Виктор Денисенко

Аппаратное резервирование в промышленной автоматизации

Часть 2

Резервирование процессорного модуля

Процессорный модуль (для краткости далее будем говорить «процессор») следует резервировать в первую очередь, так как 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 «тёплым» (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 (рис. 14 *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.

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 (рис. 14 *б*). Такие системы относят к системам с «тёплым» резервом.

К резервированным процессорным модулям предъявляются следующие основные требования:

- безударное переключение на резерв (без внесения возмущений в управляемый процесс);
- малая длительность переключения;
- высокая надёжность 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) с целью подачи тестовых воздействий и измерения реакции на них. При достаточно малой продолжительности отключённого состояния в работу системы не вносятся возмущения вследствие инерционности исполнительных устройств.

«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:

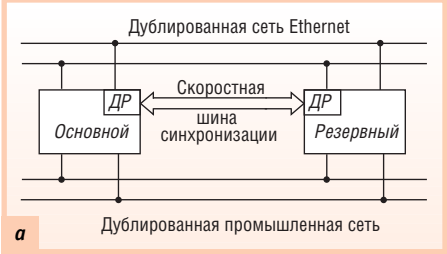
- обнаружить отказ основного процессора;
- синхронизировать с основным процессором работу прикладной программы, накопленные данные, состояния регистров, состояния входов и выходов, таблицы неисправностей;
- заместить отказавший процессор.

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 счётчиков-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 состо-



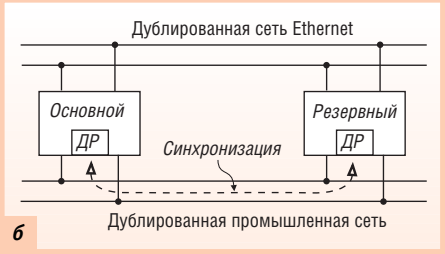


Рис. 14. «Горячее» (а) и «тёплое» (б) резервирование процессорных модулей замещением (ДР – драйвер резервирования)

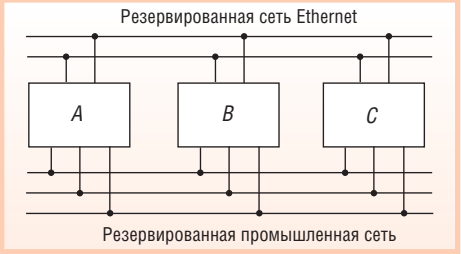


Рис. 15. Резервирование процессорных модулей и сетей с голосованием по схеме 2oo3

яния всех модулей вывода сохраняются неизменными. Процедуру перехода на резерв выполняет специальный драйвер резервирования (ДР), который

- определяет, какой из процессоров является основным, какой – резервным (обычно основным является тот, который раньше был включён 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, а 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-трёх контроллерных циклов. Для этого используется быстродействующий канал связи (может быть использован канал прямого доступа в память [16]), 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 объёма передаваемой информации. Одним из путей решения этой проблемы является передача данных только при наступлении определённых 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 не должна быть 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 трёх процессоров, что достаточно дорого. Два процессора, включённых 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 трёх параллельно работающих процессоров (*A*, *B* и *C*) отсылает в модули ввода запрос (команду). Каждый из трёх модулей ввода получает эти три команды и выполняет голосование по схеме 2oo3, в результате которого из трёх 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 из трёх 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 трёх, по которой включается или выключается исполнительное устройств (в нашем примере — ключ).

Таким образом, голосование выполняется не отдельным блоком резервирования, а каждым элементом 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 выдаёт правильной результат по итогам 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 или 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 идентичными. 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 объём тестирования существенно зависит от отведённого для него времени, постоянно исполняемый тест является достаточно сокращённым. Поэтому может быть предусмотрен второй, более полный тест, который занимает несколько минут времени и выполняется только при включении системы, до начала её 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 диагностика процессоров не выявила ошибок или неисправностей. В противном случае реализуется схема деградации при отказах.

Резервирование источников питания

Соединение источников питания с целью «горячего» резервирования замещением выполняется через диоды, как и соединение дискретных выходов (рис. 9 *а*). Поскольку падение напряжения 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 соединённый 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 отличаются меньшим падением напряжения 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.

