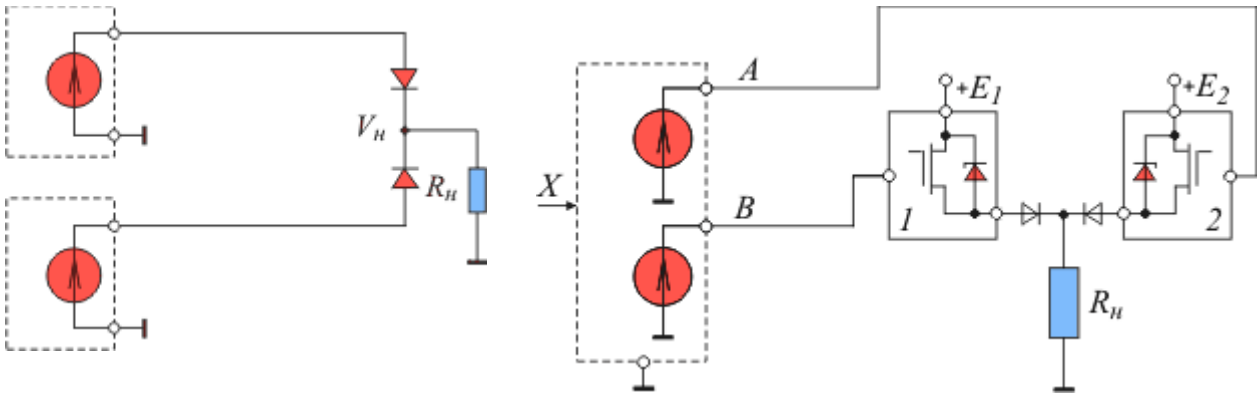
Рис. 8. Резервирование (а) и диагностика (б) линии вывода аналоговых сигналов

Резервированный вывод аналоговых сигналов реализуется наиболее сложно и в промышленной автоматике используется редко. Проблема состоит в том, что для переключения на резерв механические реле использовать нежелательно по причине их низкой надежности, а другие способы (включая метод голосования) порождают сложные схемы, которые также понижают надежность системы. Поэтому модули аналогового вывода чаще всего просто отсутствует в промышленных резервируемых системах.

Для резервирования линий связи при выводе и передаче аналоговых сигналов в нагрузку используют преимущественно стандарт 4...20 мА, поскольку он позволяет обнаружить к. з. и обрыв линии. Непосредственно у самой нагрузки ($R_н$) устанавливают диоды, которые предотвращают шунтирование нагрузки при к. з. на землю в соседнем канале (рис. 8-а).

До наступления отказа каждый источник выдает ток, равный половине тока нагрузки ($I_н/2$). При к. з. или обрыве линии связи ток через диод в этом канале становится равным нулю и срабатывает алгоритм резервирования, который устанавливает в исправном канале ток, равный $I_н$. Использование половины тока ($I_н/2$) для каждого канала уменьшает амплитуду паразитных выбросов во время переходного процесса после отказа.

Описанная схема не пригодна для резервирования самих модулей вывода, поскольку в результате отказа источника на его выходе может установиться ток, не равный нулю.



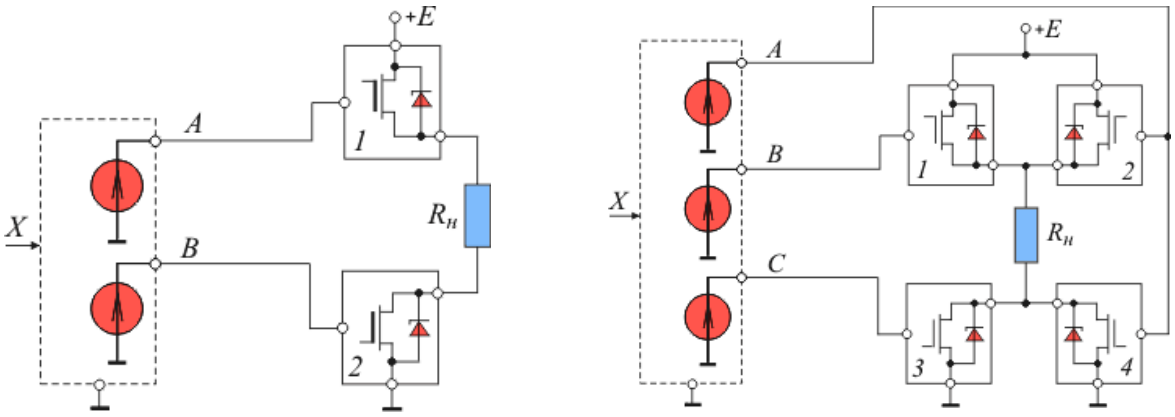
б)

Рис.9. Соединение дискретных выходов при резервировании (а) и один из вариантов реализации дискретных выходных каскадов (б)

Контроль целостности линии связи и диагностика отказа в модулях вывода тока 4...20 мА выполняется как показано на рис. 8-б. Выходной каскад модуля не только выводит ток $i_н = \frac{V_m}{R_0}$, но и измеряет напряжения $V_0 = R_0 i_н$ и V_1, которые с помощью АЦП преобразуются в цифровую форму и передаются в процессор модуля вывода. При правильном функционировании цепи, включающей нагрузку $R_н$, должно выполняться равенство $V_0 = V_m$. Если оно не выполняется, то при $V_0 = 0$ имеет место к. з. на землю или обрыв; при $V_0 = V_1$ - к. з. между линиями или в нагрузке; при $V_1 = E_{num}$ имеет место к. з. верхней (по схеме) линии на шину питания, при $V_0 = E_{num}$ - нижней. При $V_0 > V_m$ сопротивление нагрузки превышает допустимое значение и операционный усилитель находится в состоянии насыщения.

Резервирование модулей дискретного вывода и нагрузки

Резервирование модулей дискретного вывода, кабелей и нагрузки обычно выполняется методом голосования. Для этого дискретные выходы соединяются параллельно через диоды (рис. 9-а). Диоды используются для предотвращения протекания тока из одного канала в другой. При отказе одного из источников на рис. 9-а в виде к. з. на землю и обрыва управление нагрузкой продолжается от второго источника. Однако, если отказом является пробой выходного каскада на шину питания, то отказавший канал блокирует выходное напряжение и оно перестает зависеть от управляющего сигнала. Несмотря на этот недостаток, соединение дискретных выходов по схеме рис. 9-а может быть использовано в системах, связанных с безопасностью, если рассмотренный вид отказа резервированной системы не влияет на выполнение функции безопасности. Например, если безопасным состоянием выхода является наличие напряжения (для питания двигателей насосов в системе пожаротушения), рассмотренный отказ не является опасным и не влияет на величину вероятности отказа при наличии запроса.



а) б)

Рис. 10. Резервирование модулей вывода для реализации аварийного отключения и для повышения отказоустойчивости и живучести (б)

Таким образом, параллельное соединение дискретных выходов с целью резервирования может использоваться только в системах аварийного *включения* нагрузки и не может использоваться в системах аварийного отключения. Вероятность отказа при включении у такой цепи эквивалента дублированной системе, а при отключении - меньше, чем у нерезервированной.

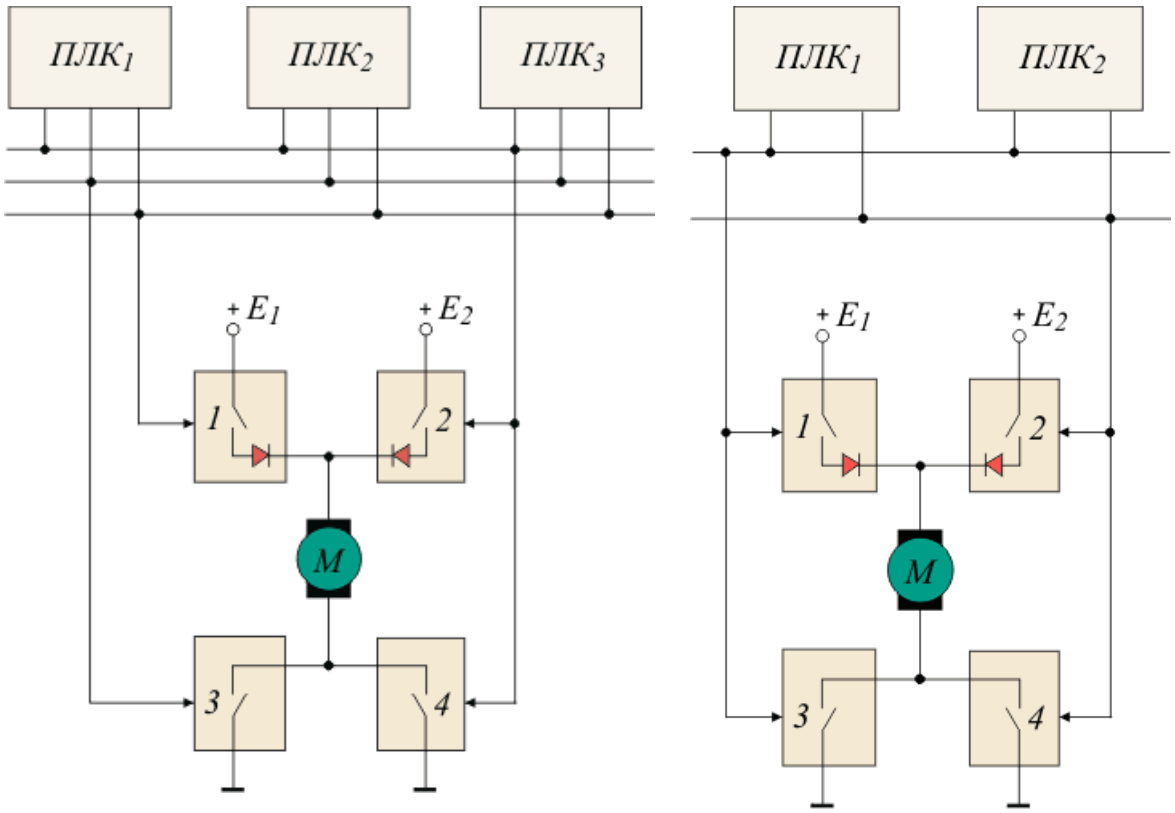
На рис. 9-б) показана реализация описанного выше принципа резервирования, выполненная на МОП-транзисторах. Для коммутации мощной нагрузки ключи *1* и *2* могут быть изготовлены в отдельном конструктиве с радиаторами и удалены от модулей дискретного вывода. Маломощные ключи конструктивно входят в состав модулей вывода. При подключении нагрузки к разным источникам питания E_1 и E_2 (как на рис. 9-б) необходимо использовать развязывающие диоды, чтобы при одновременно открытых ключах исключить протекание тока из одного источника в другой. Если же использован общий источник питания (как на рис. 10-б), то диоды не нужны.

