# Оценка надежности АСУ ТП, разрабатываемого на программируемых средствах для АЭС с ВВЭР-1000

**Токмачев Г.В., Чулухадзе В.Р.**

*Ежегодная конференция молодых специалистов ФГУП ОКБ «Гидропресс», Подольск, Московская обл., 19 – 20 января 2006 г.*

## Введение

В докладе представлены методология и результаты анализов надежности автоматизированных систем управления технологическим процессом (АСУ ТП), разрабатываемых для проектируемых АЭС с ВВЭР-1000. Исследования проводились институтом «Атомэнергопроект» (Москва) для АСУ ТП нового поколения, основанного на использовании программируемых технических средств. Анализы были выполнены для 2-й очереди Нововоронежской АЭС и АЭС «Бушер» в Иране средствами ФГУП «Атомэнергопроект» (Москва), а также 3-го энергоблока Калининской АЭС при участии коллег из института «Атомэнергопроект» (Нижний Новгород).

Анализы надежности выполнены с применением программного комплекса RISK SPECTRUM, основанного на использовании методологии деревьев событий/отказов. Для разработки логической модели, определяющей условие отказа анализируемых структур АСУ ТП, выполнен качественный анализ последствий отказов элементов. При этом учитывались ошибки персонала, отказы по общей причине и надёжность программного обеспечения АСУ ТП.

# 1 Характеристика объекта анализа: назначение, структура и состав АСУ ТП

## 1.1 Назначение

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 работы АЭС в условиях нормальной эксплуатации;
- обеспечения безопасности во всех режимах работы, включая аварийные ситуации и проектные аварии.

Для выполнения основного назначения АЭС по экономичной выработке электроэнергии в составе АСУ ТП присутствует ряд подсистем нормальной эксплуатации, формирующих и реализующих по заданным технологическим целям, критериям и ограничениям управление технологическим оборудованием систем нормальной эксплуатации блока АС.

Не менее важной задачей является обеспечение безопасности АЭС. Поэтому в составе АСУ ТП предусмотрены управляющие системы безопасности, предназначенные для инициирования действий систем безопасности, осуществления контроля и управления ими в процессе выполнения заданных функций, которые выполняются автоматически при возникновении условий, предусмотренных проектом.

## 1.2 Структура и состав АСУ ТП

Структура АСУ ТП имеет иерархический принцип построения в соответствии с разделением энергоблока, как объекта управления, на технологические функциональные области и группы, где на более высоком уровне реализуются общеблочные задачи, связанные с централизацией контроля и управления:

- своевременная обработка и представление информации,
- ведение архива,
- дистанционное управление оборудованием нормальной эксплуатации,
- информационная поддержка операторов.

На настоящем этапе разработки проекта надежность подсистем верхнего уровня не анализировалась.

На нижнем уровне средства низовой автоматики обеспечивают реализацию задач связи с технологическим объектом управления (сбор информации и выдача команд), а также задач защит, блокировок, авторегулирования, сигнализации и управления арматурой, механизмами, соленоидами и пр.

Нижний уровень включает ряд подсистем АСУ ТП, важнейшей из которых являются управляющие системы безопасности, включающие систему защиты и управления реакторной установки (СУЗ) и управляющую систему безопасности технологическую (УСБТ). СУЗ выполняет функцию аварийного останова реактора (аварийной защиты) и поддержания его в подкритическом состоянии. УСБТ предназначена для аварийного расхолаживания реакторной установки, контроля и управления в процессе расхолаживания и удержания этого режима. Эти две системы независимы друг от друга и строятся на принципах жесткой логики. Обе системы состоят из инициирующей части, обеспечивающей контроль и выдачу команд при аварийной ситуации (УСБИ), и исполнительной части. Исполнительная часть УСБТ предназначена для контроля и управления системами безопасности по командам УСБИ, дистанционного управления, технологических защит и блокировок, а также представления необходимой оператору информации по параметрам и положению объектов управления.

В рамках представленной работы выполнены анализы надежности типовых каналов контроля и управления, а также общих показателей, характеризующих выполнение АСУ ТП отдельных функций в объеме:

- подсистема аварийной защиты;
- подсистемы защит и блокировок систем безопасности и нормальной эксплуатации;
- каналы дистанционного управления механизмами систем безопасности и нормальной эксплуатации;
- каналы авторегулирования систем безопасности и нормальной эксплуатации;
- каналы представления информации на индивидуальных приборах и мониторах систем безопасности и нормальной эксплуатации.

