

УДК 658.012.011

**Е.В. БАБЕШКО, В.С. ХАРЧЕНКО**

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

## **АДАПТАЦИЯ К ОТКАЗАМ КОНТРОЛЛЕРОВ ДЛЯ ПОВЫШЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ**

Показана возможность повышения функциональной безопасности информационно-управляющих систем с помощью применения систем защиты, учитывающих отказы управляющих контроллеров. Представлены возможные способы построения систем, приведен пример реализации в инструментальной среде Step7 для программируемых логических контроллеров Siemens Simatic.

**программируемый логический контроллер, резервирование, противоаварийная защита, адаптивная система**

### **Введение**

Современные информационно-управляющие системы (ИУС) представляют собой сложные и дорогостоящие человеко-машинные комплексы. Такие системы управляют различными технологическими объектами, в том числе и объектами критического применения.

Программируемые логические контроллеры (ПЛК) как наиболее распространенные элементы для построения ИУС предоставляют достаточно широкие возможности для обеспечения безотказной работы [1, 2]. Кроме того, обеспечение безопасности может осуществляться средствами систем противоаварийной защиты [3, 4]. Однако все эти варианты не всегда являются достаточными.

Дело в том, что моделирование опасных объектов управления на этапе разработки представляет собой чрезвычайно сложную задачу. Параметры таких объектов и их структуры не всегда известны по причине неполноты информации. Кроме того, параметры могут существенно изменяться во время протекания производственного процесса в указанных отраслях. Упрощенные модели, которые строятся на этапе разработки, не могут в полной мере предусмотреть все возможные ситуации.

Поэтому обычные ИУС во многих случаях не

могут обеспечить качественного, устойчивого [5], а иногда и просто безопасного управления объектами такого класса.

В данной работе для решения вышеуказанных проблем предлагается построение адаптивных систем защиты с перестройкой структуры при обнаружении отказов управляющих контроллеров. Отличительной особенностью таких систем является наличие встроенных средств анализа и контроля состояния как элементов самой управляющей системы, так и технологического объекта с целью наиболее своевременного принятия решения по изменению структуры (адаптации) системы для достижения наиболее высокого уровня функциональной безопасности.

Применение принципов адаптивного управления позволяет обеспечить работоспособность управляющей системы в условиях изменения динамических свойств объекта в широких пределах, повысить эффективность функций автоматического контроля, диагностирования, сигнализации и аварийной защиты сложных объектов [6, 7].

Существует несколько разновидностей адаптивных систем. Если в процессе работы изменению (адаптации) подвергается структура, то адаптивная система называется самоорганизующейся системой

[8, 9]. В данной работе будут рассматриваться только самоорганизующиеся системы управления. Поэтому далее под адаптивными системами управления будут подразумеваться именно такие системы.

**Целью** данной статьи является обоснование и разработка структуры системы защиты с адаптацией к отказам управляющих контроллеров. В качестве управляющих контроллеров предлагается использовать программируемые логические контроллеры.

### Модель системы защиты

В работе [4] проводился анализ возможности альтернативного использования резервирования и систем противоаварийной защиты (ПАЗ) для обеспечения высокого уровня безопасности. В случае резервирования безопасность обеспечивается за счет безотказной работы системы, в случае с системой ПАЗ – за счет гарантированного перевода системы в безопасное состояние при выявлении отказа.

В данной работе предлагается объединить указанные выше два подхода, реализовав во всех резервируемых контроллерах кроме основных функций управления еще и функции ПАЗ. Функции защиты будут активироваться вместо функций управления в зависимости от количества работоспособных ПЛК и входной информации о состоянии объекта управления. Таким образом, структура системы не будет жестко зафиксирована, а будет изменяться в зависимости от ряда указанных факторов, т.е. предлагается придание типовой структуре свойства адаптации.

### Реализация адаптивной системы

Рассмотрим систему, состоящую из  $N$  одинаковых ПЛК, которые резервированы для повышения надежности и включены по мажоритарной схеме « $M$  из  $N$ »,  $M = \frac{N+1}{2}$ .

Рассмотрим два варианта реализации адаптивной системы. Первый (рис. 1) – когда для выполнения

функций адаптации используется дополнительное устройство (например, еще один контроллер). При этом основные контроллеры не нагружаются никакими дополнительными функциями.

