УДК 621.039

ПОВЫШЕНИЕ НАДЕЖНОСТИ ЭКСПЛУАТАЦИИ АЭС НА ОСНОВЕ РЕАЛИЗАЦИИ ПРИНЦИПА РАЗНООБРАЗИЯ

Е.В. Андропов*, И.Р. Коган, В.П. Поваров***, Л.П. Павлов*****

** ООО «Московский завод Физприбор»*
142110, Московская обл., г. Подольск, ул. Парковая, д. 2
*** АО «Атомэнергопроект», 105005, г. Москва, ул. Бакунинская, д. 5, стр.1.*
**** Филиал ОАО «Концерн Росэнегоатом», «Нововоронежская атомная станция»*
396071, Воронежская обл., г. Нововоронеж, промышленная зона Южная, 1

АСУ ТП строящихся энергоблоков должны быть защищены от отказов по общей причине, обусловленных ошибками в программном обеспечении (ПО). Защита от ошибок по общей причине в соответствии с ГОСТ Р-МЭК 60880-2011 может быть обеспечена только применением принципа разнообразия. В проекте АСУ ТП блока № 1 Нововоронежской АЭС-2 применены программно-технические комплексы в системах как нормальной эксплуатации, так и безопасности. В то же время инициирующая часть подсистем аварийной и предупредительной защит реактора, которая реализована на программно-технических средствах TELEPERM XS, не защищена от отказов, вызванных возможными ошибками в ПО.

Для исключения отказа в работе управляющих систем безопасности по общей причине в проекте реализованы дополнительные меры, исключающие отказ выполнения функций систем безопасности из-за отказа программного обеспечения.

Приводятся описание проблемы, базовые направления реализации принципа разнообразия для уменьшения вероятностей отказов оборудования, оценки показателей надежности в соответствии с рекомендациями НТЦ ЯРБ, описание диверсной системы защит (ДСЗ) и ее структура. Анализируется структура алгоритма ДСЗ по управлению исполнительными механизмами на примере защиты парогенератора. Разбирается схема взаимодействия штатной и диверсной систем защит.

На основании опыта использования ДСЗ на Нововоронежской АЭС-2 делаются выводы о практической реализации системы защит реакторной установки и необходимости анализа последствий совместного функционирования инициирующей части управляющей системы безопасности по технологическим параметрам и ДСЗ с возможной корректировкой алгоритмов.

Ключевые слова: отказ по общей причине, программное обеспечение, управляющие системы безопасности, диверсная система защит, алгоритмы защит.

ВВЕДЕНИЕ

Автоматизированная система управления технологическими процессами (АСУ ТП) предназначена для

– контроля и управления основными и вспомогательными технологическими процессами производства тепло- и электроэнергии на АЭС и обеспечения экономичности ра-

боты АЭС в условиях нормальной эксплуатации;

– обеспечения безопасности во всех режимах работы, как нормальной эксплуатации, так и аварийных ситуаций.

К современным АСУ ТП предъявляются такие требования, как высокий уровень автоматизации, внедрение цифровых управляющих систем, углубленная диагностика оборудования, использование экрана коллективного пользования.

Основой АСУ ТП АЭС-2006 являются программируемые технические средства. Они применяются и в управляющих системах безопасности (СБ), и в системах нормальной эксплуатации (СНЭ). Блочный пункт управления (БПУ) реализован на унифицированных программно-технических средствах системы верхнего блочного уровня (СВБУ). Применение цифровых технологий при построении АСУ ТП АЭС-2006 позволило получить ряд преимуществ по сравнению с предыдущим поколением системы (самодиагностика, надежность, повышение точности, доступность в процессе эксплуатации). Централизация контроля и управления осуществляется с мониторов рабочих станций на БПУ и резервном щите управления (РПУ). Резервирование управления с панелей РПУ осуществляется в полном объеме для СБ и в достаточно минимальном объеме для СНЭ.

Наряду с преимуществами использования программируемых технических средств возрастает тяжесть последствий в случае отказа систем АСУ ТП по общей причине (ООП) в результате ошибок в программном обеспечении (ПО). ООП относятся к отказам системы, возникающим в результате дефектов в функциональных требованиях, проектах системы или программного обеспечения [1].

Для снижения требований к надежности отдельных инструментальных программ при их выборе могут быть рассмотрены принципы «защиты в глубину» и разнообразие, принятые для архитектуры контроля и управления.

Российские и международные нормативные документы однозначно указывают, что надежную защиту от ООП, связанных с возможными ошибками в ПО, можно реализовать только на основе принципа разнообразия.

Разнообразие – наличие двух или более путей или средств достижения установленной цели – специально создается как защита от ООП. Оно может быть достигнуто наличием систем, которые физически отличаются одна от другой, или с помощью функционального разнообразия, если аналогичные системы достигают установленной цели различными путями.

В АЭС-2006 не защищена от ООП, вызванных возможными ошибками в ПО, инициирующая часть подсистем аварийной и предупредительной защит реактора, которые реализованы на одних программно-технических средствах TELEPERM XS (TXS) фирмы Siemens**.**

Для снижения вероятности отказа по общей причине рекомендуется применять сочетание программируемой и непрограммируемой техники [2].

После событий на АЭС Фукусима (Япония) надзорные органы ряда стран существенно ужесточили требования по выполнению действующих нормативно-технических документов (НТД) в области безопасности АЭС, включая вопросы разнообразия и глубокоэшелонированной защиты.