Для резервирования систем аварийного *отключения* используется последовательное соединение двух выходных каскадов (рис. 10-а). При отказе одного из МОП-ключей в виде к. з. нагрузка отключается вторым каналом, т.е. функция отключения в данной системе является дублированной. При необходимости же включить нагрузку достаточно отказа только одного ключа, т.е. функция включения оказывается нерезервированной. Таким образом, рассмотренный каскад может быть использован только в системах аварийного отключения, но не включения.

Для построения системы, в которой резервируется не одна из функций (включения или отключения), но обе одновременно, используется каскад из четырех ключей (рис. 10-б) [Mitsubishi]. В нем выход из строя любого выходного каскада или линии связи не приводит к нарушению ни функции включения, ни отключения. Реализация описанной цепи с помощью электромагнитных реле показана на рис. 11-а).

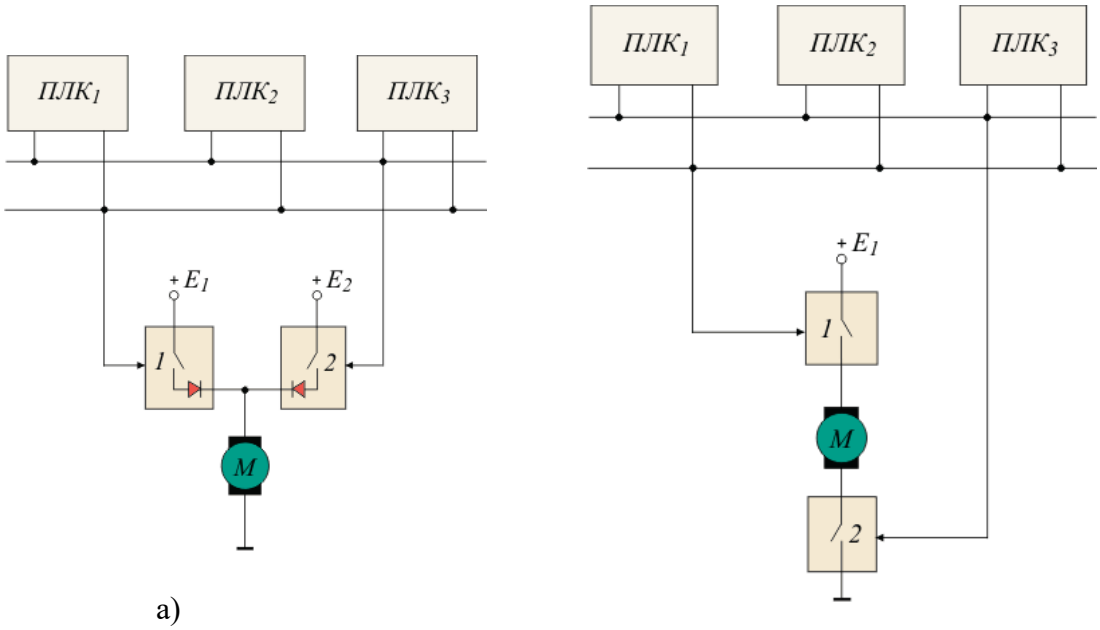
На схеме рис. 10-б) каждый выходной каскад управляется сигналом X с помощью строенного источника сигнала ($A = B = C = X$). Для повышения надежности сигнал управления X может приходить по резервированной промышленной сети от резервированного ПЛК, как на рис. 11-а. Голосование (например, по схеме 2oo3) в случае отказа одной из сетей выполняется непосредственно в модулях вывода.

При использовании горячего дублирования сети и контроллеров методом замещения аналогичная структура может иметь вид, показанный на рис. 11-б.



а) б)

Рис. 11. Резервирование модулей вывода, шины и контроллеров; M - нагрузка



а) б)

Рис. 12. Резервирование цепей дискретного вывода для систем аварийного включения (а) и аварийного отключения (б)

Структуры систем аварийного включения и отключения с дублированной сетью и ПЛК, резервированными по схеме 2oo3, показаны на рис. 12. Отметим, что для дублирования ключей на рис. 12-б было бы достаточно просто соединить их последовательно, заземлив нижний (по схеме) вывод нагрузки. Однако в этом случае становится возможным опасный отказ, вызванный к. з. верхнего по схеме вывода нагрузки на источник питания. При этом отключение нагрузки оказывается невозможным. Применение второго ключа для размыкания пути тока на землю позволяет исключить такой отказ.

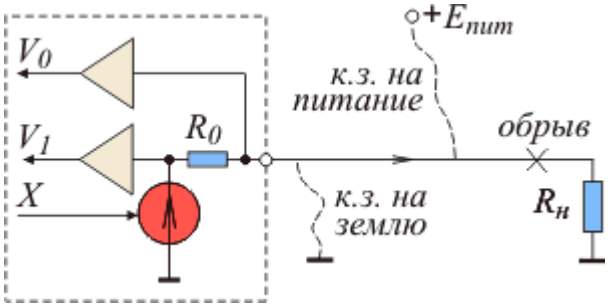


Рис. 13. Принцип обнаружения обрыва линии связи и к. з. на шину питания и земли в модуле вывода дискретных сигналов

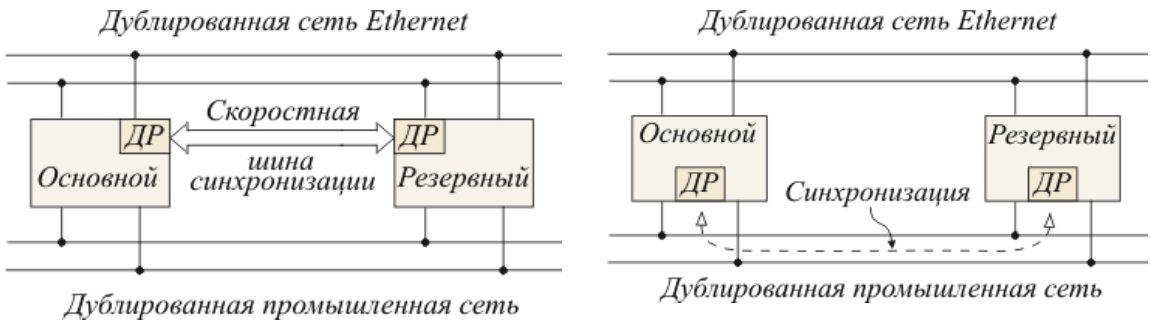
Принцип контроля и диагностики выходных каскадов и линий связи с нагрузкой иллюстрируется рис. 13. Он аналогичен использованному в модулях аналогового вывода (см. рис. 8-б). Напряжение ($V_1 - V_0$), пропорциональное току нагрузки, и V_0 преобразуются с помощью АЦП в цифровую форму и передаются в микропроцессор модуля для извлечения диагностической информации.

8.2.4. Резервирование процессорных модулей

Процессорный модуль (для краткости будем говорить "процессор") следует резервировать в первую очередь, т.к. при его отказе наступает отказ всей системы. Одновременно с процессором обычно резервируют блок питания и промышленную сеть.

Резервирование процессора с целью повышения отказоустойчивости и живучести выполняют методом замещения с горячим (рис. 14-а) или теплым (рис. 14-б) резервом, а также методом голосования по схеме 2oo3 (рис. 15). Для систем, связанных с безопасностью, используют резервирование по схеме 1oo2 или 2oo2, в том числе с диагностикой (1oo2D и 2oo2D).

Сложность резервирования процессоров заключается в том, что в момент замещения резервный процессор должен иметь внутренние состояния, идентичные состояниям основного. В системах резервирования замещением для быстрой перезаписи внутренних состояний используется специализированная высокоскоростная шина или оптический канал синхронизации (Bertocco-а). В системах с голосованием большинство внутренних состояний процессоров идентичны, поскольку они работают одновременно с одними и теми же входными данными и исполняют одну и ту же программу, поэтому синхронизация необходима только во время горячей замены отказавшего процессора.



