РАЗНООБРАЗИЕ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ АЭС

Зверков В.В.

НИЯУ МИФИ

Аннотация: Применение разнообразия кардинально повышает надежность СКУ в части безопасности АЭС, особенно в условиях формирования возможного отказа по общей причине (ООП). Учитывая огромное значение, которое придается этому обстоятельству в разработанных и будущих проектах АСУ ТП, рассматриваются более подробно основные технические решения в этой части. Материал предлагаемой статьи имеет, в основном, обзорный характер. Вместе с тем, при структурном построении СКУ предлагается учитывать наличие пассивных технологических систем безопасности.

Ключевые слова: Принцип разнообразия, отказ по общей причине, глубокоэшелонированнаязащита, программно-технические комплексы, функции безопасности, диверсная система защиты, пассивные системы безопасности.

Введение

В /1/ принцип разнообразия определяется как способ повышения надежности путем применения двух или более систем или элементов для выполнения одной функции безопасности, имеющих разные конструкции или принципы действия, с целью снижения вероятности ООП. Применение принципа разнообразия представляет собой по сути диверсификацию разрабатываемых решений. Поэтому в сложившейся практике программно-технические комплексы подсистем АСУ ТП, разработанные с использованием разнообразия, зачастую называют диверсными системами.

Предлагаемая статья имеет, в основном, обзорный характер. Вместе с тем, при структурном построении СКУ предлагается учитывать наличие пассивных технологических систем безопасности, которые выполняют свои функции без высоких требований к СКУ.

Основной причиной применения разнообразия в СКУ безопасности считается использование одинакового программного обеспечения, отказ которого в аппаратуре всех каналов и комплектов может сформировать ООП. В этой связи, использование аппаратуры с функциями «жесткой логики» при отсутствии программируемых элементов может служить основанием не использования принципа разнообразия.

Общие сведения

Разнообразие реализуется посредством измерения различных параметров для определения одной физической величины, использования различных аппаратных средств, логики голосования между каналами и алгоритмов срабатывания функции безопасности, использования различных исполнительных механизмов и регулирующих органов для обеспечения многократного обнаружения и выполнения защитных действий по каждому исходному событию. Принцип разнообразия дополняет принцип глубокоэшелонированной защиты и увеличивает вероятность того, что защита на каждом эшелоне будет приведена в действие в случае необходимости.

В современной отечественной и зарубежной НТД /2,3/ есть общее требование о необходимости применения принципа разнообразия в СКУ безопасности, но не устанавливаются способы, формы и места реализации этого принципа, что позволяет разработчикам самим определять эти условия. Степень реализации принципов разнообразия зависит от постулируемых отказов и возможных их последствий. Выбор степени реализации разнообразия учитывает результаты анализа надежности применяемых проектных, программных и технических решений, внутреннюю защиту от ООП применяемых программно-технических средств, физическое разделение комплектов систем безопасности и опыт проектирования других АЭС.

Известны следующие основные 4 типа разнообразия, которые используются при проектировании СКУ безопасности: алгоритмическое, функциональное, параметрическое и аппаратное. Наименее затратное и наиболее легкое в плане реализации – это алгоритмическое (проектное) разнообразие, которое связано с применением в аппаратуре различных методов обработки исходных данных. Но при этом сохраняются существенные риски ООП из-за применения одинаковых аппаратных и программных средств в разных комплектах аппаратуры. В этой связи использование аппаратуры или технических средств разных производителей для проектирования смешанных ПТК кардинальным образомрешает вопросы применения разнообразия в аппаратных и

программных средствах, резко снижает риски ООП и существенно повышает уровень безопасности АЭС.

Технология и алгоритмы диверсификации

Исходными данными для применения принципа разнообразия (диверсификации) служит два вида анализа безопасности: вероятностный анализ (ВАБ) и детерминистский анализ (ДАБ). ВАБ разрабатывается как качественная и количественная оценки уровня безопасности блока АЭС с целью подтверждения их соответствия установленным в /1/ вероятностным целевым показателям и выявления факторов, вносящих наибольший вклад в количественные показатели безопасности. ДАБ определены последовательности событий (сценарии), вызванных реакцией АС на возможные исходные события.

