Виктор Денисенко

Аппаратное резервирование в промышленной автоматизации

Часть 1

Введение

Резервирование является практически единственным и широко используемым методом кардинального повышения надёжности систем автоматизации. Оно позволяет создавать системы аварийной сигнализации, противоаварийной защиты, автоматического пожаротушения, контроля и управления взрывоопасными технологическими блоками [1] и другие, относящиеся к уровням безопасности SIL1...SIL3 по стандарту МЭК 61508-5 [2], а также ответственные системы, в которых даже короткий простой ведёт к большим финансовым потерям (системы распределения электроэнергии, управления непрерывными технологическими процессами, слежения за движущимися объектами и т.д.). Резервирование позволяет создавать высоконадёжные 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, [3, 4]), поэтому мы её касаться не будем.

Основные понятия и определения

Основные определения понятий теории надёжности и надёжности, связанной с функциональной безопасностью, даны в ГОСТ 27.002-89 [5] и МЭК 61508 [6, 7]. Далее 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) [8].

Отказом называется событие, заключающееся в нарушении работоспособности объекта. Факт отказа устанавливается на основании некоторых критериев отказа, то есть признаков, позволяющих судить о нарушении работоспособности. В результате отказа объект становится неисправным. Отказы возникают вследствие применения ненадёжных 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 надёжных 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 значение 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 15467-79).

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 несокра-

щаемой 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 элементы в резервированной системе выполняют одну и ту же функцию и являются равноправными, а выбор одного из 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»*, *«тёплым»* или *«горячим»* резервом. Его недостатком является зависимость от надёжности переключающих устройств.

Нагруженный резерв («горячий» резерв) — резервный элемент, который находится в таком же режиме, как и основной. 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.

Облегчённый резерв («тёплый» резерв) — резервный элемент, находящийся в менее нагруженном состоянии, чем основной. Например, резервный компьютер в «спящем» режиме является облегчённым 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 надёжностью, 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 «тёплым» резервом состоит в длительности периода переключения на резерв. При «горячем» резервировании контроллеров время переключения составляет от единиц миллисекунд до долей секунды, при «тёплом» — секунды, при «холодном» — минуты. Поэтому время переключения на резерв иногда рассматривают как основной признак при классификации резервирования замещением.

Надёжность — это свойство объекта сохранять во времени значения всех параметров и выполнять требуемые функции в заданных условиях применения. Надёжность является составным понятием. Оно может включать в себя понятия безотказности, долговечности, ремонтопригодности, сохраняемости. В промышленной автоматизации для количественной оценки надёжности чаще всего используется параметр «наработка на отказ» или параметр *«интенсивность отказов»*, а в системах безопасности — «*вероятность отказа при наличии запроса*» [9, 2].

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

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

Длительность t безотказной работы элемента (от момента включения $t = 0$ до t) является случайной величиной, поэтому её 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 её 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 (1) на $n(0)$, получим:

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

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

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

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

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

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

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

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

Таким образом, вероятность безотказной работы устройства в 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 отсчёта времени [3, 10], то есть 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) является производной от функции распределения

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

и для экспоненциальной функции распределения (5) равна

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

Зная плотность распределения (7), можно найти среднюю наработку до первого отказа $T_{ср}$, которая по определению является математическим ожиданием случайной величины длительности безотказной работы t, то есть

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

Интегрирование в (8) выполняется по частям.

Наработка на отказ $T_{ср}$ является основным параметром, который указывается в эксплуатационной документации на электронные средства промышленной автоматизации. Поскольку при $t = T_{ср}$ из (5) получается $P(T_{ср}) = 1/e = 0{,}37$, то наработку на отказ можно интерпретировать следующим образом: если в системе автоматизации имеется 100 модулей ввода-вывода, то через время $T_{ср}$ после начала эксплуатации останется в среднем 37 работоспособных и 63 отказавших модуля. 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 надёжности систем, связанных с безопасностью, вместо вероятности отказа используется понятие «*вероятность отказа при наличии запроса*» [2], то есть 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 надёжности охраны нужно рассматривать вероятность несрабатывания датчика охранной сигнализации в 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 надёжности 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 её тем самым в безопасное состояние. В такой системе отказ источника питания обмотки реле является безопасным отказом и поэтому не учитывается при расчёте 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.

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

Фактические значения наработки до отказа систем с резервированием оказываются гораздо ниже расчётных. 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 приведённых 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, 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 включённое звено со своей наработкой на отказ.