# 2 Методика выполнения анализа и исходные данные

## 2.1 Общие положения

Анализ надежности проводится на основе метода дерева отказа, который предусматривает формирование логического условия неработоспособности анализируемой структуры в форме дерева отказа, генерацию минимальных сечений и расчет показателей неготовности указанных сечений и структур в целом. Метод широко используется в мировой практике и подробно описан в литературе [1].

Дерево отказов анализируемой структуры включает вершинное событие, промежуточные логические операторы и первичные события, моделирующие различные виды отказов элементов.

В настоящей работе для каждой анализируемой схемы составляются два различных дерева: одно характеризует логическое условие «неготовности» структуры, т.е. её неработоспособности в момент поступления требования на срабатывание, а второе – логическое условие формирование ложной команды, т.е. отказа типа «ложное срабатывание».

Оценка показателей надёжности типовых структур АСУ ТП выполняется с использованием программы RISK SPECTRUM PSA Professional [2]. Программа выполняет расчеты, определяя для соответствующих деревьев отказов:

- неготовность вершинного события (вероятность неработоспособного состояния анализируемой схемы в момент поступления требования на срабатывание);
- параметр потока оцениваемого события (для «ложных срабатываний»).

При выполнении расчётов программа анализирует логическую структуру деревьев и генерирует множество минимальных сечений, т.е. минимальных наборов первичных событий, совместное существование которых обусловливает отказ или ложное срабатывание анализируемой структуры.

## 2.2 Вероятностные модели отказов элементов, используемые при расчетах

При разработке вероятностной модели АСУ ТП использованы следующие типы первичных событий:

- постоянно контролируемый, восстанавливаемый элемент, характеризующийся явными отказами. Модель предполагает экспоненциальное распределение как для интенсивности отказов, так и для восстановления, т.е. интенсивность отказов и время восстановления являются константами.
- периодически проверяемый элемент. Модель предполагает экспоненциальное распределение наработок между отказами (постоянное значение интенсивности отказов), а также постоянные значения тестового интервала и времени восстановления.
- элемент с независящей от времени неготовностью, характеризующей его отказ на требование. Эта простая модель, использует единственный параметр - вероятность отказа на требование.

## 2.3 Типовые виды отказов элементов АСУ ТП

При разработке деревьев отказов анализируемых типовых каналов структур АСУ ТП учитываются следующие виды отказов элементов:

- явные отказы (обнаруживаемые сразу или в течение короткого времени после возникновения);
- периодически контролируемые отказы (обнаруживаемые при проведении периодических проверок прохождения сигнала).

Явные отказы элементов, в свою очередь, подразделяются на отказы, приводящие к ложным срабатываниям элемента и прочие отказы, последствия которых зависят от схемы обработки сигналов неисправности, характеризующих указанные отказы.

Периодически контролируемые отказы в силу своего определения всегда приводят к невыполнению функции элемента.

Показатели надежности элементов анализируемых структур были предоставлены разработчиками отдельных узлов АСУ ТП. Кроме того, использовались данные из технических условий и технических требований на элементы и устройства, а недостающая информация взята из обобщенной базы МАГАТЭ по элементам-аналогам [3].

## 2.4 Анализ последствий отказов элементов

Для разработки логической модели, определяющей условие отказа анализируемой структуры АСУ ТП, выполнен качественный анализ последствий отказов элементов. Результаты данного анализа представлены в проектных материалах в виде таблиц, в которых приведены характеристики различных видов отказов элементов (определение отказа, способ обнаружения и возможность восстановления на работающем блоке), данные по интенсивностям отказов и времени восстановления, а также последствие каждого вида отказа на работу анализируемой схемы.