Согласно проекту АСУ ТП АЭС-2006 [3], управляющая система безопасности по технологическим параметрам (УСБТ) реализована на программируемых технических средствах.

Замечание экспертного заключения ФБУ НТЦ ЯРБ [4] к ПООБ НВАЭС-2 [5]: «проект аварийной защиты реактора, представленный в ПООБ, в части технических средств не удовлетворяет принципу разнообразия, так как инициирующая часть двух комплектов подсистем аварийной и предупредительной защит реактора реализована на одних программно-технических средствах TXS (отступление от требования п. 4.4.5.7 ОПБ-88/97)».

ПОВЫШЕНИЕ ВЕРОЯТНОСТИ БЕЗОТКАЗНОЙ РАБОТЫ ОБОРУДОВАНИЯ ПРИ ВОЗНИКНОВЕНИИ ОТКАЗА ПО ОБЩЕЙ ПРИЧИНЕ

Разнообразие специально создается как защита от ООП. В соответствии с глоссарием МАГАТЭ разнообразие – это наличие двух или более резервных систем или компонентов, выполняющих определенную функцию, когда системы или компоненты имеют различные параметры, уменьшающие возможность отказа по общей причине. Примерами таких параметров являются условия эксплуатации, принципы работы или проектные группы (представляют функциональное разнообразие); конфигурация оборудования, производители и виды оборудования (используют различные методы обеспечения физического разнообразия) [6].

Анализ требований NUREG/CR-7007 «Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems» [7] («Методы обеспечения разнообразия в АСУ ТП АЭС») с учетом опыта проектирования УСБТ АЭС позволяет выделить шесть базовых направлений реализации принципа разнообразия: функциональное, параметрическое, проектное (архитектурное и алгоритмическое), определяемое человеческим фактором, аппаратное, программное.

В УСБТ АЭС-2006 реализованы в разной степени все принципы разнообразия кроме программного. На сегодня оценок показателей надежности ПО и убедительных доказательств невозможности отказа нет.

Оценка программной продукции, надежность ПО – это набор атрибутов, относящихся к способности ПО сохранять свой уровень качества функционирования при установленных условиях за установленный период времени [8].

Согласно [9, 10], ООП ПО определяется как результат множественных отказов, не выявляемых при проверках, который надо относить к запроектной аварии (ЗПА).

Для реализации принципа разнообразия как одного из направлений по преодолению ООП необходимо наличие независимой от системы АЗ-УСБТ системы защиты, реализованной на других технических средствах, которую называют диверсной (ДСЗ). Эта система должна обеспечивать перевод энергоблока в контролируемое и безопасное состояние для различных проектных исходных событий.

Решение о применении разнообразия (диверсификации) принималось с учетом положений [1]: «Меры проекта по предотвращению отказа по общей причине связаны с архитектурой систем контроля и управления, которая включает в себя, по крайней мере, две системы контроля и управления, выполняющие функции категории А. Доказательство того, что любая индивидуальная система контроля и управления не имеет ошибок, невозможно, и поэтому существование скрытых дефектов и связанных с ними механизмов срабатывания не может быть исключено в принципе.»

В связи с этим ООП ПО постулирована как запроектная ситуация, и принято решение о ее преодолении с вводом в проект ДСЗ.

ДСЗ в случае отказа инициирующей части системы АЗ-УСБТ или исполнительной части системы АЗ по общей причине должна обеспечивать выполнение следующих основных функций безопасности при наступлении проектных исходных событий режимов категории 2, 3, 4:

– аварийная остановка реактора и поддержание его в подкритическом состоянии;

– аварийный отвод тепла от реактора;

– удержание радиоактивных веществ в установленных границах.

ИСХОДНЫЕ ДАННЫЕ

Для определения объема компенсирующих мероприятий организациями главного конструктора РУ (ОКБ ГП) и научного руководителя (РНЦ КИ) выполнен анализ исходных событий с наложением ООП, приводящих к ЗПА с наиболее тяжелыми последствиям с точки зрения выполнения функций безопасности и не удовлетворяющих критери-

ям приемки для запроектных аварий без плавления топлива. Определены необходимые исполнительные механизмы, работу которых должны инициировать дополнительные сигналы. Разработаны алгоритмы диверсных защит для выполнения всех функций безопасности, действующих на останов реактора и реализующих функции УСБТ. Выполнены поверочные расчеты последствий развития исходного события с ООП с учетом работы дополнительных алгоритмов ДСЗ и действий персонала.

Разработано и обосновано 15 алгоритмов, реализация которых удовлетворяет критериям приемки, предъявляемым для запроектных аварий без плавления топлива в случае отказа по общей причине проектной СУЗ-УСБТ. Выбраны технические средства (непрограммируемые) для реализации ДСЗ.

Значение вероятности отказа на требование при совместной работе СУЗ-УСБТ и ДСЗ с учетом отказа ПО в двух комплектах и наложением отказа датчиков или устройств размножения сигналов в одном канале СБ составило $4.74 \cdot 10^{-7}$. Предельное значение этого показателя в соответствии с техническим заданием составляет $5 \cdot 10^{-7}$.

Для двух комплектов программируемых средств УСБТ при проведении расчетов показателей надежности в соответствии с рекомендациями НТЦ ЯРБ принята вероятность отказа 10^{-5}.

