УДК 681.324:519.613

К.Е. ГЕРАСИМЕНКО, В.И. ХАХАНОВ

ПОВЫШЕНИЕ ТЕСТОПРИГОДНОСТИ КРИТИЧЕСКИХ СИСТЕМ УПРАВЛЕНИЯ

Разрабатывается и тестируется на прикладных примерах метод повышения тестопригодности оборудования защит из состава управляющей системы безопасности АЭС. Отличительной особенностью метода от существующих [1-16] является использование функциональных элементов защит, построенных на базе арифметических операций, без использования логических операций и операций отношения. Это позволяет контролировать работоспособность данных элементов по их реакции на изменения входного непрерывного сигнала от канала ввода в АЦП через все элементы защит, в которых используется данный сигнал, до дискретного выходного элемента, формирующего команду защиты на конкретный исполнительный механизм. Данный метод позволяет обеспечить контроль и диагностирование целого ряда неисправностей типа «несрабатывание», относящихся к категории скрытых в существующих реализациях оборудования защит, которіе используют логические операции и операции отношения.

1. Введение

Одним из основных показателей, характеризующих надежность оборудования защит из состава управляющих систем безопасности (УСБ) атомных электростанций (АЭС), является вероятность правильного выполнения дискретной функции по формированию последовательности команд защитных действий с учетом наличия отказов типа “несрабатывание”. Критерием такого вида отказа является отсутствие команды защиты при наличии «исходного» события, т.е. при появлении на входах оборудования защит УСБ любой совокупности данных, которая должна вызвать формирование команды.

Для введения в специфику языка, определенного стандартами, техническими условиями, эволюцией технической диагностики, как науки, занимающейся развитием теории и практики восстановления работоспособности вычислительных систем, рассмотрим следующие понятия и определения [17].

Модель – структура элементов и/или процессов, с определенной степенью адекватности описывающая объект и/или явление. Логический анализ – процесс определения логического состояния линий объекта, или его компонентов при наличии или отсутствии неисправностей в условиях существования частичной неопределенности в компонентах: модель, входные воздействия, реакции.

Техническое состояние – совокупность исправного и всех неисправных состояний. Логическое состояние характеризуется значениями сигналов на линиях объекта при наличии или отсутствии неисправностей. В качестве объекта исследования выступает вычислительная система, компьютер, цифровое устройство и их модели, описанные в виде конечных автоматов. Эквивалентным является понятие – объект тестирования – Unit Under Test (UUT). Компоненты UUT: логические элементы, интегральные микросхемы, примитивные элементы. Последние характеризуются наличием таблицы переходов (истинности) и отсутствием структуры. Объект тестирования – изделие или его составные части, техническое состояние которых подлежит определению. Диагностирование – процесс определения технического состояния с заданной точностью.

Дефект – каждое отдельное несоответствие изделия требованиям нормативной документации. Повреждение – вид дефекта, определяемый событием, заключающимся в нарушении исправного состояния при сохранении работоспособного. Несущественный дефект – событие, заключающееся в нарушении работоспособного состояния при сохранении состояния правильного функционирования. Отказ – событие, заключающееся в нарушении состояния правильного функционирования. Техническое состояние объекта – совокупность исправного и множества наперед заданных неисправных состояний. Исправным называется состояние объекта, при котором он соответствует всем требованиям нормативно-технической документации. Неисправным называется состояние объекта при наличии в

нем дефекта. Работоспособным называется состояние объекта, при котором он может выполнять свои функции при наличии повреждения. Состояние объекта, при котором он может выполнять свои функции при наличии несущественного дефекта, называется состоянием правильного функционирования. Состояние неправильного функционирования определяется объектом, имеющим отказ. Если объект имеет катастрофические отказы или морально устарел на данный момент времени, его техническое состояние определяется как предельное или не подлежащее техническому обслуживанию. Контроль (проверка) – определение технического состояния объекта с точностью до исправного (работоспособного) и множества неисправных (неработоспособных).

2. Постановка задачи исследования

Ввиду того, что отказ типа «несрабатывание» для УСБ в целом может быть причиной возникновения нештатной ситуации или аварии, разработка методов контроля и диагностирования, позволяющих выявлять такого рода отказы, является актуальной задачей и предметом различного рода исследований и конструкторских решений. В общем случае к отказам УСБ данного типа могут приводить комбинации как однотипных (отказы по общей причине), так и разнотипных видов скрытых неисправностей в резервированных компонентах УСБ, имеющих временную корреляцию [1-9].

Применительно к типовой структуре УСБ, наличие скрытых неисправностей на несрабатывание означает, что в элементах оборудования защит (электронных компонентах, блоках, программном обеспечении), реализующих алгоритмические функции, скрытая неисправность типа «несрабатывание» гарантировано может быть обнаружена не в момент ее возникновения, а только при появлении комбинации входных сигналов, соответствующих срабатыванию защиты.

Данная проблема актуальна для всех типов оборудования, реализующего дискретные функции, независимо от используемой элементной базы и принципов построения: аналоговые приборы на транзисторах или реле, программно-логические интегральные схемы (ПЛИС), микропроцессоры с инструкциями в виде программного кода.