Блок определения неисправных ПЛК и формирования корректных воздействий производит мажоритарную выборку и выдает корректные выходные воздействия. Этот же блок определяет, какие из ПЛК являются в данный момент работоспособными.

Дополнительный контроллер, выполняющий функции адаптации (ПЛК  $N+1$  на рис. 1), анализирует информацию от блока определения неисправных ПЛК и, в зависимости от входных данных, коммутирует функции управления/защиты контроллеров.

Во втором случае функции анализа состояния системы реализуются во всех контроллерах (рис. 2). Преимуществом такого подхода является то, что не требуется никаких дополнительных устройств для реализации функций адаптации. Очевидным недостатком является усложнение программного обеспечения контроллеров.

Выполним сравнение полученных структур с типовыми решениями. Вероятности безопасной работы системы с резервированием и системы с ПАЗ, состоящих из  $N$  элементов, рассчитываются по формулам (1) и (2) соответственно [4]:

$$P_{безоп}^{рез} = 1 - (1 - P_{безотк}^{нач})^{N-1} + N \cdot P_{безоп}^{нач} (1 - P_{безоп}^{нач})^{N-1}; \quad (1)$$

$$P_{безоп}^{ПАЗ} = P_{безотк}^{нач} + (1 - P_{безоп}^{нач}) \cdot P_{ПАЗ}. \quad (2)$$

Вероятность безопасной работы систем с адаптацией можно записать следующим образом:

$$P_{безоп}^{адапт} = \begin{cases} 1 - (1 - P_{безотк}^{нач})^{N-1} + N \cdot P_{безоп}^{нач} (1 - P_{безоп}^{нач})^{N-1}, & f \leq k \\ P_{безотк}^{нач} + (1 - P_{безоп}^{нач}) \cdot P_{ПАЗ}, & f > k \end{cases},$$

где  $f$  – количество обнаруженных отказов контроллеров;  $k$  – некоторый порог отказов,  $0 < k < \frac{N-1}{2}$ .