Резервирование промышленных сетей

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

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

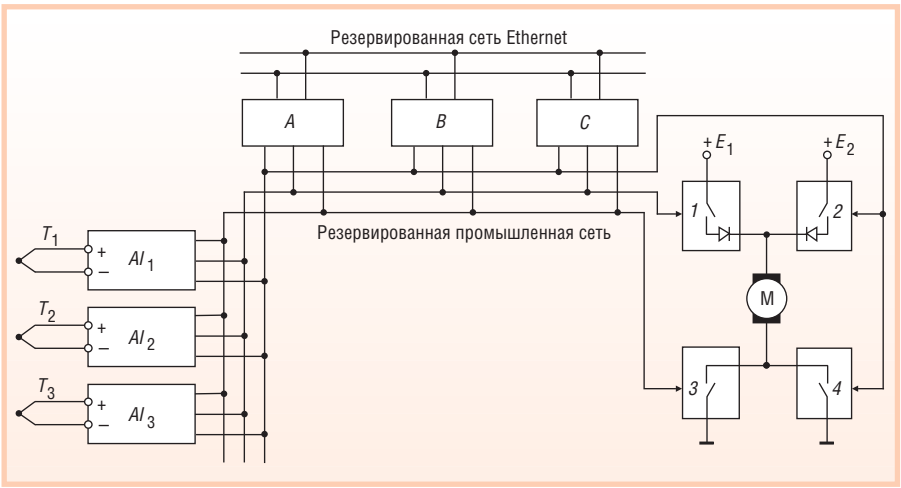


Рис. 16. Резервирование методом голосования

Резервирование сетей PROFIBUS, Modbus, CAN

Резервирование промышленных сетей выполняется обычно одновременно с резервированием контроллеров (см. раздел «Резервирование процессорного модуля»). Для этого в каждом ПЛК используют два (реже – три) сетевых порта, к одному из них подключают основную промышленную сеть, к другому – резервную (рис. 14). Каждый контроллер имеет средства контроля работоспособности сети и в случае её отказа переключает свой порт на резервную сеть. В системах с голосованием резервирование выполняется проще: исходящий поток сообще-

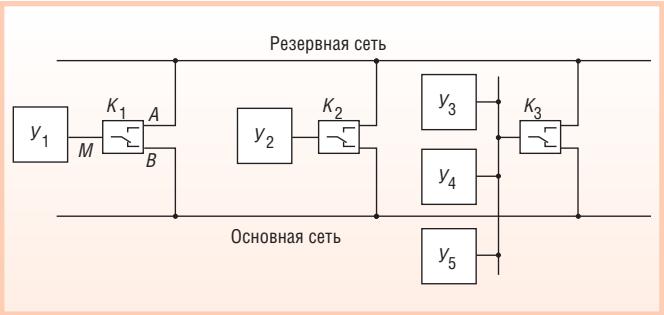


Рис. 17. Резервирование промышленной сети с помощью коммутации портов (y_1...y_5 – оконечные устройства, K_1...K_3 – модули резервирования сети)

ний 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, которые имеют один разъём (*M* на рис. 17) для подключения к порту оконечного устройства, например ПЛК, и два разъёма (*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 (y_3...y_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 отсоединённой 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.

Резервирование промышленных сетей Ethernet

Резервированию в промышленных сетях Ethernet с коммутаторами посвящена серия стандартов IEEE [17, 18]. 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., [19]) возросли требования ко времени переключения на резерв. Поэтому в 2005 году 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 её про-

пускную 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 [17], выполняющий 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 протоколов STP и RSTP;
- 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.

Окончание следует

Литература

16.Zhixun X., Yuejin H. Power System Technology // Proceedings of 2002 Int. Conf. on PowerCon. Vol. 4. P. 2448-2451.

17.IEEE Std 802.1D-2004. IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges. – IEEE. 2004. 281 p.

18.IEEE Std 802.1Q-2005. IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks. – IEEE. 2006. 303 p.

19.Prytz G. Redundancy in Industrial Ethernet Networks // 6th IEEE International Workshop on Factory Communication Systems, 27 June 2006. P. 380-385.