Цель исследования – существенное уменьшение времени подготовки тестовых данных для совместного (concurrent) анализа в рабочем режиме логических схем управления критическими системами.

Задачи: 1) Обзор существующих методов совместного тестирования систем управления критическими объектами. 2) Разработка моделей и методов совместного тестирования систем управления. 3) Верификация совместного тестирования систем управления моделями критических объектов.

3. Модели процесса тестирования

Предлагаются технологичные и эффективные процесс-модели тестирования диагностирования функциональных нарушений в цифровых системах [18-19]. Используются регистровые или матричные (табличные) структуры данных, которые ориентированы на параллельное выполнение логических операций при поиске дефектных компонентов систем управления критическими объектами.

Проблема синтеза или анализа компонентов произвольной структуры может быть сформулирована в виде взаимодействия на основе симметрической разности (xor-операции на булеане) в кибернетическом пространстве ее модели F с входными воздействиями T и реакциями L: $f(F,T,L)=\varnothing \rightarrow F\Delta T\Delta L=\varnothing$.

Киберпространство – совокупность взаимодействующих по метрике информационных процессов и явлений, использующих в качестве носителя компьютерные системы и сети. В частности, компонент пространства представлен k-мерным вектором (кортежем) $a=(a_1,a_2,...,a_j,...,a_k)$, $a_j=\{0,1\}$ в двоичном алфавите. Нуль-вектор есть k-мерный кортеж, все координаты которого равны нулю: $a_j=0, j=\overline{1,k}$. Метрика β кибернетического (двоичного) пространства определяется единственным равенством, которое формирует нуль-вектор для xor-суммы расстояний d_i между ненулевым и конечным числом точек (объектов), замкнутых в цикл: $\beta=\overset{n}{\underset{i=1}{\oplus}} d_i=0.$

Расстояние (по Хэммингу) между двумя объектами (векторами) a и b определяется в виде производного вектора: $d_i = d(a,b) = a_j \overset{k}{\underset{j=1}{\oplus}} b_j$. Иначе: метрика β векторного логического двоичного пространства есть равная нуль-вектору xor-сумма расстояний между конечным числом точек (вершин) графа, образующих цикл. Сумма n-мерных двоичных векторов, задающих координаты точек цикла, равна нуль-вектору. Данное определение метрики оперирует отношениями, что позволяет сократить систему аксиом с трех до одной и распространить ее действие на любые конструкции n-мерного киберпространства. Классическое задание метрики для определения взаимодействия одной, двух и трех точек в векторном логическом пространстве является частным случаем β-метрики при $i = 1,2,3$ соответственно:

$$M = \begin{cases} d_1 = 0 \leftrightarrow a = b; \\ d_1 \oplus d_2 = 0 \leftrightarrow d(a,b) = d(b,a); \\ d_1 \oplus d_2 \oplus d_3 = 0 \leftrightarrow d(a,b) \oplus d(b,c) = d(a,c). \end{cases}$$

Метрика β кибернетического многозначного пространства, где каждая координата вектора (объекта) определена в алфавите, составляющем булеан на универсуме примитивов мощностью p: $a_j = \{\alpha_1, \alpha_2, ..., \alpha_r, ..., \alpha_m\}, m = 2^p$, есть равная $\varnothing$-вектору (по всем координатам) симметрическая разность расстояний между конечным числом точек, образующих цикл: $\beta = \overset{n}{\underset{i=1}{\Delta}} d_i = \varnothing$. Равенство пустому вектору симметрической разности покоординатного теоретико-множественного взаимодействия подчеркивает равнозначность компонентов (расстояний), формирующих уравнения, где единственная координатная операция $d_{i,j} \Delta d_{i+1,j}$, используемая, например, в четырехзначной модели Кантора, определяется соответствующей Δ-таблицей:

Δ	0	1	x	$\varnothing$
0	$\varnothing$	x	1	0
1	x	$\varnothing$	0	1
x	1	0	$\varnothing$	x
$\varnothing$	0	1	x	$\varnothing$

$\cap$	0	1	x	$\varnothing$
0	0	$\varnothing$	0	$\varnothing$
1	$\varnothing$	1	1	$\varnothing$
x	0	1	x	$\varnothing$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$

$\cup$	0	1	x	$\varnothing$
0	0	x	x	0
1	x	1	x	1
x	x	x	x	x
$\varnothing$	0	1	x	$\varnothing$

a	0	1	x	$\varnothing$
$\tilde{a}$	1	0	$\varnothing$	x

.

Здесь также приведены таблицы истинности для других базовых теоретико-множественных операций, далее используемых по тексту. Число примитивных символов, образующих замкнутый относительно теоретико-множественных координатных операций алфавит, может быть увеличено. При этом мощность алфавита (булеана) определяется выражением $m = 2^p$, где p – число примитивных символов. Введенная метрика представляет не только теоретический интерес, но имеет и практическую направленность на обобщение и классификацию задач технической диагностики путем создания модели xor-отношений на множестве из четырех основных компонентов. Процедуры синтеза тестов, моделирования неисправностей и поиска дефектов можно свести к xor-отношениям на графе (рис. 1) полного взаимодействия четырех вершин (функциональность, устройство, тест, дефекты) $G = \{F, U, T, L\}$.

