УДК 621.3.019.3

Ар.А. МУХА[*], А.В. ФЕДУХИН[*]

РЕЗЕРВИРОВАННЫЕ МИКРОКОНТРОЛЛЕРЫ И СИСТЕМЫ НА ИХ ОСНОВЕ

[*]Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *Стаття присвячена питанням інжинірингу відмовостійких мікроконтролерів і мікроконтролерних систем. Мета досліджень – це розробка концептуальних підходів до реалізації типових двохканальних дубльованих вузлів на базі програмованих мікроконтролерів і створення на їх основі відмовостійких систем із конвеєрною обробкою даних, поблоковим резервуванням і здатністю до реконфігурації. За оцінками різних дослідників, простій комп'ютерних систем (КС) обходиться американському бізнесу в мільярди доларів (близько сотні тисяч доларів за годину простою). Ось чому технології, що підвищують надійність роботи КС, так цікаві компаніям, що працюють в області критичних інфраструктур і технологій. У роботі наведено короткий опис технічних засобів, що входять до складу сучасних мікроконтролерів (МК), розглянуті питання підвищення надійності МК шляхом побудови типових дубльованих вузлів. Наводиться зарубіжний досвід створення дубльованих МК і створення на їх основі дубльованих мікроконтролерних систем. Оскільки технічні рішення щодо створення резервованих систем на основі мікроконтролерів зі зрозумілих причин розробники не афішують, то в роботі запропоновано декілька авторських варіантів вирішення завдань щодо дублювання МК, сформульованих у результаті обговорення проблеми в мережі Інтернет. На основі дубльованих вузлів пропонується будувати дубльовані системи з конвеєрною обробкою даних, виконані у вигляді квазімостікової структури (КМС). Якщо така структура є еквівалентною заміною за функціональними можливостями дубльованого вузла, що складається, наприклад, із двох промислових комп'ютерів, то в цьому випадку досягаються додаткові переваги, властиві МК і КМС.*

Ключові слова: *відмовостійкість, дубльовані мікроконтролери, конвеєрна обробка даних, квазімостікова структура.*

Аннотация. *Статья посвящена вопросам инжиниринга отказоустойчивых микроконтроллеров и микроконтроллерных систем. Целью исследований является разработка концептуальных подходов к реализации типовых двухканальных дублированных узлов на базе программируемых микроконтроллеров и созданию на их основе отказоустойчивых систем с конвейерной обработкой данных, поблочным резервированием и способностью к реконфигурации. По оценкам различных исследователей, простой компьютерных систем (КС) обходится американскому бизнесу в миллиарды долларов (порядка сотни тысяч долларов за час простоя). Вот почему технологии, повышающие надежность работы КС, так интересны компаниям, работающим в области критических инфраструктур и технологий. В работе приведено краткое описание технических средств, входящих в состав современных микроконтроллеров (МК), рассмотрены вопросы повышения надежности МК путем построения типовых дублированных узлов. Приводится зарубежный опыт создания дублированных МК и создания на их основе дублированных микроконтроллерных систем. Поскольку технические решения по созданию резервированных систем на основе микроконтроллеров по понятным причинам разработчики не афишируют, то в работе предложено несколько авторских вариантов решения задач по дублированию МК, сформулированных в результате обсуждения проблемы в сети Интернет. На основе дублированных узлов предлагается строить дублированные системы с конвейерной обработкой данных, выполненные в виде квазимостиковой структуры (КМС). Если такая структура является эквивалентной заменой по функциональным возможностям дублированного узла, состоящего, например, из двух промышленных компьютеров, то в этом случае достигаются дополнительные преимущества, свойственные МК и КМС.*

Ключевые слова: *отказоустойчивость, дублированные микроконтроллеры, конвейерная обработка данных, квазимостиковая структура.*

Abstract. *The article is devoted to the engineering of fault-tolerant microcontrollers and microcontroller systems. The purpose of the research is to develop conceptual approaches to the implementation of typical dual-channel duplicated nodes based on programmable microcontrollers and the creation on their basis of fault-tolerant systems with pipelined data processing, block-by-block redundancy and reconfiguration capability. According to estimates of various researchers, the downtime of computer systems (CS) costs American businesses billions of dollars (about hundreds of thousands of dollars per hour of downtime). That is why technologies that increase the reliability of the work of the CS are so interesting to companies operating in the field of critical infrastructures and technologies. The paper provides a brief description of the technical devices that make up modern microcontrollers (MC), addresses the issues of improving the reliability of the MC by building typical duplicate nodes. The foreign experience of creating duplicated microcontrollers and creating duplicate microcontroller systems on their basis is given. Since technical solutions for creating redundant systems based on microcontrollers, for obvious reasons, the developers do not advertise, the paper proposes several authors' solutions to the problems of duplicating MCs, which were formulated as a result of a discussion of the problem on the Internet. Based on duplicate nodes, it is proposed to build duplicate systems with pipelining of data, made in the form of a quasi bridge structure (QBS). If such a structure is an equivalent replacement for the functionality of a duplicate node, consisting, for example, of two industrial computers, in this case, the additional advantages inherent in the MC and QBS are achieved.*
Keywords: *fault tolerance, duplicated microcontrollers, pipeline data processing, quasi bridge structure.*

1. Введение

Старый лозунг почтовой службы Federal Express: «В любом случае почта должна быть доставлена за ночь» применим сегодня и в области IT-технологий [1].

