УДК 621.3.019.3

А.В. ФЕДУХИН*

СИНТЕЗ СИСТЕМ ПРОТИВОАВАРИЙНОЙ АВТОМАТИКИ С ИСКЛЮЧЕНИЕМ ОПАСНЫХ ОТКАЗОВ

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

Анотація. *Стаття присвячена подальшим дослідженням безпеки систем протиаварійної автоматики ГЕС. Розглянуто питання структурного синтезу відмовостійкого ядра системи, наведені приклади безпечних пристроїв сполучення, розроблені методи синтезу безпечних схем комутації керованих об'єктів із виключенням небезпечних відмов.*
Ключові слова: *структурний синтез, безпечні пристрої сполучення, синтез схем комутації.*

Аннотация. *Статья посвящена дальнейшим исследованиям безопасности систем противоаварийной автоматики ГЭС. Рассмотрены вопросы структурного синтеза отказоустойчивого ядра системы, приведены примеры безопасных устройств сопряжения, разработаны методы синтеза безопасных схем коммутации управляемых объектов с исключением опасных отказов.*
Ключевые слова: *структурный синтез, безопасные устройства сопряжения, синтез схем коммутации.*

Abstract. *The article is devoted to further studies of the safety of emergency control systems of hydroelectric power plants. The questions of structural synthesis of the fault-tolerant core of the system are considered, examples of safe interface devices are given, methods are developed for synthesizing safe schemes for switching controlled objects with the exception of dangerous failures.*
Keywords: *Structural synthesis, safe interface devices, synthesis of switching schemes.*

1. Введение

В [1] проведена ревизия безопасности плотинных гидроэлектростанций (ГЭС) с позиций реализации требований по отказоустойчивости и живучести компьютерных систем противоаварийной автоматики (СПА) по результатам аварии на Саяно-Шушенской ГЭС. В работе выполнена классификация причин аварии, разработаны рекомендации по повышению уровня гарантоспособности (отказоустойчивости, безопасности и живучести) аналогичных объектов гидроэнергетики. В результате ревизии установлено, что наиболее эффективными способами решения типовых проблем недостаточного уровня гарантоспособности эксплуатируемых и вновь проектируемых ГЭС является внедрение:

- методов синтеза схем СПА с использованием элементов гравитационной автоматики;
- методов организации капсульной структуры технологических помещений;
- методов декомпозиции электронных систем;
- методов обеспечения независимости энергоснабжения.

Более подробно рассмотрим первую позицию предлагаемых мероприятий.

Группа экспертов [2] в качестве показателя безопасности объекта определила величину $Q_{ОП}$ – вероятность опасного отказа, то есть вероятность того, что в системе в течение заданного интервала времени $\tau_д$ (периода диагностирования и профилактического обслуживания с восстановлением первоначальных потребительских свойств) произойдет один

ISSN 1028-9763. Математичні машини і системи, 2017, № 3

опасный отказ при условии, что в начале этого интервала система была исправна. Принято, что эта вероятность должна быть не более $Q_{ОП} \le 10^{-11}$.

Концепция построения безопасной системы зависит от свойств элементной базы. Если используются элементы с несимметричными отказами, данную концепцию можно сформулировать так: все неисправности, с вероятностью возникновения которых необходимо считаться, не должны приводить к опасным отказам. Эта концепция [2, 3] используется при построении существующих систем железнодорожной автоматики и телемеханики (СЖАТ) на h_1-надежных элементах – реле с высоким уровнем гарантии (ВУГ).

Более сложно решается задача безопасности при использовании элементов с симметричными отказами. К ним относятся полупроводниковые приборы и вся современная микроэлектронная и микропроцессорная техника. Несмотря на то, что современные аппаратные средства более надежны, но не настолько, чтобы их отказами можно было бы пренебречь. В этой ситуации общая концепция построения безопасных систем формулируется так: одиночные дефекты аппаратных и программных средств не должны приводить к опасным отказам и должны обнаруживаться на рабочих или тестовых воздействиях не позднее, чем в системе возникает второй дефект.

Обнаружение разнообразных отказов обеспечивается либо сигнализацией отказов, либо переводом системы в защитное состояние. Это может происходить на рабочих воздействиях (в момент первого искажения алгоритма работы) или на тестовых воздействиях, которые периодически подаются на вход системы. Выбор периода диагностирования осуществляется таким, чтобы наработка между предполагаемыми моментами возникновения первого и второго отказов должна была превышать $\tau_д$, то есть диагностирование должно опережать предполагаемый момент возникновения второго отказа.

При создании безопасных СПА ГЭС следует выделить три этапа:

• структурный синтез отказоустойчивого ядра системы;

• разработка безопасных устройств сопряжения (БУС);

• разработка безопасных схем коммутации управляемых объектов (УО).

Уместно вспомнить известную поговорку: «Нет пророка в своем Отечестве». Данная поговорка справедлива и в области безопасности критических технологий и инфраструктур. У нас есть великолепная отечественная железнодорожная автоматика, по вине которой не произошло ни одной аварии за много десятилетий ее эксплуатации. Если бы элементная база и методология построения систем железнодорожной автоматики (СЖАТ), обеспечивающих безопасность движения поездов, была бы имплементирована в системы безопасности АЭС, ГЭС и т.п., большинства техногенных аварий и катастроф по вине СПА на данных объектах удалось бы избежать.

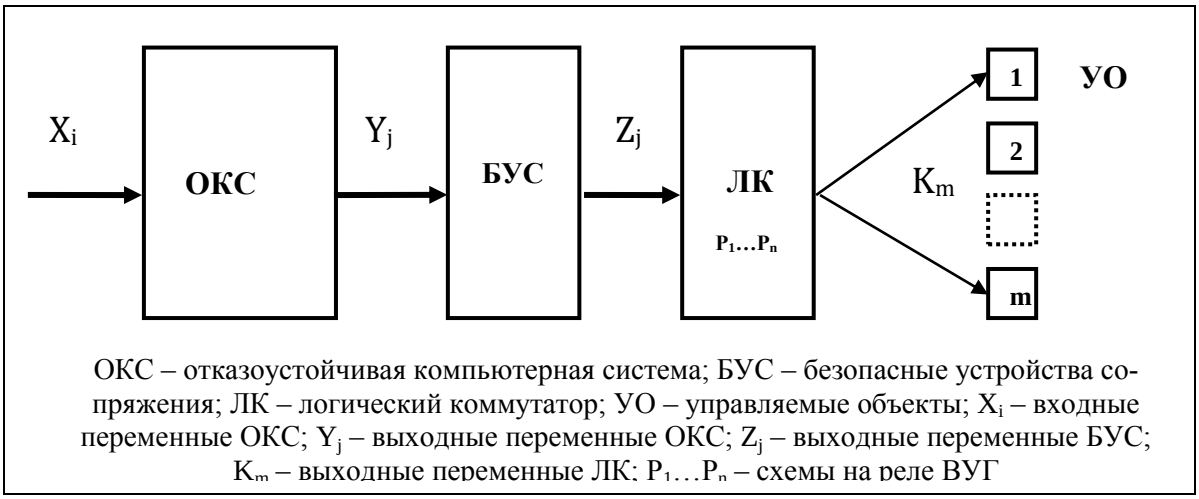
2. Цель исследований

Целью исследований является разработка рекомендаций по синтезу и инжинирингу безопасных систем противоаварийной автоматики для плотинных ГЭС.

3. Структурный синтез СПА

Структурную схему безопасной СПА можно представить в виде последовательной цепочки модулей, изображенных на рис. 1.