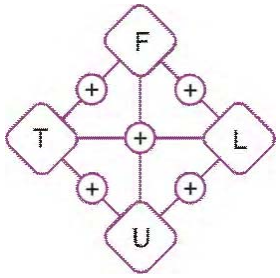

Рис. 1. Граф взаимодействия компонентов технической диагностики

Такой граф порождает четыре базовых треугольника, которые формируют 12 практически полезных триад отношений, формулирующих задачи технической диагностики:

$T \oplus F \oplus L = 0$	$T \oplus L \oplus U = 0$	$T \oplus F \oplus U = 0$	$F \oplus L \oplus U = 0$
1) $T = F \oplus L$	4) $T = L \oplus U$	7) $T = F \oplus U$	10) $F = L \oplus U$
2) $F = T \oplus L$	5) $L = T \oplus U$	8) $F = T \oplus U$	11) $L = F \oplus U$
3) $L = T \oplus F$	6) $U = T \oplus L$	9) $U = T \oplus F$	12) $U = F \oplus L$

Введение вершины U в граф взаимодействия компонентов технической диагностики расширяет функциональные возможности модели, появляются новые свойства полученной системы. Введение в структуру новой вершины должно иметь весомые аргументы в пользу ее целесообразности. Что касается представленного на рис. 1 графа, содержательно все задачи можно классифицировать в группы следующим образом. Группа 1 – теоретические эксперименты (на модели функциональности), без устройства: 1) Синтез теста по модели функциональности для заданного списка неисправностей. 2) Построение модели функциональности на основе заданного теста и списка неисправностей. 3) Моделирование неисправностей функциональности на заданном тесте. Группа 2 – реальные эксперименты (на устройстве), без модели функциональности: 4) Синтез теста путем физической эмуляции дефектов в устройстве. 5) Определение списка неисправностей устройства при выполнении диагностического эксперимента. 6) Верификация теста и дефектов в эксперименте на реальном устройстве. Группа 3 – тестовые эксперименты (верификация), без дефектов: 7) Синтез теста путем сравнения результатов моделирования модели и реального устройства. 8) Синтез функциональности по реальному устройству и заданному тесту. 9) Верификация теста и модели функциональности относительно реального устройства с существующими неисправностями. Группа 4 – эксперименты в процессе функционирования, на рабочих воздействиях: 10) Проверка правильности поведения реального устройства на существующих или заданных дефектах. 11) Проверка работоспособности устройства относительно существующей модели в процессе функционирования. 12) Верификация функциональности и списка дефектов относительно поведения реального устройства.

Наиболее популярными задачами из перечисленного выше списка являются: 1, 3, 5, 8, 9. Можно ввести и другую классификацию типов задач, которая дает возможность определить на графе $G = (F, U, T, L)$ все концептуальные пути решения целевых проблем: синтеза тестов, определения модели функциональности, генерирования модели дефектов и проектирования устройства. Все конструкции, представленные в отношениях, обладают замечательным свойством обратимости. Компонент, вычисляемый с помощью двух других, может быть использован в качестве аргумента для определения любого из двух исходных. Потому здесь можно говорить о транзитивной обратимости каждой триады отношений на полном графе, когда по двум любым компонентам всегда и однозначно можно восстановить или определить третий. При этом формат представления каждого компонента должен быть одинаковым по форме и размерности (векторы, матрицы). На основе предложенной метрики и моделей тестирования далее рассмотрены более подробно методы диагностирования дефектов или функциональных нарушений. Модель поиска функциональных нарушений в системе использует уравнение пространства $f(F, T, L, U) = 0 \rightarrow F \oplus T \oplus L \oplus U = 0$, которое трансформируется к виду $L = (T \oplus F) \oplus (T \oplus U)$. Диагностирование дефектов (функциональных нарушений) сводится к сравнению результатов модельного $(T \oplus F)$ и натурного $(T \oplus U)$ экспериментов, которое формирует список функциональных нарушений L, присутствующих в объекте диагностирования. Формула-модель процесса поиска блока F_i с функциональными нарушениями сводится к выбору решения посредством определения xor-взаимодействия между тремя компонентами: $L = F_i \leftarrow [(T \oplus F_i) \overset{p}{\underset{i=1}{\oplus}} (T \oplus U_i)] = 0.$

Одним из эффективных и технологичных подходов решения проблемы тестирования является метод сигнатурного анализа. Его математическая основа – получение остатка (сигнатуры) от деления сколь угодно длинной конечной двоичной последовательности на

определенное двоичное число (образующий полином). Практическое решение такой задачи сводится к использованию регистра сдвига с обратными связями из разрядов 7,9,12,16, которые заведены совместно с линией X, являющейся входом сигнатурного анализатора, на сумматор по модулю 2, как показано на рис. 2.