При всей важности обоих видов анализа, в разных странах разными разработчиками приоритет могут отдавать одному из видов анализа безопасности и в зависимости от этого принимаются разные решения. Например, если результаты ВАБ показывают, что вероятность ООП аппаратуры СКУ безопасности во всех каналах или комплектах меньше величины, установленной нормативными документами, то применение диверсификации технических решений не обязательно. Но при этом, всегда остаются вопросы погрешности расчетных методов ВАБа и исходных данных по надежности оборудования как основы этих методов. Поэтому, во многих случаях используют положения ДАБ, в соответствии с которыми применяют диверсные системы безопасности, не учитывая результаты ВАБ.

Конечной целью любой диверсификации решений в части СКУ является обеспечение работы технологических систем безопасности по выполнению предусмотренных алгоритмов в части управления проектными и запроектными авариями. И в этой связи принцип разнообразия иногда используют частично, в приложении к составлящим СКУ, обеспечивающие контроль и управление наиболее важными технологическими системами безопасности. В этих случаях диверсные системы защит используются на заключительных этапах аварийного управления при отказах ПТС СКУ на предыдущих этапах.

Разнообразие как одно из направлений по преодолению ООП, предусматривает альтернативное управление системами безопасности. Это управление обеспечивает преодоление запроектных аварий, связанных с наложением отказа по общей причине СКУ СБ на исходные события, которые потенциально могут привести к повреждению активной зоны. Оптимальным способом обеспечения надежности выполнения функций АЗ и УСБ является наличие независимой подсистемы диверсной защиты. Эта подсистема обеспечивает перевод энергоблока в контролируемое и безопасное состояние и реализуется обычно на технических средствах, отличающихся от средств, на которых построена основная подсистема АЗ-УСБИ. Диверсная подсистема защиты обеспечивает выполнение следующих основных функций безопасности: аварийная остановка реактора и поддержание его в подкритическом состоянии; аварийный отвод тепла от реактора; удержание радиоактивных веществ в установленных границах.

Примерный объем сигналов и логика формирования условий срабатывания подсистемы диверсной защиты для проекта «АЭС02006» приведены в таблице 1.

Основные структурные решения

- Функциональные области, где используется принцип разнообразия:
- Инициирование срабатывания АЗ-ПЗ СУЗ реактора.
- Инициирование срабатывания УСБ.
- Исполнительная часть АЗ-ПЗ.
- Исполнительная часть УСБ.

Структурные решения по применению принципа разнообразия зависят от ряда обстоятельств в части архитектурных решений АСУ ТП по функциональным областям и объема применяемых технологических систем безопасности. Например, есть проекты АСУ ТП с объединенными функциями инициирования АЗ-ПЗ и УСБ в одном ПТК, но есть проекты и с разнесенными функциями инициирования по разным ПТК. Иногда разработчик считает достаточным применить принцип разнообразия на заключительных этапах аварийного реагирования или ограничивается применением наиболее простого способа разнообразия - алгоритмического.

На рис.1 показано место диверсной системы защиты (ДСЗ) по функциям инициирования АЗ-УСБИ при объединении этих функций в одном ПТК. Из схемы следует, что основная часть

системы и ДСЗ получают информацию от одних и тех же датчиков и воздействуют на одинаковые исполнительные органы.