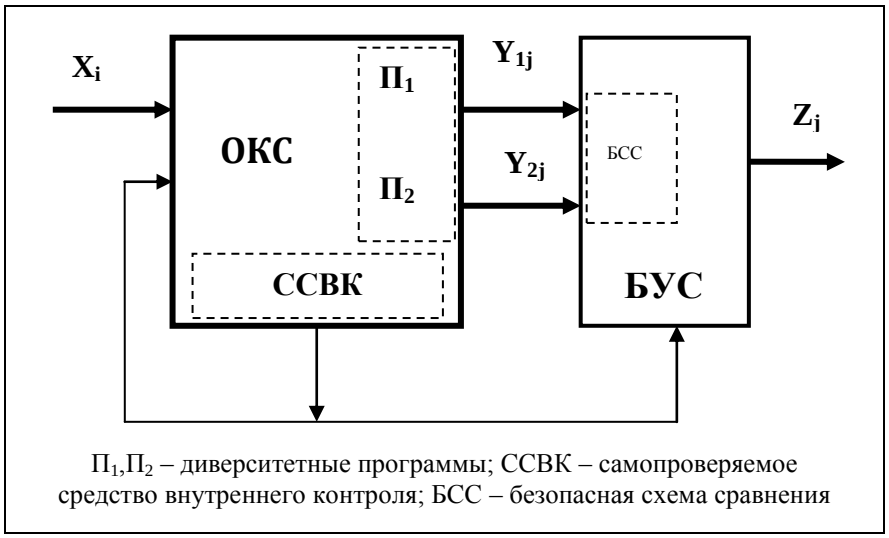
Функцию ядра системы, в котором исполняется основной рабочий алгоритм функционирования СПА, выполняет ОКС, формирующая управляющие воздействия, которые посредством БУС и ЛК, построенного на h_1-надежных элементах, передаются на УО.



ОКС – отказоустойчивая компьютерная система; БУС – безопасные устройства сопряжения; ЛК – логический коммутатор; УО – управляемые объекты; X_i – входные переменные ОКС; Y_j – выходные переменные ОКС; Z_j – выходные переменные БУС; K_m – выходные переменные ЛК; $P_1 \ldots P_n$ – схемы на реле ВУГ

Рис. 1. Структурная схема отказобезопасной СПА

Для реализации ОКС предлагается использовать самопроверяемую одноканальную структуру с диверситетными программами (СОСДП) (рис. 2) [2]. Структура использует две различные и независимые программы (П1 и П2) для реализации одних и тех же функций. Результаты выполнения программ Y_1 и Y_2 сравниваются внешней безопасной схемой сравнения (БСС), входящей в состав БУС.



$П_1$,$П_2$ – диверситетные программы; ССВК – самопроверяемое средство внутреннего контроля; БСС – безопасная схема сравнения

Рис. 2. Самопроверяемая одноканальная структура ОКС с диверситетными программами

Уровень безопасности такой структуры зависит от степени различия (диверситета) двух программ. Наиболее известными формами программной диверситетной избыточности являются многоверсионное программирование и инверсионное повторение решения.

При многоверсионном программировании разными группами программистов разрабатываются две программы, которые реализуют одну и ту же задачу по разным алгоритмам, с использованием разных языков программирования, подходов к программному обеспечению и методов описания спецификаций.

Структура функционирует следующим образом:

• в фиксированные моменты времени считываются и запоминаются входные данные;

• выполняется обработка данных программой $П_1$ и запоминание результатов;

• выполняется обработка данных программой $П_2$ и сравнение результатов на совпадение;

• в случае совпадения происходит передача результирующих выходных воздействий на УО с использованием БУС и логического коммутатора (ЛК) (рис. 1), а в противном случае – блокировка структуры.

При инверсионном повторении решения задача решается повторно, но по обратному алгоритму. Сначала реализуется программа $П_1$, результаты выполнения которой служат входными данными для программы $П_2$. Программа $П_2$ решает обратную задачу. Результаты выполнения программы $П_2$ должны совпадать с входными данными программы $П_1$, что и сравнивается внешней БСС.

Достоинством СОСДП является достаточная простота ее технической реализации и способность к обнаружению ошибок программного обеспечения (ПО). СОСДП может быть дополнена проверкой вычислительного канала с помощью самопроверяемых средств внутреннего контроля (ССВК). Задачей ССВК является обнаружение неисправностей как в вычислительном канале, так и собственных неисправностей. При возникновении отказа ССВК формирует сигнал, с помощью которого структура может быть переведена в защитное состояние, когда выходы ОКС отключаются от УО посредством БУС.

Для реализации ОКС можно использовать и самопроверяемые двухканальные структуры с аппаратной реализацией.

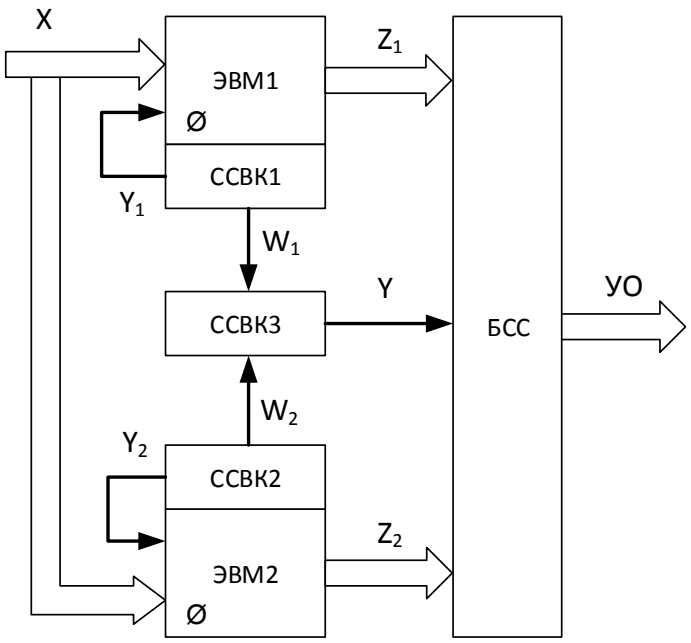


Рис. 3. Самопроверяемая двухканальная структура ОКС

Рассмотрим самопроверяемую двухканальную структуру (СДС) [2] (рис. 3), состоящую из двух вычислительных каналов (условно ЭВМ), снабженных ССВК, задачей которой является обнаружение неисправностей заданного класса в вычислительном канале и собственных неисправностей.

ССВК каждого канала при обнаружении ошибки вырабатывают сигнал Y_1 или Y_2, который отключает соответствующий вычислительный канал (рис. 3). Выходные сигналы Z_1 и Z_2 поступают на БУС, где они сравниваются БСС. При совпадении сигналов формируется управляющее воздействие через ЛК на УО. Сигналы контроля W_1 и W_2, формируемые с помощью ССВК1 и ССВК2, сравниваются в ССВК3. При обнаружении ошибки ССВК3 вырабатывает сигнал Y, который переводит БСС в защитное состояние. Самоконтроль каналов может быть аппаратный и программный. Возможно использование независимых (диверситетных) программ в каждом вычислительном канале.

Основным достоинством СДС являются высокая глубина контроля вычислительных каналов, возможность диагностики отказавшего канала; а также высокая безопасность структуры в целом. В качестве недостатков следует отметить невысокую эксплуатационную готовность, так как любой отказ канала или ССВК переводит структуру в нерабочее защитное состояние. Двухканальные структуры нашли широкое распространение в архитектурах современных отказоустойчивых компьютеров [4].