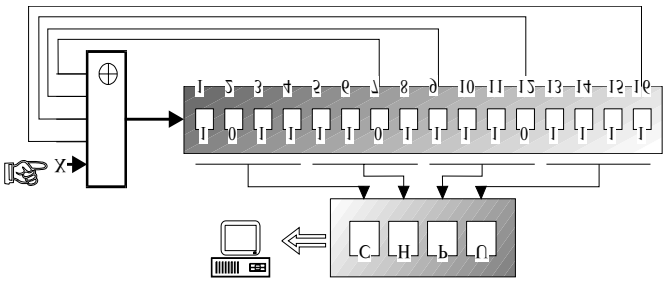

Рис. 2. Структура сигнатурного анализатора

После подачи двоичной последовательности на вход X полученный код-сигнатура состояний разрядов регистра с вероятностью P=0,9998 отображает исходный входной вектор произвольной длины. Триггеры регистра априорно должны быть обнулены. Идентификация двоичного вектора длиной не более 2^{16} выполняется с вероятностью P=1. Для удобства 16-разрядная двоичная сигнатура записывается в шестнадцатеричном алфавите (0,1,...,9,A,C,F,H,P,U) четырьмя символами, которые служат паспортом для каждого вывода микросхемы или внешних контактов разъема при выполнении тестового диагностирования. Сигнатура контакта, полученная в виде реакции на заданный тест без наличия в схеме неисправностей, называется эталонной. Если в реальном объекте экспериментальная сигнатура на контакте не равна эталонному значению, то рассматриваемый контакт или его предшественники подозреваются неисправными. Количество полных циклов подачи теста для поиска дефекта с использованием сигнатурного анализа в худшем случае может быть равно числу контрольных точек для снятия зондом анализатора экспериментальных сигнатур, расположенных на логическом пути от неисправного выхода до входа. Для уменьшения времени цикла подача теста осуществляется на частотах, близких к рабочим реального ЦУ. Понятие сжатой двоичной последовательности можно использовать в качестве входного слова для входов логических элементов цифровой системы управления. В данном случае имеется структура, представленная на рис. 3, где аналоговые сигналы от датчиков $T = (T_1, T_2, ..., T_i, ..., T_n)$ критической системы преобразуются блоком ADC (Analog Digital Coder) в цифровой код произвольной, но фиксированной длины.

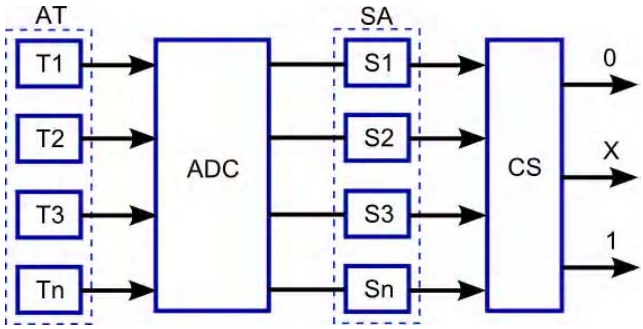

Рис. 3. Структура проверки исправности

Затем двоичные последовательности сжимаются в сигнатуры $T = (S_1, S_2, ..., S_i, ..., S_n)$, которые подаются на входы логического устройства управления (CS – Control System). При этом достигается вероятность P = 0,9998, что две различные последовательности будут иметь одинаковые сигнатуры на различных входах или на двух соседних тактах. Платой за быстродействие такой системы контроля является аппаратурная избыточность в виде системы сигнатурных анализаторов на всех входах CS. При этом состояния выходов CS определяются на алфавите $A = \{0,1, X = (S_1, S_2, ..., S_j, ..., S_m)\}$, где S_j – шестнадцать битов

двоичного слова, которые интерпретируются как мантисса, определенная в открытом интервале $[0 < S_j < 1]$. Таким образом, естественные флуктуации аналоговых датчиков трансформируются в шестнадцатеричные сигнатуры, которые подаются на логическую схему, где каждая (входная, выходная) переменная есть регистровая, фиксирующая практически любые изменения на аналоговых терминалах, что дает возможность контролировать работоспособность логической структуры управления критическими объектами. Следует также добавить, что неоднородность битовой информации в сигнатуре (слове) позитивно влияет на активизацию выходов, что дает возможность практически в каждом цикле съема информации из терминальных устройств отслеживать работоспособность системы управления критическими объектами.

4. Технологии тестирования систем управления критических объектов

Существующие методы решения данной проблемы, описаны в [10-14] и сводятся к проверке работоспособности элементов оборудования защит путем контроля их реакции на специальные тестовые воздействия, поскольку использование данных о рабочих воздействиях от объекта, как правило, недостаточно. Данные методы реализуют контроль работоспособности на срабатывание либо отдельных блоков и устройств, участвующих в реализации функции защит, либо всего оборудования защит или его части (как минимум инициирующей части защит). Методы обоих типов имеют ряд существенных ограничений и недостатков, подробно рассмотренных и проанализированных в [15].

При этом основное ограничение вытекает из самой структуры элементов оборудования защит («сравнение с эталоном», «и», «или», «2 из 4-х»), построенных на базе дискретных функций, с выходом, определяемым только двумя состояниями 0 (режим ожидания) или 1 (срабатывание защиты). Это в принципе не позволяет обеспечить выполнение непрерывного контроля работоспособности данных элементов на срабатывание. Метод, предполагающий изменение структуры элементов защит, как средство повышения эффективности контроля (проверки) и диагностирования скрытых неисправностей на несрабатывание, предложен в [15, 16]. Основная идея данного метода – функциональный элемент защит на базе арифметических операций формирует значение на всем диапазоне от 0 до 1. При этом в нем отсутствуют какие-либо ветвления (условные переходы), определяющие отличия режима ожидания от режима срабатывания защит. Функция работает одинаково в обоих из этих режимов, что позволяет непрерывно контролировать работоспособность соответствующего функционального элемента. Все функции, которые используются в элементах, строятся на базе арифметических операций (сложение, вычитание, умножение, деление), без применения логических операций и операций отношения, за исключением выходных пороговых элементов формирования команд на исполнительные механизмы (ИМ), что связано с физическими принципами работы приводов ИМ.