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 — 2 out of 3 voting, 1oo2 voting и др.). Реже используется «тёплый» 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.

Общие принципы резервирования

В основе метода резервирования лежит очевидная идея замены отказавшего элемента исправным, находящимся 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 определённого 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 разъёмными клеммными соединителями и с возможностью «горячей» замены [11] при условии наличия развитой системы диагностики неисправности. Для обеспечения «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, разъёмы с контактами разной длины и секвенсоры внутри устройства);
- защиту системы от броска тока, вызванного зарядом ёмкостей подключаемого устройства, например с помощью токоограничительных резисторов или отдельного источника питания;
- защиту устройства от перенапряжения, короткого замыкания, переполюсовки, превышения напряжения питания, ошибочного подключения.

Кроме того, для обеспечения «горячей» замены 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, а в алгоритмах автоматического регулирования должен быть предусмотрен «безударный» режим смены контроллера или модулей ввода-вывода [12].

Если резервный элемент входит в состав системы (а не лежит, скажем, на складе), 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 нечётного 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 подсистемы диагностики снижает также вероятность накопления скрытых неисправностей, которые со временем могут явиться причиной отказа.

Принцип работы схемы голосования рассмотрим на примере резервирования датчиков (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 измеряемой величины располагаются в порядке возрастания, и на выход схемы голосования поступает то из них, которое расположено между двумя крайними (но не среднее арифметическое!). Например, если в результате измерения темпера-

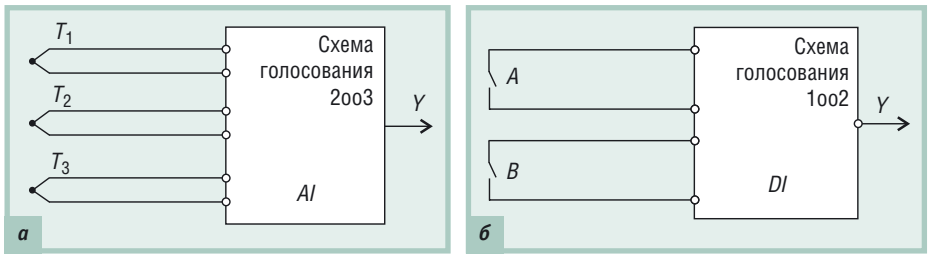

Рис. 1. Устройства с голосованием по схеме 2oo3 (*а*) и по схеме 1oo2 (*б*)

туры получены значения 0,12°C, 39,5°C и 39,4°C, то используется только значение 39,4°C, остальные игнорируются.

Резервирование элементов с дискретными сигналами выполняется аналогично. 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 нечётным. Однако в системах безопасности возможно применение любого числа «голосов». Вместо недостающего «голоса» используется условие, что система считается работоспособной, если отказ является безопасным. Это порождает системы, в которых выбирается один «голос» из двух, и такие системы по стандарту МЭК 61508 [2] обозначаются как 1oo2 (1 out of 2). Используются также системы 2oo2 (два «голоса» из двух), 2oo3 (два «голоса» из трёх), 2oo4 (два «голоса» из четырёх), 3oo4 (три «голоса» из четырёх). Нерезервированные системы обозначаются как 1oo1. Если в резервированной системе имеется развитая подсистема диагностики неисправностей, то к обозначению добавляется буква «D», например 1oo2D.

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 нарушении является опасным отказом, то становится очевидным, что схема голосования должна считать достаточным наличие одного «голоса» из двух, чтобы принять решение о подаче аварийного сигнала. Если сигналом срабатывания сигнализации является логическое значение 1, а сигналом отсутствия нарушения является значение 0, то блок голосования реализует логическую функцию $Y = A + B$.

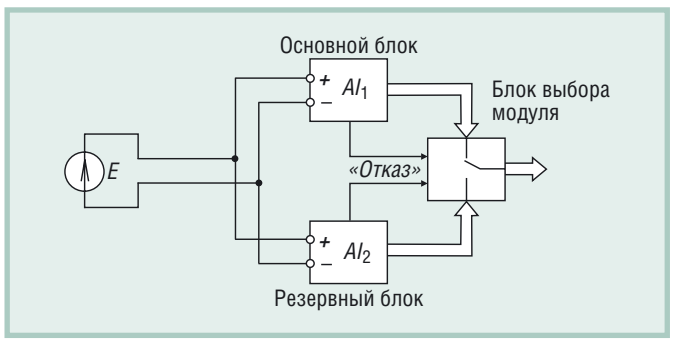

Рис. 2. Дублирование модуля ввода методом замещения

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 2oo2. 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 (два из двух). Выход из строя одного датчика не должен позволить системе выработать сигнал готовности к погружению, чтобы опасная ситуация не возникла. Такой блок голосования реализует логическую функцию $Y = AB$.