С целью повышения отказоустойчивости, безотказности и эксплуатационной готовности двухканальной структуры (рис. 3) предложен в [5] новый класс самопроверяемой двухканальной структуры с реконфигурацией, получившей название самопроверяемой двухканальной квазимостиковой структуры (СДКМС) (рис. 4).

Каждый вычислительный канал (ЭВМ) разбивается на n функциональных субблоков (ФСБ), которые с помощью схем реконфигурации (СР) образуют n дублированных узлов (например, ЭВМ1.1 и ЭВМ1.2, ЭВМ2.1 и ЭВМ2.2). Если каналы разбиваются на равнонадежные ФСБ, то средняя наработка до отказа такого ФСБ может быть ориентировочно вычислена по формуле $T_{ФСБ} = \sqrt{n} \cdot T_{ЭВМ}$ [6].

Схема декомпонированной структуры, состоящей из двух узлов, приведена на рис. 4.

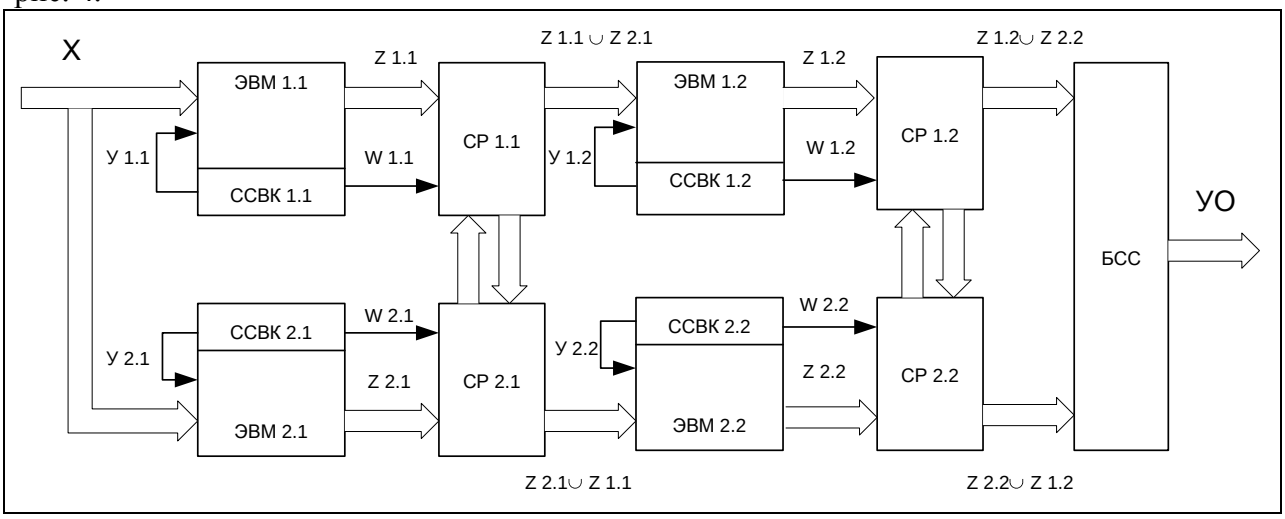


Рис. 4. Самопроверяемая квазимостиковая структура ОКС из 2-х узлов

Запишем логическую функцию дублированной структуры, изображенной на рис. 3.

$$F_Д = z_1 \cdot z_2. \tag{1}$$

Проводя аналогию двух структур (рис. 3 и рис. 4), можно записать:

$$z_1 = z_{1.1} \cdot z_{1.2} \text{ и } z_2 = z_{2.1} \cdot z_{2.2}. \tag{2}$$

Откуда

$$F_Д = z_1 \cdot z_2 = z_{1.1} \cdot z_{1.2} \cdot z_{2.1} \cdot z_{2.2}. \tag{3}$$

Запишем логические функции узлов для квазимостиковой структуры, изображенной на рис. 4.

$$\begin{aligned} f_{1.1} &= z_{1.1} \cup z_{2.1}, \ f_{1.2} = z_{1.2} \cup z_{2.2}, \\ f_{2.1} &= z_{2.1} \cup z_{1.1}, \ f_{2.2} = z_{2.2} \cup z_{1.2}. \end{aligned} \tag{4}$$

Запишем логическую функцию квазимостиковой структуры через логические функции узлов:

$$F_{КМ} = (f_{1.1} \cdot f_{1.2}) \cdot (f_{2.1} \cdot f_{2.2}) = [(z_{1.1} \cup z_{2.1})(z_{1.2} \cup z_{2.2})] \cdot [(z_{2.1} \cup z_{1.1})(z_{2.2} \cup z_{1.2})]. \tag{5}$$

С учетом (2) и принимая во внимание (3), получим

$$F_{KM} = z_1 \cup z_2 \cup z_1 \cdot z_2 \cup z_1 \cdot z_{1.2} \cdot z_{2.1} \cup z_1 \cdot z_{1.1} \cdot z_{2.2} \cup z_2 \cdot z_{1.1} \cdot z_{2.2} \cup$$
$$\cup z_2 \cdot z_{1.2} \cdot z_{2.1} \cup z_{1.1} \cdot z_{2.2} \cup z_{1.2} \cdot z_{2.1}. \quad (6)$$

Рассматривая (6), не трудно видеть, что квазимостиковая структура характеризуется более высоким уровнем отказоустойчивости и, как следствие, эксплуатационной готовности, так как имеет значительно большее количество работоспособных состояний, чем простая дублированная структура. Наличие работоспособных состояний на импликантах $z_1 \cup z_2$ свидетельствует о том, что квазимостиковая структура, изображенная на рис. 4, способна к автоматической реконфигурации в одноканальную структуру без дополнительного вмешательства и изменения функции ВО.

Исследованиями также установлено [7], что средняя наработка до отказа СДКМС интенсивно возрастает с уменьшением времени восстановления и имеет тенденцию к увеличению с ростом количества узлов при фиксированном времени восстановления. Вероятность безотказной работы СДКМС также возрастает с уменьшением времени восстановления и возрастает при увеличении количества узлов, а коэффициент вариации наработки до отказа СДКМС снижается с уменьшением времени восстановления и ростом количества узлов.

При увеличении количества узлов тенденция уменьшения коэффициента вариации наработки до отказа является дополнительным фактором, влияющим на рост вероятности безотказной работы восстанавливаемой СДКМС. Кроме того, с ростом количества узлов уменьшается сложность ФСБ, из которых состоит узел, что упрощает программную и/или техническую реализацию ССВК, повышает точность контроля и диагностики неисправностей структуры и, как следствие, приводит к уменьшению времени восстановления и возрастанию показателей надежности восстанавливаемой СДКМС в целом.

Обнаруженные положительные эффекты от разбиения структуры на дублированные узлы и использование реконфигурации структуры в случае отказа составных частей позволяют разработчикам проектировать более эффективные ОКС.

4. Обеспечение безопасности СПА средствами гравитационной автоматики

Классическая задача, которую нужно решать при синтезе систем, обеспечивающих безопасность критических инфраструктур – «сторожить сторожа». В чем она заключается?

Все изделия электронной техники, а именно, полупроводниковые приборы, интегральные микросхемы, а также большинство электромагнитных реле являются элементами с симметричными отказами, у которых вероятность возникновения отказа одного вида (0→1 или 1→0) примерно одинакова и ею нельзя пренебречь.