В настоящей статье представлены результаты дальнейшего исследования метода, предложенного в [15, 16], в части его теоретического обоснования.

5. Модель процесса совместного тестирования

На рис. 4 представлена концептуальная схема контроля и диагностирования оборудования защит УСБ на базе функциональных элементов, использующих арифметические операции. Здесь $f(x)$ – функция на базе арифметических операций; $fd(x)$ – функция на базе логических операций и операций отношения; Min-Max – диапазон изменения значения технологического параметра; 0-1 – диапазон изменения значений в элементах на базе арифметических операций; 0/1 – дискретные значения (0 или 1) в элементах на базе логических операций и операций отношения; (- - - -) – цифровые каналы передачи данных и команд; (——) – нецифровые каналы передачи данных и команд. Основная идея метода – использование в диагностическом оборудовании (В) идентичных ему защит (А) функциональных элементов (блоков), реализованных в программном коде. При этом как в оборудование защит, так и в диагностическое оборудование поступают функционально-идентичные входные данные (переменные). С помощью арифметических операций обеспечивается возможность вычисления рассогласования по каждой выходной переменной в каждом функциональном блоке, при этом различие сигналов вычисляется в самом диагностическом оборудовании.

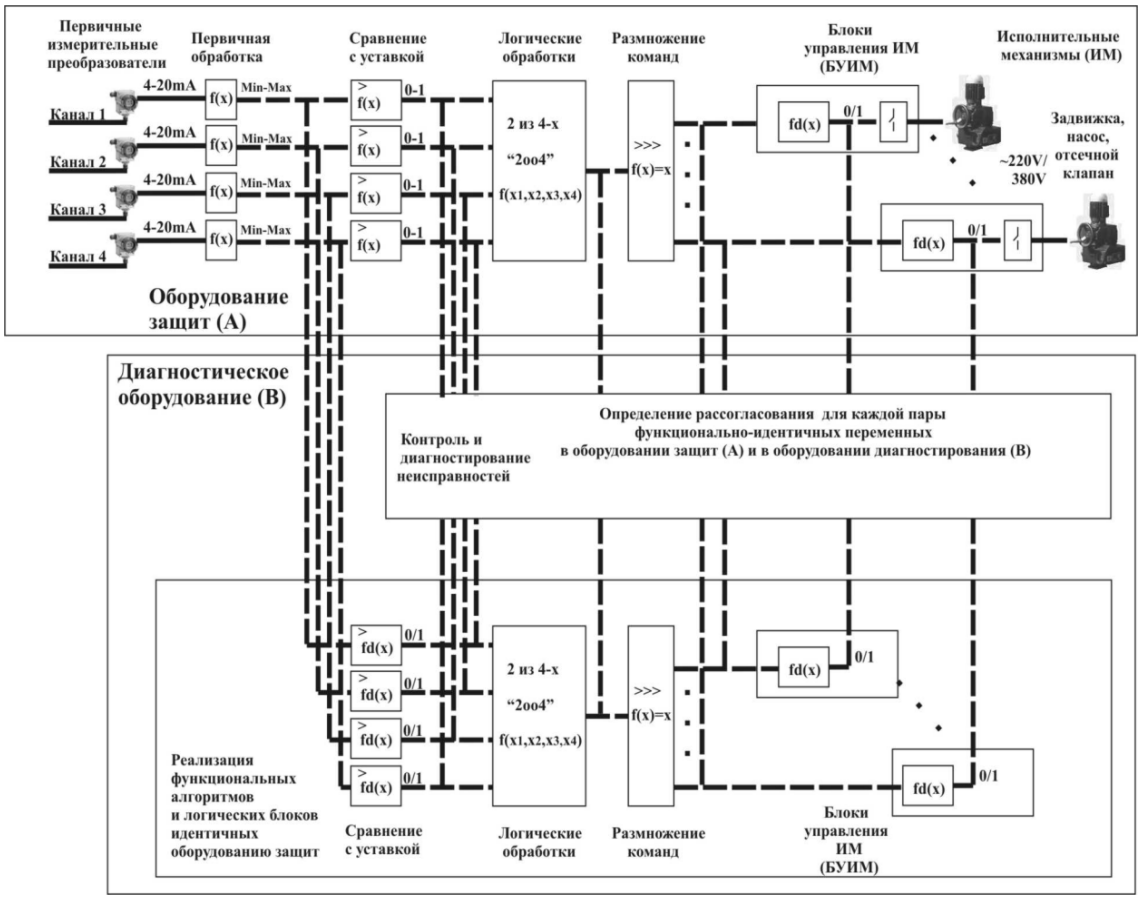

Рис. 4. Концептуальная схема контроля и диагностирования оборудования защит УСБ

Теоретическое обоснование метода может быть сведено к следующим ключевым моментам: 1) разработка базовых функциональных элементов, использующих арифметические операции и позволяющих комбинировать все остальные типы элементов, применяемые в алгоритмах защит; 2) обоснование наличия реакции каждого функционального элемента (изменение его выходного значения) при изменении любого входного непрерывного сигнала, в пределах разрешающей способности АЦП, имеющего корреляцию с данными функциональными элементами по условиям проектных алгоритмов (т.е. обоснование «прохождения» изменения от канала ввода в АЦП через все элементы защит, в которых участвует данный сигнал, до дискретного выходного элемента, формирующего команду защиты на конкретный исполнительный механизм).