Несмотря на высокую эффективность схем голосования с чётным 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 нечётным количеством голосов, которые снижают вероятность отказов обоих типов. Выбор наилучшей системы осуществляется на основании результатов экономических расчётов.

При отказе одного из элементов резервированной системы безопасности 2oo3 её уровень безопасности понижается и она может начать функционировать как система 1oo2. Если замена неисправного элемента не произведена и произошёл второй отказ, то система переходит в режим без резервирования 1oo1, однако в этом режиме система не может находиться долго по требованиям безопасности. Очерёдность 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 перестаёт функционировать (останавливается). Перед остановкой система должна перевести все свои выходы в безопасные состояния. Понятие безопасного состояния для каждой системы определяется при её 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, не существует более простых схем голосования, чем 2oo3, которые сами по себе являются достаточно дорогими. Однако уникальным свойством систем с голосованием выступает 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 (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.

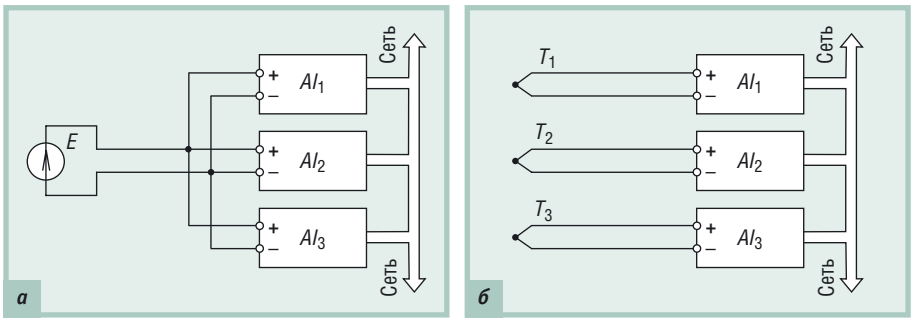

Рис. 3. Резервирование модулей ввода (*а*) и датчиков с модулями (*б*)

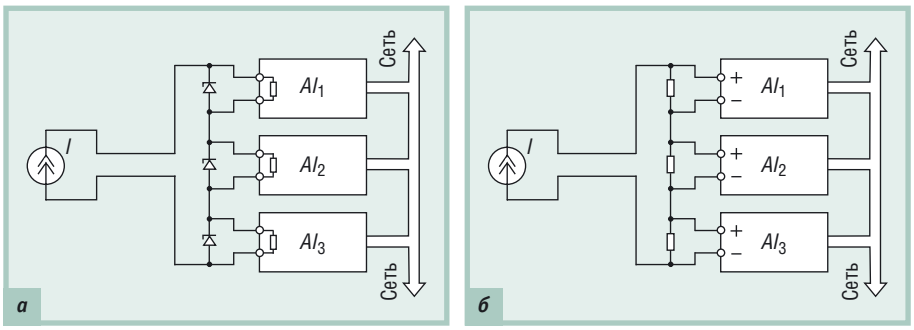

Рис. 4. Резервирование модулей ввода тока с измерительными резисторами внутри модулей (*а*) и снаружи (*б*)

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

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 приведён в ГОСТ Р 51841 [13]. 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 надёжных элементов, выбрать различную кратность резервирования для разных элементов системы и тем самым достичь максимального отношения надёжности к цене.

Общее резервирование не требует анализа соотношений между надёжностью отдельных элементов системы, исключает ошибки при расчёте надёжности 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 отказавших элементов расположен в основной системе, а второй – в резервной. При поэлементном резервировании вероятность такого отказа существенно ниже, поскольку для его реализации необходимо, чтобы один из отказавших элементов был основным, а второй – его резервом, что крайне маловероятно.