ХАРАКТЕРИСТИКИ ДСЗ [6, 11, 12]

В каждом канале СБ устанавливается по одному одинаковому комплекту ДСЗ. В состав каждого комплекта входят по три шкафа комплекса средств автоматизации (КСА) ДСЗ производства ООО «Московский завод Физприбор».

КСА ДСЗ предназначен для

– ввода и обработки аналоговых и дискретных сигналов от первичных преобразователей (датчиков) и смежных систем (аппаратуры контроля нейтронного потока, панелей БПУ);

– реализации функций защит на непрограммируемых средствах;

– выдачи сигналов для представления на блочном пункте управления и в СВБУ энергоблока информации о контролируемых параметрах и состоянии частей комплекса.

Для выполнения функций, возложенных на КСА ДСЗ с учетом требований [13 – 15], использовались следующие инновационные подходы:

– реализация алгоритмов защиты на непрограммируемых средствах (логических вентилях, счетчиках, регистрах и т.п.) без использования микроконтроллеров и ПЛИС любой степени интеграции;

– цифровая обработка аналоговых сигналов непрограммируемыми средствами (преобразование шкал, фильтрация, 50 Гц, демпфирование, линеаризация, компенсация температуры холодного спая, необходимая коррекция значений параметров) с помощью табличной обработки на микросхемах энергонезависимой памяти;

– периодическая автоматизированная проверка (опробование) основной доли оборудования, включая проверку алгоритмов, внутрисистемных линий связи, линий связи с исполнительными механизмами, непрограммируемыми средствами;

– резервирование (троирование) не только датчиков, но и аппаратных средств реализации алгоритмов защит с возможностью опробования оборудования без вывода его из эксплуатации и без потери функции защит на работающем энергоблоке;

– использование внутренней резервированной локальной сети и резервированной сети связи с информационно-управляющей системой энергоблока для выдачи информации о дискретных и аналоговых сигналах, срабатывании системы, состоянии технических средств (при этом невозможность влияния программируемых сетевых средств на средства непрограммируемой логики обеспечивается аппаратно).

Встроенные средства проверки обеспечивают диагностику от выходов датчиков до линий связи с модулями управления исполнительными механизмами, входящими в УСБТ.

Канал защит (в каждом шкафу) запитан от источника как постоянного, так и переменного тока.

Формирование логики «два из трех» защит на останов реактора производится на входных клеммниках двух выключателей прерывания питания ОР СУЗ по переменному и двух по постоянному току.

Формирование логики «два из трех» защит инициирующей части УСБТ производится в шкафах КСА и проводными связями передается в существующую исполнительную часть УСБТ, ПТК приоритетного управления (ПТК ПУ) на модули приоритетного управления (МПУ) исполнительными механизмами. Один МПУ управляет одним механизмом. Для исключения отказов МПУ по общей причине внутри них реализован принцип разнообразия.

Распределение приоритетов выполнения команд защит УСБТ, реализованных в МПУ в порядке убывания:

– автоматическое управление от TXS (штатная работа при отсутствии отказа);
– от ДСЗ (при отказе TXS при невыдаче команд);
– от ключей БПУ, РПУ;
– от систем управления нормальной эксплуатации.

При срабатывании ДСЗ так же, как и при срабатывании TXS, налагается 30-минутный запрет на выполнение команд оператора.

Для выполнения команд защит на останов реактора команды от TXS и ДСЗ равноприоритетны.

В качестве источников аналоговых параметров для TXS и ДСЗ используются существующие датчики. Для исключения влияния работы TXS и ДСЗ выполнено гальванически разделенное размножение сигналов на имеющихся в составе СУЗ-УСБТ непрограммируемых модулях гальванического разделения в шкафах УГРС.

Такое решение было принято для обеспечения строгой последовательности работы вначале защиты на TXS, при отсутствии отказа, затем ДСЗ из-за того, что уставки срабатывания защит TXS и ДСЗ отличаются незначительно. В случае использования различных датчиков не исключается возможность срабатывания ДСЗ раньше TXS, что может спровоцировать оператора на неправильные действия.

Например, в СУЗ-УСБТ уставка аварийной защиты по уровню в парогенераторах составляет $H_{ном}$ = 650 мм, а в ДСЗ – $H_{ном}$ = 700 мм. Отличие составляет менее трех погрешностей измерения, что при разных датчиках может привести к нарушению последовательности работы систем.

Таким образом, основной причиной использования общих датчиков является необходимость обеспечения последовательности срабатывания вначале СУЗ-УСБТ, затем ДСЗ при исправности обеих систем.

В части выполнения функции АЗ системы ДСЗ и СУЗ-УСБТ равноприоритетны. По отношению к управлению системами безопасности приоритет отдан командам СУЗ-УСБТ. В соответствии с алгоритмами ДСЗ формирует команды на обесточивание приводов СУЗ для останова реактора, локализацию гермообъема и ввод в работу системы пассивного отвода тепла (СПОТ).

Реализация функций защиты на непрограммируемых средствах позволяет исключить из рассмотрения непредсказуемую надежность ПО и влияние на функцию защиты аспектов информационной безопасности. Расчеты надежности возможны для непрограммируемых технических средств, в том числе с учетом ООП, и невозможны для ПО.

