Анализ возможностей современных ППК для построения отказоустойчивых АСУТП.

Бабешко Е.В., Кривоносов А.И., Харченко В.С.

Рассмотрены существующие варианты резервирования программируемых логических контроллеров, применяемых при построении отказоустойчивых АСУТП.

Введение

В настоящее время при построении отказоустойчивых автоматизированных систем управления технологическим процессом (АСУТП) на базе программируемых логических контроллеров (ПЛК) широко применяются резервированные структуры. Это обусловлено тем, что современные ПЛК имеют различные встроенные средства поддержки резервирования, предоставляя широкие возможности для обеспечения отказоустойчивости.

Существующие способы резервирования ПЛК рассмотрены в технической документации производителей [1-3]. Кроме того, в литературе достаточно подробно описано построение резервированных систем на основе отдельных семейств ПЛК (например, [4]).

Однако на этапе проектирования отказоустойчивых систем все же достаточно сложно сделать обоснованный выбор из существующего множества решений, поскольку:

1) значительная часть опубликованной информации является устаревшей, так как технология автоматизации в настоящее время переживает период скачкообразных изменений;

2) в литературе практически отсутствуют обзоры независимых экспертов с объективными и достаточно полными сведениями об имеющихся на рынке контроллерах различных производителей, различных способах построения автоматизированных систем на основе ПЛК;

3) в недостаточном объеме изложены рекомендации по выбору ПЛК;

4) отсутствует классификация возможных технологий резервирования ПЛК и других технологий повышения надежности, нет сравнения характеристик и особенностей этих технологий.

Целью данной статьи является анализ существующих на данный момент технологий резервирования программируемых логических контроллеров, предлагаемых различными производителями для построения отказоустойчивых систем. Планируется произвести сравнение, выделить достоинства и недостатки, указать возможные области применения этих технологий.

Сложность поставленной задачи заключается в том, что требуется сопоставить по множеству критериев довольно большое число способов построения систем, произвести сравнение их характеристик, и затем найти некий разумный компромисс, который позволит сделать выбор наиболее оптимальной структуры системы для заданного конкретного объекта. Кроме того, приводимые в документации различных фирм решения, их свойства и технические характеристики часто не сопоставимы между собой, в то время как многие важные сведения вообще не предоставляются.

Существующие варианты резервирования

Производители ПЛК предлагают достаточно большой выбор резервированных архитектур, начиная от простых дублированных (1002, one-out-of-two, один из двух) и заканчивая троированными и квадрированными структурами с различными степенями самодиагностики [5]. При этом, как правило, предоставляется возможность резервирования любого компонента системы (модуля центрального процессора, модулей ввода/вывода, блока питания, линий связи и т. п.).

Как видно из рис. 1, на практике применяются две реализации механизмов поддержки резервирования - аппаратная и программная.

Аппаратная реализация поддержки резервирования

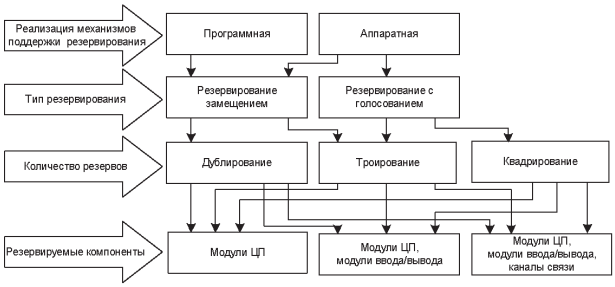

Рис. 1. Существующие варианты резервирования ППК

Как правило, в ассортименте контроллеров любого производителя можно выделить три основных семейства:

- малые контроллеры" (до 300 входов), не поддерживающие механизмов резервирования;
- средние контроллеры" (до 4000 входов), поддерживающие программный способ резервирования;
- большие контроллеры" (свыше 4000 входов), поддерживающие аппаратный способ резервирования.

На рис. 2 показано соотношение стоимости и мощности контроллеров.

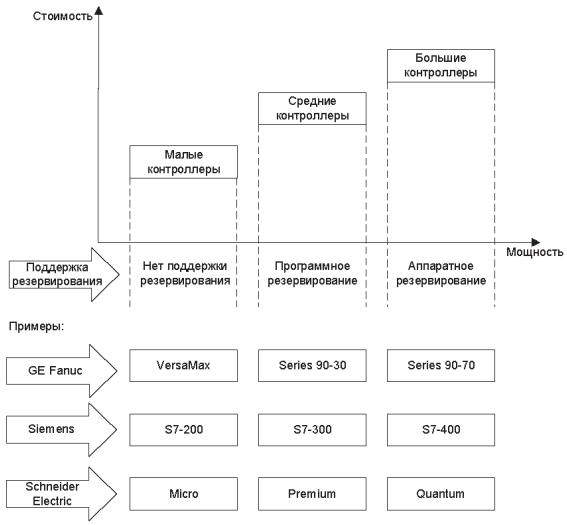

Рис. 2. Соотношение стоимости и мощности контроллеров.