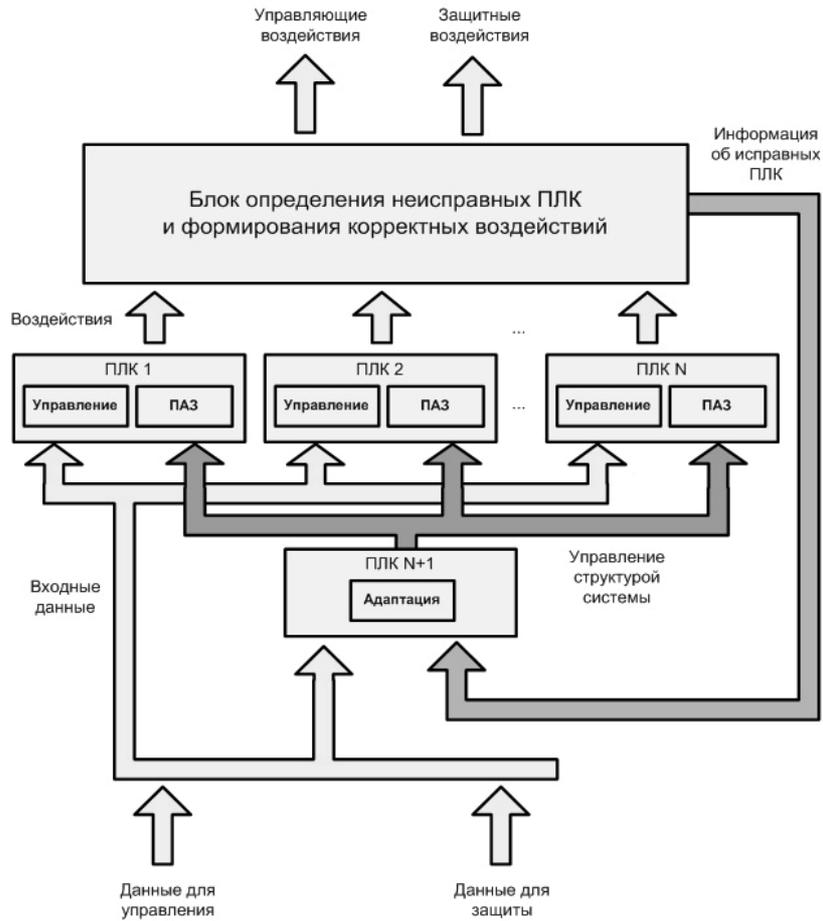


Рис. 1. Система с дополнительным контроллером адаптации

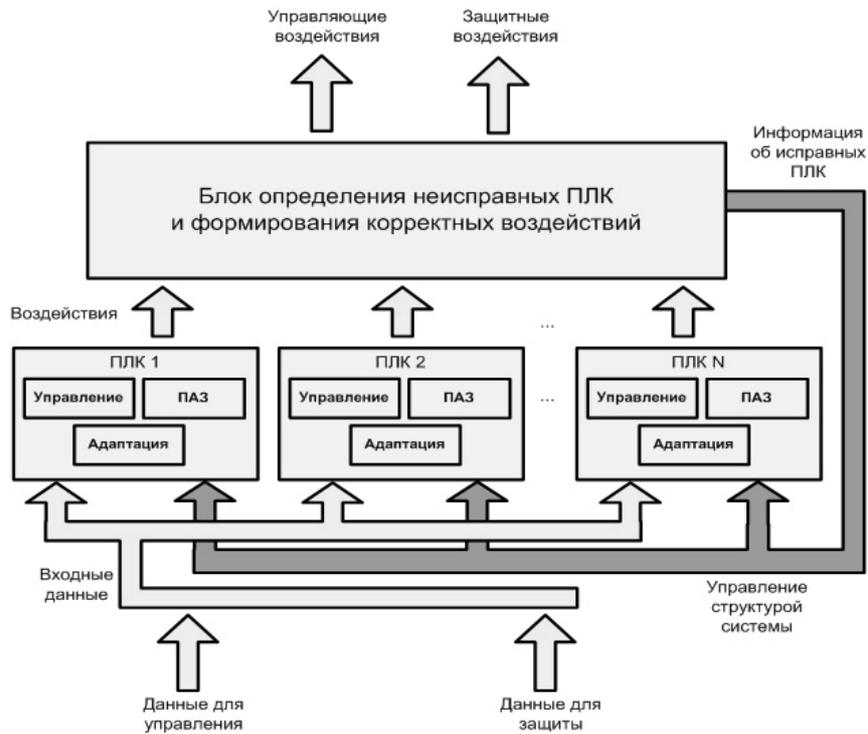


Рис. 2. Система с внутренней адаптацией

Для определения того, какой из рассмотренных вариантов предпочтительнее, необходимо произвести более детальный анализ всех структур и выполнить сравнение по критериям безопасности, сложности реализации, стоимости.

### Пример реализации системы

Рассмотрим в качестве примера систему, состоящую из трех одинаковых по функциональности контроллеров. Во всех контроллерах реализованы функции управления, защиты и адаптации.

Пока все контроллеры работоспособны, наиболее надежным вариантом является известная мажоритарная схема, выборка «2 из 3».

В случае отказа любого из контроллеров получается ситуация, когда решение о правильности результата принять невозможно (например, оставшиеся два контроллера выдают абсолютно различные выходные воздействия). При этом дальнейшее использование резервирования контроллеров теряет

смысл, поскольку вероятность безотказной работы такой системы даже меньше, чем у нерезервированной системы [10].

Поэтому при отказе первого ПЛК функции управления возлагаются, например, на второй ПЛК, а третий контроллер в этом случае обеспечивает противоаварийную защиту. В случае отказа второго ПЛК функции управления выполняет третий ПЛК, а первый используется для ПАЗ и т.д. Функции контроллеров для рассмотренных случаев приведены в табл. 1.

После проведения работ по восстановлению система должна автоматически переходить в оптимальный по критериям надежности и безопасности режим.

Таким образом, система с предложенной структурой при отсутствии отказов будет обеспечивать надежную работу. При выявлении отказов приоритет отдается обеспечению безопасности.

Таблица 1

Выполнение контроллерами функций управления и защиты

Ситуация	ПЛК 1		ПЛК 2		ПЛК 3	
	Упр.	ПАЗ	Упр.	ПАЗ	Упр.	ПАЗ
Все ПЛК работоспособны	+	-	+	-	+	-
Отказ ПЛК 1			+	-	-	+
Отказ ПЛК 2	-	+			+	-
Отказ ПЛК 3	+	-	-	+		

Рассмотренный вариант был реализован в среде Step7 для ПЛК Simatic фирмы Siemens. На рис. 3 показан фрагмент реализации системы на языке релейно-контактной логики.