а) б)

Рис. 14. Горячее (а) и теплое (б) резервирование процессорных модулей замещением; ДР - драйвер резервирования

Для систем, некритичных ко времени перехода на резерв, может быть использован медленный последовательный канал синхронизации с интерфейсами, например, RS-232, USB, RS-485 или обычная промышленная сеть (CAN, Modbus, Profibus и др.) общего назначения (Bertocco-б). Такие системы относят к системам с "теплым" резервом.

К резервированным процессорным модулям предъявляются следующие основные требования:

- безударное переключение на резерв (без внесения возмущений в управляемый процесс);
- малая длительность переключения;
- высокая надежность общих средств, выполняющих функцию переключения (шина синхронизации и программное обеспечение).

Контроль работоспособности процессоров может выполняться на каждом контроллерном цикле, перед считыванием сигналов с модулей ввода и перед выводом сигналов на исполнительные устройства. Для выполнения контроля без остановки процесса функционирования системы источники сигнала и нагрузки отключаются на короткое время (например, 1 мс) для подачи тестовых воздействий и измерения реакции на них. При достаточно малой продолжительности отключенного состояния оно не вносит возмущений в работу системы вследствие инерционности исполнительных устройств.

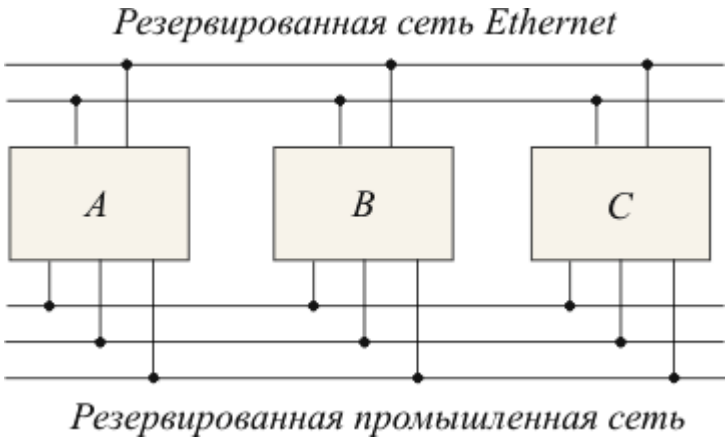


Рис. 15. Резервирование процессорных модулей и сетей с голосованием по схеме 2oo3

Горячее резервирование замещением

Основной сложностью при резервировании процессорного модуля является обеспечение синхронизации между основным и резервным процессором. Для того, чтобы перейти в рабочее состояние, резервный процессор должен иметь возможность:

- синхронизировать с основным процессором работу прикладной программы, накопленные данные, состояния регистров, состояния входов и выходов, таблицы неисправностей;
- обнаружить отказ основного процессора;
- заместить отказавший процессор.

При первоначальном включении резервного процессора из выключенного состояния или после горячей замены он должен получить от основного следующую информацию:

- все данные, полученные со входов;
- все данные, отправленные на выходы;
- состояния ПИД-регуляторов;
- уставки и другие значения, заданные пользователем в процессе работы системы;
- содержимое регистров, в том числе счетчиков-таймеров;
- другие данные, которые пользователь считает нужным синхронизировать.

После первоначальной синхронизации она повторяется в каждом контроллерном цикле. Это позволяет иметь уверенность, что резервный контроллер всегда готов к замещению основного. В этом заключается суть термина "горячий резерв".

Процедура перехода на резерв обычно занимает один контроллерный цикл. В течение этого времени выходные состояния всех модулей вывода сохраняются неизменными. Процедуру перехода на резерв выполняет специальный драйвер резервирования, который:

- определяет, какой из процессоров является основным, какой - резервным. Обычно основным является тот, который раньше был включен или назначен пользователем;
- убирает из основного процессора уставки, идентифицировавшие его как основной;
- рассылает всем участникам сети сообщения о том, какой процессор стал основным и какого типа система получилась после перехода на резерв (в соответствии со схемой деградации);
- выполняет синхронизацию;
- выполняет диагностический тест, который идентифицирует ошибки шины, потерю связи с сетевыми устройствами, изменение статуса процессора.

Переключение процессора обычно выполняется без коммутатора, с помощью изменения в сетевых устройствах адреса процессора. Например, если по умолчанию основной процессор имеет адрес 31, но после отказа драйвер резервирования указал, что основной процессор изменил адрес на 30, то модули вывода не принимают данные с

адреса 31, но принимают с адреса 30. Если данные не поступают ни с адреса 31, ни с адреса 30, то модули вывода переводят свои выходы в безопасные состояния.

Приложения-клиенты верхнего уровня системы автоматизации, которые используют данные из контроллера, во время переключения на резерв должны перерегистрироваться на получение информации от нового процессора.

Для выполнения безударного переключения необходим быстрый обмен информацией между процессорами в течение одного или максимум двух-трех контроллерных циклов. Для этого используется быстродействующий канал связи (может быть использован канал прямого доступа в память [Zhixun]), выполненный в виде параллельной электрической шины или с помощью оптического кабеля. Оптоволоконный канал, в отличие от параллельной шины, может использоваться для разнесения основного и резервного контроллеров на большое расстояние (километры), что необходимо для снижения вероятности отказа по общей причине, например, вследствие стихийного бедствия.

Необходимость постоянной синхронизации является причиной того, что у резервированных процессоров контроллерный цикл длиннее или используются более мощные процессоры, чем обычно.

Поскольку продолжительность синхронизации является очень важным параметром, от которого зависит коэффициент готовности системы и возможность безударного переключения на резерв, появляется задача минимизации объема передаваемой информации. Одним из путей решения этой проблемы является передача данных только при наступлении определенных событий в системе, которые могут приводить к различию во внутренних состояниях основного и резервного процессоров. В частности, синхронизация по событиям выполняется, если:

- происходит обмен информацией с модулями ввода-вывода;
- поступает запрос на прерывание;
- срабатывают запрограммированные пользователем таймеры;
- изменяются данные в результате обмена по сети.

Синхронизация по событиям должна выполняться средствами операционной системы контроллера в фоновом режиме и быть не связанной с программой пользователя. Это позволяет использовать одну и ту же прикладную программу как на резервированных процессорах, так и в системах без резервирования.

Недостатком систем с резервированием замещением является наличие нерезервированных подсистем: канала синхронизации, программного драйвера резервирования и процессора, на котором этот драйвер исполняется. Отказ этих элементов приводит к отказу всей резервированной системы.

Резервирование методом голосования

Метод голосования проще, чем резервирование замещением, поскольку не требует постоянной синхронизации состояний процессоров. Кроме того, метод голосования позволяет выполнять задачу управления без остановки во время перехода на резерв. Однако голосование с целью обеспечения безотказности возможно только в системе, состоящей не менее чем из трех процессоров, что достаточно дорого. Два

процессора, включенные по схеме голосования, могут быть использованы только в системах безопасности.

Типовая система с голосованием по схеме 2oo3 показана на рис. 16. В ней три процессорных модуля A, B и C исполняют одну и ту же программу пользователя, получая одни и те же данные от датчиков через модули ввода AI. Каждый процессорный модуль имеет три сетевых контроллера, которые исполняют протокол обмена по сети.

Работает система следующим образом. Каждый из трех параллельно работающих процессоров (A, B и C) отсылает в модули ввода запрос (команду). Каждый из трех модулей ввода получает эти три команды и выполняет голосование по схеме 2oo3, в результате которого из трех полученных входных значений выбирается одно, которое используется для выработки ответа на команду. Поскольку модулей ввода три, в процессор отправляется также три ответа на его команду, из которых каждый их трех процессоров выбирает один ответ по схеме 2oo3, который и используется в дальнейшей работе прикладной программы.

Аналогично происходит процедура вывода. Каждый процессор посылает в модули вывода команду вывода; каждый из модулей вывода (*1*, *2*, *3* и *4* на рис. 16) принимает три команды. Далее в каждом модуле вывода выполняется голосование по схеме 2oo3, в результате которого для исполнения выбирается одна команда из трех, по которой включается или выключается исполнительное устройств (в нашем примере ключ).

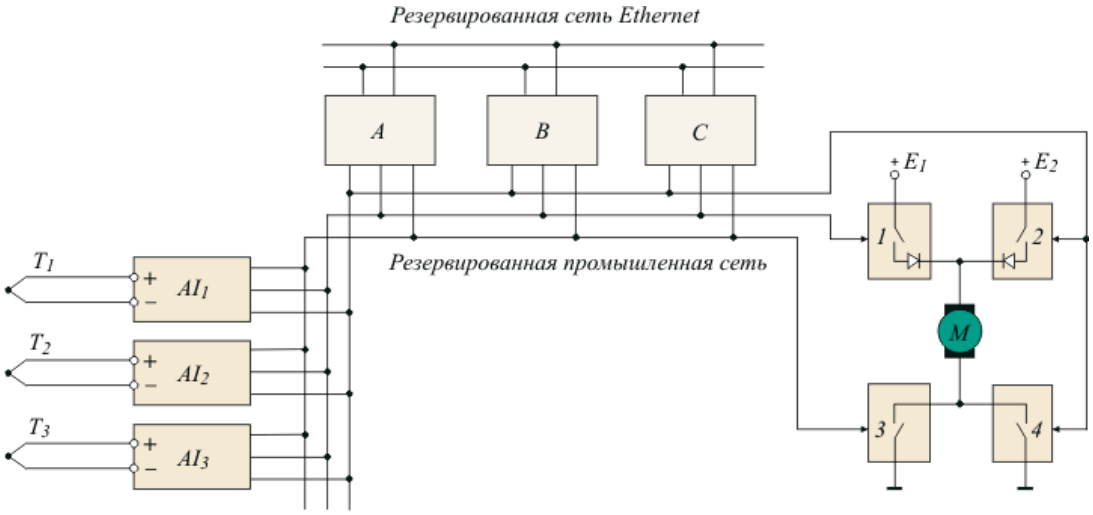


Рис. 16. Резервирование методом голосования

Таким образом, голосование выполняется не отдельным блоком резервирования, а в каждом элементе системы отдельно, поэтому отказ любого блока голосования не приводит к отказу всей системы.