Резервирование модулей ввода и датчиков

Типичными отказами при вводе сигналов в ПЛК являются обрыв и короткое замыкание линии связи. На долю отказов линий связи датчиков и исполнительных устройств в системах автоматизации приходится 85% всех отказов [14]. Линии связи могут повреждаться в результате стихийных явлений (например обмерзание проводов), земляных работ, неправильного монтажа, злонамеренных действий и т.п., поэтому их надёжность часто не связана напрямую с надёжностью кабеля.

Резервирование аналоговых модулей ввода и датчиков

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 (рис. 3 *б*). При одновременном резервировании датчиков и модулей ввода 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, иллюстрирует 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 выполняется, как правило, программно.

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

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.

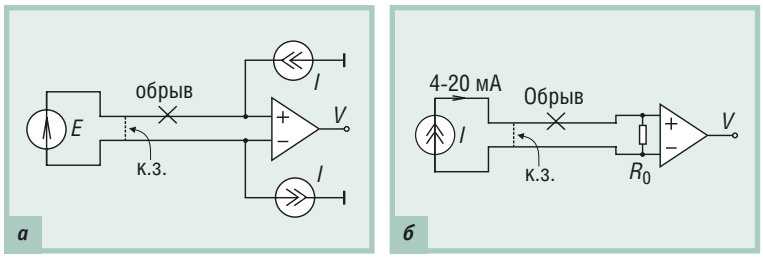

Рис. 5. Обнаружение обрыва и к.з. в линии связи или датчике, когда носителем сигнала является напряжение (*а*) либо ток (*б*)

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

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

Типовым методом обнаружения к.з. является измерение сопротивления входной цепи с помощью источников тока, подключённых, 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.

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 токовом стандарте 4-20 мА, где вся информация о сигнале содержится в диапазоне токов от 4 до 20 мА (рис. 5 *б*). В этом случае появление нулевого напряжения на входе приёмника 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.

Схемы подключения датчика типа «сухой» контакт, которые обеспечивают диагностику обрыва, к.з. на землю и на шину питания, показаны на рис. 6 и 7. При обрыве линии на входе модуля появляется сигнал, величина которого определяется делителем напряжения $\frac{R_4}{R_3+R_4}E_{\text{пит}}$ (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 $\frac{R_4}{R_4+R_3\left\|\left(R_1+R_2\right)\right.}E_{\text{пит}}$, при замкнутом – $\frac{R_4}{R_4+R_3\|R_1}E_{\text{пит}}$.

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 (рис. 2)

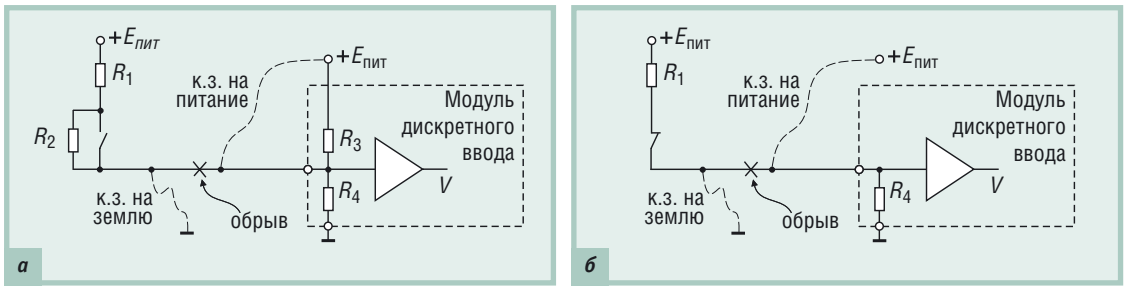

Рис. 6. Схема обнаружения обрыва и к.з. в цепи датчика с пятью различимыми состояниями (*а*) и с тремя состояниями (*б*)

поступает информация о неисправности. Тип неисправности выдаётся на пульт оператора системы автоматизации и заносится в журнал ошибок.

В ряде случаев достаточно иметь упрощённую схему диагностики. Например, если на рис. 6 *а* убрать резисторы R_2 и R_3 (рис. 6 *б*), то при замкнутом датчике получим напряжение на входе модуля, равное $\frac{R_4}{R_4 + R_1} E_{пит}$; при разомкнутом 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 разомкнутое. 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, то есть отказа, приводящего к несрабатыванию функции безопасности, произойти не может. Поэтому такая упрощённая схема контроля может быть использована в системах безопасности только с датчиками, у которых нормальным состоянием считается замкнутое.

При выборе упрощённых 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 путём подачи на вход тестовых комбинаций логических уровней (см. раздел «Общие принципы резервирования»).