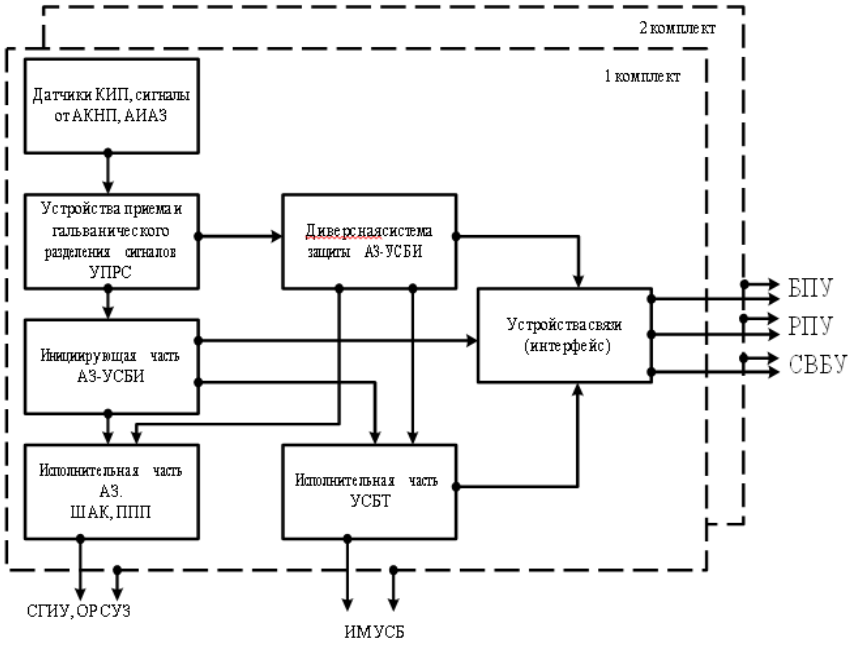

Рис. 1. Диверсная система защиты по функциям инициирования АЗ-УСБИ

На рис.2 представлена схема ПТК УСБ смешанного типа при реализации функций инициирования (УСБИ) и исполнения (УСБТ) в одном канале на ПТС разных производителей как вариант аппаратного разнообразия в схемах УСБ. При проектировании смешанных ПТК используется как программируемая аппаратура (ТПТС- ЕМ), так и аппаратура с функциями «жесткой логики» (АЗТП, АЛОС, АФСЗ), что исключает возможные ООП в части программных средств и дополнительно усиливает безопасность процессов контроля и управления АЭС за счет использования свойств диверсификации структурных схем СКУ.

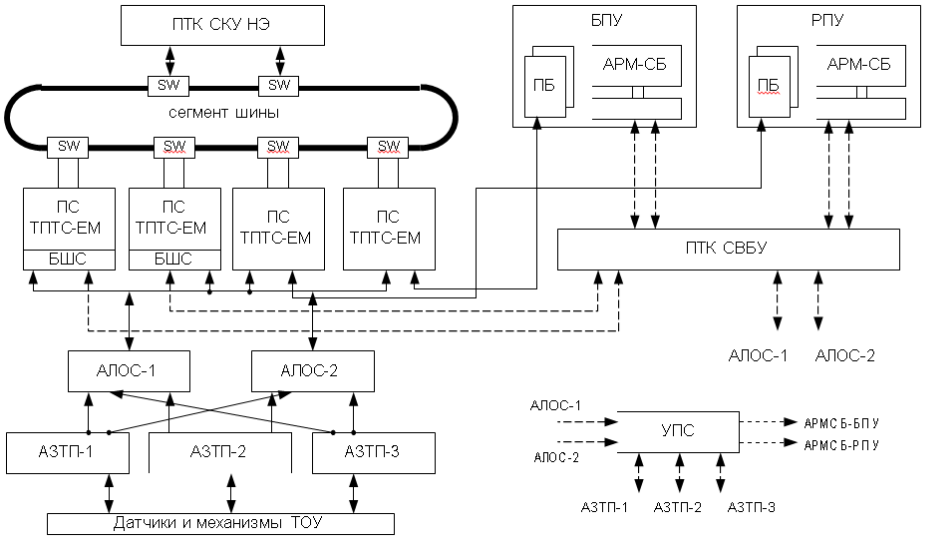

Рис. 2. Структурная схема ПТК канала УСБ с аппаратурой разных производителей

Модуль приоритетного управления (МПУ) исполнительным механизмом с внутренним разнообразием (рис. 3) предназначен для применения в исполнительной части УСБТ индивидуальным управлением одним исполнительным механизмом по автоматическим и дистанционным командам, поступающим от инициирующей части АЗ-УСБИ и от системы нормальной эксплуатации. Автоматические команды от инициирующей части АЗ-УСБИ и

дистанционные команды от панелей безопасности БПУ, РПУ поступают по проводным связям. Защитные и автоматические команды от ПТК СКУ НЭ, а также дистанционные команды от СВБУ поступают в МПУ по шинным связям.