В случае управляющих систем автоматики, какими являются СПА, как бы мы не повышали надежность и достоверность работы вычислительных каналов ОКС, когда мы выходим на управление реальными УО (например, аварийными заслонками ГЭС), нам не обойтись без силовых элементов (мощных транзисторов, тиристоров, реле и т.д.), которые являются последними «сторожами» в структурной схеме обеспечения надежности и безопасности и относятся к элементам с симметричными отказами. Эти «сторожа» успешно «съедают» все успехи, достигнутые ранее в области безопасности ОКС и требуют «сторожить» их самих. Данная задача успешно решена специалистами в области железнодорожной автоматики и телемеханики [2] и этот опыт рекомендуется распространить на другие критические инфраструктуры, например, плотинные ГЭС.

Важной проблемой при построении безопасных систем является организация сопряжения микроэлектронной аппаратуры ОКС с УО.

В настоящее время производится и эксплуатируется много различных УО с разнообразными характеристиками по входам-выходам. В цепях СПА, к которым не предъявляют-

ся требования безопасности, как правило, применяют стандартные УСО, выпускаемые промышленностью в составе управляющих ЭВМ и контроллеров. При разработке микроэлектронных ОКС, к которым предъявляются специфичные для ответственных систем требования безопасности, чаще используются специализированные устройства – безопасные устройства сопряжения (БУС).

К БУС предъявляются следующие основные требования [2]:

• обеспечение минимально допустимой вероятности возникновения ложного сигнала включения УО на выходе БУС при любом отказе его элементов;

• выполнение временного и энергетического согласования электронных схем и УО;

• сохранение временных и энергетических параметров БУС в заданных пределах в течение всего срока эксплуатации;

• обеспечение минимально допустимой чувствительности к электромагнитным помехам и влияниям;

• высокая технологичность производства в сочетании с низкой стоимостью.

Схемные решения устройств сопряжения с УО не должны иметь опасных отказов, то есть с определенной вероятностью должны исключать ложное включение УО на выходе БУС при любом отказе его элементов. Обычно учитываются следующие отказы элементов и выходных каналов:

• короткое замыкание выходного полупроводникового элемента;

• обрыв выходного полупроводникового элемента или их соединений;

• трансформация одного типа выходного полупроводникового элемента в другой;

• самовозбуждение (автогенерация) выходных электронных схем;

• кратковременное или длительное отключение источника питания выходных элементов;

• повреждение источника питания выходных элементов, при котором на его шинах появляется значительная переменная составляющая;

• изменение параметров выходных элементов или режимов их работы в установленных пределах;

• появление двух или более отказов выходных элементов или соединений, не выявленных за время нахождения схемы в статическом состоянии.

Для исключения накопления отказов БУС, как правило, строятся по принципу обеспечения динамической работы всех элементов, что позволяет диагностировать их электронные элементы путем периодического переключения их из состояния логической «1» в состояние логический «0» и обратно.

Наиболее часто БУС выполняют в виде безопасных электронных схем с несимметричными отказами (БЭС), у которых при появлении неисправности искажаются рабочие функции. Возникающие в этом случае выходные сигналы неисправной БЭС не приводят к ложному включению исполнительного реле (ИР) высокого уровня гарантии (ВУГ), являющегося элементом гравитационной автоматики [1].

Примером БЭС, входящих в состав БУС, являются безопасные схемы сравнения (БСС), изображенные на рис. 5, 6 [2]. Только при совпадении по фазе импульсов, поступающих на входы X_1 и X_2, на выходе схемы Y (рис. 5) появляется выходной сигнал. Рассогласование по фазе входных импульсов или неисправность любого элемента схемы приводят к исчезновению импульса на выходе Y. На рис. 6 изображена синхронная схема сравнения с использованием тактовой последовательности, поступающей на вход T. На входы X_1 и X_2 поступают парафазные (находящиеся в противофазе) последовательности импульсов. Сигнал на выходе Y появляется только в случае совпадения по времени сигналов на входах T, X_1 и X_2, в случае рассогласования сигналов, а также в случае неисправности любого элемента схемы, сигнал на выходе исчезает.

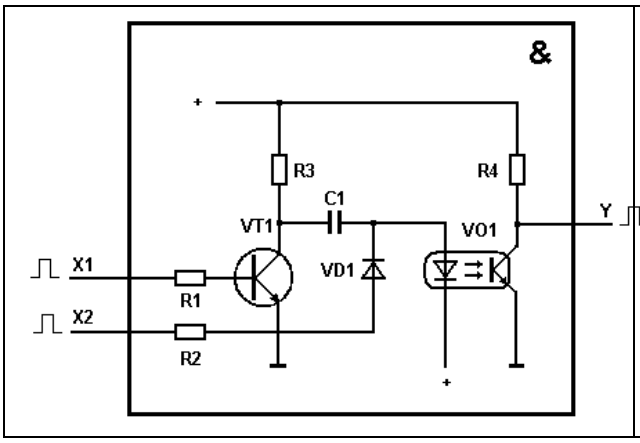


Рис. 5. Безопасная схема сравнения

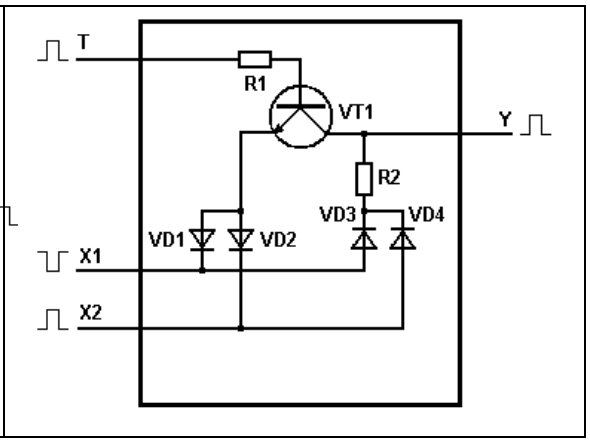


Рис. 6. Безопасная синхронная схема сравнения с парафазными входами

5. Релейные схемы управления в СПА: шаг назад – два шага вперед

С выходов БСС сигналы поступают на безопасные устройства включения исполнительных реле (УВИР). Контакты ИР ВУГ коммутируют рабочие цепи УО. Преимуществами такого решения является то, что ИР ВУГ имеют высокую безопасность, устойчивость к электромагнитным помехам и перенапряжениям, являются элементами идеальной гальванической развязки с несимметричными отказами [1].

Рассмотрим основные принципы построения безопасных УВИР [2]. Наиболее распространена схема УВИР, представленная на рис. 7. Безопасное поведение этой схемы при отказах обеспечивается за счет двойного преобразования входных импульсных сигналов - дифференцирования с помощью трансформатора и интегрирования с помощью диода и конденсатора. При нарушении любого из этих двух законов преобразования сигналов на выходе схемы либо отсутствует напряжение, либо оно меньше напряжения выключения ИР, поэтому реле гарантированно выключится (отпустит свой якорь и разомкнет фронтовые контакты).

Для включения реле, то есть для достижения напряжения срабатывания ИР, необходимо поступление на вход схемы серии импульсов. Кратковременные случайные сбои в работе ОКС не приводят к ложному выключению или включению ИР из-за инерционности заряда и разряда конденсатора. Во включенном состоянии реле находится до тех пор, пока поступают импульсные сигналы.

Кроме УВИР с трансформаторной гальванической развязкой, разработаны УВИР с конденсаторной гальванической развязкой (рис. 8).