Аналогичные требования предъявляются к современным компьютерным системам (КС), за исключением того, что доставка перерабатываемой ими информации должна гарантированно обеспечиваться не за одну ночь, а непрерывно, вне зависимости от проблем, которые могут возникнуть в конкретных аппаратных или программных компонентах информационной системы. Такая концепция называется отказоустойчивостью.

Отказоустойчивость – свойство архитектуры компьютерной системы (КС), обеспечивающее выполнение заданных функций в случаях, когда в аппаратных и программных средствах системы возникают отказы [2].

По способу реализации отказоустойчивость подразделяется на активную и пассивную.

*Активная отказоустойчивость (*Active *Fault Tolerance)* базируется на отдельно выделенных процессах обнаружения отказа, локализации отказа и реконфигурации системы. Отказы обнаруживаются средствами контроля, локализуются при помощи средств диагностики и устраняются автоматической реконфигурацией системы, которая заключается в перестройке структуры системы таким образом, чтобы ее отказавшие компоненты были устранены от участия в работе.

Пассивная отказоустойчивость (Passive Fault Tolerance) заключается в способности системы не потерять свои функциональные свойства в случае отказа отдельных элементов. В таких случаях говорят, что отказ маскируется системой. Пассивная отказоустойчивость связана с увеличением количества аппаратуры в несколько раз; она применяется обычно тогда, когда недопустимы даже кратковременные перерывы в работе КС, а также для обеспечения отказоустойчивости важнейших блоков или устройств системы.

Применение активной отказоустойчивости характеризуется более экономным расходом аппаратных средств, однако связано с некоторыми потерями времени при восстановлении работы системы после отказа (иногда возможны потери некоторой части данных). Активная отказоустойчивость реализуема только в многопроцессорных системах. В

то же время применение пассивной отказоустойчивости гарантирует практически бесперебойную работу КС и сохранение всей информации. Эти обстоятельства определяют области применения активной и пассивной отказоустойчивости. В настоящее время для различных разновидностей систем, основным свойством которых является отказоустойчивость, выделяют следующие типы.

Системы высокой готовности (High Availability). Предполагается, что конфигурация таких систем обеспечивает ее быстрое восстановление после обнаружения неисправности, для чего в ряде мест используются избыточные аппаратные и программные средства. Длительность задержки, в течение которой программа, отдельный компонент или система простаивает, может находиться в диапазоне от нескольких секунд до нескольких часов, но более часто в диапазоне от 2 до 20 минут.

Системы, эластичные к отказам (Fault Resiliency). Ключевым моментом в определении эластичности к отказам является более короткое время восстановления, которое позволяет системе быстро откатиться «назад» после обнаружения неисправности.

Системы, устойчивые к отказам (Fault Tolerance). Такие отказоустойчивые системы имеют в своем составе избыточную аппаратуру для всех функциональных блоков, включая процессоры, источники питания, подсистемы ввода/вывода и подсистемы дисковой памяти. Если соответствующий функциональный блок неправильно функционирует, всегда имеется «горячий» резерв. Часто избыточные аппаратные средства можно использовать для распараллеливания обычных работ. Время восстановления после обнаружения неисправности для переключения отказавших компонентов на избыточные для таких систем обычно меньше одной секунды.

Системы непрерывной готовности (Continuous Availability). Системы с непрерывной готовностью устраняют любое время простоя как плановое, так и неплановое. Разработка такой системы охватывает как аппаратные средства, так и программное обеспечение, и позволяет проводить модернизацию (upgrade) и обслуживание в режиме on-line. Дополнительным требованием к таким системам является отсутствие деградации в случае отказа. Время восстановления после отказа не превышает одной секунды.

Резервирование как способ обеспечения отказоустойчивости широко используется для достижения безотказной роботы различного вида систем. На сегодняшний день практически все сложные системы аппаратно подкрепляются дублирующими комплектами, а вычисления и процессы обработки сигналов, протекающие в таких системах, становятся все ответственнее.

Наиболее экономичным способом введения избыточности является способ дублирования частей системы, находящихся в нагруженном («горячем») резерве. Примером такой системы является система автоматизации SIMATIC S7–400H от производителя SIEMENS [3].

Для решения поставленной задачи система сконструирована таким образом, что она всегда остается готовой к работе при любых событиях (отказах или сбоях в работе ее функциональных блоков (ФБ)). Такое свойство достигается за счет организации двухканальной структуры с поблочным дублированием и режимом функционирования Non-Stop, обеспечивающим «горячую» замену отказавших ФБ без прекращения функционирования системы.

Целью исследований является разработка концептуальных подходов к реализации типовых двухканальных дублированных узлов на базе программируемых микроконтроллеров и созданию на их основе отказоустойчивых систем с конвейерной обработкой данных, поблочным резервированием и способностью к реконфигурации.

2. Устройство микроконтроллера

Микроконтроллер (МК) – это микросхема, представляющая собой мини-компьютер, предназначенный для выполнения различных функций [4].

Данная микросхема работает в соответствии с заложенной в нее программой, которую создает программист. Самой главной особенностью микроконтроллеров, с точки зрения конструктора-проектировщика, является то, что с их помощью легче и зачастую гораздо дешевле реализовать различные схемы.