СТРУКТУРА СИСТЕМЫ

Структура системы (рис. 1) предусматривает резервирование (троирование) не только датчиков, но и аппаратных средств реализации алгоритмов с возможностью опробования оборудования без вывода его из эксплуатации и без потери функции защит на работающем энергоблоке.

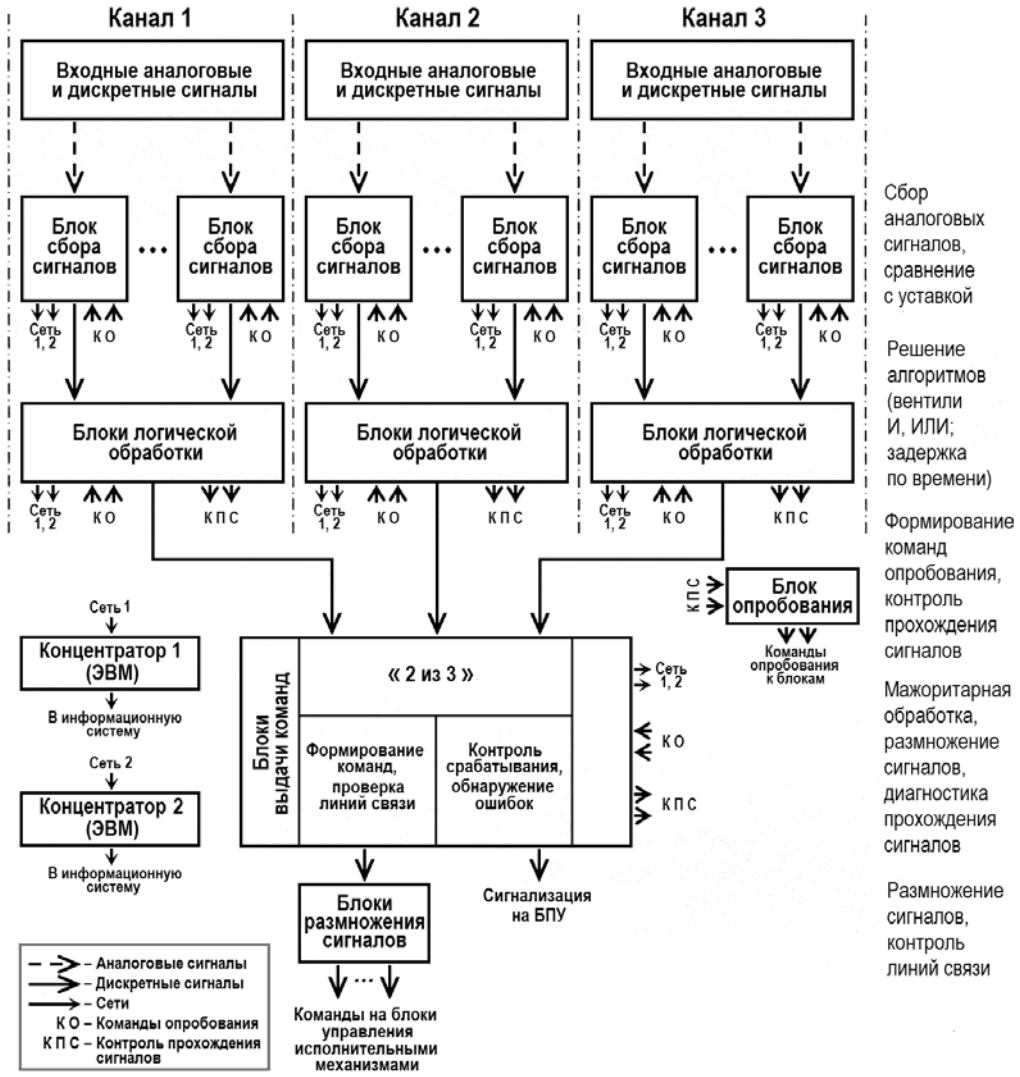

Рис. 1. Структурная схема КСА ДСЗ

Блоки сбора сигналов осуществляют ввод сигналов от датчиков (первичных преобразователей) и смежных систем.

Блоки сбора аналоговых сигналов на непрограммируемых средствах обеспечивают

– ввод сигналов термопар, термометров сопротивления, унифицированных токовых сигналов;

– преобразование шкал, фильтрацию помехи промышленной частоты (50 Гц);

– демпфирование (с постоянной времени, настраиваемой в диапазоне 50 мс – 10 с индивидуально для каждого входа блока);

– линеаризацию сигналов по стандартным (или нестандартным по согласованию с заказчиком) номинальным статическим характеристикам термопар и термометров сопротивлений (тип характеристики и диапазон сигналов задаются индивидуально для каждого входа блока);

– компенсацию температуры холодного спая термопар, коррекцию показаний уровнемеров;

– сравнение с уставкой на повышение или понижение с регулируемой зоной возврата (зона возврата задается индивидуально для каждой уставки и может быть любой

в пределах диапазона входных сигналов);

– при необходимости питание датчиков с индивидуальной гальванической развязкой источников питания.

Вычисление рассогласований аналоговых сигналов и контроль диапазонов сигналов осуществляются программируемыми средствами с помощью микроконтроллеров функциональных блоков и концентраторов (промышленных ЭВМ).

Сбор дискретных сигналов от аппаратуры контроля нейтронного потока предусматривает ввод сигналов типа «сухой контакт» с обеспечением питания датчиков.

