УДК 004.052

Е.В. БАБЕШКО

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

АНАЛИЗ ВОЗМОЖНОСТЕЙ СОВРЕМЕННЫХ ПРОМЫШЛЕННЫХ КОНТРОЛЛЕРОВ ДЛЯ РАЗРАБОТКИ ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ

Проанализированы существующие варианты построения отказоустойчивых систем с применением промышленных контроллеров различных производителей. Предложены критерии сравнения таких систем.

промышленный контроллер, резервирование, отказоустойчивая система

Введение

В настоящее время одним из главных требований, которые предъявляются к автоматизированным системам, является их надежность [1].

Целью использования отказоустойчивых автоматизированных систем является сокращение производственных потерь. Чем выше расходы, связанные с остановом производства, тем более целесообразно использование отказоустойчивой системы.

Применение различных схем резервирования промышленных контроллеров позволяет значительно повысить надежность и отказоустойчивость систем. Практически все производители контроллеров предлагают готовые решения для повышения надежности системы, добавляя поддержку резервирования в изготовляемые контроллеры. При этом на практике применяются самые разнообразные схемы и варианты построения резервированных систем. Соответственно, существенно отличается и эффективность, достигаемая за счет применения резервирования.

Существующие варианты резервированных систем, построенных на промышленных контроллерах различных производителей, описаны в технической документации [2 – 5] и упоминаются в ряде публикаций [6 – 9]. Однако в указанных источниках отсутствует сравнение решений различных производителей.

Целью данной статьи является анализ и сравнение схем резервирования, которые предлагаются ведущими современными производителями промышленных контроллеров.

Наиболее популярными вариантами построения резервированных систем являются решения с программной либо аппаратной поддержкой резервирования. При этом реализуются, как правило, дублированные или мажоритарно-резервированные структуры.

Программная поддержка резервирования

В большом количестве приложений требования к кратности резервирования невелики, чтобы минимизировать затраты, связанные с использованием специальной отказоустойчивой системы. Часто достаточно простых программных механизмов, чтобы в случае ошибки сделать возможным продолжение выполнения задачи управления на заменяющей системе.

Основное достоинство данного варианта – малая стоимость реализации.

Главным же недостатком является довольно большое время переключения на резервный

контроллер (порядка 6 – 10 с), что ограничивает применение данного метода в системах с быстротекущими технологическими процессами.

Аппаратная поддержка резервирования

Другим популярным решением является применение дополнительных модулей. Специальные модули горячего резерва устанавливаются на шасси основной и резервной системы, соединяются между собой волоконно-оптической линией связи. Каждый модуль производит мониторинг состояния соответствующего контроллера, и в начале каждого сканирования текущие значения регистров и таблица состояния ввода-вывода основного контроллера передаются на резервный. Если основной контроллер отказывает, модуль горячего резерва переключает управление на резервный. Время переключения при таком варианте построения системы не превышает 50 мс.

Как правило, резервный контроллер содержит программу, идентичную программе основного (решения Siemens и Schneider Electric). Однако программа резервного контроллера может не совпадать с программой основного (решение GE Fanuc). В этом случае при отказе основного контроллера резервный обеспечивает выполнение наиболее важных для технологического объекта управления функций, другие функции управления выполняются при помощи локальных регуляторов или вручную.

Основные варианты аппаратного резервирования следующие:

1) горячий резерв отдельных компонентов или контроллера в целом (при отказе основного контроллера управление переходит к резервному);

2) троирование основных компонентов и/или контроллера в целом с голосованием по результатам обработки сигналов всеми контроллерами, составляющими группу (выходным сигналом является тот, который выдан большинством контроллеров группы, а контроллер, рассчитавший иной результат, объявляется неисправным).

На рис. 1 изображена схема реализации первого варианта с двумя резервными контроллерами.