Микроконтроллер может в себе содержать различное количество так называемых периферийных модулей, которые определяют его возможности, а также стоимость. К периферии микроконтроллера относятся, например, АЦП (аналого-цифровой преобразователь), различные таймеры, аналоговый компаратор, COM-порт, USB-порт и т.д.

Микроконтроллер может управлять различными устройствами и принимать от них данные при минимуме дополнительных узлов, так как большое число периферийных схем уже имеется непосредственно на кристалле микроконтроллера. Это позволяет уменьшить размеры конструкции и снизить потребление энергии от источника питания.

Для сравнения: при использовании традиционных микропроцессоров приходится все необходимые схемы сопряжения с другими устройствами реализовывать на дополнительных компонентах, что увеличивает массу, размеры и потребление электроэнергии.

<table>
<tr><th colspan="2">Микроконтроллер</th></tr>
<tr><td></td><td rowspan="2">ЦПУ
АЛУ
Таймер</td></tr>
<tr><td>Тактовый генератор</td></tr>
<tr><td>Таймер реального времени</td><td>ПЗУ</td></tr>
<tr><td>Сторожевой таймер</td><td>ОЗУ</td></tr>
<tr><td colspan="2">Цифровой порт ввода-вывода
Аналоговый порт ввода-вывода
Последовательный порт
Цепь сброса</td></tr>
</table>

Рисунок 1 – Составные части микроконтроллера

Как правило, любой микроконтроллер содержит следующие основные узлы (рис. 1):

- центральное процессорное устройство (ЦПУ);
- арифметико-логическое устройство (АЛУ);
- оперативную память (ОЗУ);
- постоянную память (ПЗУ);
- тактовый генератор;
- порты ввода/вывода;
- таймеры.

Сердцем микроконтроллера является центральное процессорное устройство (ЦПУ), состоящее из арифметико-логического устройства (АЛУ) и регистров. ЦПУ принимает из памяти программ коды команд, декодирует их и выполняет.

АЛУ производит все арифметические и логические операции с двоичными данными. Бывают АЛУ различной разрядности: 8, 16 или 32-разрядные. К арифметическим операциям относятся сложение, вычитание, сравнение и т.д. К логическим операциям относятся операция умножения «**И**», сложения «**ИЛИ**», отрицания «**НЕ**», «исключающее **ИЛИ**», сдвиг вправо, сдвиг влево и т.д. Есть также операции, которые не относятся ни к логическим, ни к арифметическим, например, сброс в «0» или установка в «1».

Как было сказано выше, АЛУ производит операции над числами и возвращает результат операции в виде числа. Данные числа помещаются в регистры общего назначения – своеобразную временную память. У каждого микроконтроллера количество регистров может быть разным.

Однако, для нормальной работы микроконтроллера регистров общего назначения недостаточно. Для того чтобы можно было хранить больше информации, используется оперативная память данных – оперативно-запоминающее устройство (ОЗУ). Здесь хранятся переменные программ. У большинства микроконтроллеров здесь расположен также стек. Регистры общего назначения содержат данные, с которыми АЛУ работает в данный момент, а ОЗУ – остальные.

В памяти программ хранятся коды команд, последовательность которых формирует программу для микроконтроллера. Команды, а точнее последовательности команд, которые выполняет АЛУ, хранятся в постоянно-запоминающем устройстве (ПЗУ). Обычно это Flash-память. Данные последовательности команд являются ничем иным, как программой микроконтроллера, которую создает программист. Все команды находятся в ПЗУ по определенным адресам.

Для того чтобы достать какую-то команду из ПЗУ, необходимо обратиться к ее адресу, чем занимается программный счетчик или счетчик команд**.**

Данные из ПЗУ попадают в регистр команд. АЛУ постоянно «смотрит» содержимое регистра команд и если в нем появляется команда, то АЛУ сразу же начинает ее выполнять.

Необходимо также заметить, что вся работа микроконтроллера синхронизируется генератором тактовой частоты**,** который может быть внутренним или внешним.

Тактовый генератор определяет скорость работы микроконтроллера.

Цепь сброса. Эта цепь служит для правильного запуска микроконтроллера.

Все эти устройства микроконтроллера были бы бесполезны без портов ввода-вывода, с помощью которых микроконтроллер взаимодействует с внешним миром. Порты ввода-вывода можно настраивать таким образом, чтобы они работали как в качестве входов, так и в качестве выходов. Управление портами осуществляется через специальные регистры. По умолчанию все порты микроконтроллера настроены на выход.

Последовательный порт – очень полезный элемент микроконтроллера. Он позволяет обмениваться данными с внешними устройствами при малом количестве проводов.

Цифровой порт ввода-вывода – с помощью этого устройства можно одновременно управлять или проверять несколько цифровых линий.

Аналоговый порт ввода-вывода – с помощью этого устройства можно одновременно управлять или проверять несколько аналоговых линий.

Таймер. Используется для отсчета временных интервалов.

Сторожевой таймер – специальный таймер, предназначенный для предотвращения сбоев программы, который работает следующим образом: после запуска он начинает отсчет заданного временного интервала. Если программа не перезапустит его до истечения этого интервала времени, сторожевой таймер перезапустит микроконтроллер. Таким образом, программа должна давать сторожевому таймеру сигнал: все в порядке. Если она этого не сделала, значит, по какой-либо причине произошел сбой.