После отказа одного из процессоров система продолжает непрерывно работать, поскольку схема голосования выдает правильной результат в результате мажоритарного голосования. После отказа двух процессоров наступает отказ системы. Однако в системах безопасности достаточно резервировать только функцию безопасности, что позволяет использовать голосование по схеме 1oo2, 2oo2 и использовать результат диагностики неисправности в качестве одного из "голосов". Поэтому после отказа одного из процессоров в системе 2oo3 она может перейти в режим 1oo2 (или 2oo2), после отказа

второго процессора - в режим 1oo1 и только после отказа третьего перевести свои выходы в безопасные состояния.

В системах с голосованием непрерывная синхронизация процессоров не требуется, поскольку при идентичных входных и выходных сигналах внутренние состояния процессоров оказываются также идентичны. Однако синхронизация необходима после горячей замены процессора, когда новый процессор должен получить стартовую информацию для своего функционирования синхронно с остальными процессорами. Отсутствие общего аппаратного и программного обеспечения, выполняющего функции перехода на резерв, повышает отказоустойчивость всей резервированной системы.

Несмотря на отсутствие необходимости в синхронизации, между процессорами выполняется обмен диагностическими данными и статусом. Данные, доступные всем элементам системы, называются глобальными и передаются от каждого процессора двум другим. Эти данные используются прикладными и системными программами, в частности, для реализации схемы деградации при появлении отказов. Для голосования по схеме 2oo3 в качестве третьего "голоса" каждый процессор использует свои собственные данные.

Тестирование процессорного модуля

Тестирование необходимо для своевременного перехода на резерв в системах с резервированием замещением, а также для информирования обслуживающего персонала о необходимости ручной замены отказавшего процессора. Поэтому каждый процессор постоянно исполняет программу самотестирования для обнаружения неисправностей.

Обычно тестируются следующие компоненты и функции:

- скоростной канал связи между процессорами;
- ядро центрального процессора;
- внутренние ОЗУ центрального процессора;
- флэш-память;
- шины ввода-вывода.

Каждый процессор выполняет также сравнение контрольной суммы своей программы с другими процессорами в резервированной группе и если возникает различие, то сигнализирует об ошибке. Ошибки памяти обнаруживаются в процессе чтения-записи с помощью анализа паритета или контрольной суммы. "Зависание" обнаруживается с помощью сторожевого таймера и обработки нештатных состояний процессора.

Поскольку объем тестирования существенно зависит от отведенного для него времени, постоянно исполняемый тест является достаточно сокращенным. Поэтому может быть предусмотрен второй, более полный тест, который занимает несколько минут времени и выполняется только при включении системы, до начала ее функционирования, или по инициативе оператора.

Каждый процессор получает информацию об ошибках в других процессорах и ошибках голосования. В системах с голосованием результаты тестирования могут быть использованы как дополнительные условия при голосовании. Например, выдача сигнала управления на исполнительный механизм может быть разрешена только при условии, что

результат диагностики процессоров положительный. В противном случае реализуется схема деградации при отказах.

8.2.5. Резервирование источников питания

Соединение источников питания с целью горячего резервирования замещением выполняется через диоды, как и соединение дискретных выходов (см. рис. 9-а). Поскольку падение напряжение на кремниевых диодах составляет около 1 В, напряжение источников питания следует выбирать на 1 В больше, чем требуемое напряжение на нагрузке. При падении напряжения основного источника соединенный с ним диод запирается и питание нагрузки осуществляется от резервного источника. Однако такая схема не может быть использована при отказах, когда напряжение основного источника становится больше допустимого. Эта проблема решается применением внутри источника питания резервированных элементов, снижающих вероятность отказа такого типа.

Если в качестве резервного источника используется батарея, которая не должна разряжаться, пока она находится в резерве, то напряжение основного источника должно быть больше напряжения батареи на величину разброса напряжений открытых диодов.

Для уменьшения потерь энергии используют германиевые диоды или диоды Шоттки, которые имеют меньшее напряжение в открытом состоянии по сравнению с кремниевыми.

Информация об отказе источника питания индицируется на его передней панели и пересылается на пульт оператора для принятия решения о замене.

8.3. Резервирование промышленных сетей

В состав промышленной сети входят линии связи, коммутаторы, сетевые мосты, маршрутизаторы, сетевые контролеры, преобразователи интерфейсов и источники питания. Однако чаще всего резервируются только линии связи, как наименее надежные элементы.

Основной характеристикой метода резервирования промышленных сетей является длительность перехода на резерв.

8.3.1. Сети Profibus, Modbus, CAN

Резервирование промышленных сетей выполняется обычно одновременно с резервированием контроллеров (см. раздел "Процессорные модули"). Для этого в каждом ПЛК используют два (реже - три) сетевых порта, к одному из них подключают основную промышленную сеть, к другому - резервную (Bertocco). Каждый контроллер имеет средства контроля работоспособности сети и в случае ее отказа переключает свой порт на резервную сеть. В системах с голосованием резервирование выполняется проще: исходящий поток сообщений посылается во все сети одновременно, а входящие потоки из всех сетей проходят через схему голосования (см. раздел "Общие принципы резервирования").

Для контроллеров, имеющих один сетевой порт и не предназначенных для работы в резервированных сетях, выпускаются специальные модули резервирования (см. www.abb.com), которые имеют один разъем (на рис. 17) для подключения к порту

оконечного устройства, например, ПЛК, и два разъема (A и B) для подключения к основной и резервной сети (рис. 17). Модули могут работать в многомастерных сетях как с ведущими, так и с ведомыми устройствами. Ведомых устройств, подключаемых к одному модулю резервирования, может быть несколько ($У_3 \ldots У_5$ на рис. 17). Модуль работает как коммутируемый повторитель интерфейса, одновременно контролируя исправность сети. Отказ обнаруживается по первому символу в передаваемом сообщении и при его появлении модуль переключается на резервный порт.

Основной проблемой резервирования сетей методом замещения является обнаружение отказа. Поскольку после отказа (например, обрыва) сети на некотором участке доставка сообщений к отсоединенной части сети невозможна, обнаружение отказа должно выполняться каждым участником сети автономно. Но это возможно только в многомастерных сетях или в сетях, имеющих специальные аппаратные средства контроля.

Протоколы резервирования промышленных сетей являются узкоспециализированными закрытыми разработками фирм-производителей контроллеров и в общедоступной литературе не описаны.

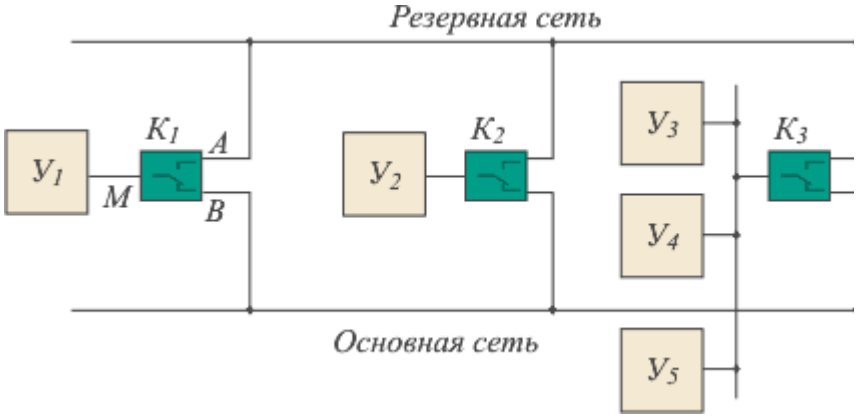


Рис. 17. Резервирование промышленной сети с помощью коммутации портов; $У_1 \ldots У_5$ - оконечные устройства, $К_1 \ldots К_3$ - модули резервирования сети

8.3.2. Сети Ethernet

Резервированию в промышленных сетях Ethernet с коммутаторами посвящена серия стандартов IEEE [IEEE, IEEE]. Однако первоначально они были предназначены только для исключения замкнутых контуров в сетях, поэтому требования к быстродействию алгоритмов учтены не были. В связи с резким ростом спроса на промышленный Ethernet (рост около 50% в год с 2004 г. [Prytz]) возросли требования ко времени переключения на резерв. Поэтому в 2005 г. началась работа над новым стандартом IEC 62439 “ High Availability Automation Networks” ("Сети промышленной автоматизации с высокой готовностью"), которая была инициирована комитетом IEC по цифровой коммуникации TC65C.

Основной проблемой при резервировании сетей Ethernet с коммутаторами является устранение замкнутых логических контуров (петель, циклов). Логические петли не допускаются потому, что при их наличии коммуникационные пакеты могли бы вечно путешествовать по сети, ограничивая ее пропускную способность. При возрастании трафика был бы возможен также отказ в обслуживании из-за превышения пропускной

способности сети. Кроме того, в таблице MAC-адресов коммутаторов появились бы одни и те же адреса для разных портов.