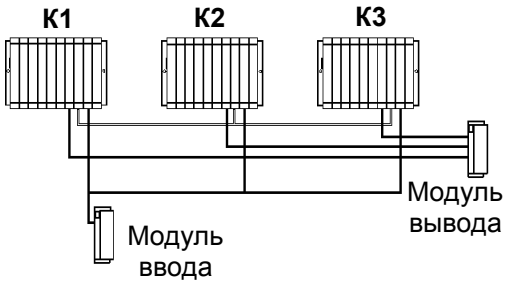

Рис. 1. Тройное горячее резервирование

В случае отказа любых двух контроллеров система продолжает работать как нерезервированная система. В случае отказа третьего контроллера система переходит в нерабочее состояние.

На рис. 2 изображен другой вариант построения системы. Этот вариант имеет значительное преимущество, так как позволяет нейтрализовать не только явные отказы (останов ЦПУ, ошибка ОЗУ и т. п.), но и неявные (когда все контроллеры работают, но при этом выдают различный результат).

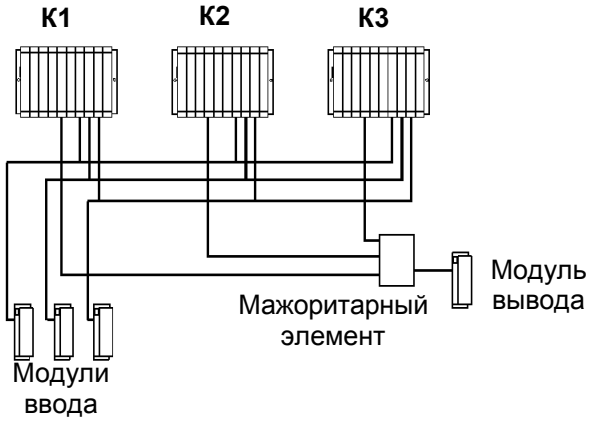

Рис. 2. Троирование компонентов с голосованием

Решение о том, какой из результатов является правильным, принимает мажоритарный элемент «2 из 3».

При построении отказоустойчивой системы особое внимание следует уделять резервированию

модулей центрального процессора. Остальные компоненты системы (например, модули ввода/вывода) также можно резервировать для повышения надежности системы, однако среднее время безотказной работы этих модулей значительно выше, чем MTBF модулей центрального процессора.

Критерии сравнения и результаты анализа отказоустойчивых систем

В качестве меры надежности часто называют среднее время безотказной работы MTBF (Mean Time Between Failures). Данные о MTBF предоставляется большинством производителей промышленных контроллеров и периодически обновляются (например, [10]). Другим важным параметром является средняя длительность отказа MDT (Mean Down Time), т.е., в сущности, время восстановления работоспособности системы MTTR (Mean Time to Repair). MTTR состоит из времени обнаружения ошибки и времени, необходимого для ремонта или замены неисправных модулей. Как правило, MTTR принимают равным 90 мин.

Для системы можно рассчитать вероятность ее безотказной работы. Эта вероятность равна произведению вероятностей безотказной работы всех компонентов системы. Вероятность безотказной работы любого компонента рассчитывается на основании его MTBF.

Рассчитаем вероятность безотказной работы системы, изображенной на рис. 1, для периода в 3 года, приняв MTBF контроллера равным 100000 ч., MTBF модулей ввода и модулей вывода – 500000 ч.

$$P_{сист1} = [1-(1-P_1)(1-P_2)(1-P_3)]P_{in}P_{out},$$

где P_i – вероятность безотказной работы контроллера K_i, $i = 1 \div 3$;

P_{in}, P_{out} – вероятности безотказной работы модулей ввода и вывода соответственно;

Так как контроллеры равнонадежные, то:

$$P_{сист1} = [1-(1-P_1)^3]P_{in}P_{out} = 0{,}89.$$

Рассчитаем вероятность безотказной работы системы, изображенной на рис. 2, приняв MTBF мажоритарного элемента равным 500000 ч.

$$P_{сист2} = (3P_K{}^2 - 2P_K{}^3)P_{МЭ}(3P_{in}{}^2 - 2P_{in}{}^3)P_{out} = 0{,}76.$$