3. Резервированные промышленные контроллеры System Q

Новые промышленные контроллеры System Q производства компании Mitsubishi Electric обладают исключительно высоким быстродействием, выполняют широкий набор функций и позволяют создать резервированные системы, повышающие общую надежность АСУ ТП [5].

Программируемый логический контроллер (ПЛК или PLC) – устройство, используемое для автоматизации технологических процессов. В отличие от встраиваемых микропроцессоров и систем на их основе ПЛК изготавливается как самостоятельное изделие отдельно от управляемого с его помощью оборудования. В системах управления технологическими процессами ПЛК взаимодействуют с различными компонентами систем человеко-машинного интерфейса (например, панелями оператора) или рабочими местами операторов на базе персонального компьютера. Датчики и исполнительные устройства подключаются непосредственно к самому ПЛК или к дополнительным модулям входов/выходов.

От систем управления критическими объектами в первую очередь требуется высокая надежность аппаратной части и выполнения алгоритмов, а также возможность резервирования элементов системы.

Чтобы повысить надежность систем на уровне контроллеров и таким образом исключить остановку критического технологического процесса при выходе из строя некоторых элементов системы, применяют резервированные конфигурации промышленных контроллеров, в частности, с дублированием основных элементов промышленного контроллера.

При этом выход из строя одной из цепей питания или одного из процессорных модулей не приводит к сбою в технологическом процессе. Резервируются также линии связи с верхним уровнем системы управления, а также некоторые или все каналы ввода-вывода.

Корпорация Mitsubishi Electric входит в тройку крупнейших мировых производителей оборудования для промышленной автоматизации и предлагает широкую линейку мощных промышленных контроллеров, отличающихся исключительно высокой надежностью и дающих возможность строить системы с аппаратным резервированием.

Рисунок 2 – Промышленные контроллеры System Q

Промышленные контроллеры System Q (рис. 2) – это программируемые логические контроллеры (ПЛК), обладающие исключительно высоким быстродействием и широким набором функций. Среди характерных особенностей этой серии является компактность аппаратной части, возможность построения многопроцессорных систем, в том числе с аппаратным резервированием.

Контроллеры System Q поддерживают многопроцессорный режим обработки данных, что подразумевает параллельное использование в одном ПЛК до четырех процессорных модулей одного или нескольких типов.

Наличие нескольких процессорных модулей в одном промышленном контроллере позволяет увеличить производительность системы и обеспечить ее высокое быстродействие за счет деления сложных алгоритмов между несколькими специализированными процессорными модулями, повысить ее надежность за счет распределенного алгоритма обработки данных, а также в ряде случаев снизить стоимость системы за счет использования одного многопроцессорного промышленного контроллера вместо нескольких однопроцессорных компьютеров, объединенных по сети.

Для повышения надежности системы при управлении критичными процессами предусмотрено аппаратное резервирование промышленного контроллера по процессорному модулю, источнику питания и сетевым соединениям. Архитектура резервированных контроллеров подразумевает наличие двух промышленных контроллеров идентичной конфигурации, один из которых задействован в обработке алгоритма, а второй находится в «горячем» резерве. При этом одна или несколько станций ввода-вывода, подключенных по

сети MELSECNET/H (рис. 3), являются общими для этих промышленных контроллеров и обладают дублированными источниками питания.

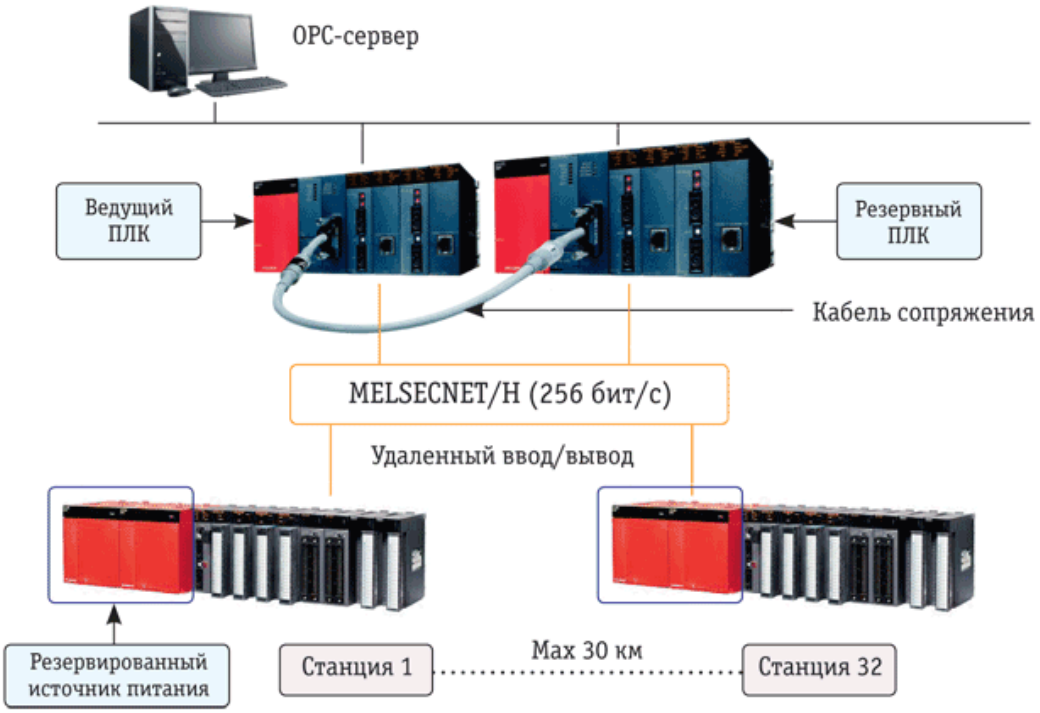

Рисунок 3 – Построение резервированной системы на базе промышленных контроллеров System *Q*