Для исключения логических петель служит стандартизованный алгоритм STP [IEEE], который выполняет блокировку портов коммутатора, через которые петли замыкаются. После появления промышленного Ethernet оказалось, что алгоритм STP позволяет искусственно вводить в сеть резервные ветви, которые, однако, не создают логических петель благодаря STP-алгоритму. При отказе некоторых ветвей протокол STP выбирает новые сетевые маршруты, в которых участвуют зарезервированные ранее связи.

Существует несколько методов резервирования промышленного Ethernet:

- агрегирование линий связи;
- резервирование на основе STP и RSTP протоколов;
- организация в сети физического кольца;
- полное резервирование всей сети.

Первые два метода стандартизованы, вторые два являются нестандартными разработками фирм-производителей и многие из них защищены патентами.

Метод агрегирования

Метод агрегирования линий связи описан в стандарте IEEE 802.3ad "Aggregation of Multiple Link Segments", который является разделом общего стандарта IEEE 802.3 [IEEE]. Этот метод использует два и более параллельных кабелей и портов для каждой линии связи. Объединение нескольких физических линий связи в один логический канал осуществляется с помощью протокола Link Aggregation Control Protocol (LACP). При этом группа (агрегат) линий связи и портов представляется одним логическим сервисным интерфейсом с одним MAC-адресом. В протоколе LACP полные Ethernet фреймы попеременно отсылаются по параллельным линиям связи и объединяются в приемнике. Пропускная способность такого агрегированного канала оказывается прямо пропорциональна количеству физических линий. При отказе одной линии данные пересылаются по другой. Этот стандарт поддерживается многими производителями Ethernet коммутаторов.

Метод резервирования, изложенный в стандарте IEEE 802.3ad, предполагает, что все агрегированные линии связи должны исходить из одного и того же коммутатора, т.е. сеть должна иметь топологию звезды. Для устранения этого ограничения фирмой Nortel были предложены три модификации метода агрегирования: SMLT ("Split Multi-Link Trunking"), DSMLT (Distributed Split Multi-Link Trunking) и R-SMLT ("Routed-SMLT) (см. www.nortel.com). Модификации этого метода предложены также фирмами Cisco и Adaptec, однако они несовместимы между собой и со стандартом.

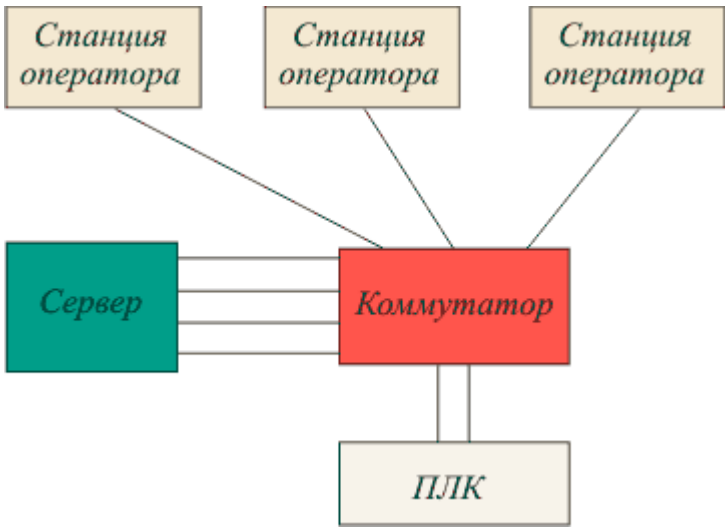


Рис. 18. Резервирование в сети Ethernet методом агрегирования линий связи

Метод агрегирования используется для резервирования соединений между коммутаторами, между коммутатором и сервером, а также между двумя компьютерами. Для дублирования связи между ПЛК и коммутатором ПЛК должен иметь два Ethernet-порта и драйвер, поддерживающий протокол LACP (IEEE 802.3ad), который предоставляет операционной системе один сетевой порт, физически состоящий из двух линий связи (рис. 18). При использовании 4-кратного резервирования связи между сервером и коммутатором (рис. 18) в сервер вставляется специальная 4-портовая Ethernet-карта с соответствующим драйвером, который заменяет 4 физических Ethernet порта одним логическим.

Достоинством метода является увеличение пропускной способности сети, возможность добавления произвольного количества линий связи для согласования пропускной способности разных каналов, малое время восстановления после отказа. Однако для резервирования сети в целом необходимо удвоенное количество кабелей и коммутаторов, что может быть неоправданно дорого. Кроме того, практически используемые схемы агрегирования часто не соответствуют стандартам IEEE, а оборудование разных производителей может быть несовместимым.

Метод агрегирования в соответствии с IEEE 802.3ad обеспечивает резервирование только линий связи; коммутаторы или сетевые контроллеры подключенного к сети оборудования остаются нерезервированными. Однако некоторые фирмы (см., например, www.syskonnect.com) предлагают дополнительное программное обеспечение, позволяющее объединять в один логический порт несколько каналов, проходящих через разные коммутаторы, которые, таким образом, оказываются резервированными.

Протокол STP и его модификации

Базовый Ethernet протокол STP (Spanning Tree Protocol), переводимый как "протокол остового дерева" или "протокол связующего дерева", является протоколом 2-го уровня модели OSI и описан в стандарте IEEE 802.1D [IEEE], который был принят в 1990 г. Первоначально протокол был использован для того, чтобы избежать петель в больших и сложных офисных сетях с мостами, которые могли иметь сложную запутанную

топологию. С появлением промышленного Ethernet этот протокол стал использоваться для горячего резервирования сетей с коммутаторами.

Цель STP протокола состоит в том, чтобы сконфигурировать сеть в виде дерева (т. е. без циклов) таким образом, чтобы каждый узел сети (лист дерева) был связан с корнем по пути с наименьшим временем доставки сообщений. Дерево формируется путем отключения ветвей, которые могут образовывать физические (не логические) петли в сети. Таким образом, при проектировании сети в нее могут быть добавлены избыточные ветви с целью резервирования, которые будут логически отключены протоколом STP при формировании дерева сети.

STP-протокол выполняет постоянный мониторинг сети с целью обнаружения происходящих в ней изменений. Если такие изменения выявлены, (например, если одна ветвь стала неработоспособной), то STP протокол автоматически выполняет перестроение дерева, включая в него при необходимости резервные ветви. Таким образом, после отказа ветви сеть оказывается вновь работоспособной через время, необходимое для выполнения STP алгоритма. Работоспособность сети сохраняется до тех пор, пока количество отказавших ветвей не станет настолько большим, что протокол не сможет построить дерево, используя все резервные ветви.

Для формирования дерева с минимальным временем доставки сообщений используются сообщения BPDU (Bridge Protocol Data Unit), встроенные в стандартный (IEEE 802.3) Ethernet-фрейм. Протокол BPDU использует два таймера для оценки времени доставки сообщений, которое по умолчанию не может превышать 20 с.

Время построения дерева при использовании STP алгоритма может доходить до 30 секунд и даже единиц минут [Prytz], что для многих приложений недопустимо много. Поэтому в 1998 году был разработан и закреплен стандартом IEEE 802.1w [IEEE], а позже стандартом IEEE 802.1D-2004 [IEEE] более быстрый алгоритм RSTP (Rapid Spanning Tree Protocol), который строит дерево за время не более 2 с. Протоколы STP и RSTP поддерживаются большинством производителей сетевых коммутаторов.

Для виртуальных сетей, граф которых представляется несколькими деревьями, был разработан протокол MSTP (Multiple Spanning Tree Protocol), который является расширением протокола STP и описан в стандартах IEEE 802.1s и IEEE 802.1Q-2003 [IEEE].

Недостатком STP и RSTP протоколов является часто недопустимо большое время перехода на резерв, а также невозможность резервирования связей между коммутатором и устройством, которое является участником сети.

Метод физического кольца

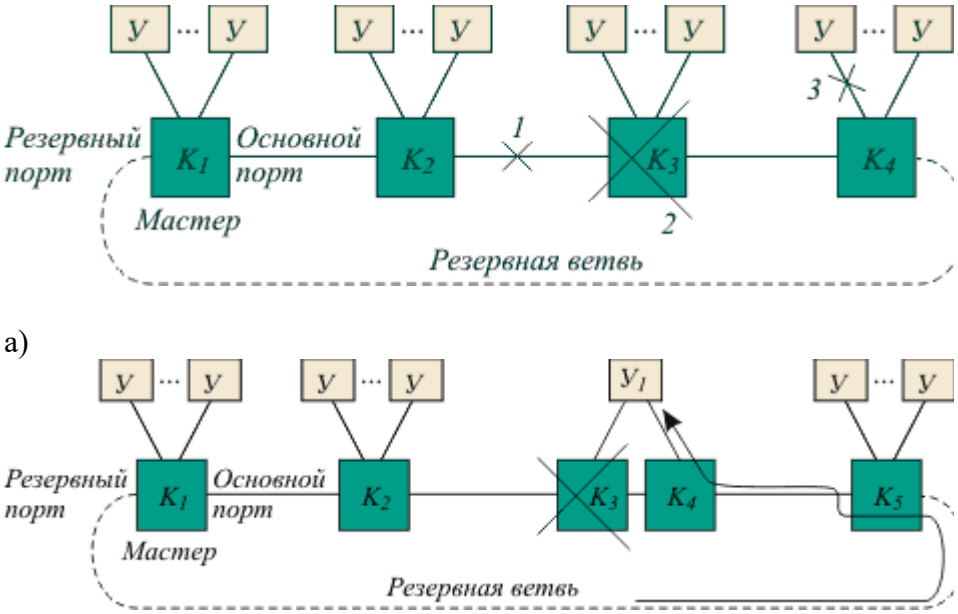


Рис. 19. Метод физического кольца для резервирования линии передачи (а) и линии передачи с коммутатором (б); K_1 ... K_5 - коммутаторы, Y - оконечные устройства (компьютеры, серверы, ПЛК)

Методы резервирования, основанные даже на усовершенствованном протоколе RSTP, имеют слишком большое время переключения на резерв (до 2 сек. [Prytz]). В то же время ряд приложений требует сокращения этого времени до единиц миллисекунд (как, например, в робототехнике) или до долей секунды (во многих химических технологических процессах). Поэтому некоторые фирмы разработали собственные нестандартные методы резервирования, которых в настоящее время насчитывается более 15 [Prytz].

