Виктор Денисенко

Аппаратное резервирование в промышленной автоматизации

Часть 3

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 [20]. 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. По протоколу LACP полные Ethernet-фреймы попеременно отсылаются по параллельным линиям связи и объединяются в приёмнике. Пропускная способность такого агрегированного канала оказывается прямо пропорциональной 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, то есть 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). Модификации этого метода предложены также фирмами Cisco и Adaptec, однако они не совместимы между собой и со стандартом.

Метод агрегирования используется для резервирования соединений между коммутаторами, между коммутатором и сервером, а также между двумя компьютерами. Для дублирования связи между ПЛК и коммутатором контроллер 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 сервере устанавливается 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 подключённого к сети оборудования остаются нерезервированными. Однако некоторые фирмы (например, компания SysKonnect) 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, что переводится как «протокол остовного дерева», или «протокол связующего дерева») является протоколом 2-го уровня модели OSI [21] и описан в стандарте IEEE 802.1D [17], базовая версия которого была принята в 1990 году. Первоначально протокол был использован для того, чтобы избежать петель в больших и сложных офисных сетях с мостами (в современных сетях Ethernet мосты практически полностью вытеснены коммутаторами [21]), которые могли иметь сложную запутанную топологию. С появлением промышленного Ethernet этот протокол стал использоваться для «горячего» резервирования сетей с коммутаторами.

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

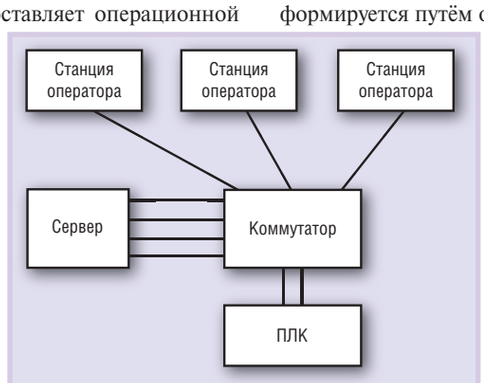

Рис. 18. Резервирование в сети Ethernet методом агрегирования линий связи

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 секунд.

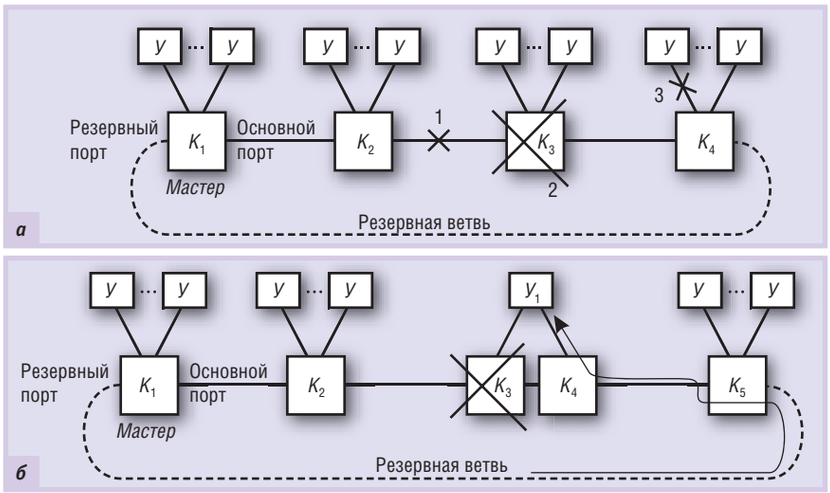

Рис 19. Метод физического кольца для резервирования линии передачи (*а*) и линии передачи с коммутатором (*б*) (K_1...K_5 – коммутаторы; *У* – оконечные устройства: компьютеры, серверы, ПЛК)

Время построения «дерева» при использовании STP-алгоритма может доходить до 30 секунд и даже единиц минут [19], что для многих приложений недопустимо долго. Поэтому в 1998 году был разработан и закреплён стандартом IEEE 802.1w [17], а позже стандартом IEEE 802.1D-2004 [17] более быстрый алгоритм RSTP (Rapid Spanning Tree Protocol), который строит «дерево» за время не более 2 секунд. 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-2005 [18].

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

Методы резервирования, основанные даже на усовершенствованном протоколе RSTP, имеют слишком большое время переключения на резерв (до 2 секунд [19]). В то же время ряд приложений требует сокращения этого времени до единиц миллисекунд (как, например, в робототехнике) или до долей секунды (как, например, во многих АСУ химическими технологическими процессами). Поэтому некоторые фирмы разработали собственные нестандартные методы резервирования, которых в настоящее время насчитывается более 15 [19, 22].

В основе этих методов лежит использование сети с кольцевой физической топологией. Одна из ветвей сети блокируется коммутатором (*Мастер* 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, то есть 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 тайм-аута, 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* остаётся в сети до тех пор, пока не будет выполнен ремонт отказавшей ветви.