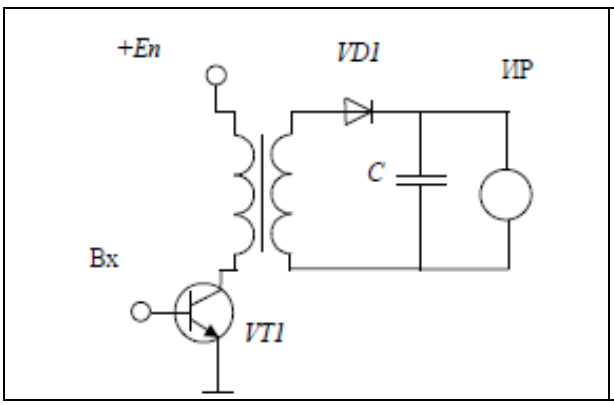


Рис. 7. УВИР с трансформаторной гальванической развязкой

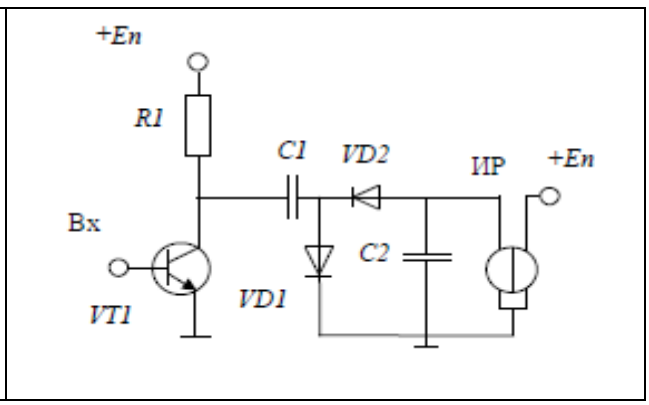


Рис. 8. УВИР с конденсаторной гальванической развязкой

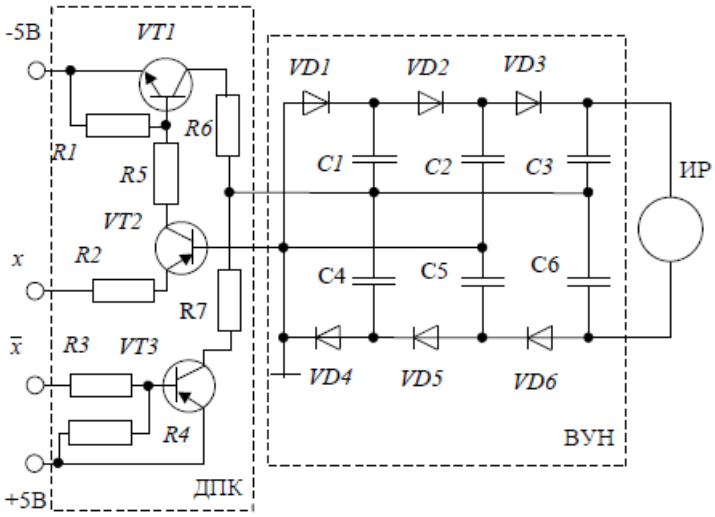


Рис. 9. УВИР на основе выпрямителя с умножением напряжения

Рассмотренные УВИР имеют один вход и могут использоваться в микроэлектронных системах, достоверность выходных сигналов которых контролируется специальными средствами - БСС. В дублированных системах могут использоваться УВИР, принцип работы которых основан на преобразовании импульсных сигналов малой амплитуды (3 ÷ 5 В) в рабочее напряжение ИР (12÷24 В) с помощью выпрямителей с умножением напряжения (рис. 9).

В схеме УВИР (рис. 9) входные сигналы в виде последовательности импульсов поступают на прямой и инверсный входы двухполюсного ключа (ДПК). При парафазности сигналов, поступающих от разных вычислительных каналов, на входе выпрямителя с умножением напряжения (ВУН) появляется переменное напряжение прямоугольной формы. ВУН выпрямляет и умножает исходное напряжение до уровня, необходимого для срабатывания ИР при поступлении нескольких импульсов.

Повреждение любого элемента УВИР ведет к прекращению умножения напряжения или снижению выходного напряжения ВУН до напряжения выключения ИР, что исключает возможность его ложного включения. Кроме того, УВИР контролирует правильность работы двух каналов (парафазность выходных сигналов), выполняя роль выходных электронных компараторов.

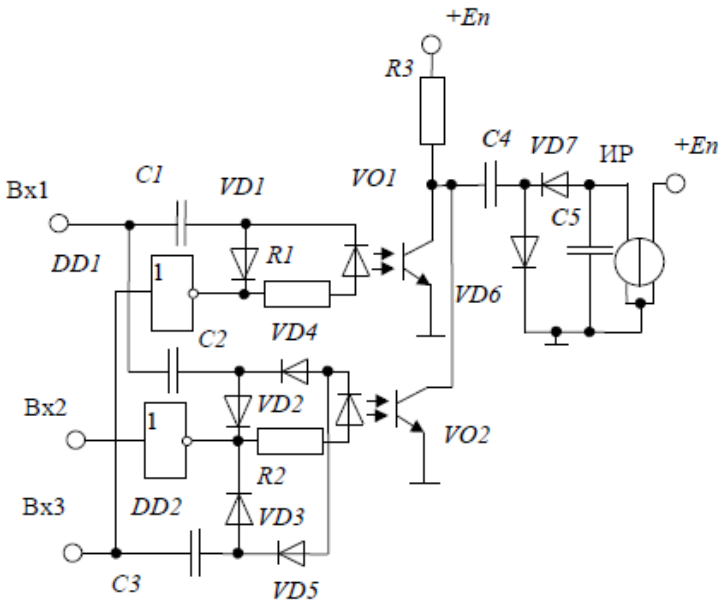


Рис. 10. Мажоритарное УВИР

В ОКС, выполненных с использованием мажоритарной структуры, например, «2 из 3», разработано УВИР, представленное на рис. 10. При синхронном поступлении импульсных сигналов на входы 1, 2, 3 происходит заряд конденсаторов C_1, C_2, C_3 в течение времени действия входных импульсов. Во время паузы они разряжаются на светодиоды оптопар VO_1 и VO_2 через резисторы R_1, R_2**.** При этом напряжение, воздействующее на них, равно сумме напряжений на конденсаторе и источнике питания. В результате этого фототранзисторы оптопар переключаются и формируют импульсы, поступающие на вход преобразователя полярности (элементы C_4, C_5, VD_6, VD_7*)*, в результате чего ИР притягивает якорь.

При отсутствии импульсов на двух входах из трех на светодиоды воздействует только напряжение заряда конденсаторов приблизительно в два раза меньшей величины, чем в случае синхронного поступления импульсных сигналов на все входы. В результате оптроны не переключаются и ИР отпустит свой якорь. В данной схеме для обеспечения ее безопасного функционирования используются функции дифференцирования, удвоения напряжения и гальванической развязки.

Все ИР СПА объединены в логический коммутатор (ЛК), предназначенный для формирования управляющих воздействий на УО. ЛК представляет собой комбинационную схему, выполненную на реле ВУГ. Пример ЛК приведен на рис. 11, который реализует 5 функций f_1, f_2, f_3, f_4, f_5 по управлению УО.