Логическая обработка сигналов предусматривает

– мажоритарную обработку по логике «2 из 3» («2 из 4»);

– использование функций И, ИЛИ, НЕ;

– выдержку времени.

Каждый из аналоговых сигналов вводится от трех одноименных датчиков в три шкафа ДСЗ.

Результаты сравнения с уставкой из каждого шкафа раздаются в два других шкафа и подвергаются в каждом шкафу мажоритарной обработке «2 из 3» (в блоках мажоритарной логики «2 из 3», логической обработке и в блоках управления силовыми ключами) для формирования команды на обесточивание ОР СУЗ. Сформированные команды поступают на силовые ключи – «сухие» контакты (блоки силовых ключей). Указанная обработка реализована в трех шкафах одинаково. На силовых ключах реализована мажоритарная обработка «2 из 3».

РЕАЛИЗАЦИЯ ДСЗ

Пример структуры алгоритма ДСЗ по управлению исполнительными механизмами на примере защиты парогенератора показан на рис. 2.

Каждый из аналоговых сигналов вводится от трех одноименных датчиков в три шкафа ДСЗ. В шкафах ДСЗ каждый сигнал подвергается обработке: фильтрации помехи частотой 50 Гц, демпфированию, коррекции уровня, компенсации температуры холодного спая, сравнению с уставкой с учетом зоны возврата.

Результаты сравнения с уставкой из каждого шкафа раздаются в два других шкафа и подвергаются в каждом шкафу мажоритарной обработке «2 из 3» и логической обработке для формирования команды. Указанная обработка реализована в трех шкафах одинаково.

Сформированные команды поступают на блоки выдачи команд (БВК). Команда на выходе БВК формируется по логике «два из трех» на схеме шести ключей (оптореле). Команда размножается на несколько модулей приоритетного управления (МПУ) на диодном размножителе блоков размножения сигналов БРС. Один выход БРС подключается к одному или более МПУ.

Сбор аналоговых и дискретных сигналов с технических средств комплекса для их выдачи в информационную систему энергоблока через две взаиморезервирующие локальные сети осуществляют микроконтроллеры, встроенные в функциональные блоки.

Локальные сети работают под управлением двух взаиморезервирующих концентраторов – промышленных ЭВМ. Концентраторы установлены непосредственно в шкафах комплекса. Концентраторы реализуют следующие программные функции:

– сбор и обработку сигналов от оборудования ДСЗ по двум взаиморезервирующим локальным сетям;

– проверку рассогласования одноименных аналоговых сигналов, проверку диапазонов сигналов с целью обнаружения отказов узлов аналого-цифрового преобразования блоков и (или) датчиков;

– формирование диагностических сообщений о состоянии аппаратных и программных средств комплекса;

– передачу в информационную систему энергоблока информации о состоянии технологического процесса и технических средств.

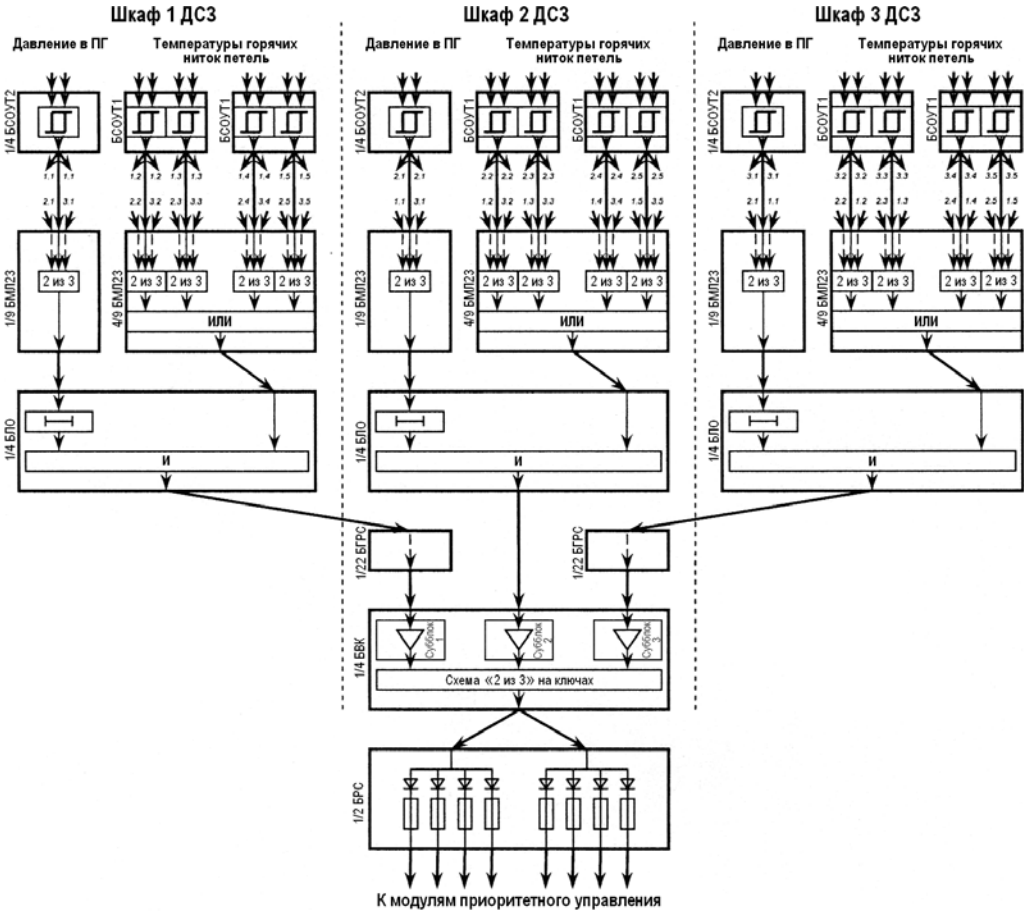

Рис. 2. Структура алгоритма ДСЗ по управлению исполнительными механизмами

ПРАКТИЧЕСКИЙ РЕЗУЛЬТАТ ПРИМЕНЕНИЯ ПРИНЦИПА РАЗНООБРАЗИЯ

Схема взаимодействия штатной и диверсной систем защит показана на рис. 3.