Результаты расчетов показывают, что вероятность безотказной работы первой системы больше. Однако это совсем не означает, что на практике первая система всегда сможет проработать большее время до возникновения отказа. Дело в том, что характеристика MTBF, на основании которой рассчитывается вероятность безотказной работы, не может достаточно точно определить основные характеристики надежности промышленных контроллеров. Это обусловлено тем, что отказы в работе компонентов промышленных контроллеров весьма редки, поскольку современные вычислительные элементы и платы обладают высокой надежностью. Поэтому провести достаточно чистый эксперимент, чтобы набрать необходимую статистику для расчета числа часов наработки на отказ, хотя бы по средней по объему выборке, производители обычно не могут; тем более что сами вычислительные элементы модифицируется быстрее, чем мог бы закончиться указанный эксперимент.

По этой причине характеристики надежности иногда оценивают следующими косвенными показателями и возможностями промышленных контроллеров:

1) полнота имеющихся тестов самодиагностики для определения неисправностей в отдельных компонентах контроллеров;

2) возможности и варианты резервирования всех компонентов контроллеров;

3) наличие встроенных в систему блоков бесперебойного питания (UPS) и время их работы при прекращении питания системы от сети, а также возможность и длительность перерыва питания без нарушения функций управления.

В табл. 1 приведено сравнение существующих технологий ведущих производителей промышленных контроллеров.

Таблица 1

Сравнение основных параметров промышленных контроллеров, поддерживающих резервирование

Производитель		Siemens	Schneider Electric	GE Fanuc
Серия		Simatic S7-400	TSX Quantum	Series 90-70
Критерии	Типовое время переключения с основного контроллера на резервный	30 мс	13 – 48 мс	25 мс
	MTBF	130 тыс. часов	100 тыс. часов	80 тыс. часов
	Возможность резервирования отдельных компонентов системы	есть	есть	есть
	Поддержка встроенных UPS	есть	есть	есть
	Программная поддержка	есть	нет	нет
	Аппаратная поддержка (дублирование)	есть	есть	есть
	Аппаратная поддержка (троирование)	есть	нет	есть

Заключение

Проведенный анализ вариантов построения систем показал, что промышленные контроллеры предоставляют широкие возможности для создания отказоустойчивых систем.

Однако для некоторых критических приложений обеспечиваемый стандартными средствами уровень надежности не всегда является достаточным. В этом случае необходимо применить один из методов повышения надежности. При этом следует учитывать, что по MTBF нельзя в полной мере адекватно оценить надежность системы, и исходить из того, что отказ в системе может произойти в любой момент времени.

Дальнейшим направлением исследования является создание решений, позволяющих повысить отказоустойчивость систем в случае недостаточного уровня надежности, достигаемого при использовании стандартных вариантов.

Литература

1. Скворцов М.С. Применение ПК АСМ для обоснования надежности АСУ ТП на стадии проектирования. – [Электрон. ресурс]. – Режим доступа: http://www.szma.ru/art5.shtml.

2. Siemens SIMATIC S7-400H. Отказоустойчивые системы. Руководство.

3. GE Fanuc Automation. Series 90-70. Hot Standby CPU Redundancy. User's Guide.

4. Modicon Quantum CHS 110 Hot Standby System. Planning and Installation Guide.

5. Genius™ Modular Redundancy Flexible Triple Modular Redundant System. Technical Product Overview.

6. Захаров Н.А. Программные и технические средства GE Fanuc // Автоматизация в промышленности. – 2003. – № 3. – С. 23-24.

7. В.С. Громов, В.Н. Тимофеев. Структуры резервирования в АСУ ТП // Мир компьютерной автоматизации. – 2003. – № 1.

8. Ремизевич Т.В. Современные программируемые логические контроллеры // Приводная техника. – 1999. – № 3-4. – С. 6-17.

9. SIMATIC S7-400H – Резервированные системы автоматизации. – [Электрон. ресурс]. – Режим доступа: http://www.aldis.ru/siemens/products/controllers/s7-400H.shtml.

10. Mean Time Between Failures (MTBF) - list for SIMATIC products. – [Электрон. ресурс]. – Режим доступа: http://support.automation.siemens.com/WW/view/en/16818490.

Поступила 1.03.2006

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.