В основе этих методов лежит использование сети с кольцевой физической топологией. Одна из ветвей сети блокируется коммутатором (мастером на рис. 19-а) и поэтому в режиме нормального функционирования сеть приобретает логическую шинную топологию. В случае отказа одной из ветвей мастер включает резервный порт. При этом подключается резервная ветвь и граф сети вновь становится связным, т. е. работоспособность сети оказывается полностью восстановленной.

Существует два метода обнаружения отказа в сети: циклический опрос и отправка уведомления об отказе.

При циклическом опросе мастер периодически посылает в сеть специальный тестирующий пакет через свой основной порт. При нормальном функционировании сети пакет проходит по кольцу и возвращается к мастеру через его резервный порт. Если пакет не приходит за время таймаута, мастер считает, что в сети произошел отказ и немедленно включает резервный порт, затем очищает свою таблицу адресов и рассылает всем коммутаторам инструкцию сделать то же самое. После очистки таблиц адресов все коммутаторы автоматически выполняют "обучение" (обновление таблицы адресов). В результате сеть вновь становится полнофункциональной, но уже с новой ветвью и новыми

таблицами адресов в коммутаторах. Разрыв *1* на рис. 19-а остается в сети до тех пор, пока не будет выполнен ремонт отказавшей ветви.

В методе уведомления об отказе циклический опрос не выполняется. Вместо этого каждый коммутатор самостоятельно контролирует целостность примыкающих к нему связей и при обнаружении отказа сообщает об этом мастеру с помощью уведомления. Далее мастер поступает точно так, как в методе циклического опроса.

После ремонта или замены отказавшей ветви она обнаруживается тем же методом тестирования кольца. Если связь по кольцу восстановлена, то мастер сразу же блокирует свой резервный порт (который был задействован на время выполнения ремонта), сбрасывает таблицу адресов и инструктирует оставшиеся коммутаторы сделать то же самое. В результате все коммутаторы обновляют таблицы адресов для сети с восстановленной ветвью.

Табл. 8.43. Параметры некоторых методов резервирования сетей Ethernet [Prytz]

Протокол	**Разработчик, стандарт**	**Время переключения на резерв**	**Топология**	**Наличие стандарта**
STP	IEEE 802.1D	30 с	Любая	Есть
RSTP	IEEE 802.1w	2 с	Любая	Есть
Hyper Ring	Hirschmann	0,3 с	Кольцевая	Нет
Turbo Ring	Moxa	0,15...0,3 с	Кольцевая	Нет
Rapid Ring	Contemporary Controls	0,3 с	Кольцевая	Нет
S-Ring	GarretCom	0,25 с	Кольцевая	Нет
Real time Ring	Sixnet	0,08 с	Кольцевая	Нет
Ring Healing	N-Tron	0,3 с	Кольцевая	Нет
Super Ring	Korenix	0,3 с	Кольцевая	Нет
Self healing Ring	TC Communications	0,25 с	Кольцевая	Нет
Jet Ring	Volktek	0,3 с	Кольцевая	Нет

Метод физического кольца имеет два существенных достоинства: во-первых, он предельно экономичен, поскольку способен восстановить работу сети при отказе любой ее ветви практически без затрат оборудования (дополнительно требуется всего один кабель для замыкания кольца и два лишних порта в двух коммутаторах). Во вторых, он позволяет примерно на порядок сократить время восстановления сети после отказа по сравнению со стандартным методом, использующим RSTP протокол (см. табл. 43).

К недостаткам метода относится неудобство кольцевой архитектуры, невозможность резервирования коммутаторов и сетевых адаптеров, а также ветвей, идущих от коммутаторов к конечным устройствам. При отказе коммутатора K_3 на рис. 19-а сеть оказывается разорванной и устройства, подключенные через коммутатор K_3, становятся недоступны. Аналогично, рассмотренный метод резервирования не дает эффекта при отказе связи *3* на рис. 19-а.

Два последних недостатка можно преодолеть, если в методе физического кольца использовать оконечные сетевые устройства с двумя Ethernet-портами (устройство

$У_1$ на рис. 19-б), и каждый из этих портов подключить к двум соседним коммутаторам $К_3$ и $К_4$. При отказе коммутатора $К_3$ на рис. 19-б мастер включает резервную ветвь и в сети появляется резервный путь к устройству $У_1$ через резервную ветвь и коммутаторы $К_5$, $К_4$.

К недостаткам методов физического кольца относится также отсутствие стандартов и, как следствие, несоответствие идеологии открытых систем.

Полное резервирование сети

Наименьшее время переключения на резерв предоставляет метод полного дублирование всей сети целиком. Вторым его достоинством является живучесть при отказах не только соединений между коммутаторами, но также и самих коммутаторов, сетевых портов устройств и линий связи устройств с коммутатором. Недостатком является высокая цена, поскольку метод предполагает, что все сетевое оборудование используется в удвоенном количестве.

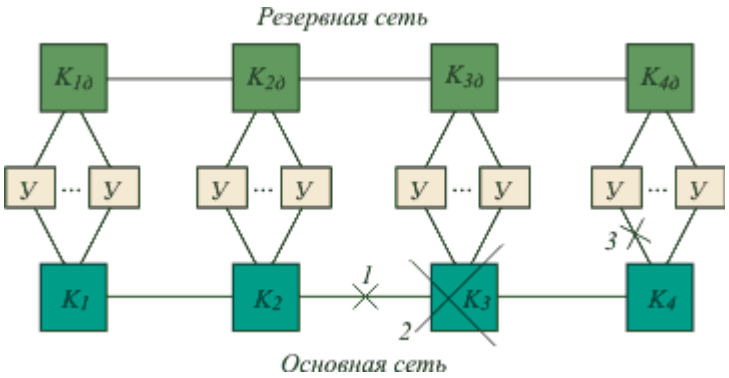


Рис. 20. Полное резервирование сети Ethernet

На рис. 20 показан пример дублированной сети с шинной топологией. Здесь $К_1$ ... $К_4$ - коммутаторы основной сети, $К_{1д}$ ... $К_{4д}$ - коммутаторы дублирующей сети. Каждое оконечное устройство $У$ имеет по два Ethernet-порта, один из которых подключается к основной сети, второй - к резервной. При любом отказе в основной сети (обрыв *1* в ветви между коммутаторами, отказ *2* коммутатора, обрыв *3* ветви между портом оконечного устройства и коммутатором на рис. 20) связь по сети восстанавливается путем переключения портов оконечных устройств на резервную сеть. Переключение выполняется быстро, поскольку метод не требует построения дерева, как в алгоритме STP.

Разновидностью полного резервирования является одновременное резервирование сети и оконечных устройств [Моха]. В этом случае получаются две полностью независимые системы автоматизации и резервированным оказывается не только сетевое оборудование, но и вся система. Для выбора одной из сетей и обнаружения отказа необходимы средства диагностики, которые могут быть реализованы на основе стандарта IEEE 802.1p/Q [Моха].

8.3.3. Резервирование беспроводных сетей

Основным фактором, определяющим надежность связи по беспроводным сетям, является замирание электромагнитных волн. Поэтому резервирование приемопередающей аппаратуры не приводит к повышению коэффициента готовности сети.

Как показывают эксперименты, поток ошибок в канале существенно изменяется с течением времени, поэтому беспроводной канал не может гарантировать доставку сообщений в заданный срок, речь может идти только о вероятности такой доставки. Одним из методов повышения вероятности доставки сообщений является резервирование физического канала связи с помощью применения нескольких антенн или нескольких передатчиков с антеннами [Willig].

Метод основан на том факте, что у приемной антенны электромагнитная волна представляет собой суперпозицию многих волн, пришедших с разных направлений после отражений, преломлений и дифракции на окружающих предметах. Если две приемные антенны расположены близко, то они принимают один и тот же сигнал с одинаковыми замираниями. Для того, чтобы сигналы в антеннах не были коррелированны, расстояние между ними должно быть больше некоторого расстояния, называемого дистанцией когерентности.

Для реализации метода резервирования антенн используется несколько антенн, например, по три антенны на каждом конце канала связи. Передача сообщений выполняется пакетами. Один и тот же пакет передается по очереди первой антенной, второй, затем третьей. На приемном конце пакеты сравниваются методом мажоритарного голосования или проверяются их контрольные суммы, чтобы выделить пакет без ошибок. Используется также выделение достоверных сообщений с помощью анализа отдельных символов сообщения, а не пакетов [Alamouti], избыточное кодирование и сложная обработка сигналов [Paulraj].