## 2.5 Анализ отказов по общим причинам

В настоящее время при проведении анализов надёжности систем АС общепризнанным является подход, при котором для резервируемых элементов допускается возможность наступления множественных зависимых отказов вследствие одной общей причины. Эта общая причина может быть связана с наличием явно не учитываемых в модели зависимостей, связанных с общим расположением, одинаковыми условиями эксплуатации, общими процедурами технического обслуживания и одинаковым конструкционным типом элементов. Наличие таких факторов «общности» может привести к тому, что вероятность возникновения отказов нескольких резервируемых элементов на рассматриваемом периоде времени значительно превысит

произведение указанных вероятностей, т.е. результат, получаемый в предположении независимости отказов элементов.

При проведении анализа был принят следующий подход к моделированию отказов по общей причине:

- Традиционный параметрический подход к учёту в модели отказов по общей причине применялся для групп резервированных однотипных элементов, принадлежащих одному комплекту аппаратуры (датчики, ТПТС, каналы АЗТП, АЛОС и т.д.) применительно как к явным, так и скрытым отказам. При этом такие отказы элементов учитывались в рамках простой модели бета-фактора. Для определения параметра бета использовались обобщённые данные.

- При моделировании отказов по общей причине для групп однотипных элементов, составленных из разных комплектов, было учтено, что такие отказы могут быть обусловлены только общностью конструкции, вследствие чего невозможно их возникновение на коротких промежутках времени, сравнимых со средним временем восстановления элементов АСУ ТП (8 ч). Поэтому такая возможность учитывалась только для скрытых отказов. При этом значение параметра бета-фактора было принято в 10 раз меньше, чем для групп, относящихся к одному комплекту аппаратуры. При выборе указанной величины было также учтено, что скрытый отказ одного канала аппаратуры представляет собой наложение отказов двух неоднотипных элементов (один из которых является блоком контроля). Вследствие этого множественный скрытый отказ аппаратуры разных комплектов возможен вследствие реализации как минимум двух различных общих причин: одной - для блоков контроля и другой - для однотипных функциональных модулей, что крайне маловероятно.

## 2.6 Анализ надежности функционирования программных средств

В соответствии с требованиями основного нормативного документа Госатомнадзора России ОПБ-88/97 [3] проекты УСНЭ и УСБ должны содержать анализ надежности функционирования программных средств (пп. 4.4.4.5 и 4.4.5.9).

Показатели надежности программных средств характеризуют их способность выполнять заданные функции в соответствии со спецификациями в условиях естественных отклонений в среде функционирования, вызванных различными дестабилизирующими факторами. К числу указанных факторов относятся, в частности, изменения условий работы технических средств, их отказы и сбои, изменения во входных данных, изменения в распределении ресурсов памяти.

Анализ надежности функционирования программных средств выполнен только для модулей программируемых технических средств ТПТС, которые являются программируемыми. Остальные средства низовой автоматики функционируют по принципу жесткой (аппаратно реализованной) логики, и рассматривать отказы программного обеспечения таких средств во время эксплуатации отдельно от самих средств бессмысленно.

При анализе надежности программного обеспечения ТПТС в модели рассмотрены два вида отказов программного обеспечения: сбои и общие ошибки программирования, потенциально приводящие к невыполнению функций ТПТС сразу в нескольких каналах АСУ ТП.

Наиболее характерным последствием сбоев в функционировании программного обеспечения, которое и рассматривается в модели, является отказ типа «несрабатывание» соответствующего ТПТС. Сбои программного обеспечения вызываются невыявленными программными ошибками, которые главным образом влияют на организацию обмена данными. Как следствие наличия таких ошибок, программа выдает неправильные результаты несмотря на то, что входные данные удовлетворяют спецификации требований, например, из-за проблем с динамическим распределением ресурсов.

Комбинаторный характер обработки и накопления информации и множество условных переходов создают большое количество путей выполнения программой той или иной команды.

Этим объясняется, с одной стороны, невозможность выявить абсолютно все программные ошибки на этапах тестирования и опытной эксплуатации, несмотря на то, что большинство программистских ошибок выявляются во время тестирования средств на полигоне и во время пуско-наладочных работ.

При этом, хотя коренная причина отказа программного обеспечения не устраняется, и в такой же точно ситуации отказ должен повториться, точное повторение данных и, соответственно, связанного с ним отказа маловероятно. Поэтому указанная ошибка программирования проявляется в виде перемежающихся отказов, т.е. сбоев, которые устраняются преимущественно автоматизированными методами (повторной инициализацией программ).