### Заключение

Рассмотренные структуры систем объединяют два классических подхода – мажоритарную схему и схему с системой противоаварийной защиты. Такой

вариант построения позволяет создавать системы с более высоким уровнем надежности и безопасности при относительно небольших затратах на реализацию функций адаптации.

В дальнейшем планируется проведение оценок уровней безопасности систем с различным числом каналов и схемами резервирования, а также доработка средств поддержки функций адаптации.

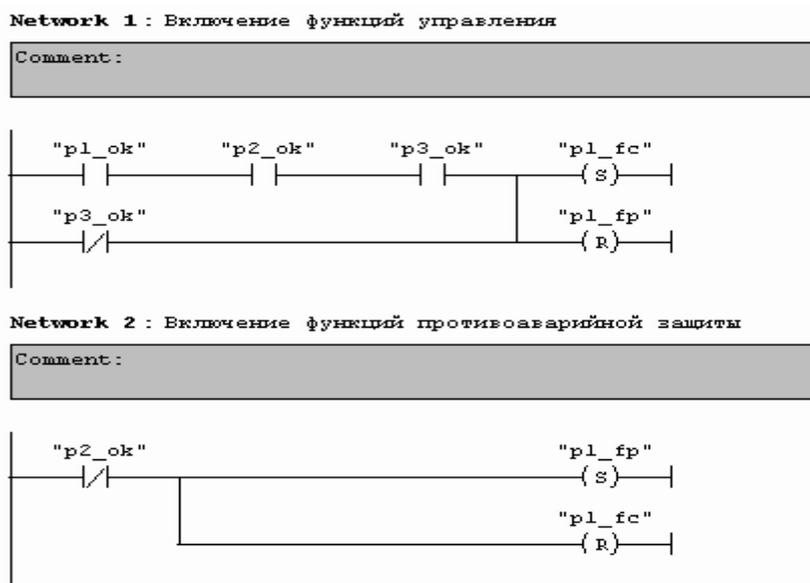


Рис. 3. Реализация адаптивной системы

## Литература

1. Громов В.С., Тимофеев В.Н. Структуры резервирования в АСУ ТП // Мир компьютерной автоматизации. – 2003. – №1. – С. 17-21.
2. Бабешко Е.В., Кривоносов А.И., Харченко В.С. Анализ возможностей современных ПЛК для построения отказоустойчивых АСУТП // Інформаційні інфраструктури та технології. – 2007. – №2. – С. 37-41.
3. Алексеев А.А., Алексеев В.А., Морозов А.И. Об использовании контроллеров противоаварийных защит в системах автоматизации объектов магистральных трубопроводов // Промышленные АСУ и контроллеры. – 2007. – №6. – С. 14-19.
4. Бабешко Е.В., Харченко В.С. Використання систем протиаварійного захисту як альтернативи резервуванню при автоматизації небезпечних виробництв // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. – Х.: ХНТУСГ, 2007. – Вип. 57. – С. 144-148.
5. Ядыкин И.В., Шумский В.М., Осепян Ф.А. Адаптивное управление непрерывными технологическими процессами. – М.: Энергоиздат, 1986. – 240 с.
6. Андриевский Б.Р., Фрадков А.Л. Избранные главы теории автоматического управления. – СПб: Наука, 1999. – 466 с.
7. Петров Б.Н., Рутковский В.Ю., Крутова И.Н., Земляков С.Д. Принципы построения и проектирования самонастраивающихся систем управления. – М.: Машиностроение, 1972. – 260 с.
8. Ким Д.П. Теория автоматического управления. Т. 2. Многомерные, нелинейные, оптимальные и адаптивные системы: Учеб. пос. – М.: ФИЗМАТЛИТ, 2004. – 464 с.
9. Воройский Ф.С. Информатика: Новый систематизированный толковый словарь-справочник (введение в современные информационные и телекоммуникационные технологии в терминах и фактах). – М.: ФИЗМАТЛИТ, 2003. – 760 с.
10. Основи надійності цифрових систем: Підручник. Рекомендовано Міністерства України // За ред. В.С. Харченка, В.Я. Жихарева. – Х.: ХАІ, 2004. – 573 с.

Поступила в редакцію 15.02.2008

**Рецензент:** д-р техн. наук, проф. В.М. Варталян, Национальний аерокосмічний університет ім. Н.Е. Жуковського «ХАІ», Харків.