В качестве исполнительного механизма для снятия напряжения с ОР СУЗ используются выключатели с двумя независимыми соленоидами. На каждый соленоид действует команда от одного комплекта ДСЗ. Выключатели, управляемые ДСЗ (отличающиеся по конструкции от штатных), включены последовательно со штатными выключателями. Таким образом, действия команд на останов реактора от защит ДСЗ и штатной СУЗ равноприоритетны. Формирование команды на отключающий соленоид по логике «два из трех» производится проводными связями из шести команд из блоков силовых ключей (по два из каждого канала) на клеммах соленоида.

Управление исполнительными механизмами осуществляется через имеющиеся модули приоритетного управления, причем более высокий приоритет имеют команды штатной СУЗ-УСБТ. Так как уставки срабатывания защит штатной УСБТ ниже уставок работы защит ДСЗ, то при отсутствии отказа по общей причине управление осуществляется от штатной УСБТ, а при ее отказе – от ДСЗ.

ОПЫТ ВВОДА ДСЗ В ЭКСПЛУАТАЦИЮ

Реализация ДСЗ на Нововоронежской АЭС-2 происходила в исключительно сжатые сроки.

Все работы, начиная от выпуска «Технического решения о разработке и внедрении дополнительной диверсной системы защит на энергоблоках № 1 и № 2 Нововоронежской АЭС-2» от 30.12.2014, по определению поставщика, изготовлению оборудования,

проведению заводских испытаний, выполнению монтажа, проведению ПНР, внесению изменений в смежные системы (СУЗ-УСБТ, АКНП, СВБУ, БПУ), в проектную и эксплуатационную документацию выполнены за 13 месяцев.

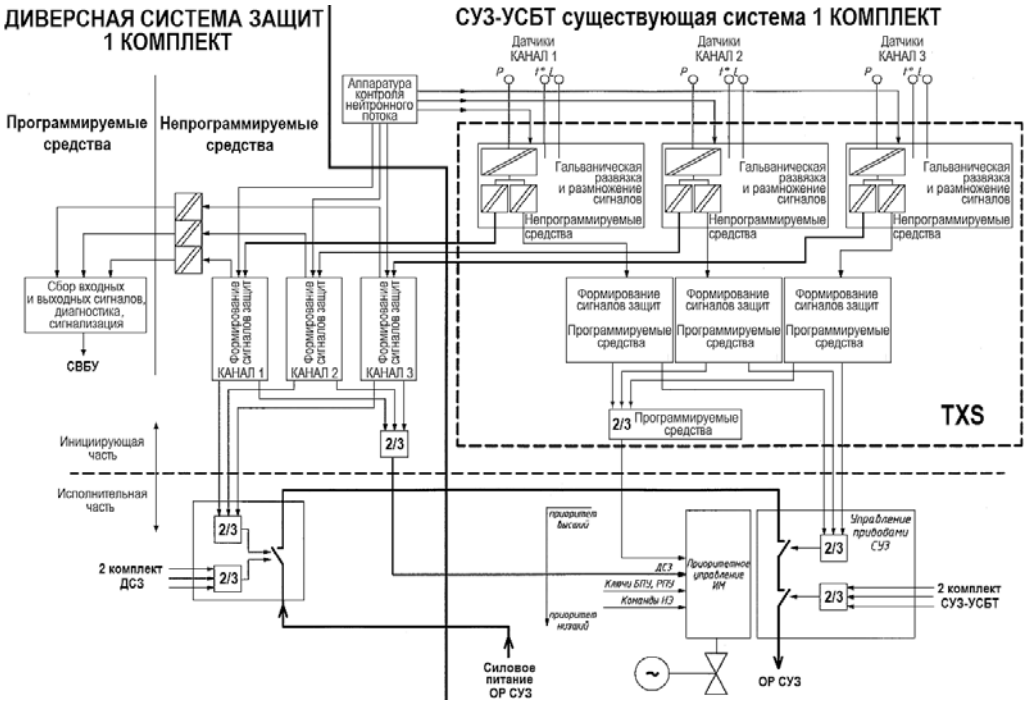

Рис. 3. Схема взаимодействия штатной и диверсной систем защит

Вследствие отказа регулятора уровня в компенсаторе давления (система нормальной эксплуатации) из-за дебаланса подпитки-продувки по факту снижения уровня в компенсаторе давления менее 4 м 12.07.2016 г. произошло срабатывание аварийной защиты (функция штатной СУЗ-УСБТ). При дальнейшем снижении уровня в компенсаторе давления менее 3.6 м сработала ДСЗ. В соответствии с алгоритмами произошло отключение всех ГЦНА, подключение к ПГ 1 – 4 СПОТ и началось расхолаживание реакторной установки. При расхолаживании реакторной установки сработали «разрывная» защита инициирующей части штатной АЗ-УСБТ, изоляция парогенераторов по пару и питательной воде, 30-минутный запрет на действия оператора. Хотя все действия штатной СУЗ-УСБТ и ДСЗ были направлены на обеспечение безопасности, результат их совместных действий потребовал большее количество операций и, соответственно, времени на перевод энергоблока в исходное состояние.