Ключевой особенностью резервированных систем является необходимость сохранять в регистрах резервного промышленного контроллера те же данные, что и в регистрах промышленного контроллера, обрабатывающего алгоритм. Это обеспечивает «мягкий» переход на резервный контроллер в случае отказа основного: в резервном контроллере поддерживаются те же установки, алгоритм и все текущие значения величин, что и в ведущем ПЛК. Данные функции обеспечиваются посредством специального кабеля, связывающего процессорные модули. При внезапном выходе из строя линии питания либо какого-то компонента ведущего контроллера резервный промышленный контроллер подхватывает управление, обладая всеми актуальными для текущего момента значениями регистров. При этом переход управления от ведущей системы к резервной занимает всего 21 мс.

Одной из сложных задач, с которыми сталкиваются программисты при работе с резервированными промышленными контроллерами, является организация обмена данными с сервером верхнего уровня (например, со SCADA-системой) как коммуникационного модуля Ethernet основного контроллера, так и аналогичного модуля резервного промышленного контроллера. Поскольку модули, как правило, включены в одну и ту же сеть Ethernet, они обязаны иметь различные IP-адреса, что осложняет программирование SCADA-системы. OPC-сервер, поставляемый Mitsubishi Electric, располагает специальной функцией для работы с резервированными системами, что позволяет программировать SCADA так, как если бы она работала с обычным одиночным промышленным контроллером.

Для программирования резервированных промышленных контроллеров используется исключительно удобная среда разработки GX IEC Developer или ПО GX Works, поддерживающая все 5 языков программирования ПЛК согласно МЭК 61131.3 и применимая для всего модельного ряда контроллеров Mitsubishi. В случае, если резервированная система служит для обработки большого числа аналоговых контуров регулирования, эффективно применять утилиту PX Developer.

К настоящему времени в странах СНГ на основе резервированных контроллеров производства Mitsubishi Electric реализован ряд проектов на предприятиях энергетики, нефтеперерабатывающей промышленности и нефтехимии. АСУ ТП, созданные на базе резервированных промышленных контроллеров System Q, обеспечили надежное решение всех поставленных задач.

4. Основные подходы к резервированию МК

Поскольку технические решения по созданию резервированных систем на основе микроконтроллеров не публикуются в открытой печати, то было решено привести несколько вариантов решения этой технической задачи, сформулированных разными участниками форумов на специализированных интернет-ресурсах, например, https://electronix.ru/forum/.

При создании резервированных компьютерных систем в первую очередь необходимо определить критерии отказов системы, а именно ситуации выхода из строя основного и резервного микроконтроллеров (МК). Если этого не сделать, то возможны случаи, при которых вероятна неправильная обработка входных сигналов при любом из принятых технических решений. При этом должны быть сформулированы некоторые допущения относительно составных частей и системы в целом. Например, допущение, при котором выход из строя одновременно двух МК невозможен или такой вариант не рассматривается как маловероятный и т.д.