В методе отправки 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.

Метод физического кольца имеет два существенных достоинства: во-первых, он предельно экономичен, поскольку способен восстановить работу сети при отказе любой её 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 (табл. 1).

К недостаткам метода относятся неудобство кольцевой архитектуры, невозможность резервирования коммутаторов и сетевых адаптеров, а также ветвей, идущих от коммутаторов к оконечным устройствам. При отказе коммутатора K_3 на рис. 19 *а* сеть оказывается разорванной и устройства, подключённые через коммутатор K_3, становятся недоступны. Аналогично рассмотренный метод резервирования не даёт 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 ка-

Таблица 1

Параметры некоторых методов резервирования сетей Ethernet [19]

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
HIPER-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

ждый из этих портов подключить к двум соседним коммутаторам K_3 и K_4. При отказе коммутатора K_3 на рис. 19 *б* мастер включает резервную ветвь, и в сети появляется резервный путь к устройству $У_1$ через резервную ветвь и коммутаторы K_5, K_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 дублирования всей сети целиком. Вторым его

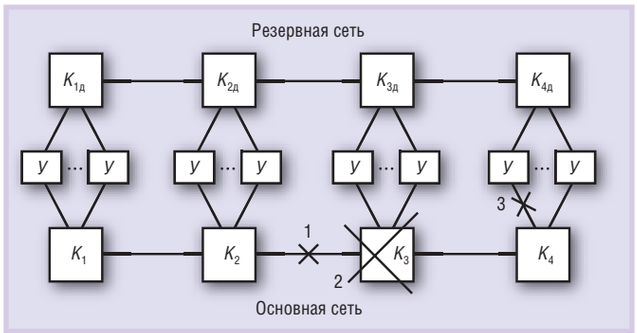

Рис. 20. Полное резервирование сети Ethernet

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 всё сетевое оборудование используется в удвоенном количестве.

На рис. 20 показан пример дублированной сети с шинной топологией. Здесь $K_1...K_4$ – коммутаторы основной сети, $K_{1д}...K_{4д}$ – 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 путём 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 [23]. 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.

Резервирование беспроводных сетей

Основным фактором, определяющим надёжность связи по беспроводным сетям, является замирание электромагнитных волн. Поэтому резервирование приёмопередающей 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 [24].

Метод основан на том факте, что у приёмной антенны электромагнитная волна представляет собой суперпозицию многих волн, пришедших с разных направлений после отражений, преломлений и дифракции на окружающих предметах. Если две приёмные 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 передаётся по очереди первой антенной, второй, затем третьей. На приёмном 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 [25], избыточное кодирование и сложная обработка сигналов [26].

Как показано в работе [24], 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 [24] был использован метод ARQ (Automatic Repeat Request – автоматический повтор запроса), когда передающая станция повторяет передачу до тех пор, пока не получит подтверждение об успешном приёме или пока не истечёт установленное время тайм-аута.

Оценка надёжности резервированных систем

Надёжность 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), обозначающейся 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 расчёта показателей надёжности сложных систем, состоящих из большого количества элементов, используют метод декомпозиции (расчёт надёжности по частям). Если показатели надёжности отдельных элементов (в том числе резервированных) заданы или рассчитаны, то вероятность безотказной работы системы рассчитывают следующим образом. Событие, состоящее в безотказной работе i-го элемента системы, обозначают как A_i, а противоположное событие (отказ элемента) – как $\overline{A_i}$. Отказ системы без резервирования наступает при отказе хотя бы одного элемента. Поэтому событие, состоящее в безотказной работе системы A_Σ, выражается произведением событий A_i, то есть

$$A_\Sigma = \prod_{i=1}^{N} A_i,$$

где N – количество элементов в системе. Вероятность произведения независимых событий равна произведению вероятностей событий. Поэтому вероятность работоспособного состояния системы равна:

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

Учитывая зависимость вероятности безотказной работы элементов от времени (5) для каждого i-го элемента, выражение (9) можно записать в виде:

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

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

λ_c – интенсивность отказа всей системы, λ_i – интенсивность отказа i-го 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:

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

где T_i – наработка до отказа i-го элемента.

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

$$T_c = \frac{T_o}{N}, \qquad (13)$$

то есть наработка на отказ системы обратно пропорциональна количеству её элементов.

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

Поскольку в системах автоматизации используются, как правило, только два вида резервирования: «горячее» резервирование замещением и резервирование методом голосования, то при расчёте их показателей безотказной работы можно обойтись без аппарата цепей Маркова [12], ограничившись алгеброй случайных событий и теорией вероятностей. При расчёте вероятности отказа «тёплое» резервирование не отличается от «горячего».