Для функциональных элементов сравнения с эталоном («>=», «<=»), использующих операции отношения, реализация с применением арифметических операций может быть представлена в форме линейной функции вида:

$$y = ax + b\ ,\ «>=»: y = \frac{(x - p_2)}{(p_1 - p_2)}\ ,\ «<=»:\ y = \frac{(p_2 - x)}{(p_2 - p_1)}\ ,$$

$$a = \frac{1}{(p_1 - p_2)}\ ,\ b = \frac{-p_2}{(p_1 - p_2)}\ ,\ x\ \in R\ ,\ y \in R_{0-1} = [0;1],$$

где a, b – коэффициенты масштабирования (постоянные); p_1 – пороговое значение (эталона); p_2 – предел диапазона измерения, противоположный знаку эталона.

Для функциональных элементов «не», «и», использующих логические операции, реализация с применением арифметических операций может быть представлена как линейная функция следующего вида:

$$\text{«не»: } y = 1 - x,$$

$$\text{«и»: } y = (1/n)*(x_1 + x_2 + ... + x_n),$$

$$x_1,....,x_n, y \in R_{0-1} = [0;1].$$

Все остальные функциональные элементы, использующие логические операции («или», «2 из 4»), могут быть скомбинированы при помощи базовых «не» и «и».

С учетом линейности базовых функциональных элементов, применяющих арифметические операции, аналитическое выражение, описывающее состояние любого i-го элемента в алгоритме защит, может быть представлено как:

$$y_i = a_0 + a_1 x_1 + a_2 x_2 + ... + a_n x_n, \quad (1)$$

где x_i – значение внешних входных переменных (входные непрерывные сигналы); y_i – значение выхода i-го элемента в алгоритме защит (промежуточного, внутри алгоритма или выходного, в форме выходной команды на механизм).

С учетом зависимости от времени выражение (1) может быть переписано так:

$$y_i(t) = a_0 + a_1 x_1(t) + a_2 x_2(t) + ... + a_n x_n(t). \quad (2)$$

С учетом (2) «прохождение» (отклик) изменения по входным непрерывным сигналам между моментами времени t-1 и t на выходе любого функционального элемента может быть представлено так:

$$\Delta y_i(t) = a_0 + a_1 \Delta x_1(t) + a_2 \Delta x_2(t) + ... + a_n \Delta x_n(t). \quad (3)$$

В случае изменения между моментами времени t-1 и t значения только одного входного непрерывного сигнала из n всех возможных (изменения по остальным входным сигналам равны 0) выражение (3) может быть преобразовано в следующий вид:

$$\Delta y_i(t) = a_k \Delta x_k(t),$$

$$\Delta x_1(t) = \Delta x_2(t) = ... = \Delta x_{k-1}(t) = \Delta x_{k+1}(t) = ... = \Delta x_n(t) = 0. \quad (4)$$

Формула (4) описывает аналитическое выражение для зависимости между величиной изменения входного непрерывного сигнала Δx_k и соответствующего ему изменения выхода функционального элемента, имеющего корреляцию с данным входом по условиям проектного алгоритма защит УСБ. Последнее теоретически подтверждает возможность контроля и диагностирования всех функциональных элементов оборудования защит УСБ за счет наличия реакции («отклика») данных элементов (изменение их выходов) при изменении значений соответствующих входных сигналов, в том числе за счет наличия постоянно присутствующих «технологических» и «электрических» шумовых колебаний.

Проведем анализ предлагаемого метода на примере одной из 4-канальных защит САОЗ в соответствии с рис. 5 при наличии неисправности в элементе оборудования, реализующем функцию мажоритарной обработки “2oo4” (2 из 4-х).

Строки схемы, относящиеся к части А, соответствуют значениям переменных в оборудовании защит, а аналогичные строки (с подстрокой рассогласования) в части В соответствуют значениям этих же переменных, но в диагностическом оборудовании. При этом рассматриваемая неисправность в элементе мажоритарной обработки “2oo4” (2 из 4-х) характеризуется формированием выходного значения, не соответствующего входным значениям от 4-х каналов (значение на выходе 0,6256995 меньше номинального 0,8256995, т.е. того, которое должно быть при соответствующей комбинации входных значений). Данный тип неисправности может привести к отказу оборудования защит типа «несрабатывание по требованию» при наличии исходного события и поэтому является наиболее критичным в

части влияния на безопасность. Как следует из рис. 5, признак неисправности “fault” сформирован до наступления исходного события, по результату рассогласования значений выходных переменных функционального блока мажорирования “2oo4” (2 из 4-х) в оборудовании защит (А) с одной стороны и оборудовании диагностирования (В) – с другой.