Как показано в работе [Willig], добавление каждой очередной антенны позволяет снизить вероятность ошибки в канале в 10 раз. При этом под вероятностью ошибки понимается вероятность неполучения пакета за заданное время, поскольку в [Willig] был использован метод ARQ (Automatic Repeat reQuest - "автоматический повтор запроса"), когда передающая станция повторяет передачу до тех пор, пока не получит подтверждение об успешном приеме или пока не истечет установленное время таймаута.

8.4. Оценка надежности резервированных систем

Надежность автоматизированной системы является комплексной характеристикой системы и состоит из нескольких показателей, основными из которых являются безотказность и ремонтопригодность. Безотказность численно характеризуется средней наработкой до отказа (MTTF - "Mean Time to Failure"), обозначается буквой T, или интенсивностью отказов λ ("Average probability of failure per hour"), а также вероятностью безотказной работы $P(t)$ в течение заданного времени t.

Ремонтопригодность характеризуется средним временем восстановления после отказа $T_в$ (MTTR - "Mean Time To Repair") или вероятностью восстановления в течение заданного времени.

Для расчета показателей надежности сложных систем, состоящих из большого количества элементов, используют метод декомпозиции (расчет надежности по частям). Если показатели надежности отдельных элементов (в том числе резервированных) заданы или рассчитаны, то вероятность безотказной работы системы рассчитывают следующим образом. Событие, состоящее в безотказной работе i-того элемента системы, обозначают символами A_i, а противоположное событие (отказ элемента) обозначают как $\overline{A_i}$. Отказ

системы без резервирования наступает при отказе хотя бы одного элемента. Поэтому событие, состоящее в безотказной работе системы A_Σ, равно произведению событий A_i, т. е. $A_\Sigma = \prod_{i=1}^{N} A_i$, где N - количество элементов в системе. Вероятность произведения независимых событий равна произведению вероятностей событий. Поэтому вероятность работоспособного состояния системы равна

$$P(A_\Sigma) = P\left(\prod_{i=1}^{N} A_i\right) = \prod_{i=1}^{N} P(A_i) \quad (9)$$

.

Учитывая зависимость вероятности безотказной работы элементов от времени (5) для каждого i-того элемента, предыдущее выражение можно записать в виде

$$P(A_\Sigma) = \prod_{i=1}^{N} \exp(-\lambda_i t) = \exp\left(-\sum_{i=1}^{N} \lambda_i t\right) = \exp(-\lambda_c t), \quad (10)$$

где

$$\lambda_c = \sum_{i=1}^{N} \lambda_i, \quad (11)$$

λ_c - интенсивность отказа всей системы; λ_i - интенсивность отказа i-того элемента.

Поскольку в эксплуатационной документации обычно указывают среднюю наработку до отказа, которая связана с интенсивностью отказов соотношением (8), то, пользуясь выражением (11), наработку до отказа всей системы T_c можно представить в виде

$$T_c = \left(\sum_{i=1}^{N} \frac{1}{T_i}\right)^{-1}, \quad (12)$$

где T_i - наработка до отказа i-того элемента.

В частности, для системы из N одинаковых элементов с наработкой $T_i = T_0$

$$T_c = \frac{T_0}{N}, \quad (13)$$

т. е. наработка на отказ системы обратно пропорциональна количеству ее элементов.

Резервированный элемент (контроллер, датчик и др.) при расчете надежности можно рассматривать как один элемент системы, если для него найдены показатели надежности.

Поскольку в системах автоматизации используются, как правило, только два вида резервирования: горячее резервирование замещением и резервирование методом

голосования, то при расчете их показателей безотказности можно обойтись без аппарата цепей Маркова [Александровская], ограничившись алгеброй случайных событий и теорией вероятностей. При расчете вероятности отказа "теплое" резервирование не отличается от горячего.

В случае горячего резервирования два элемента (например, два ПЛК) находятся постоянно во включенном состоянии и при отказе одного из них в работу включается второй. Если считать, что общие элементы, обеспечивающие процесс резервирования, *абсолютно надежны*, то безотказная работа резервированной системы A_Σ, состоящей из двух ПЛК, будет обеспечена, если работоспособен хотя бы один из них. Обозначим событие, состоящее в безотказной работе 1-го элемента как A_1, 2-го как A_2, а противоположные им события (отказы элементов) как $\overline{A}_1$ и $\overline{A}_2$. Тогда событие, состоящее в работоспособности резервированной системы (в данном примере система состоит из двух ПЛК), будет иметь место, если работоспособен первый ПЛК и одновременно работоспособен второй (A_1A_2) ИЛИ работоспособен первый и отказал второй ($A_1\overline{A}_2$) ИЛИ отказал первый и работоспособен второй: ($\overline{A}_1A_2$), т.е.

$$A_\Sigma = A_1A_2 + A_1\overline{A}_2 + \overline{A}_1A_2 = A_1\left(A_2 + \overline{A}_2\right) + \overline{A}_1A_2 = A_1 + \overline{A}_1A_2 . \qquad (14)$$

Найдем теперь вероятность работоспособности системы $P(A_\Sigma)$, пользуясь тем, что события A_1A_2, $A_1\overline{A}_2$ и $\overline{A}_1A_2$ несовместны (т.е. не могут иметь место в одно и то же время), следовательно, вероятность суммы событий равна сумме вероятностей каждого из них, а вероятность произведения событий равна произведению вероятностей:

$$\begin{aligned} P(A_\Sigma) &= P\left(A_1A_2 + A_1\overline{A}_2 + \overline{A}_1A_2\right) = P(A_1A_2) + P\left(A_1\overline{A}_2\right) + P\left(\overline{A}_1A_2\right) = \\ &P(A_1)P(A_2) + P(A_1)P\left(\overline{A}_2\right) + P\left(\overline{A}_1\right)P(A_2) = P(A_1) + P\left(\overline{A}_1\right)P(A_2) = \\ &P(A_1) + \left[1 - P(A_1)\right]P(A_2) . \end{aligned} \qquad (15)$$

Здесь использовано также свойство $P(A) + P\left(\overline{A}\right) = 1$.

Поскольку элементы в резервированной системе идентичны, то $P(A_1) = P(A_2) = P_o$ и, обозначая $P(A_\Sigma) = P_\Sigma$, получим

$$P_\Sigma = 2P_o - P_o^{\,2} . \qquad (16)$$

Подставляя сюда вместо P_o его зависимость от времени (5), получим вероятность безотказной работы системы при горячем резервировании в виде

$$P_\Sigma(t) = 2e^{-\lambda_o t} - e^{-2\lambda_o t} , \qquad (17)$$

где λ_o - интенсивность отказов элемента без резервирования.

Плотность распределения времени до отказа (частота отказов) согласно (6) равна

$$f_\Sigma(t) = 2\lambda_o\left(e^{-\lambda_o t} - e^{-2\lambda_o t}\right), \qquad (18)$$

а среднее время наработки до отказа

$$T_{cp} = \int_0^\infty t f_\Sigma(t)dt = 2\lambda_o \int_0^\infty t\left(e^{-\lambda_o t} - e^{-2\lambda_o t}\right)dt = \frac{3}{2\lambda_o} = 1{,}5T_o \qquad (19)$$

,

где T_o - средняя наработка на отказ одного контроллера. Интеграл в (8.19) берется по частям.

Рассуждая аналогично, можно получить вероятность безотказной работы системы из трех элементов, например, трех контроллеров, в схеме голосования 2оо3. Обозначим события, состоящие в работоспособности трех элементов соответственно A_1, A_2 и A_3, а противоположные им события (отказы) - как $\overline{A}_1, \overline{A}_2$ и $\overline{A}_3$. Тогда резервированная система будет работоспособной, если работоспособны первый И второй И отказал третий контроллер ИЛИ работоспособен первый И третий И отказал второй контроллер ИЛИ работоспособен второй И третий И отказал первый контроллер ИЛИ работоспособны все три контроллера одновременно, т.е.

$$A_\Sigma = A_1 A_2 \overline{A}_3 + A_1 \overline{A}_2 A_3 + \overline{A}_1 A_2 A_3 + A_1 A_2 A_3 . \qquad (20)$$

Переходя от событий к их вероятностям и учитывая, что слагаемые в (20) являются событиями несовместными, а также считая, что все контроллеры идентичны, т.е. $P(A_1) = P(A_2) = P(A_2) = P_o$, получим:

$$P_\Sigma = P_o^2(1-P_o) + P_o^2(1-P_o) + P_o^2(1-P_o) + P_o^3 = 3P_o^2 - 2P_o^3 , \qquad (21)$$

поэтому

$$P_\Sigma(t) = 3e^{-2\lambda_o t} - 2e^{-3\lambda_o t} . \qquad (22)$$

Графики зависимостей (8.17) и (8.22) показаны на (рис. 21-а).