Следует отметить, что программы, реализуемые на ТПТС, являются достаточно простыми программами прямого действия, т.е. не происходит обмена данными с другими программными комплексами и библиотеками, что значительно уменьшает вероятность сбоев как таковых и в принципе исключает ситуации, которые приводят к самопроизвольному генерированию выходного сигнала при отсутствии входного сигнала (т.е. отказы типа «ложное срабатывание»). Поэтому моделировались только сбои программного обеспечения ТПТС, приводящие к невыполнению основной функции (несрабатыванию на требование соответствующих модулей), причем предполагалось, что все сбои программного обеспечения ТПТС проявляются явно, т.е. являются непрерывно контролируемыми, учитывая высокую степень самоконтроля исправности ТПТС. Данный вывод подтверждается успешным опытом эксплуатации программируемых модулей-аналогов на тепловых электростанциях.

Для оценки надежности функционирования программных средств ТПТС был изучен опыт эксплуатации их аналогов, и проведен сбор информации по фактам отказов программного обеспечения модулей на действующих блоках. Так как модули ТПТС не установлены на действующих АЭС, то в качестве источника информации был использован опыт эксплуатации функционально-системных модулей ТПТС, выполняющих функции защиты котла и турбины на ТЭЦ-12 в г. Москве.

Дополнительно к событиям этого типа рассмотрены крайне маловероятные программистские ошибки глобального характера, которые приводят к отказу всего программного обеспечения по общей причине при реализации не предусмотренных при программировании конфигураций и граничных условий. Предполагалось, что такие отказы по общей причине возможны только в отношении отказов типа «несрабатывание» и приводят к отказу всех каналов в составе которых есть аналогичные программируемые технические средства. Вероятность такого глобального отказа не может быть оценена из опыта эксплуатации в силу малой вероятности и оценена экспертно.

### 2.7 Анализ надежности персонала

В соответствии с требованиями ОПБ-88/97 [4] (п. 4.1.12) анализ надежности систем и элементов безопасности должен проводиться с учетом ошибок персонала. При выполнении настоящего анализа использовано руководство, разработанное специалистами НТЦ ГАН [5] и использованное при выполнении ряда вероятностных анализов безопасности (ВАБ).

Методы анализа надежности персонала рассматривают три основные типа действий персонала:

♦ Действия, основанные на навыке - Хорошо отработанные до автоматизма действия по сценариям, изложенным в инструкциях (аналогичные, например, вождению автомобиля по знакомому маршруту). Ошибки при этом типе действий связаны в основном с комбинацией факторов вынужденности, пространства и времени.

♦ Действия, основанные на правилах - Действия в знакомых ситуациях, основанные на ранее отработанных последовательностях действий, которые подробно изложены в инструкциях и/или получены из опыта, или при обучении. Действия по правилам менее отработаны, чем действия, основанные на навыке, поскольку они выполняются реже и являются более сложными и зачастую требуют повышенного осознанного контроля. Ошибки при этом типе действий обычно связаны с неправильной диагностикой ситуации, приводящей к использованию неверного правила или инструкции.

♦ Действия, основанные на знаниях - Действия в незнакомых ситуациях, когда имеющиеся правила и опыт не могут быть применены непосредственно. Для этих действий обычно не существует готовых инструкций, они основаны на общих знаниях и выполнять которые необходимо в режиме реального времени. Ошибки при этом типе действий являются следствием ограниченности времени на принятие решения и выполнения действия, а также недостаточности или неверности знаний.

При выполнении количественного анализа персонала в рамках ВАБ обычно рассматриваются две составляющие ошибок персонала при выполнении действий, являющихся ответными на аварийную ситуацию после наступления исходного события: когнитивную (диагностика и принятие решения) и исполнительную части. Следует отметить, что настоящий анализ не являлся комплексным анализом безопасности всей АЭС и был ограничен только рамками АСУ ТП. Поэтому здесь рассмотрены действия, которые являются элементарными и не требующими диагностики и принятия решения, т.е. основанные на навыке.

## 3 Результаты анализов

Ниже приведены наиболее важные результаты анализа надежности АСУ ТП для 3-го энергоблока Калининской АЭС.