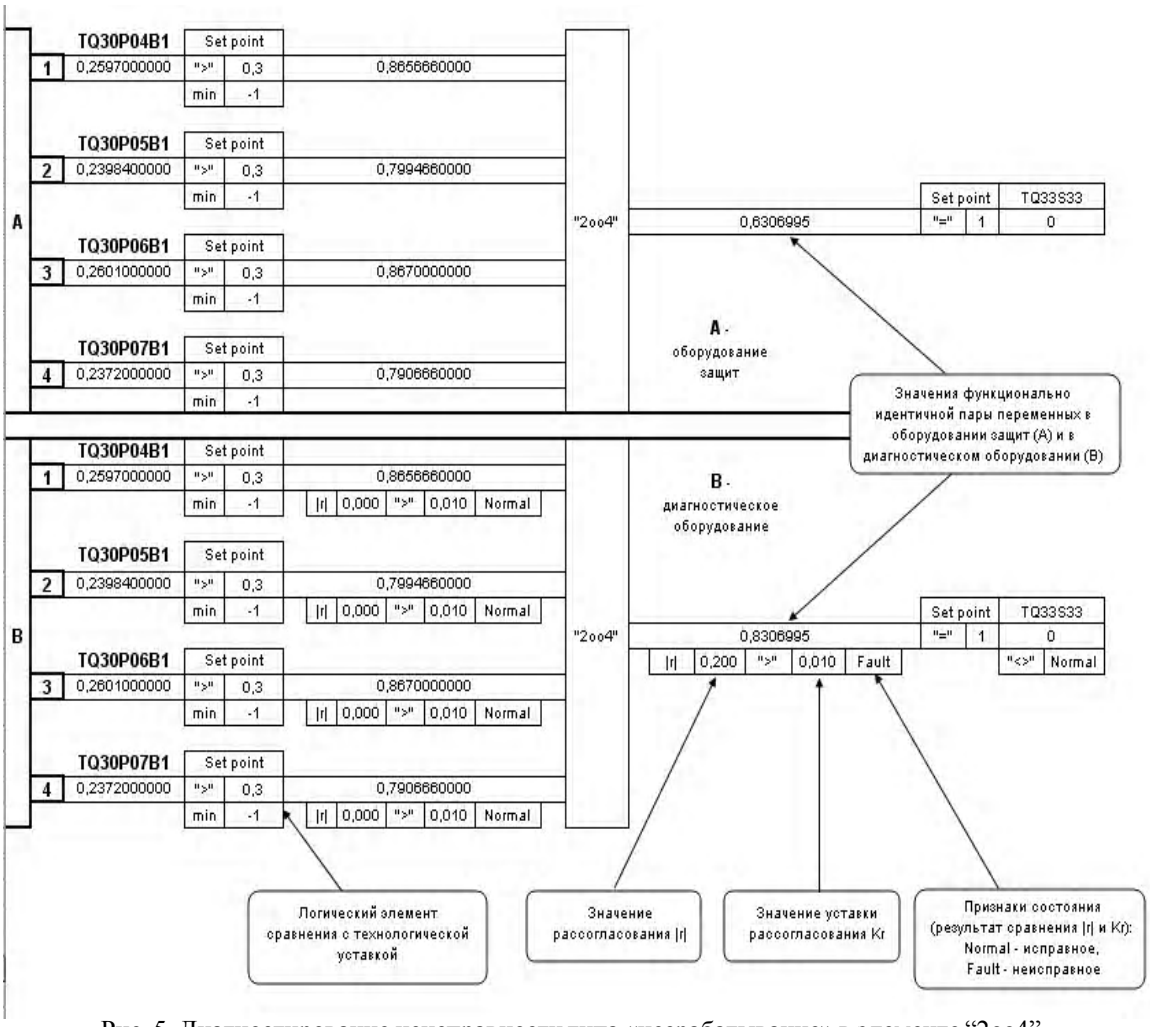

Рис. 5. Диагностирование неисправности типа «несрабатывание» в элементе “2oo4” («2 из 4-х») оборудования защит УСБ (4-канальная защита САОЗ по давлению >0,3 кгс/см2)

6. Заключение

Разработанный метод повышения тестопригодности оборудования защит, использующий функциональные элементы на базе арифметических операций, характеризуется такими особенностями:

1) Обеспечивает проверку и диагностирование следующих видов скрытых неисправностей типа «несрабатывание»: дефекты функциональных элементов, характеризуемые несоответствием значений входных и выходных переменных проектному или конструкторскому алгоритму функционирования (с учетом предыстории входных, выходных значений, в случае наличия «памяти» в алгоритме функционального элемента); неисправности связей между функциональными элементами, характеризуемые отсутствием или искажением данных между источником и приемником.

2) Повышение тестопригодности обеспечивается за счет использования в функциональных элементах оборудования защит только арифметических операций (сложение, вычитание, умножение, деление) без применения логических операций и операций отношения.

3) Метод обеспечивает контроль прохождения любого изменения значения входного сигнала, в пределах разрешающей способности используемых АЦП, от входа через все функциональные элементы («сравнение с эталоном», «и», «или», «2 из 4»), в которых

участвует данный сигнал, до дискретного элемента управления исполнительным механизмом.