В случае «горячего» резервирования два элемента (например, два ПЛК) находятся постоянно во включённом состоянии, и при отказе одного из них в работу включается второй. Если считать, что общие элементы, обеспечивающие процесс резервирования, *абсолютно надёжны*, 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 ($\overline{A_1}A_2$), то есть

$$A_\Sigma = A_1A_2 + A_1\overline{A_2} + \overline{A_1}A_2 = A_1(A_2 + \overline{A_2}) + \overline{A_1}A_2 = A_1 + \overline{A_1}A_2. \qquad (14)$$

Найдём теперь вероятность работоспособности системы $P(A_\Sigma)$, пользуясь тем, что события A_1A_2, $A_1\overline{A_2}$ и $\overline{A_1}A_2$ несовместны (то есть 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:

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

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

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

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

а среднее время наработки до отказа

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

где T_o – средняя наработка на отказ одного контроллера. Интеграл в (19) берётся по частям.

Рассуждая аналогично, можно получить вероятность безотказной работы системы из трёх элементов, например трёх контроллеров, в схеме голосования 2oo3. Обозначим события, состоящие в работоспособности трёх 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 работоспособны первый И третий И отказал второй контроллер, ИЛИ работоспособны второй И третий И отказал первый контроллер, ИЛИ работоспособны все три контроллера одновременно, то есть

$$A_\Sigma = A_1A_2\overline{A_3} + A_1\overline{A_2}A_3 + \overline{A_1}A_2A_3 + A_1A_2A_3. \qquad (20)$$

Переходя от событий к их вероятностям и учитывая, что слагаемые в (20) являются событиями несовместными, а также считая, что все контроллеры идентичны, то есть $P(A_1) = P(A_2) = P(A_3) = P_o$, получим:

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

поэтому

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

Графики зависимостей (17) и (22) показаны на рис. 21 *а*.

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

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

а среднее время наработки до отказа

$$T_{ср} = \int_0^\infty t f_\Sigma(t)dt = 6\lambda_o \int_0^\infty t(e^{-2\lambda_o t} - e^{-3\lambda_o t})\,dt = \frac{5}{6\lambda_o} = 0{,}833T_o, \quad (24)$$

где T_o – 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, то есть 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*), начиная с некоторого значения наработки, идёт ниже, чем график для системы без резервирования, а средняя наработка до отказа получается меньше.

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, приведённые 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. 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 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, 2oo3-1oo2-1oo1-0). Таким образом, для анализа вероятности *опасного отказа* система 2oo3 имеет кратность резерва не 2:1, а 1:2, то есть она является троированной; после отказа одного элемента становится дублированной, после отказа двух элементов становится нерезервированной, и только после отказа всех трёх элементов наступает отказ системы. Кроме того, для анализа систем, связанных с безопасностью, важна не вероятность отказа, а вероятность отказа при наличии запроса [2], которая рассчитывается иным путём.

Поскольку автоматизированная система выполняет множество самостоятельных задач (функций), то параметры надёжности по ГОСТ 24.701-86 [27] оцениваются не для всей системы, а для каждой выполняемой функции отдельно.

При количественных оценках параметров надёжности, а также при интерпретации полученных результатов следует учитывать достоверность исходных данных. Существующие методы экспериментальной оценки показателей надёжности [27, 28] 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 надёжности 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. Надёжность электронных изделий возросла настолько, что экспериментальные данные невозможно накопить в достаточном количестве не только при стендовых испытаниях у изготовителя, но даже путём анализа отказов изделий, возвращённых потребителями в течение гарантийного срока [29]. Так, из 3 тыс. модулей ввода-вывода серии NL [30], 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 расчёта наработки на отказ. Получить же зависимость показателей надёжности от условий эксплуатации ещё более проблематично.

Ускоренные испытания [31], широко используемые в полупроводниковом производстве, не применимы к ПЛК из-за невозможности экспериментального или расчётного определения коэффициентов подобия.

В то же время органы сертификации в соответствии с существующими стандартами требуют обязательного указания параметров надёжности в ТУ и эксплуатационной документации на изделие. Одним из реально осуществимых методов оценки показателей надёжности является использование статистических данных объектов-аналогов по ГОСТ 27.301-95 [28]. Поскольку аналоги, как правило, являются изделиями, изготовленными по устаревшей технологии, показатели надёжности оказываются заниженными, по крайней мере, на порядок.

Рассмотрим, например, вероятность безотказной работы процессорного модуля CPU 313C-2DP фирмы Siemens, для которого изготовителем указана наработка на отказ (MTBF) λ=16,9 лет (http://support.automation.siemens.com/WW/view/

en/16818490 – Product Support. Mean Time Between Failures (MTBF), list for SIMATIC products). В соответствии с (4) и (5) вероятность отказа процессорного модуля в течение гарантийного срока продолжительностью 18 месяцев 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 процессорных модулей 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 её экспериментальном определении условия испытаний были выбраны предельными. Однако документ «Reliability Consulting» («Консультация по надёжности»), расположенный рядом с таблицей наработок на отказ в том же разделе упомянутого сайта фирмы Siemens, указывает только одно условие: температура при испытаниях составляет 40°C – и не даёт методики пересчёта для других условий эксплуатации. Также выглядит странным указание наработки на отказ тремя значащими цифрами, что по теории погрешностей должно означать, что приведённые данные отличаются от действительных не более чем на 1%.