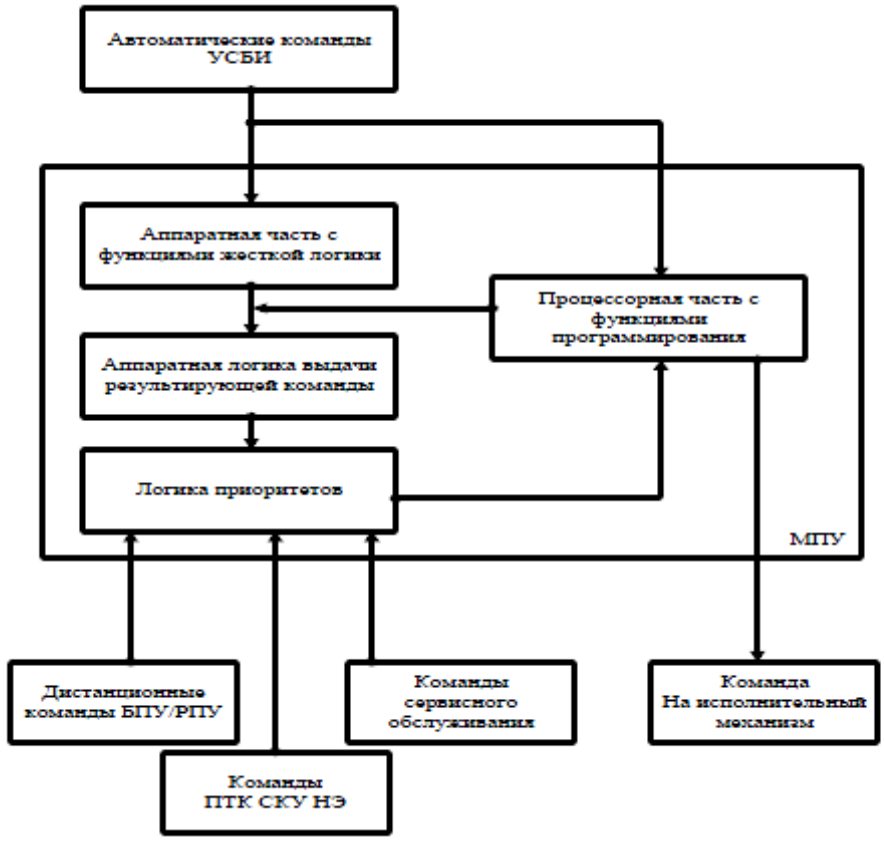

Рис. 3. Модуль приоритетного управления с внутренним разнообразием

В МПУ принцип разнообразия реализован в части автоматических команд СКУ безопасности следующим образом. Автоматические команды систем безопасности принимаются по аппаратному интерфейсу и отрабатываются двумя независимыми способами – в аппаратной и процессорной частях модуля. Выходные команды из аппаратной и процессорной части объединяются между собой в блоке «Аппаратная логика выдачи результирующей команды». Далее результирующие автоматические команды систем безопасности по логике приоритетов объединяются с дистанционными командами СБ и командами СНЭ, которые обрабатываются только в процессорной части. Обобщенные команды выдаются на исполнительный механизм по аппаратному интерфейсу. В МПУ имеется возможность выбора приоритета выдачи команд управления, сформированных процессорной или аппаратной логикой.

Разнообразие по WENRA

В соответствие с требованиями WENRA вводится расширенная шкала уровней глубокоэшелонированной защиты ГЭЗ 1,2,3a,3b,4,5. Основные из них, связанные с управлением безопасностью АЭС это уровни 3a и 3b, где используются несколько дополнительных диверсных систем защиты на разных уровнях. Делается это для того, чтобы на нормативном уровне расширить возможности управляющих систем по контролю и управлению режимами, которые ранее относились к запроектным авариям с расширенными возможностями использования принципа разнообразия в составе аппаратуры 3-х разных типов.

На рис. 4 представлена схема управляющих систем для уровня 3a, в основе которой два функционально разных комплекта защит с использованием аппаратуры разных типов и классов. Первый комплект выполнен на аппаратуре типа 1 по 2-му классу безопасности и включает в себя:

- 4 канала АКНП с функциями контроля нейтронной мощности и периода,
- 4 канала АЗ-УСБИ с функциями инициирования срабатывания аварийной защиты реактора и управляющих систем безопасности,

- группа панелей прерывателей питания ОР СУЗ (ППП-1,2) с функциями исполнительной части АЗ-ПЗ,
- набор модулей приоритетного управления типа 1 (МПУ 1) с функциями реализации исполнительной части УСБ.

Второй комплект выполнен на аппаратуре типа 2 по 3-му классу безопасности и включает в себя:

- 4 канала диверсной системы контроля нейтронного потока дСКНП с функциями контроля нейтронной мощности и периода,
- 4 канала диверсной системы аварийной защиты дСАЗ с функциями инициирования срабатывания аварийной защиты реактора через систему управления и контроля положения органов регулирования СУКПОР на уровне ГЭЗ 2.