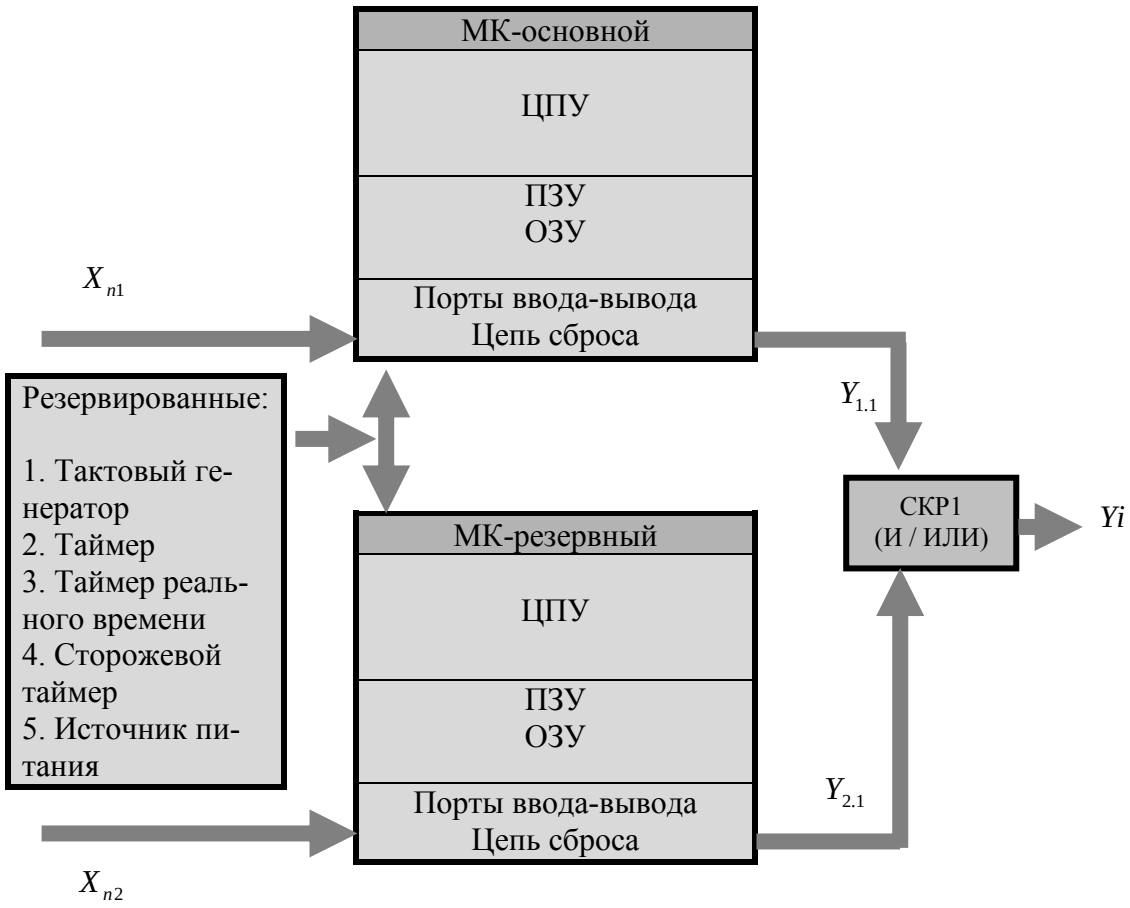

Рисунок 4 – Дублированный узел на МК

Вариант 1. В Программе основного МК устанавливается программный блок, который (так же, как и основная Программа) будет исполняться в цикле, но не будет мешать основной Программе. В начале цикла генерируется некая последовательность импульсов, которую нужно передавать на другой МК (резервный) (рис. 4).

Резервный МК принимает ее, сравнивает с оригиналом и генерирует ответ (другую последовательность), который передается на основной МК, и далее по кругу. Такую систему даже не нужно синхронизировать: какой МК первым поймал сигнал, тот и становится ведущим.

Если сигнал не поступил или не был опознан, резервный МК переключает управление на себя. Если сигнал не опознан и резервный МК перевел управление на себя, то он может провести некие реанимирующие действия, например, перезагрузку другого МК.

Можно подавать сигнал состояния на резервный МК с использованием таймера, но если резервный МК в какой-то момент не получит этот сигнал, то он должен начать выполнение Программы с точки останова основного МК.

Вариант 2. Допустим, два МК одновременно отрабатывают одну и ту же Программу, выходы основного МК подключены к исполнительным устройствам (ИУ), а выходы резервного – к GND через имитацию нагрузки. Каждый из них передает другому постоянный сигнал, и каждый из них одновременно принимает сигнал другого.

Если сигнал пропал, то тот МК, который не нашел сигнал, сначала определяет, какой он – основной или резервный. Например, если на всех его входах будет логический «0», значит, он резервный и переключает управление ИУ на себя. Если другой МК после самотестирования и пуска восстановит работоспособность, то он становится резервным.

Так как МК синхронизированы и выполняют Программу одновременно, то после зависания необходимо синхронизировать параметры управления. У одного МК Программа будет актуальная, а у того, который восстановился после сбоя, просроченная. В этом случае необходимо решить вопрос, что делать с восстановленным МК: маскировать и вывести его из системы или осуществить мероприятия по автоматическому введению в работу системы.

Резервный МК после перевода управления на себя в конце каждого цикла формирует сигнал reset основному МК и, если он восстановит работоспособность, то начало циклов обоих МК будут синхронизированными или будет некоторая разница во времени, которую несложно откорректировать программно.

Вариант 3. Пусть имеются два МК: условно основной и резервный. После старта и прохождения самоконтроля инициализируется основной МК и, если он исправен, то берет управление на себя, исполняет Программу, выполняет собственную диагностику и передаёт её в резервный МК. Резервный МК после старта и прохождения самоконтроля инициализируется и, если он исправен, начинает выполнять такую же Программу, как и основной, но не управляет объектом, а отслеживает диагностику основного МК. Соответственно, если диагностика не была принята, то резервный МК становится основным МК, это означает, что основной МК завис и его нужно «сбросить».

Выбор между основным и резервным МК по первому старту можно сделать, например, с помощью элемента задержки или аппаратно. С помощью перемычки на «ножках» установить – это основной МК или резервный. Если МК заработал после «сброса», то нужно проконтролировать, есть ли диагностика. Если есть, то МК идентифицируется как резервный, если нет, то основной. Синхронизация двух МК получится за два цикла основной Программы.

Основной МК в начале каждого цикла посылает резервному МК команду на обновление цикла. В этом случае резервный МК будет синхронизироваться с основным постоянно, а не только при включении. В аварийной ситуации они просто меняются ролями. В любом случае резервный МК должен отрабатывать одну и ту же Программу и постоянно

синхронизироваться. Синхронизация будет происходить во время приема диагностики, поэтому еще один сигнал можно не подавать.

Примечание.