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 приёмниками 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

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 надёжности, а другие способы (включая метод голосования) порождают сложные схемы, которые также понижают надёжность системы. Поэтому модули аналогового вывода чаще всего просто отсутствуют 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 выдаёт 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.

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 $i_н = \frac{V_{in}}{R_0}$, 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 $V_0 = V_{in}$. 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 $V_1 = E_{пит}$ – к.з. верхней (по схеме) линии на шину питания, а при $V_0 = E_{пит}$ – к.з. нижней линии. При $V_0 > V_{in}$ 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

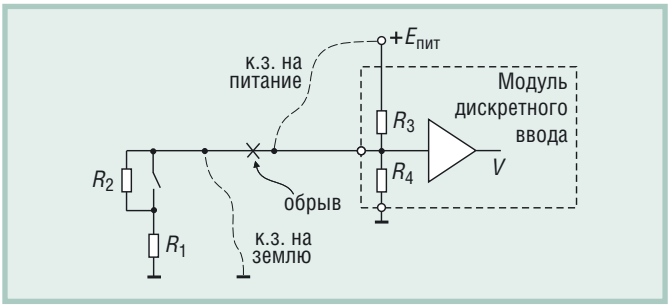

Рис. 7. Схема обнаружения обрыва и к.з. в цепи датчика

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 перестаёт зависеть от управляющего сигнала. Несмотря на этот недостаток, соединение дискретных выходов по схеме, представленной на 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.

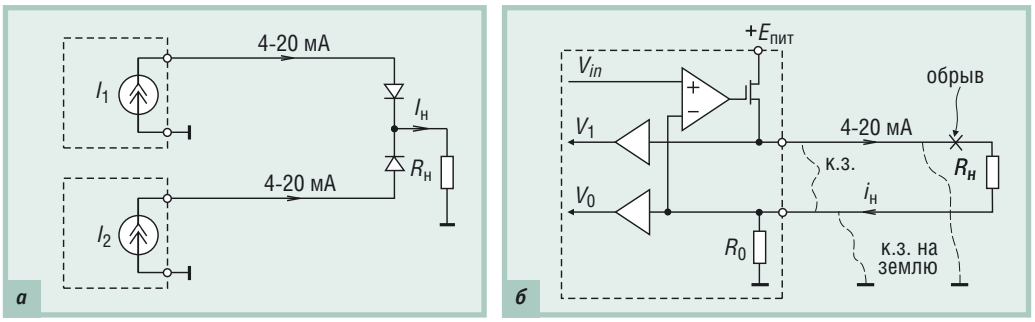

Рис. 8. Резервирование (*а*) и диагностика (*б*) линии вывода аналоговых сигналов

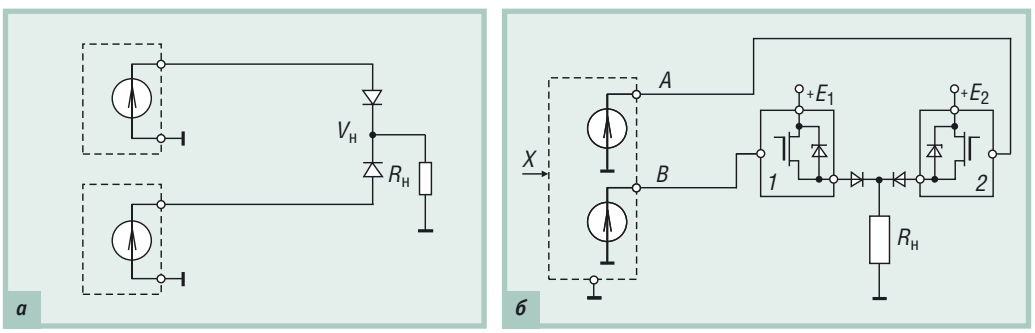

Рис. 9. Соединение дискретных выходов при резервировании (*а*) и один из вариантов реализации дискретных выходных каскадов (*б*)