ВЫВОДЫ

1. В первоначальном проекте ВВЭР-2006 была не защищена от отказов по общей причине, вызванных возможными ошибками в ПО, инициирующая часть подсистем АЗ-УСБТ и предупредительной защит реактора, которая реализована на одних программно-технических средствах TELEPERM XS.

2. Защита от ошибок по общей причине может быть обеспечена только применением принципа разнообразия.

3. Реализация принципа разнообразия в виде создания ДСЗ, реализованной без применения ПО, является эффективным средством преодоления ООП.

4. Необходимо провести анализ последствий совместного функционирования инициирующей части АЗ-УСБТ, реализованной на TXS и ДСЗ во всем диапазоне инициирую-

щих их работу параметров при отсутствии отказов в работе TXS и ДС3. При необходимости провести корректировку алгоритмов.

Литература

1. ГОСТ Р-МЭК 60880-2011 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А». – М.: Стандартинформ, 2011. – 147 с.

2. *Алпеев А.С.* Надежность программного обеспечения управляющих систем и безопасность атомных станций. // Надежность. – 2015. – № 4. – С. 75-77.

3. *Аркадов Г.В., Дунаев В.Г., Боженков О.Л.* Российские АСУ ТП АЭС сегодня: через сотрудничество – к прогрессу. // Ядерные измерительно-информационные технологии. – 2009. – № 2. – С. 4-21.

4. Экспертное заключение ФБУ НТЦ ЯРБ ДНП-5-2088/1-2012. – М.: НТЦ ЯРБ, 2012. – 4 с.

5. *Швыряев Ю.В., Морозов В.Б., Токмачев Г.В., Байкова Е.В., Чулухадзе В.Р., Федулов М.В.* Использование вероятностного анализа при обосновании безопасности АЭС-2006, проектируемой для площадки Нововоронежской АЭС. // Атомная энергия. – 2009. – Т. 106. – № 3. – С. 123-129.

6. *Алпеев А.С.* Диверсные защиты. Обеспечение разнообразия при проектировании аварийных защит атомных станций. // Ядерная и радиационная безопасность. – 2015. – № 2 (76). – С. 11-14.

7. NUREG/CR-7007 «Diversity Strategies for Nuclear Power Plant Instrumentation and Control Sys-tems». ORNL/TM-2009/302. – U.S. NRC, Washington, DC, 2010. – 230 p.

8. ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению». – М.: Изд-во стандартов, 1994. – 10 с.

9. ГОСТ Р-МЭК 62340-2011. «Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине». – М.: Стандартинформ, 2012. – 18 с.

10. NUREG/CR-5497. «Common-Cause Failure Parameter Estimations», – U.S. NRC, Washington, DC, October, 1998. – 120 p.

11. *Андропов Е.В., Коган И.Р., Поваров В.П., Павлов Л.П.* Алгоритмизация управления диверсной системой комплексной защиты блоков АЭС. // Вестник Воронежского государственного технического университета. – 2015. – Т. 11. – № 5. – С. 51-58.

12. *Коган И.Р., Полетыкин А.Г., Промыслов В.Г., Жарко Е.Ф.* Эволюция АСУТП АЭС для ВВЭР, проблемы, нерешенные вопросы, новые угрозы и возможные направления развития. / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014) Сборник. – М.: ИПУ РАН, 2014. – С. 4200-4211.

13. Computer security at nuclear facilities reference manual. International Atomic Energy Agency. – Vienna, 2011. Электронный ресурс http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (дата доступа 20.06.2017).

14. НП-026-16. Федеральные нормы и правила в области использования атомной энергии. «Требования к управляющим системам, важным для безопасности атомных станций». – М.: Роспотребнадзор, 2016. – 30 с.

15. NS-G-1.1. Программное обеспечение систем, важных для безопасности, выполненных на основе компьютерной техники для атомных энергетических станций. – Вена: МАГАТЭ, 2000. – 89 с.

Поступила в редакцию 26.06.2017 г.

Авторы

Андропов Евгений Владимирович, зам. главного конструктора
E-mail: ogk@fizpribor.ru

Коган Исаак Рувимович, главный технический эксперт
E-mail: kogan_IR@aep.ru

Поваров Владимир Петрович, директор НВАЭС, канд. техн. наук
E-mail: PovarovVP@ nvnpp1.rosenergoatom.ru

Павлов Леонид Павлович, главный технолог
E-mail: PavlovLP@ nvnpp1.rosenergoatom.ru

UDC 621.039

NPP OPERATIONAL RELIABILITY IMPROVEMENT BASED ON THE DIVERSITY PRINCIPLE

Andropov E.V.*, Kogan I.R.**, Povarov V.P.***, Pavlov L.P.***

* LLC Moscow Plant Fizpribor.
2 Parkovaya str., Podolsk, Moscow reg., 142110 Russia
** JSC «Atomenergoproekt»,
7 Bakuninskaya str., build. 1, Moscow, 107996
***Branch of JSC «Concern Rosenergoatom» «Novovoronezh Nuclear Power Plant»
1 Promyshlennaya zona Yuzhnaya, Novovoronezh, Voronezh reg.,
396071 Russia

ABSTRACT

Automated Process Control Systems (APCS) of the power units under construction must be protected from common cause failures due to software errors. Protection from common cause failures in accordance with GOST R-IEC 60880-2011 can only be ensured by applying the diversity principle.