4) Предложена сигнатурная структура контроля работоспособности логической схемы управления критическими объектами, основанная на преобразовании естественных флуктуаций аналоговых датчиков в шестнадцатеричные сигнатуры, подаваемые на логическую схему, где каждая (входная, выходная) переменная есть регистровая, активизирующая практически любые изменения от входов до выходов.

Список литературы: **1.** *Безопасность* атомных станций. Информационно-управляющие системы / М.А. Ястребенецкий, В.Н. Васильченко, С.В. Виноградская и др. К.: Техника, 2004. 470 с. **2.** *Instrumentation* and control systems important to safety in Nuclear Power Plants: Nuclear Energy Series / International Atomic Energy Agency. Vienna: IAEA, 2002. No. NS-G-1.3. 91 p. **3.** *Safety* of Nuclear Power Plants: Design, Safety Standards Series / International Atomic Energy Agency. Vienna: IAEA, 2000. No. NS-R-1. 125 p. **4.** Software for Computer Based Systems Important to Safety in Nuclear Power Plants: Safety Standards Series / International Atomic Energy Agency. Vienna: IAEA, 2000. No. NSG-1.1. 150 p. **5.** *International* Electrotechnical Commission (IEC) 60880 – 2004, Nuclear Power Plants — Instrumentation and Control Systems Important to Safety — Software Aspects for Computer-Based Systems Performing Category A Functions. **6.** *International* Electrotechnical Commission (IEC) 60987 – 2007, Nuclear Power Plants – Instrumentation and Control Important to Safety – Hardware Design Requirements for Computer-Based Systems. **7.** *Institute* of Electrical and Electronic Engineers (IEEE) 7-4.3.2 , Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. **8.** *Макдональд Д.* Промышленная безопасность, оценивание риска и системы аварийного останова: Пер. с англ./ Д. Макдональд. М.: ИДТ, 2007. 409 с. **9.** *Смит Д.* Безотказность, ремонтопригодность и риск: Пер. с англ. / Д. Смит. М.: ИДТ, 2007. 432 с. **10.** *НП* 306.2.141-2008. Общие положения безопасности атомных станций. К: ГКЯРУ, 2008. 42 с. **11.** *Protecting* against common cause failures in Digital I&C Systems of Nuclear Power Plants: Nuclear Energy Series / International Atomic Energy Agency. Vienna: IAEA, 2009. No. NP-T-1.5. 65 p. **12.** *Ястребенецкий М.А.* Информационные и управляющие системы АЭС Украины: результаты и проблемы / М.А. Ястребенецкий // Проблемы обеспечения безопасности информационных и управляющих систем АЭС // Сб. науч. тр. Одесса: «Астропринт», 2010. С. 9-19. **13.** *Modern* Instrumentation and Control for Nuclear Power Plants: Technical Reports Series / International Atomic Energy Agency. Vienna: IAEA, 1999. No. 387. 629 p. **14.** *Application* of the Single Failure Criterion: Safety Series / International Atomic Energy Agency. Vienna: IAEA, 1990. No. 50-P-1. 134 p. **15.** *Герасименко К.Е.* Методы непрерывного контроля и диагностирования оборудования управляющих систем безопасности энергоблоков АЭС по функции защит / К.Е. Герасименко // Радіоелектронні і комп'ютерні системи. 2010. №3 (44). С. 152-156. **16.** *Герасименко К.Е.* Использование непрерывных функций в элементах оборудования защит АЭС для диагностирования неисправностей типа «несрабатывание по требованию» / К.Е. Герасименко // Радіоелектронні і комп'ютерні системи. 2011. №1 (49). С. 29-33. **17.** *Бондаренко М.Ф., Кривуля Г.Ф., Рябцев В.Г., Фрадков С.А., Хаханов В.И.* Проектирование и диагностика компьютерных систем и сетей. К.: НМЦ ВО. 2000. 306 с. **18.** *Хаханов В.И., Литвинова Е.И., Чумаченко С.В., Гузь О.А.* Логический ассоциативный вычислитель // Электронное моделирование. 2011. № 1(33). С. 73-89. **19.** *Hahanov V., Wajeb Gharibi, Litvinova E., Chumachenko S.* Information analysis infrastructure for diagnosis // Information an international interdisciplinary journal. 2011. Japan. Vol.14. № 7. P. 2419-2433.

Поступила в редколлегию 16.12.2011

Герасименко Константин Евгеньевич, заведующий отделом информационно-управляющих систем ЧАО «СНПО "Импульс"». Научные интересы: техническая диагностика цифровых систем управления объектами с повышенными требованиями к безопасности. Адрес: Украина, 93405, Северодонецк, пл. Победы 2, тел. 60194. E-mail: gerasymenko.k.e@yandex.ua.

Хаханов Владимир Иванович, декан факультета КИУ ХНУРЭ, д-р техн. наук, профессор кафедры АПВТ ХНУРЭ. Научные интересы: техническая диагностика цифровых систем, сетей и программных продуктов. Увлечения: баскетбол, футбол, горные лыжи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-326. E-mail: hahanov@kture.kharkov.ua.