1. Для упрощения синхронизации в работе МК все типы таймеров, тактовый генератор и цепи сброса резервированы и работают на оба МК одновременно.
2. Для обеспечения высокого уровня готовности дублированные МК питаются от резервированного источника питания, обеспечивающего возможность «горячей» замены отказавшего комплекта.

Восстанавливающим органом дублированной структуры является схема контроля и реконфигурации (СКР) с функцией «**И/ИЛИ**», осуществляющая контроль за синхронной работой МК и реконфигурацию дублированной системы при возникновении отказов ее составных частей в одноканальную.

5. К вопросу о собственной безотказности МК

В общем случае дублирование – один из методов увеличения срока службы системы на МК, иначе – только технология изготовления чипа, и производственная сертификация (сортировка) под определенный стандарт чипа может указывать на его прогнозную долговечность.

Чипы бывают общего назначения (General purpose), промышленного назначения (Industrial purpose), военного назначения (Military purpose) и т.п. Все они имеют совершенно разный уровень приемки и разный уровень надежности.

Что касается собственной долговечности МК, то в документации можно найти следующие характеристики:

- Write/Erase Cycles: 10,000 Flash/100,000 EEPROM;
- Data retention: 20 years at 85°C/100 years at 25°C.

То есть, производитель дает гарантию на ресурс памяти и срок удержания программы (срок удержания данных во FLASH без внешнего питания). Но даже если взять срок в 10 лет, то вполне возможно, что за этот срок устройство либо устареет, будет заменено, обновлено, либо может выйти из строя.

Чем ближе условия эксплуатации МК к их установленным средним значениям (питание, температура, нагрузка), тем дольше он проработает. Существуют также методы увеличения надежности за счет введения поэлементной избыточности проведения самодиагностики. Например, во FLASH можно осуществить две прошивки МК, каждая из которых будет проверяться перед стартом (допустим, на чек-сумму) и запускаться только в случае ее соответствия. В итоге мы получим более надежную систему и даже в случае единичной ошибки во FLASH можно будет запускаться с резервной копии.

6. Резервированная система конвейерного типа на МК

На основе дублированных узлов (рис. 4) можно строить дублированные системы с конвейерной обработкой данных (результаты обработки данных предыдущего МК являются входными данными для последующего МК), выполненные в виде квазимостиковой структуры (КМС) (рис. 5) [6].

Если такая структура является эквивалентной заменой по функциональным возможностям дублированного узла, состоящего, например, из промышленных компьютеров, то в этом случае получим дополнительные преимущества, свойственные КМС.

Структурная схема системы с конвейерной обработкой данных содержит следующие составные части:

- МК1.1, МК2.1, МК3.1 – микроконтроллеры первого канала системы;
- МК1.2, МК2.2, МК3.2 – микроконтроллеры второго канала системы;

• СКР1, СКР2, СКР3 – схемы контроля и реконфигурации.