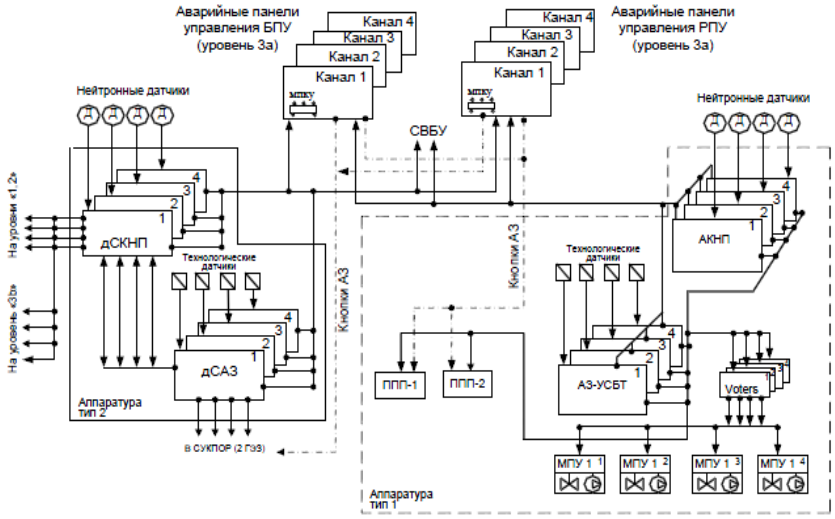

Рис. 4. Схема управляющих систем защиты реактора на уровне «3a»

Оба комплекта независимы друг от друга, но имеют выходы на аварийные панели БПУ, РПУ и в СВБУ. По информационным функциям дСКНП имеет связи с другими уровнями ГЭЗ. Каждый комплект имеет свой набор нейтронных и технологических датчиков. Считается, что данная схема с указанным набором разнообразия достаточна для преодоления проектных аварий с привлечением, в основном, активных технологических систем безопасности под контролем и управлением УСБ. Схема диверсной системы защиты для уровня 3b выполняется на аппаратуре типа 3.

Интерфейсы и общие схемы

Принцип разнообразия реализуется не только по функциональным областям, но и при проектировании линий связи (интерфейсов) между этими областями для того, чтобы также исключить отказы по общей причине этих интерфейсов.

В настоящее время разнообразие интерфейсов определяется двумя видами соединений, использующих разные технические средства: аналоговые и дискретные сигналы по прямым проводным связям или цифровая связь с применением оптоволоконных линий при построении локальных вычислительных сетей между ПТК. Использование прямых проводных линий считается более надежным способом связи из-за отсутствия программного обеспечения, но приводит к росту кабельных соединений, увеличению затрат, ухудшению пожарной обстановки в кабельных помещениях. Применение цифровой связи считается менее надежным из-за использования программного обеспечения, которое может отказать, но повышает оперативность управления, увеличивает объем и глубину всех видов диагностики, позволяет снизить количество кабельных соединений с уменьшением затрат и улучшением пожарной обстановки в помещениях.

Применение вида интерфейса в конкретном месте и конкретном проекте определяется многими обстоятельствами и, прежде всего, классификацией по безопасности систем и оборудования. Так, на рис. 5 представлена общая схема АСУ ТП некоторых отечественных АЭС, где используются

прямые проводные связи с резервными средствами контроля и управления на панелях, а для соединения ПТК низовой автоматики систем нормальной эксплуатации с верхним уровнем применяется цифровая связь.

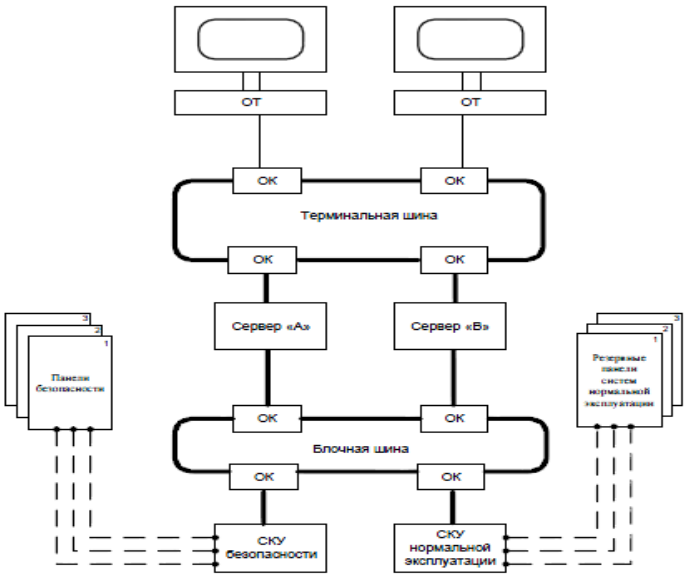

Рис. 5 Схема интерфейсов между системой верхнего уровня, индивидуальными панелями и системами низовой автоматики.
Обозначения
ОТ - операторский терминал,
ОК - оптический коммутатор,
___ - оптоволоконные линии связи,
- - - - прямые проводные связи