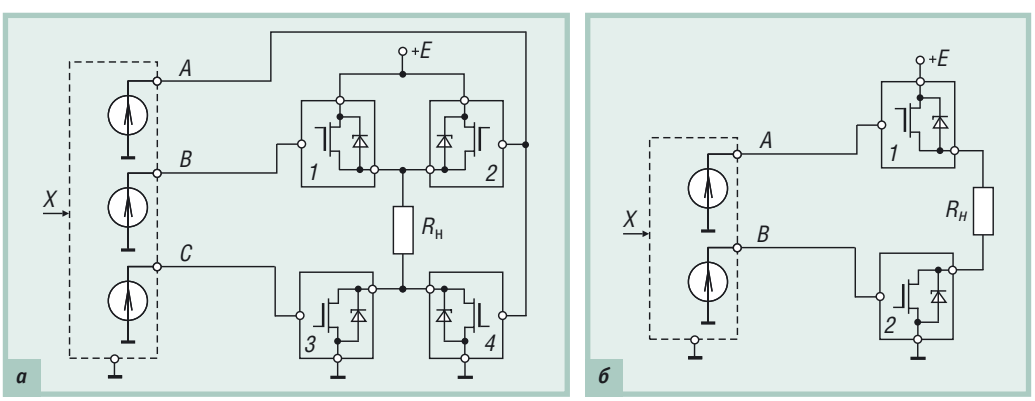

Рис. 10. Резервирование модулей вывода для повышения отказоустойчивости и живучести (*а*) и для реализации аварийного отключения (*б*)

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 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 *а*), то диоды не нужны.

Для резервирования систем аварийного отключения используется последовательное соединение двух выходных каскадов (рис. 10 *б*). При отказе одного из МОП-ключей в виде к.з. нагрузка отключается вторым каналом, то есть функция отключения в данной системе является дублированной. При необходимости же включить нагрузку достаточно отказа только одного ключа, то есть 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 четырёх ключей (рис. 10 *а*) [15]. В нём выход из строя любого выходного каскада или линии связи не приводит к нарушению ни функции включения, ни функции отключения. Реализация описанной цепи с помощью электромагнитных реле показана на рис. 11 *а*).

На схеме, представленной на рис. 10 *а*, каждый выходной каскад управляется сигналом *X* с помощью строенного источника сигнала ($A = B = C = X$). Для повышения надёжности 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*.

Структуры систем аварийного включения и отключения с дублированной сетью и ПЛК, резервированными по схеме 2oo3, показаны на рис. 12 *а, б*. 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.

Принцип контроля и диагностики выходных каскадов и линий связи с нагрузкой иллюстрирует рис. 13. Он аналогичен использованному в модулях аналогового вывода (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. ●

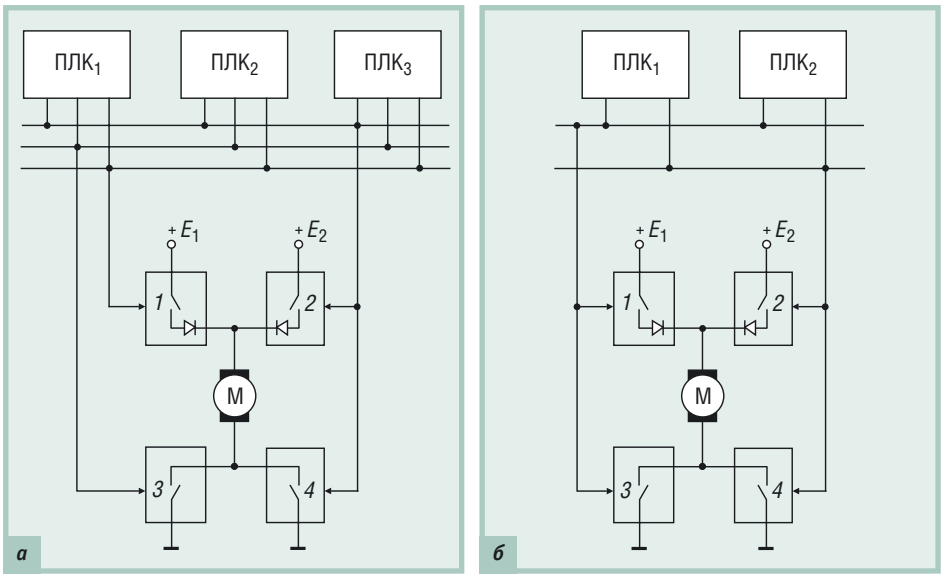

Рис. 11. Резервирование модулей вывода, шины и контроллеров (М – нагрузка)