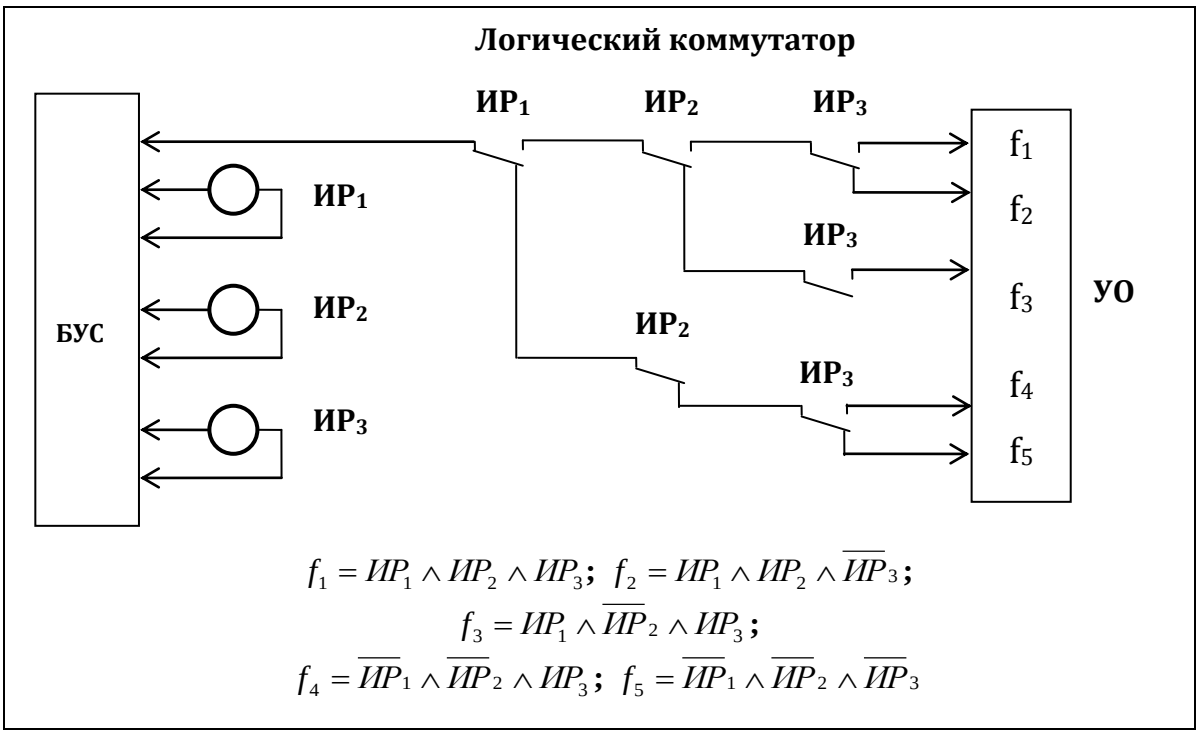


Рис. 11. Пример схемы логического коммутатора на реле ВУГ

Примечание. Примером элемента ВУГ являются реле НМШ и РЭЛ и их замыкающий (фронтовой контакт Ф) [1]. У этих реле можно пренебречь вероятностью сваривания контакта (отказ типа 0→1). Несимметричность отказов достигается специальными технологическими мерами, а именно, применены контактные материалы, которые практически не свариваются (графит – серебро), а также используются специальные гравитационные противовесы и антимагнитные бронзовые штифты для гарантированного размыкания контактов Ф.

Реле с несимметричными отказами создают специально для решения проблемы безопасности. В дальнейшем элементы, у которых вероятность отказов типа 0→1 мала, будем называть h_1-надежными. Комбинационную схему будем называть h_1-надежной, если на выходе схемы не допускается замена сигналов типа 0→1. Наиболее экономичными такие схемы могут быть получены с использованием h_1-надежных элементов, у которых нет отказов типа 0→1. Рассмотрим методы синтеза h_1-надежных комбинационных схем на h_1-надежных элементах.

6. Синтез цифровых автоматов с исключением опасных отказов на h_1-надежных элементах

Несмотря на использование h_1-надежных элементов при синтезе ЛК, существуют специальные требования, позволяющие реализовывать h_1-надежные безопасные схемы коммутации управляющих сигналов. Рассмотрим теоретические основы построения таких схем [2, 8–11].

В своей классической постановке проблема синтеза надежных автоматов из ненадежных элементов не связана с качественным анализом искажений в алгоритме функционирования автомата, которые происходят при возникновении отказов. Предполагается, что все отказы равноправны, то есть, что их последствия при воздействии на УО одинаковы. Однако для СПА это предположение несправедливо. Особенность СПА состоит в том, что она обеспечивает безопасность функционирования ГЭС, поэтому некоторые ее отказы могут приводить к опасным (аварийным) ситуациям.

Рассмотрим, например, цифровой автомат (ЦА), управляющий аварийной заслонкой (АЗ) ГЭС (рис. 12).

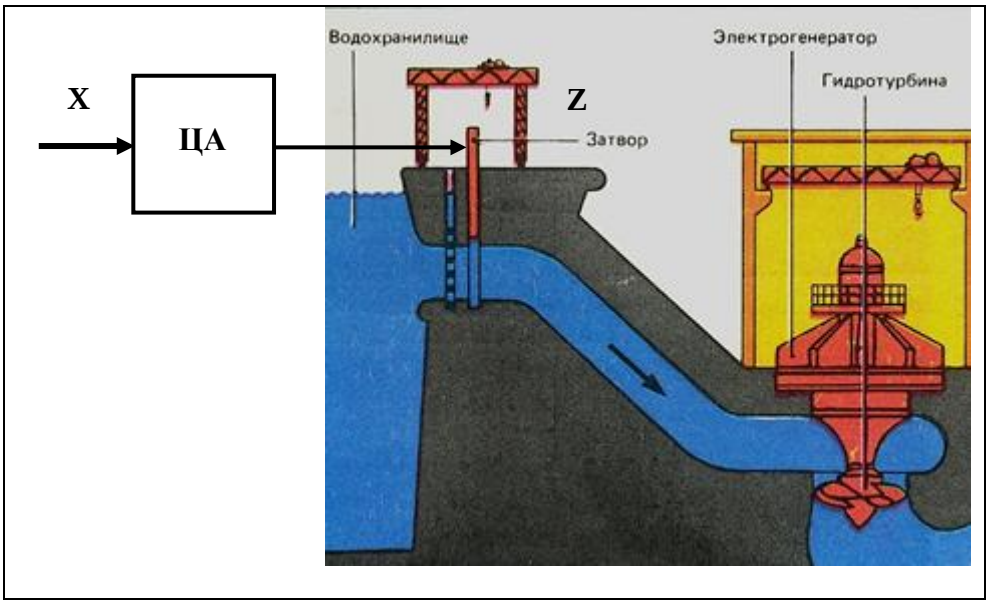


Рис. 12. Схема управления аварийной заслонкой ГЭС

Отказы ЦА могут приводить к двум последствиям:

• заслонка Z ошибочно опущена, то есть перекрыла поток воды к турбине в то время, когда не должна быть опущена при исправной схеме;

• заслонка Z ошибочно не опущена, то есть не перекрыла поток воды к турбине в то время, когда должна быть опущена при исправной схеме.

С точки зрения влияния на безопасность ГЭС эти два отказа неравноправны. Первый отказ (защитный) может привести к потере объема выработанной гидроагрегатом (ГА) электроэнергии. Это, естественно, нежелательно, но с точки зрения безопасности допускается. Второй отказ (опасный) может вызвать аварийную ситуацию или способствовать увеличению последствий аварии, что с точки зрения безопасности не допускается.

Итак, отказы в схемах КА следует делить на опасные и неопасные (защитные) и схемы строить так, чтобы предотвратить в них в первую очередь возникновение опасных отказов. Таким образом, безопасность – это свойство системы не давать опасных отказов в течение заданного времени при определенных условиях эксплуатации.