На рис. 6 представлена комбинированная схема соединений в части безопасности проекта /4/ с реактором EPR фирмы AREVA. Для реализации информационно- управляющих функций в части безопасности здесь используется система QDS как с прямой проводной связью (жесткое соединение), так и с цифровой связью для разных функций.

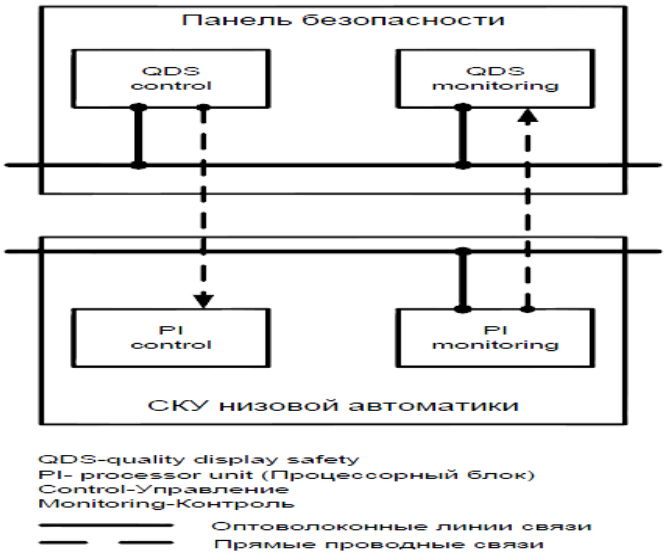

Рис. 6 Схема интерфейсов системы видеодисплеев безопасности QDS

Архитектура АСУ ТП отечественного перспективного проекта АЭС с ВВЭР-ТОИ /5/ строится с учетом наличия как активных, так и пассивных систем безопасности. При этом активные системы, в основном, используются на этапе «проектная авария», а пассивные системы на этапе «запроектная авария». В этой связи архитектура АСУ ТП содержит набор типов разнообразия в схемах инициирующей и исполнительных частей АЗ реактора и УСБ для контроля и управления

проектными авариями с целью повышения надежности и недопущения перерастания проектной аварии в запроектную. И тем не менее, при отказе СКУ на этапе «проектная авария» для управления запроектными авариями в технологической части проекта по расхолаживанию РУ используются пассивные системы безопасности на время до 72 часов без участия операторов.

В архитектуре АСУ ТП проекта с реактором АР-1000 /6/ предусмотрена одноканальная диверсная система DAS (diverse actuation system), которая использует свои датчики, не имеет связей с СВБУ, управляется только прямыми проводными связями с одной панели БПУ и воздействует на электропитание ОР СУЗ реактора и некоторое количество исполнительных механизмов систем безопасности. Подобная функциональная и структурная ограниченность DAS в данном проекте связана с тем, что здесь в технологической части используются практически только пассивные системы безопасности, контроль и управление которыми не требуют высокой надежности СКУ. Пассивные системы безопасности срабатывают безотносительно от СКУ, необходим только некоторый контроль за их работой.