Под обобщенным термином "мощность" понимается разрядность и быстродействие центрального процессора, объем разных видов памяти, число портов и сетевых интерфейсов [6]. Однако справедливо и следующее утверждение: чем "мощнее" контроллер, тем больше он имеет встроенных средств поддержки резервирования.

Таким образом, для построения резервированной системы, в которой необходимо малое время переключения с основного контроллера на резервный, требуются значительные затраты. Во-первых, придется приобретать наиболее функциональный (и, следовательно, наиболее дорогой) контроллер. Во-вторых, требуются дополнительные аппаратные средства (модули горячего резерва, средства синхронизации и т. п.).

На рис. 3 представлена схема технологии аппаратной реализации поддержки резервирования. В этом случае задачи синхронизации данных, переключения с основного ППК на резервный возлагаются на специальные модули - модули горячего резерва. Эти модули устанавливаются на шасси основной и резервной системы, соединяются между собой скоростной линией связи (как правило, волоконно-оптической). Каждый из модулей производит мониторинг состояния соответствующего контроллера, и в начале каждого сканирования текущие значения регистров и таблица состояния ввода-вывода основного ППК передаются на резервный. Если основной ППК отказывает, модуль горячего резерва переключает управление на резервный. Время переключения при таком варианте построения системы не превышает 50 мс.

Как правило, на практике применяются дублированные структуры. Однако для особо ответственных

систем дублирования может оказаться недостаточно, поскольку данный способ, например, не позволяет избавиться от ложного срабатывания отдельных элементов системы. Для этого случая рядом производителей предусмотрены архитектуры с тройным модульным резервированием (TMR - Triple Modular Redundancy).

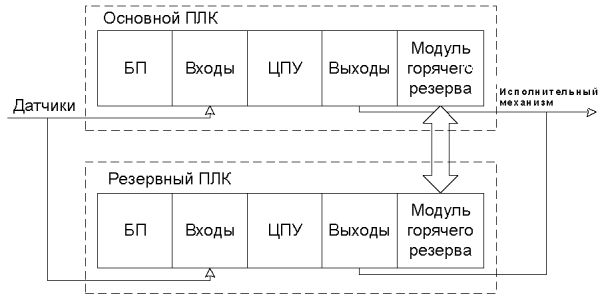

Рис. 3. Аппаратная реализация поддержки резервирования

Такие архитектуры включают:

- полное тройное резервирование главных процессоров и каналов ввода/вывода;

- диагностику всех элементов контроллера и внешних цепей;

- непрерывный обмен данными между центральными процессорами, который обеспечивает идентичность данных в памяти каждого из процессорных модулей на каждом цикле выполнения программы ППК;

- мажоритарную обработку данных исправных дискретных каналов - по схеме "два из трех";

- арифметическое усреднение данных между исправными аналоговыми каналами;

- тройное резервирование внутрисистемных шин и коммуникаций.

ППК, поддерживающие архитектуру TMR, обладают не только полной устойчивостью к единичным отказам элементов, но также устойчивы и ко множественным отказам. Даже в самом худшем случае, при двух отказах элементов, работа может продолжаться на оставшемся третьем канале.

Решение всех вопросов взаимодействия между троированными элементами реализовано в операционной системе ППК. Примерами описанной технологии являются контроллеры Tricon и Trident от Triconex, Hima.

Программная реализация поддержки резервирования

Если к скорости переключения с основной системы на резервную не предъявляются высокие требования, то наиболее целесообразно использовать специальное программное обеспечение, позволяющее создавать относительно недорогую резервированную систему. Поддержка функций резервирования при этом полностью осуществляется на программном уровне. Синхронизирующая связь реализуется через любой из поддерживаемых контроллером интерфейсов: MPI, PROFIBUS, Ethernet и т. д.

На рис. 4 показаны циклы работы основного и резервного контроллеров.

Чтобы при отключении основного контроллера программа в резервном контроллере не начала выполняться "с нуля", основной контроллер постоянно передает текущие данные в резервный.

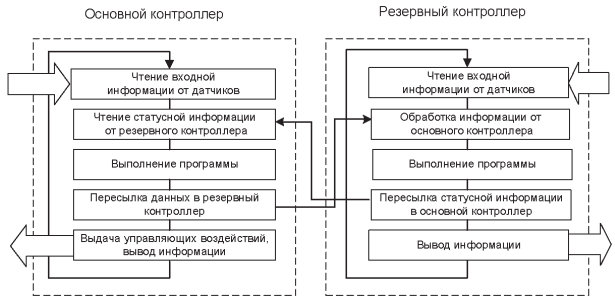

Рис. 4. Циклы программ основного и резервного контроллеров

Однако такая передача в зависимости от выбранного типа коммуникации и передаваемого объема данных может занимать несколько циклов, т.е. модуль центрального процессора резервного ППК может отставать от основного на несколько циклов. Такой тип подготовки к переключению обозначается как теплое резервирование (warm-standby), в отличие от рассмотренного

выше горячего резервирования (hot-standby).

В целом же время переключения с основного контроллера на резервный составляет несколько секунд. Это время зависит от причины сбоя или отказа, а также от следующих факторов:

- коммуникационная нагрузка центрального процессора;
- объем передаваемых данных;
- среда, тип и скорость передачи данных через синхронизирующее соединение.