Возникновение защитного отказа (рис. 13) нарушает надежность (работоспособность) системы, но не нарушает ее безопасность. При появлении опасного отказа наруша-

ются как безопасность, так и работоспособность системы. Необходимо понимать, что при длительном нахождении системы в неработоспособном безопасном состоянии (защитном состоянии) возможна ситуация накопления неопасных отказов, что, в свою очередь, может привести к возникновению опасного отказа. Вопросы прогнозирования и обеспечения периода диагностирования состояния системы и методы проведения планово-предупредительной профилактики с полным восстановлением всех потребительских свойств являются особенно важными.

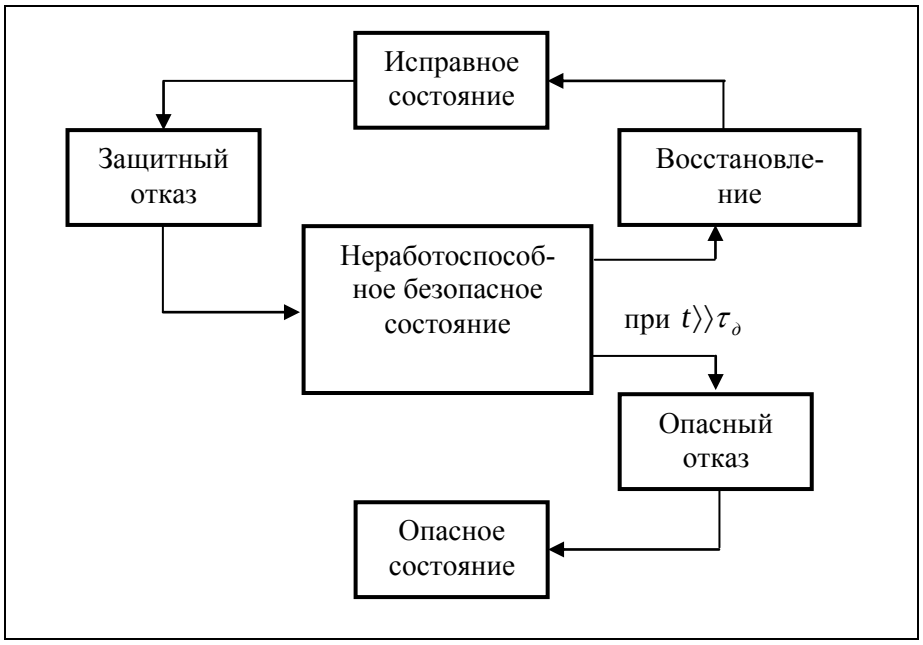


Рис. 13. Состояния схем автоматики

Рассмотрим методологию построения h_1-надежных схем на h_1-надежных элементах. Пусть имеется произвольная схема ЛК (рис. 14), содержащая h_1-надежные элементы $Э_1$, $Э_2$,...,$Э_s$, каждый из которых реализует некоторую функцию алгебры логики (ФАЛ) $f_1, f_2, ..., f_s$.

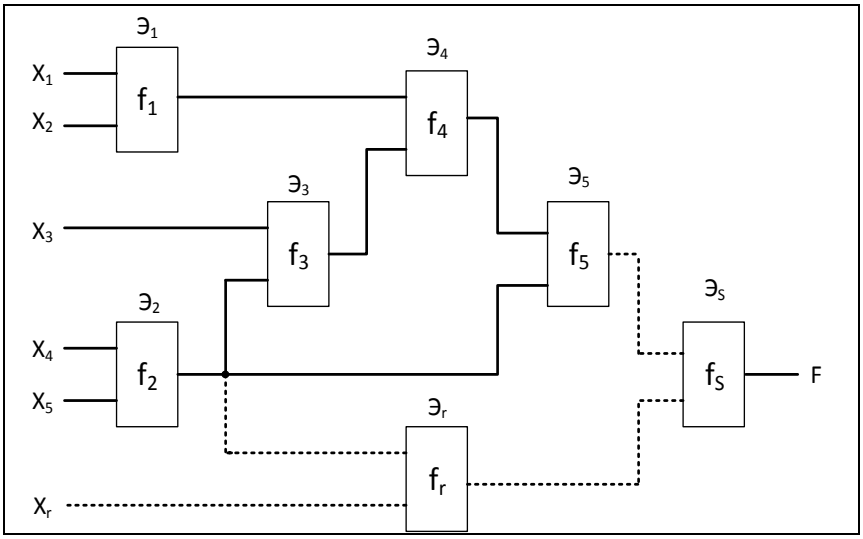


Рис. 14. Схема на h_1-надежных элементах

Примеры реализации ФАЛ на h_1-надежных элементах (контактах реле ВУГ) приведены на рис. 15.

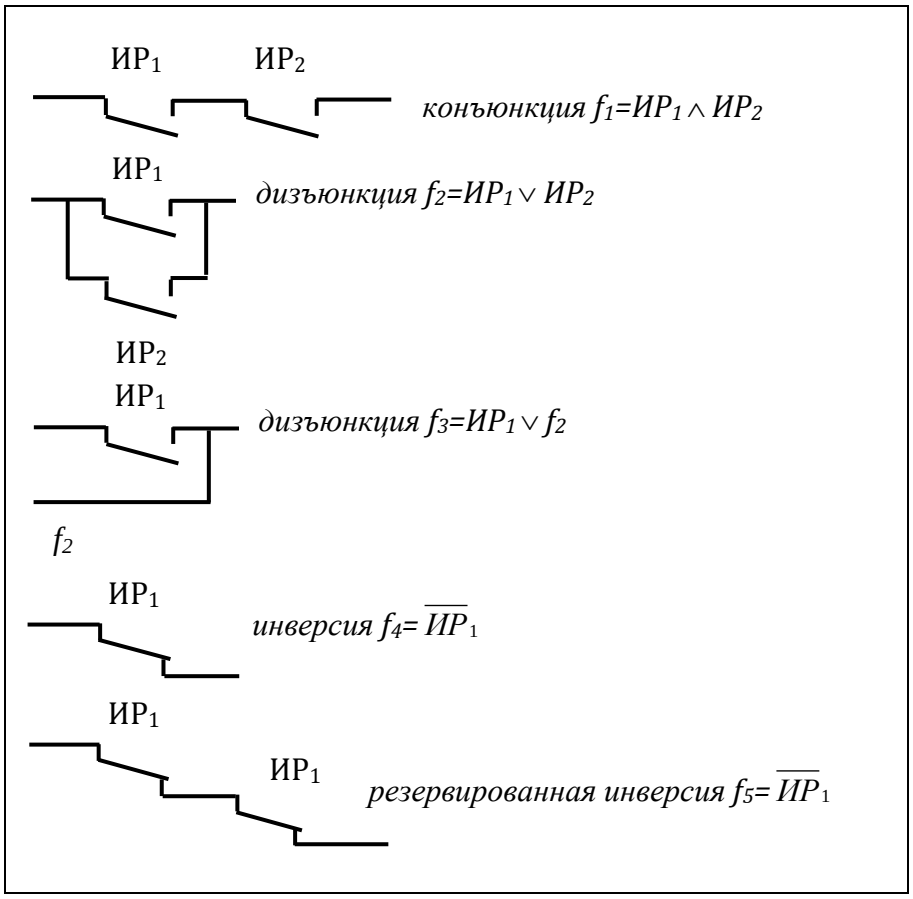


Рис. 15. Примеры реализации ФАЛ на контактах реле ВУГ

Присвоим каждому элементу (рис. 14) свой ранг. Первый ранг имеют элементы, соединенные только со входами схемы, ранг r – элементы, входы которых соединены с выходами элементов с рангом не выше, чем $r-1$. Первый ранг имеют элементы $Э_1$ и $Э_2$, второй – $Э_3$, третий – $Э_4$, четвертый – $Э_5$ и т.д.