Плотность распределения времени до отказа (частота отказов) согласно (6) равна

$$f_\Sigma(t) = 6\lambda_o\left(e^{-2\lambda_o t} - e^{-3\lambda_o t}\right), \qquad (23)$$

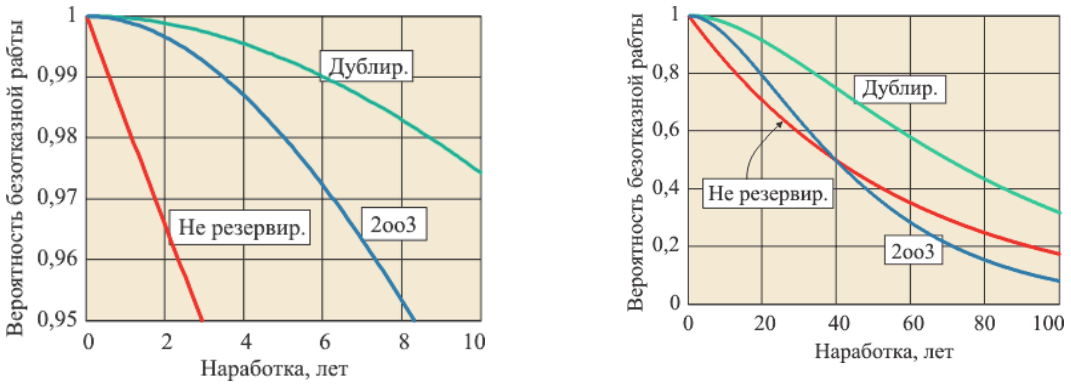
а среднее время наработки до отказа

$$T_{cp} = \int_0^\infty t f_\Sigma(t)dt = 6\lambda_0 \int_0^\infty t\left(e^{-2\lambda_0 t} - e^{-3\lambda_0 t}\right)dt = \frac{5}{6\lambda_0} = 0{,}833T_0 \quad (24)$$

,

где T_0 - средняя наработка на отказ одного контроллера.

Обратим внимание, что средняя наработка до отказа у системы с голосованием получилась ниже, чем у нерезервированной системы. Это объясняется тем, что система с *тремя* контроллерами и голосованием по схеме 2oo3 не является троированной, а имеет дробную кратность резервирования 1:2, т.е. в ней резервный элемент - один, а резервируемых - два, поскольку в схеме голосования только наличие двух работоспособных контроллеров обеспечивает работоспособность системы. Поэтому эффект снижения безотказности вследствие нарастания числа элементов в системе (13) при больших наработках оказывается сильнее эффекта резервирования. График вероятности безотказной работы для системы с голосованием (рис. 21-б) идет ниже, чем у системы без резервирования, начиная с некоторого значения наработки, а средняя наработка до отказа получается меньше.



а) б)

Рис. 21. Вероятность безотказной работы ПЛК с T_0=500 тыс. час. в течение времени наработки для случаев дублирования, голосования по схеме 2oo3 и при отсутствии резервирования. Графики а) и б) отличаются масштабом.

Сравнение систем только по средней наработке до отказа может вводить в заблуждение так же, как "средняя температура по больнице". Такое сравнение эффективно только для случаев, когда функциональные зависимости $P_\Sigma(t)$ элементов имеют одинаковый вид. Для систем с резервированием это условие не выполняется. Поэтому следует делать сравнение по более информативному показателю - вероятности безотказной работы, которая у системы с голосованием в течение практически всего времени эксплуатации значительно больше, чем у системы без резервирования (рис. 21-а и -б).

Графики, приведенные на рис. 21, иллюстрируют вероятность безотказной работы системы, в которой после отказа одного из элементов не выполняется его замена или ремонт. Если же замена элемента производится сразу, то понятие вероятности безотказной работы теряет значение, поскольку после замены вероятность отказа без замены элемента реализоваться не может. Актуальной становится длительность перехода на резерв, а также продолжительность выполнения горячей замены или восстановления после отказа. Поэтому для обслуживаемых систем автоматизации целью резервирования

является обеспечение непрерывности процесса управления или увеличение коэффициента готовности, но не увеличение вероятности безотказной работы. По этим же характеристикам система с голосованием превосходит все остальные.

Проделанный выше сравнительный анализ двух методов резервирования не может быть использован для систем безопасности, в которых вероятности опасного и безопасного отказов различны. Если в системах 2oo3, где требуется безотказность, после отказа двух элементов наступает отказ всей системы, то в системах безопасности *опасный отказ* наступает только после того, как исчерпаны все варианты деградации (например, 2oo3 - 1oo2 - 1001 - 0). Таким образом, для анализа вероятности *опасного отказа* система 2oo3 имеет кратность резерва не 2:1, а 1:2, т.е. она является троированной; после отказа одного элемента становится дублированной, после отказа двух элементов становится не резервированной и только после отказа всех трех элементов наступает отказ системы. Кроме того, для анализа систем, связанных с безопасностью, важна не вероятность отказа, а вероятность отказа при наличии запроса [МЭК] которая рассчитывается иным путем.

Поскольку автоматизированная система выполняет множество самостоятельных задач (функций), то параметры надежности по ГОСТ 24.701-86 [ГОСТ] оцениваются не для всей системы, а для каждой выполняемой функции отдельно.

При количественных оценках параметров надежности, а также при интерпретации полученных результатов следует учитывать достоверность исходных данных. Существующие методы экспериментальной оценки показателей надежности [ГОСТ, ГОСТ] были разработаны во времена, когда наработка на отказ вычислительных машин (ЕС-1061, "Электроника Д3-28" и др.) составляла от нескольких часов до нескольких суток. Экспериментальный материал по отказам, собранный в течение месяца, был достаточен не только для оценки наработки на отказ, но даже для построения функций распределения, изучения зависимостей параметров надежности от условий эксплуатации (температуры, вибрации, влажности и т. п.).

С тех пор ситуация изменилась коренным образом. Появилась технология поверхностного монтажа, увеличилась степень интеграции микросхем, были разработаны новые материалы для монтажа и изготовления печатных плат. Надежность электронных изделий возросла настолько, что экспериментальные данные невозможно накопить в достаточном количестве не только при стендовых испытаниях у изготовителя, но даже путем анализа отказов изделий, возвращенных потребителями в течение гарантийного срока (такая методика используется фирмой GE Fanuc [Programmable]). Так, из 3 тыс. модулей ввода-вывода ***RealLab!*** серии NL [Денисенко], проданных фирмой НИЛ АП, в течение гарантийного срока не было ни одного возврата по причине аппаратного отказа.

Кроме того, ПЛК не относятся к изделиям массового производства и поэтому за период между сменой их поколений количество отказавших изделий может оказаться недостаточным для расчета наработки на отказ. Получить же зависимость показателей надежности от условий эксплуатации еще более проблематично.

Ускоренные испытания [Федоров], широко применяемые в полупроводниковом производстве, неприменимы к ПЛК из-за невозможности экспериментального или расчетного определения коэффициентов подобия.

В то же время органы сертификации, в соответствии с существующими стандартами, требуют обязательного указания параметров надежности в ТУ и

эксплуатационной документации на изделие. Одним из реально осуществимых методов оценки показателей надежности является использование статистических данных объектов-аналогов по ГОСТ 27.301-95 [ГОСТ]. Поскольку аналоги, как правило, являются изделиями, изготовленными по устаревшей технологии, показатели надежности оказываются заниженными, по крайне мере, на порядок.

Рассмотрим, например, вероятность безотказной работы процессора CPU 313C-2DP фирмы Siemens, на который изготовителем указывается наработка на отказ (MTBF) λ=16,9 лет [Product]. В соответствии с (8.4) и (8.5), вероятность отказа процессора в течение гарантийного срока 18 мес. будет равна $1-\exp(-1{,}5/16{,}9)$=0,08. Поскольку оценка вероятности отказа рассчитывается как доля отказавших изделий в испытуемой партии, то, например, из 1000 находящихся в эксплуатации процессоров в течение гарантийного срока должны отказать в среднем 80 шт. и только 920 шт. остаться исправными. Однако любой пользователь продукции Siemens скажет, что эта цифра отличается от реальной, по крайней мере, на порядок. Можно было бы предположить, что наработка на отказ занижена потому, что при ее экспериментальном определении условия испытаний были выбраны предельными. Однако документ "Reliability Consulting" ("Консультация по надежности"), расположенный рядом с таблицей наработок на отказ [Reliability] указывает только одно условие: температура при испытаниях составляет 40 °C, и не дает методики пересчета для других условий эксплуатации. Выглядит странным также указание наработки на отказ тремя значащими цифрами, что по теории погрешностей должно означать, что приведенные данные отличаются от действительных не более чем на 1%.

Наличие большого числа парадоксов наводит на мысль, что показатели надежности, указываемые производителями электронных средств автоматизации, определяются политическими, а не техническими факторами, и по мере совершенствования технологии производства мы будем наблюдать только снижение достоверности этих показателей. В этих условиях о надежности изделий лучше судить по общей репутации фирмы и наличии системы управления качеством на базе стандартов ISO 9001 или ISO 9014, но не по наработке на отказ.

5. Заключение к главе «Аппаратное резервирование»

В системах автоматизации нашли широкое применение только два метода резервирования: горячее резервирование замещением и метод голосования. Основной целью резервирования является обеспечение высокого коэффициента готовности. Вероятность безотказной работы важна только для редко обслуживаемых систем автоматизации. Метод голосования позволяет также обеспечить непрерывность процесса управления.

Методы резервирования систем, связанных с безопасностью, имеют ряд особенностей, порождаемых делением отказов на опасные и безопасные.

При проектировании резервированных систем особое внимание следует уделять устранению отказов по общим причинам, которые могут обесценить все затраты на резервирование.

Наиболее эффективным методом резервирования промышленных сетей является метод физического кольца, если в качестве критерия эффективности использовать отношение надежности к стоимости.

Достоверность оценок вероятности безотказной работы электронных средств автоматизации крайне низка и по мере совершенствования технологии производства будет только снижаться.