При таком способе построения резервированной системы контролируются:

- исчезновение напряжения питания центрального процессора;
- аппаратный или программный сбой в работе центрального процессора;
- обрывы в резервированных каналах связи;
- обрывы синхронизирующей связи между центральными процессорами основной и резервной систем.

Примером реализации рассмотренного метода является система Software Redundancy от Siemens [7,8].

Резервирование в системах противоаварийной защиты

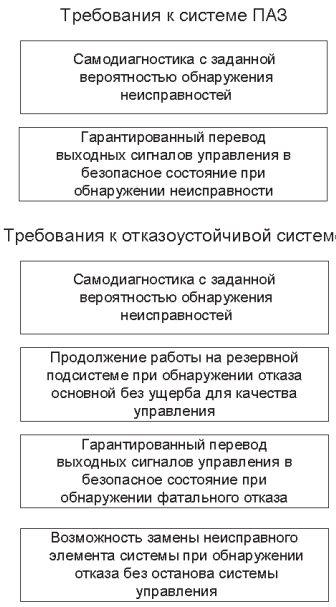

Рис. 5. Требования к системе безопасности и отказоустойчивой системе

Современные производственные процессы имеют сложную техническую структуру, связаны со значительным использованием энергетических ресурсов и в случае аварии могут причинить серьезный ущерб людям и имуществу. Поэтому отдельно следует выделить применение схем резервирования в системах противоаварийной защиты (ПАЗ).

Как показано на рис. 5, к системе ПАЗ предъявляется гораздо меньше требований, чем к отказоустойчивой системе. Поэтому для построения таких систем применение "больших" контроллеров не всегда является экономически оправданным. Для этого случая некоторые производители предлагают специальные устройства - контроллеры противоаварийной защиты (например, Yokogawa, Triconex). Согласно приведенной выше классификации контроллеры ПАЗ следует отнести к классу "малых" (как правило, они поддерживают не более 200 входов), но они содержат встроенные средства поддержки резервирования и в случае возникновения аварии гарантируют перевод системы в безопасное состояние.

Достоинства и недостатки резервирования. Выбор способа резервирования

Главное очевидное достоинство применения резервирования - это повышение надежности и отказоустойчивости системы.

Недостатки применения резервирования следующие:

- увеличение стоимости системы;
- усложнение структуры системы;
- увеличение цикла сканирования модуля центрального процессора вследствие переноса данных из основного в резервный на каждом такте работы;
- уменьшение допустимого размера программы, т. к. часть памяти должна быть отведена под обеспечение поддержки механизмов резервирования.

Обоснование необходимости и выбор способа резервирования производятся на этапе проектирования

системы. На данном этапе возможны два похода - это обеспечение требуемой надежности при минимальной стоимости и обеспечение максимальной надежности при ограниченной стоимости.

При проектировании АСУТП, как правило, используется первый подход, поскольку современные системы управляют опасными производствами и производствами с непрерывными технологическими процессами, где выполнение требований к надежности имеет приоритет, поскольку отказ может привести к значительным материальным потерям либо возникновению аварийной ситуации.

Способ резервирования должен выбираться прежде всего в зависимости от свойств технологического процесса. Если процесс достаточно медленный (управление нагревом/охлаждением, регулирование уровня воды и т. п.), то наиболее оптимальным вариантом является использование программной реализации резервирования. Если же процесс исключает малейшие простои, то следует использовать аппаратную реализацию поддержки резервирования.

Заключение

Проведенный анализ показал, что программируемые логические контроллеры предоставляют достаточно широкие возможности для построения отказоустойчивых систем. При этом очень важно сделать правильный выбор класса контроллеров и способа резервирования еще на этапе проектирования, что является возможным лишь при достаточно точной количественной оценке надежности системы. Поэтому одним из дальнейших направлений является разработка методов оценки надежности, учитывающей особенности систем, построенных на ПЛК.

Литература

1. Modicon Quantum Hot Standby with Unity. User Manual.
2. SIMATIC. Система автоматизации S7-400 H. Отказоустойчивые системы. Руководство.
3. GE Fanuc Automation. Programmable Control Products. Genius Modular Redundancy. User's Manual.
4. Захаров Н.А. Средства промышленной автоматики GE Fanuc и системы на их основе. - М.: СИНТЕГ, 2004. - 108 с.
5. Mike Scott, Bud Adler. How to Select a Safety PLC. http://www.isa.org/Content/Microsites838/Safety_Division/Home818/ISA_2004_Safety_Papers/How_to_Select_a_Safety_PLC.pdf
6. Ицкович Э.П. Классификация современных контроллеров и их сетевых комплексов. // Оборудование. - 2004. - № 7.
7. Программное резервирование для SIMATIC S7-300 и S7-400. http://www.automation-rives.ru/as/download/doc/software/runtime/SWR_RUS.pdf
8. Программное обеспечение для программной реализации дублирования SW Redundancy // Интерактивный каталог продуктов Siemens A&D (http://www.ca01.ru)