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Компания ПРОСОФТ совместно с FASTWEL и НИИВК создала УМС для решения прикладных вычислительных задач

Компания ПРОСОФТ (www.prosoft.ru) совместно с ОАО «Научно-исследовательский институт вычислительных комплексов им. М.А.Карцева» (НИИВК, www.niivk.ru) и компанией FASTWEL (www.fastwel.ru) завершила работы по созданию высокопроизводительной универсальной мультипроцессорной системы (УМС), предназначенной для решения прикладных вычислительных задач, требующих параллельных вычислений. Система построена на базе 24 новейших двухъядерных процессоров микроархитектуры Intel Core, объединённых высокоскоростным интерконнектом реального времени Infiniband.

Отличительными особенностями данной системы являются рекордные значения плотности вычислений и использование высокоскоростной сети обмена данными между вычислительными узлами с низкими уровнями задержки сигнала. В качестве вычислительных узлов были использованы одноюнитовые серверы компании Intel с двумя двухъядерными процессорами Intel Xeon серии 5100, работающими при пониженном напряжении питания и соответственно с пониженными значениями рассеиваемой тепловой мощности. Это позволило создать компактное решение, в котором все компоненты системы: вычислительные узлы, коммутаторы Gigabit Ethernet, коммутаторы Infiniband и система бесперебойного питания – размещаются в одной стандартной закрытой 19-дюймовой стойке, в качестве которой был использован новый шкаф для электронного оборудования VARISTAR производства компании Schroff (Германия). Шкаф имеет пылебрызгозащитное исполнение (степень защиты IP54), что позволяет использовать мультипроцессорную систему не просто вне специально подготовленных кондиционированных помещений, а непосредственно в производственных помещениях без предъявления каких-либо требований к их обустройству.

Другой отличительной особенностью выбранной архитектуры является возможность гибкого масштабирования и наращивания возможностей системы. Архитектура вычислительных узлов и характеристики используемых чипсетов позволяют добиться удвоения вычислительной мощности без существенного увеличения теплового бюджета системы и с сохранением объёмных характеристик.

Вычислительные узлы объединены двумя различными типами сетей, предназначенными для обмена данными в процессе вычислений и обмена обслуживающей информацией ,– Gigabit Ethernet и Infiniband, каждая из которых коммутируется соответствующим коммутатором сети. Использование сети Infiniband позволяет практически в 10 раз повысить скорость обмена данными между узлами и в 20-30 раз понизить задержки при передаче данных. Результаты тестов, проведённых на УМС, определили реальные значения скорости обмена по сети Infiniband в диапазоне от 700 до 1000 Мбайт/с с латентностью в диапазоне 3-4 мс.

Максимальная теоретическая вычислительная мощность текущей конфигурации составляет 447 GFLOPS при энергопотреблении 4,5 кВт. Таким образом, благодаря оптимизации архитектуры кластера по мощности и использованию низковольтных версий процессоров достигнуто высокое реальное значение вычислительной плотности 75 GFLOPS/кВт. При этом общая архитектура построения УМС настолько гибка, что позволяет провести замену двухъядерных процессоров на четырёхъядерные с ростом теоретической мощности до 890 GFLOPS.

Pepperl+Fuchs предлагает бесплатно технологию DTM

Компания Pepperl+Fuchs (www.pepperl-fuchs.com) была среди основных движущих сил в разработке и становлении технологии FDT/DTM (**F**ield **D**evice **T**ool/**D**evice **T**ype **M**anager). Технология DTM (небольшие программы, описывающие не только средства связи, но и данные об устройствах) стала распространённым во всём мире стандартом, она позволяет быстро и легко сконфигурировать даже сложные полевые устройства перед началом их эксплуатации. Заказчики продукции Pepperl+Fuchs одними из первых применили эту передовую технологию конфигурации и установки параметров устройств, подключённых к сети для эффективной эксплуатации устройств Fieldbus, HART-мультиплексоров, интерфейсных устройств, систем удалённого ввода/вывода (Remote I/O), средств измерения уровня.

В знак признательности заказчикам, использующим эту технологию в течение многих лет и содействовавшим одобрению FDT/DTM, компания Pepperl+Fuchs решила приостановить начисление лицензионной платы за ряд модулей DTM с января 2008 года.