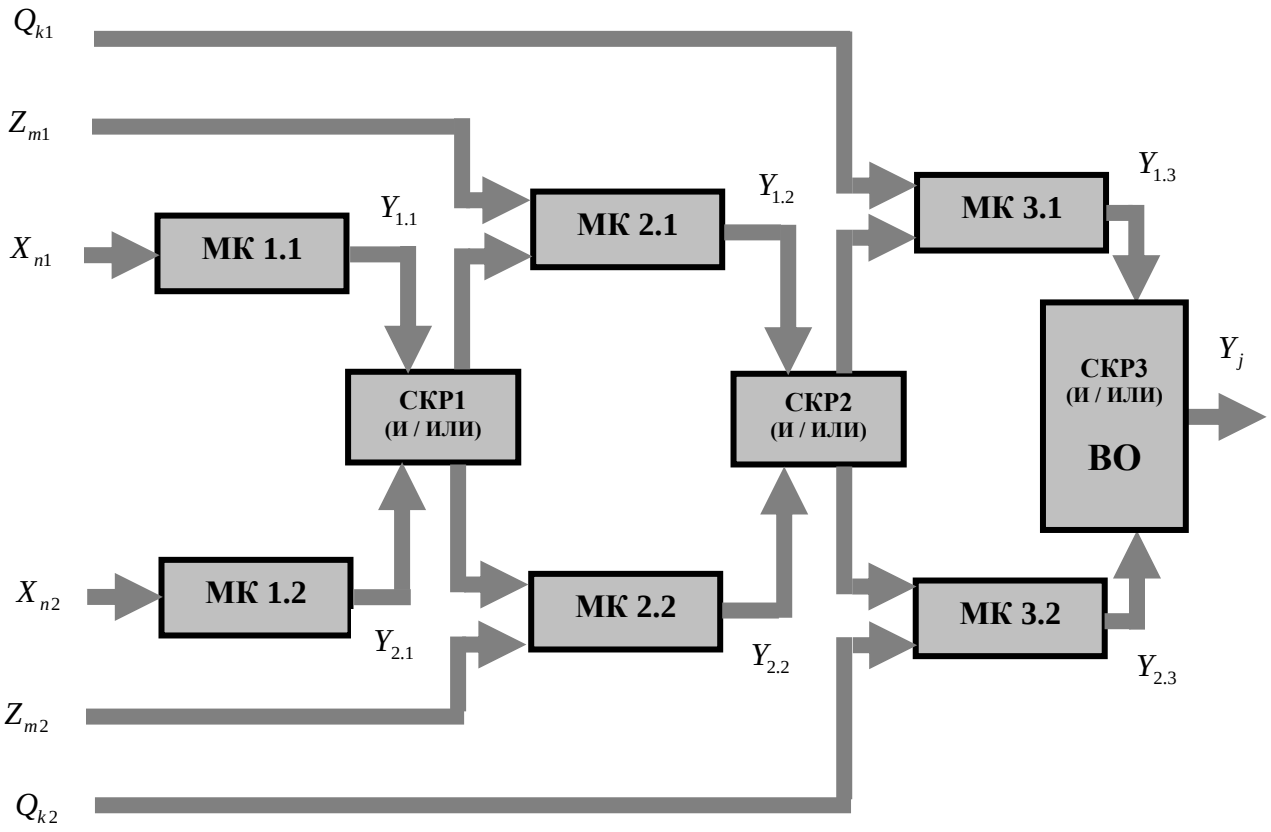

Рисунок 5 – Трехузловая конвейерная система на МК

Система является устойчивой к отказам и сбоям оборудования с управляющей функцией Y_j и обеспечивает исключение возникновения критических ситуаций на управляемом объекте. Такое свойство достигается за счет организации ядра системы в виде двухканальной структуры с поблочным дублированием, перекрестными связями, восстанавливающим органом с функцией «**И/ИЛИ**» и способностью к реконфигурации структуры системы при возникновении отказов ее составных частей с помощью специальных логических схем контроля и реконфигурации (СКР) [7].

Электронное ядро большой системы (например, промышленный компьютер или рабочая станция) разбивается на три функционально обособленных субблока, выполненных на МК (МК1, МК2 и МК3). Каждый МК функционально обособлен и выполняет заданную функцию или несколько функций в конечном (завершенном) виде. Поскольку МК обоих каналов идентичны, то автоматически выполняется условие равнонадежности узлов, свойственное КМС, при котором данная структура имеет наивысшую вероятность безотказной работы [7, 8].

В нормальном режиме СКР имеют логическую функцию «**И**» (осуществляется непрерывный контроль синхронности работы каналов). В случае отказа одного из МК (появление сигнала от аппаратных и/или программных средств внутреннего контроля) СКР изменяет свою логическую функцию на «**ИЛИ**» и осуществляет беспрепятственное прохождение информации с выхода исправного МК узла к следующему узлу, распараллеливая ее на два канала. В таком состоянии система находится до момента восстановления работоспособности отказавшего МК либо в автоматическом режиме (за счет самодиагностики и самовосстановления), либо в результате осуществления «горячей» замены со стороны оператора.

7. Заключение

Поскольку технические решения по созданию резервированных систем на основе микроконтроллеров разработчики по понятным причинам не афишируют, то в работе предложены несколько авторских вариантов решения задач по созданию дублированных узлов на МК.

На основе дублированных узлов предлагается строить дублированные системы с конвейерной обработкой данных, выполненные в виде квазимостиковой структуры (КМС). Для достижения отказоустойчивости системы в целом обеспечивается функциональная автономность и независимость каждого МК от других компонентов системы, чтобы при выходе из строя любого элемента внутри МК последний не оказывал негативного влияния на работу других МК и всей системы в целом. Конкретный выбор компонентов для дублирования (МК) осуществляется проектировщиком с учетом конкретной аппаратной реализации системы.

Структура такой системы остается работоспособной при выходе из строя любого из шести МК обоих каналов. Только одновременный выход из строя одноименных МК сразу в двух каналах системы приводит к ее отказу (потере работоспособности). Наличие встроенных функций прогнозирования технического состояния системы, оперативного контроля исправности МК, своевременной сигнализации об отказе оборудования и самовосстановления (например, за счет встроенной избыточности на элементном уровне) делают вероятность появления такой кратной неисправности маловероятной.

Если конвейерная система на основе МКС является эквивалентной заменой по функциональным возможностям дублированному узлу, состоящему, например, из двух промышленных компьютеров, то в этом случае достигаются дополнительные преимущества, свойственные совместному применению МК и КМС.

СПИСОК ИСТОЧНИКОВ

1. Отказоустойчивые системы. URL: http://www.osp.ru/cw/2000/47/8534/.
2. Отказоустойчивые вычислительные системы. URL: http://lektsii.org/1-26641.html.
3. Fault-TolerantPLC. URL: http:// automation-drives.ru/as/.../doc/.../01_Fault-TolerantPLC_r.pdf.
4. Устройство микроконтроллера. URL: http://www.hamlab.net/mcu/training/introduction.html.
5. Вечканова О.А. Резервированные промышленные контроллеры System Q: Mitsubishi Electric Europe B.V. URL: http://isup.ru/articles/4/5225/.
6. Федухин А.В., Муха Ар.А. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией. *Математичні машини і системи*. 2010. № 4. С. 156–159.
7. Федухин А.В., Пасько В.П., Муха Ар.А. К вопросу моделирования надежности восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей. *Математичні машини і системи*. 2016. № 1. С. 158–167.
8. Федухин А.В., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о надежности невосстанавливаемой системы с квазимостиковой структурой элементов. *Математичні машини і системи*. 2017. № 4. С. 160–168.

Стаття надійшла до редакції 22.01.2019