Таблица 1. Алгоритмы диверсной защиты

Наименование параметра	**Уставка срабатывания**	**Защитное действие**
Давление в первом контуре, МПа, более Температура в одной из горячих ниток петель, ^{o}С, более	18,11 260	Срабатывание аварийной защиты реактора
Нейтронная мощность, % Nном, более (Nном - номинальное значение нейтронной мощности)	110	Срабатывание аварийной защиты реактора
Давление в первом контуре, МПа, менее Температура в одной из горячих ниток петель, ^{o}С, более	13,5 260	Срабатывание аварийной защиты реактора
Уровень в КД, м, менее Температура в одной из горячих ниток петель, ^{o}С, более	3,6 150	Срабатывание аварийной защиты реактора
Уровень воды в ПГ, мм, менее Температура в одной из горячих ниток петель, ^{o}С, более	Нном – 700* 150	Срабатывание аварийной защиты реактора
Давление в паропроводе ПГ, МПа, более Температура в одной из горячих ниток петель, ^{o}С, более	8,1 150	Запуск СПОТ
Уровень воды в ПГ, мм, менее Температура в одной из горячих ниток петель, ^{o}С, более	Нном – 1000* 150	Запуск СПОТ
Уровень в КД, м, менее Температура в одной из горячих ниток петель, ^{o}С, более	3,6 150	Запуск СПОТ
Давление в ПГ, МПа, менее Температура в одной из горячих ниток петель, ^{o}С, более	5,14 260	Отключение и Локализация аварийной петли
Уровень воды в ПГ, мм, более Нейтронная мощность, % Nном, более	Нном + 500 5	Отключение и локализацияаварийной петли
Давление (избыточное) под герметичной оболочкой, кПа, более	0,5	Закрытие вентиляционной локализующей арматуры

Наименование параметра	Уставка срабатывания	Защитное действие
Давление (избыточное) под герметичной оболочкой, кПа, более	40	Закрытие локализующей Арматуры на технологических трубопроводах

Выводы

1. Применение разнообразия при создании ПТК управляющих систем безопасности и связей между ними считается одним из основных положений, повышающих надежность срабатывания этих подсистем, а значит и уровень безопасности АЭС.

2. Наиболее успешным способом реализации из всех возможных видов разнообразия следует признать применение аппаратного разнообразия, основанного на использовании разных технических средств в разных каналах и комплектах.

3. Объем и глубина применения разнообразия должна сочетаться с типом используемых технологических систем безопасности. Чем больше активных систем безопасности, тем более надежными должны быть СКУ за счет применения разнообразия. Предлагается в пассивных системах безопасности, не требующих высокой надежности СКУ, в меньшем объеме использовать разнообразия.

Перечень сокращений

АЗ-ПЗ - аварийная и предупредительная защита реактора

АЗТП- аппаратура защиты по технологическим параметрам АКНП - аппаратура контроля нейтронного потока

АЛОС - аппаратура логической обработки сигналов

АРМСБ – автоматизированное рабочее место систем безопасности

АСУТП – автоматизированная система управления технологическим процессом АФСЗ- аппаратура формирования сигналов защит

БПУ- блочный пункт управления БШС - блок шлюза сопряжения ДСЗ - диверсная система защиты

МПУ- модуль приоритетного управления ООП - отказ по общей причине

ОР- органы регулирования СУЗ реактора ПБ- панель безопасности

ПЗ- предупредительная защита ПС- приборная стойка

ПТК- программно-технический комплекс

ПТК ПУ – программно-технический комплекс приоритетного управления ПТС - программно-технические средства

РПУ - резервный пункт управления СБ- система безопасности

СВБУ - система верхнего блочного уровня

СКУ НЭ – система контроля и управления нормальной эксплуатацией СКУ СБ - система контроля и управления системами безопасности СУЗ- система управления и защиты реактора

ТПТС-ЕМ – типовые программно-технические средства типа ЕМ УСБ - управляющая система безопасности

УСБИ - управляющая система безопасности инициирующая УСБТ - управляющая система безопасности технологическая

Литература

1. «Общие положения обеспечения безопасности АС», НП-001-2015.
2. Требования к управляющим системам, важным для безопасности атомных станций НП-026-04: Утверждены постановлением Федеральной службы по экологическому, технологическому и атомному надзору от 4 октября 2004 г. № 2. Введены в действие с 5 января 2005 г.
3. МАГАТЭ, № SSG-39. Проектирование автоматизированных систем управления технологическим процессом для атомных электростанций. Специальное руководство по безопасности. Вена,. 2016 год.
4. Фирма AREVA «Окончательный отчет по обоснованию безопасности (FSAR) американских эволюционных энергетических реакторов EPR». Глава 7 – «Контрольно- измерительные приборы и управление». 2009 год (на русском языке).
5. Курская АЭС-2 (проект ВВЭР-ТОИ) «Предварительный отчет по обоснованию безопасности». Глава 7 «Контроль и управление». KUR- PSAR0107-BAA0001. 2014 год.
6. Презентация: «AP-1000. Nuclear Power Plant». Terry L. Schulz, Westinghouse Electric Company. July 22, 2008.еречень сокращений.