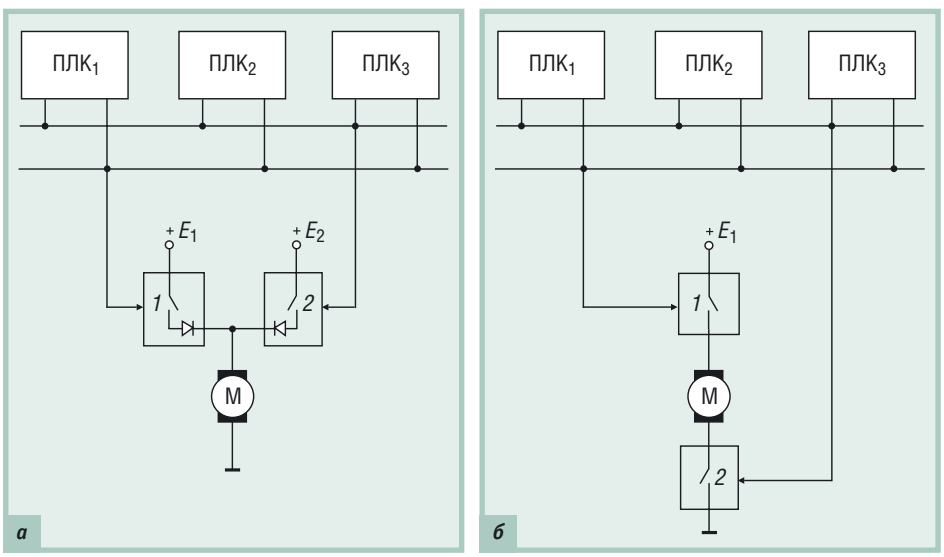

Рис. 12. Резервирование цепей дискретного вывода для систем аварийного включения (*а*) и аварийного отключения (*б*)

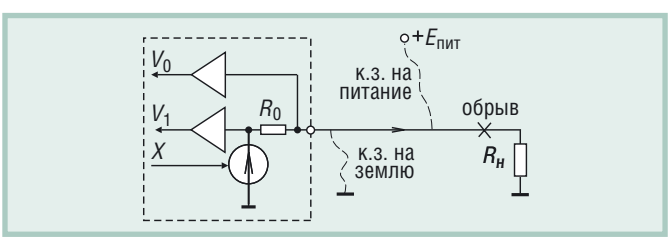

Рис. 13. Принцип обнаружения обрыва линии связи и к.з. на шину питания и на землю в модуле вывода дискретных сигналов

Литература

1. Денисенко В.В. Выбор аппаратных средств автоматизации опасных промышленных объектов // Современные технологии автоматизации. 2005. № 4. С. 86-94.
2. МЭК 61508-5 (1998). Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 5. Примеры методов для определения уровней целостности защиты.
3. Черкесов Г.Н. Надёжность аппаратно-программных комплексов. — СПб. : Питер, 2004. — 480 с.
4. Липаев В.В. Надёжность программных средств. — М. : Синтег, 1998. — 232 с.
5. ГОСТ 27.002-89. Надёжность в технике. Основные понятия. Термины и определения.
6. МЭК 61508-7 (2000). Функциональная безопасность электрических/электронных/программируемых электронных систем, обеспечивающих безопасность. Часть 7. Обзор методов и средств измерения.
7. МЭК 61508-3 (1998). Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению.
8. ГОСТ 15467-79. Управление качеством продукции. Основные понятия. Термины и определения.
9. Смит Д.Д., Симпсон К.Д. Функциональная безопасность. — М. : Издательский дом «Технологии», 2004. — 208 с.
10. Александровская Л.Н., Афанасьев А.П., Лисов А.А. Современные методы обеспечения безотказности сложных технических систем. — М. : Логос, 2001. — 206 с.
11. Беломытцев В. Замена элементов управляющей вычислительной системы без отключения питания // Современные технологии автоматизации. 2000. № 2. С. 72-77.
12. Денисенко В. ПИД-регуляторы: вопросы реализации // Современные технологии автоматизации. 2007. № 4. С. 86-97.
13. ГОСТ Р 51841-2001. Программируемые контроллеры. Общие технические требования и методы испытаний.
14. SIMATIC Automation System S7-300. Fail-Safe Signal Modules: Manual. — Edition 04/2006. — Siemens. 236 p.
15. Mitsubishi Safety Programmable Controller. MELSEC QS Series. CC-Link Safety System. Remote I/O Module: User's Manual. — Mitsubishi Electric Corp. P. 114.