In the APCS design of the Novovoronezh NPP II-1, software and hardware complexes are used both in normal operation systems and in safety systems. At the same time, the initiating part of the reactor emergency and preventive protection subsystems based on the TELEPERM XS hardware and software is not immune from failures caused by possible errors in the software.

To exclude common cause failures of the control safety systems, the project provides for additional measures that eliminate failures of the safety systems due to the software failure.

Consideration is given to the problem description, basic directions of the diversity principle implementation to reduce the probability of equipment failures, evaluation of reliability indicators in accordance with the SSTC NRS recommendations as well as the description of the diverse protection system (DPS) and its structure. The structure of the DPS algorithm for controlling actuators is exemplified by the steam generator protection. The interaction scheme of normal and diverse protection systems is analyzed.

Based on the experience of using the DPS at the NvNPP II, conclusions are drawn about the practical implementation of the reactor plant protection system and the need to analyze the consequences of joint operation of the initiating part of the safety management system in terms of technological parameters and DPS with possible algorithm adjustments.

Key words: common cause failure, software, control safety systems, diverse protection system, protection algorithms.

REFERENCES

1. GOST R-IEC 60880-2011. Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions. Moscow. Standartinform Publ., 2011, 147 p. (in Russian)

2. Alpeev A.S. Software's reliability of the controlling systems and safety of nuclear power plants. *Nadyozhnost',* 2015, no. 4, pp. 75-77 (in Russian).

3. Arkadov G. V., Dunayev V.G., Bozhenkov O.L. Russian NPPs PCSs today: through cooperation to progress. *Yadernye izmeritel'no-informatsionnye tekhnologii.* 2009, no. 2, pp. 4-21 (in Russian).

4. Expert conclusion of FBU NTTs YaRB DNP-5-2088/1-2012. Moscow. NTTs YaRB Publ., 2012,

4 p. (in Russian).

5. Shvyryaev Yu.V., Morozov V.B., Tokmachev G. V., Baykova E.V., Chulukhadze V.R., Fedulov M.V. Use of the probability analysis in case of reasons for safety of AES-2006 projected for a site of the Novovoronezh NPP. Atomnaya energiya. 2009, v. 106, no. 3, pp. 123-129 (in Russian).

6. Alpeev A.S. Diversity protection. Support of diversity principle in case of design of abnormal protection for nuclear power plants. *Yadernaya i radiatsionnaya bezopsnost'*. 2015, no. 2 (76), pp. 11-14 (in Russian).

7. NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Sys-tems. ORNL/TM-2009/302. U.S. NRC, Washington, DC, 2010, 230 p.

8. GOST R ISO/IEC 9126-93. Information technology. Software product evaluation. Quality characteristics and guidelines for their use. Moscow. Izdatel'stvo Standartov Publ., 1994, – 10 p. (in Russian).

9. GOST R-IEC 62340-2011. «Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure». Moscow. Standartinform Publ., 2012, 18 p. (in Russian).

10. NUREG/CR-5497. Common-Cause Failure Parameter Estimations, U.S. NRC, Washington, DC, October, 1998, 120 p.

11. Andropov E.V., Kogan I.R., Cooks of V. P., Pavlov L.P. Algorithmization of operating of the diversity system of complex protection for NPP' units. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta*, 2015, v. 11, no. 5, pp. 51-58 (in Russian).

12. Kogan I.R., Poletykin A.G., Promyslov V.G., Zharko E.F. Evolution of the NPP PCS for VVER, problems, unresolved questions, new threats and the possible directions of development. Proc. of the XII All-Russian meeting on problems of control (VSPU-2014). Moscow. IPU RAN Publ., 2014. pp. 4200-4211 (in Russian).

13. Computer security at nuclear facilities reference manual. International Atomic Energy Agency Vienna, 2011. Available at http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf (accessed Jun 26 2017).

14. NP 026-16. Requirements for Control Systems Significant for Nuclear Power Plants' Safety. Moscow. Rospotrbnadzor Publ., 2016, 30 p. (in Russian).

15. NS-G-1.1. The Software of the Systems Important for Safety Executed on the Basis of the Computer Equipment for Nuclear Energetic Power Plants. Vienna, IAEA, 2000, 89 p.

Authors

Andropov Evgeny Vladimirovich, Deputy Chief Software Designer
E-mail: ogk@fizpribor.ru

Kogan Isaak Ruvimovich, Chief Technical Expert
E-mail: kogan_IR@aep.ru

Povarov Vladimir Petrovich, Deputy Director General of JSC «Concern Rosenergoatom», NvNPP Director, Cand. Sci. (Engineering)
E-mail: PovarovVP@ nvnpl.rosenergoatom.ru

Pavlov Leonid Pavlovich, NvNPP SG Chief Process Engineer
E-mail: PavlovLP@nvnpp1.rosenergoatom.ru