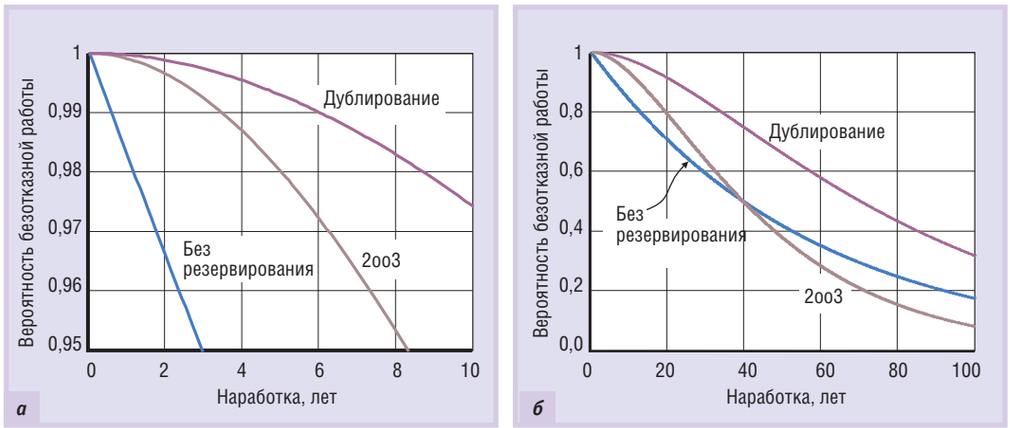

Рис. 21. Вероятность безотказной работы ПЛК с T_0 = 500 тыс. ч в течение времени наработки для случаев дублирования, голосования по схеме 2oo3 и при отсутствии резервирования (графики *а* и *б* отличаются масштабом)

Наличие большого числа парадоксов наводит на мысль, что показатели надёжности, 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 надёжности изделий лучше судить по общей репутации фирмы и наличию системы управления качеством на базе стандартов ISO 9001 или ISO 9014, но не по наработке на отказ.

Заключение

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 является целью резервирования только для редко обслуживаемых систем автоматизации. Системы с голосованием позволяют обеспечить также непрерывность процесса управления.

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

Резервирование промышленных сетей наиболее эффективно при использовании метода физического кольца, если в качестве критерия эффективности рассматривать отношение надёжности к стоимости.

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

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

Литература

20. IEEE Std. 802.3. IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area network – Specific requirements. Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. – IEEE Computer Society. 2005. Section 1–5. 2628 p.
21. Руководство по технологиям объединённых сетей/ пер. с англ.; под общ. ред. Е.Л. Полонской. – 3-е изд. – М. : Вильямс, 2002. – 1040 с.
22. Киселёв В. Промышленный Ethernet в стиле Hirschmann // Современные технологии автоматизации. 2005. № 2. С. 6–12.
23. Moxa White Paper. Redundancy in automation. – Moxa Networking Co., Ltd. 16 p.
24. Willig A. Redundancy concepts to increase transmission reliability in wireless industrial LANs // IEEE Trans. on Industrial Informatics. 2005. Vol. 1. No. 3. P. 173-182.
25. Alamouti S.M. A simple transmit diversity technique for wireless communications // IEEE J. Select. Areas Commun. Oct. 1998. Vol. 16. P. 1451-1458.
26. Paulraj A.J., Gore D.A., Nabar R.U., B?lcskei H. An overview of MIMO communications – A key to gigabit wireless // Proc. IEEE. 2004. Vol. 92. No. 2. P. 198-218.
27. ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надёжность автоматизированных систем управления. Основные положения.
28. ГОСТ 27.301-95. Надёжность в технике. Расчёт надёжности. Основные положения.
29. Programmable control products. Genius modular redundancy for fire and gas applications. – GE Fanuc Automation, GFK-1649A. Sept. 1999. 50 p.
30. Денисенко В.В., Ерещенко П.В., Кильметов Р.С., Метёлкин Е.Е., Халявко А.Н. Модули RealLab! серии NL для тяжёлых условий эксплуатации // Промышленные АСУ и контроллеры. 2005. № 2. С. 44-49.
31. Федоров В.К., Сергеев Н.П., Кондрашин А.А. Контроль и испытания в проектировании и производстве радиоэлектронных средств. – М. : Техносфера, 2005. – 504 с.