Теорема 1. Неизбыточная логическая схема, построенная на h_1-надежных элементах, является h_1-надежной тогда и только тогда, когда все ее элементы ранга $k \geq 2$ реализуют монотонные ФАЛ.

Теорема 1 накладывает жесткие ограничения на способы построения h_1-надежных схем. Единственными формами представления ФАЛ, у которых немонотонная операция (инверсия) применяется только к переменным функции, являются дизъюнктивная (ДНФ) и конъюнктивная (КНФ) нормальные формы, а также скобочные формы, полученные из них, СДНФ и СКНФ.

Определение 1. Дизъюнктивной нормальной формой (ДНФ) функции $F(x_1, x_2, x_3)$ называется равносильная ей $f(x_1, x_2, x_3)$, представляющая собой дизъюнкцию элементарных конъюнкций, например, $f(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge \bar{x}_3) \vee (\bar{x}_1 \wedge x_2) \vee x_3$.

Элементарной конъюнкцией n переменных называется конъюнкция переменных или их отрицаний.

Определение 2. Совершенной дизъюнктивной нормальной формой (СДНФ) функции $F(x_1, x_2, x_3)$ называется ДНФ $z(x_1, x_2, x_3)$, обладающая следующими свойствами:

• каждое логическое слагаемое функции $z(x_1, x_2, x_3)$ содержит все переменные, входящие в функцию $F(x_1, x_2, x_3)$;

• все логические слагаемые функции $z(x_1, x_2, x_3)$ различны;

• ни одно логическое слагаемое функции $z(x_1, x_2, x_3)$ не содержит одновременно переменную и ее отрицание;

• ни одно логическое слагаемое функции $z(x_1, x_2, x_3)$ не содержит одну и ту же переменную дважды.

Например, $z(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge \bar{x}_3) \vee (\bar{x}_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$.

Определение 3. Конъюнктивной нормальной формой (КНФ) функции $F(x_1, x_2, x_3)$ называется равносильная ей функция $y(x_1, x_2, x_3)$, представляющая собой конъюнкцию элементарных дизъюнкций, например, $y(x_1, x_2, x_3) = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2) \wedge x_3$.

Элементарной дизъюнкцией n переменных называется дизъюнкция переменных или их отрицаний.

Определение 4. Совершенной конъюнктивной нормальной формой функции (СКНФ) $F(x_1, x_2, x_3)$ называется КНФ $u(x_1, x_2, x_3)$, удовлетворяющая следующим свойствам:

• все элементарные дизъюнкции, входящие в $u(x_1, x_2, x_3)$, содержат все переменные;

• все элементарные дизъюнкции, входящие в $u(x_1, x_2, x_3)$, различны;

• каждая элементарная дизъюнкция, входящая в $u(x_1, x_2, x_3)$, содержит переменную один раз;

• ни одна элементарная дизъюнкция, входящая в $u(x_1, x_2, x_3)$, не содержит переменную и ее отрицание.

Например, $u(x_1, x_2, x_3) = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3)$.

Из теоремы 1 следует теорема 2.

Теорема 2. Схемная реализация ФАЛ на h_1-надежных элементах является h_1-надежной тогда и только тогда, когда она осуществлена по одной из четырех форм представления выходной функции: ДНФ, КНФ, СДНФ и СКНФ.

Часто на практике встречается ситуация, когда у реле отсутствует h_1-надежный размыкающий (тыловой) контакт, поскольку из трех элементов: конъюнкция (И), дизъюнкция (ИЛИ) и инверсия (НЕ) наиболее трудно реализовать безопасный элемент НЕ. В нашем случае у реле ВУГ типов НМШ и РЭЛ также отсутствует безопасный h_1-надежный элемент НЕ (тыловой контакт), поэтому, если возникает необходимость использования размыкающих контактов в ответственных цепях, обеспечивающих безопасность, то это делается путем дополнительной проверки их исправной работы схемным путем на реле ВУГ или же путем резервирования для тыловых контактов реле путем последовательного их включения (рис. 15).

7. Заключение

Итак, при создании безопасных СПА ГЭС рекомендуется выделять три основных этапа инжиниринга:

• структурный синтез отказоустойчивого ядра системы;

• разработка безопасных устройств сопряжения;

• разработка безопасных схем коммутации УО.

В качестве ядра СПА предлагается использовать следующие самопроверяемые отказоустойчивые структуры:

• одноканальную с диверситетными программами;
• двухканальную;
• двухканальную квазимостиковую.

Предпочтение следует отдавать СДКМС. Обнаруженные положительные эффекты от разбиения двухканальной структуры на дублированные узлы и использование реконфигурации структуры в случае отказа составных частей позволяют проектировать наиболее эффективные ОКС.

В качестве безопасных устройств сопряжения БСУ между ОКС и УО предлагается ряд электронных безопасных схем сравнения БСС и устройств включения исполнительных реле УВИР.

Для коммутации УО предлагается использовать ЛК, построенный на релейных h_1-надежных элементах с ВУГ. Отличительной особенностью схем ЛК является то, что они должны строиться в виде комбинационных схем на контактах реле, описываемых монотонными ФАЛ. Решение данной проблемы состоит в получении такой схемы автомата, которая не содержит элементов НЕ (инверсий). Такая реализация автомата называется монотонной и описывается монотонными функциями алгебры логики по одной из четырех форм представления: ДНФ, КНФ, СДНФ и СКНФ.

СПИСОК ЛИТЕРАТУРЫ

1. Федухин А.В. Гравитационная автоматика в системах защиты объектов критических инфраструктур / А.В. Федухин // Математичні машини і системи. – 2017. – № 1. – С. 106 – 121.
2. РТМ 32 ЦШ 1115842.01 – 94. Безопасность железнодорожной автоматики и телемеханики. Методы и принципы обеспечения безопасности микроэлектронных СЖАТ. – М.: Транспорт, 1994. – 115 с.
3. Теоретические основы железнодорожной автоматики и телемеханики / А.С. Переборов, А.М. Брылеев, А.В. Смирнова [и др.]. – М.: Транспорт, 1984. – 384 с.
4. Stratus Computer Inc. [Электронный ресурс]. – Режим доступа: http://www.stratus.com.
5. Федухин А.В. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией / А.В. Федухин., Ар.А. Муха // Математичні машини і системи. – 2010. – № 4. – С. 156 – 159.
6. Стрельников В.П. Оценка и прогнозирование надежности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.
7. Федухин А.В. К вопросу моделирования надежности восстанавливаемой квазимостиковой структуры с учетом тренда параметров надежности составных частей / А.В. Федухин, В.П. Пасько, Ар.А. Муха // Математичні машини і системи. – 2016. – № 1. – С. 158 – 167.
8. Сапожников В.В. Дискретные устройства железнодорожной автоматики, телемеханики и связи / В.В. Сапожников, Ю.А. Кравцов, Вл.В. Сапожников. – М.: Транспорт, 1988. – 255 с.
9. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В.В. Сапожников, Вл.В. Сапожников, Х.Л. Христов, Д.В. Гавзов. – М.: Транспорт, 1995. – 272 с.
10. Сапожников В.В. Дискретные автоматы с обнаружением отказов / В.В. Сапожников, Вл.В. Сапожников. – Л.: Энергоатомиздат, 1984. – 109 с.
11. Сапожников В.В. Самопроверяемые дискретные устройства / В.В. Сапожников, Вл.В. Сапожников. – СПб.: Энергоатомиздат, 1992. – 224 с.

Стаття надійшла до редакції 16.05.2017