Максимальное значение вероятности отказа формирования сигнала аварийной защиты реактора с учетом полного количества комплектов аппаратуры и критериев выполнения функций составляет 1,13E-06 для защиты по сигналу заклинивания вала ГЦН.

В соответствии с требованиями НТД вероятность отказа на требование аварийной защиты в целом (с учётом исполнительной части, не рассмотренной в данном анализе), не должна превышать 1,0E-05. Таким образом, полученное значение, которое фактически является консервативной оценкой (по наихудшему случаю), вероятности невыполнения функции аварийной защиты по вине АСУ ТП примерно на порядок меньше требуемой величины неготовности.

Суммарное значение параметра потока ложных срабатываний аварийной защиты с учётом наличия двух комплектов аппаратуры составляет 2,86E-05 1/ч или 2,23E-01 1/год, что примерно на порядок меньше суммарного параметра потока срабатываний аварийной защиты по всем причинам, определённого по опыту эксплуатации АС с ВВЭР-1000.

Максимальное значение вероятности отказа формирования сигнала, инициирующую технологическую защиту (УСБИ), составляет 2,24E-06 с учётом количества комплектов аппаратуры и критериев выполнения функций. Это значение получено для схемы формирования команды ступенчатого пуска.

Следует отметить, что вероятности отказа схем формирования сигнала технологической защиты УСБИ в среднем выше показателей надежности схем формирования сигнала аварийной защиты реактора. Эта разница обуславливается различной логикой обработки сигналов неисправности элементов (при формировании сигнала аварийной защиты аппаратно выявленная неисправность канала приравнивается в логике аварийному сигналу). Поэтому вероятность отказа схемы формирования сигнала технологической защиты УСБИ в основном определяется вкладом от обнаруживаемых отказов элементов, приводящих к несрабатыванию канала (до 97 %), в то время как в схемах аварийной защиты реактора указанные вкладчики отсутствуют.

Для исполнительных цепей формирования сигнала технологической защиты УСБТ максимальное значение вероятности отказа на требование составляет 1,53E-04 для схем отключения насоса по локальной защите - рост температуры масла картера или воздуха перед электродвигателем. Максимальное значение параметра потока ложных срабатываний одного комплекта технологических защит УСБИ составляет 1,66E-06 1/ч для некоторых защит. Ложное формирование команды в данном случае приводит к запуску соответствующих механизмов систем безопасности, относящихся к одному из каналов систем безопасности, и не вызывает аварийный останов блока.

Анализ результатов показал, что отказы программного обеспечения в целом оказывают незначительное влияние на надёжность работы схем низовой автоматики. Наибольшее влияние указанные отказы (сбои) оказывают на надежность схем УСБТ и защит и блокировок систем нормальной эксплуатации. Максимальный вклад от отказов программного обеспечения в вероятность отказов каналов типовых структур АСУ ТП составляет 32 % для схем УСБТ и 15 % для схем защит и блокировок систем нормальной эксплуатации. При этом следует отметить, что согласно принятой в анализе методике моделирования таких отказов, оценка надёжности программного обеспечения для средств низовой автоматики является консервативной, так как получена в условиях нулевой статистики.

Максимальный вклад от ошибок персонала при выполнении переключений составляет 96 % для схем дистанционного управления механизмами нормальной эксплуатации. Максимальный вклад от ошибок персонала при считывании информации составляет 95 % для схем каналов представления информации.

Рассматривая результаты работы в целом, уровень надёжности типовых структур и подсистем АСУ ТП следует признать отвечающим существующим требованиям.

## Перечень сокращений

| | |
|---|---|
| АЗТП | аппаратура защиты по технологическим параметрам |
| АЛОС | аппаратура логической обработки сигналов |
| АСУ ТП | автоматизированная система управления технологическими процессами |
| АЭС | атомная электрическая станция |
| ВАБ | вероятностный анализ безопасности |
| ГЦН | главный циркуляционный насос |
| МАГАТЭ | Международное агентство по атомной энергии |
| НТД | нормативно технический документ |
| НТЦ ГАН | Научно-технический центр Госатомнадзора РФ |
| СБ | система безопасности |
| СУЗ | система управления и защиты |
| ТПТС | комплекс программно-технических средств |
| УСБ | управляющая система безопасности |
| УСБИ | управляющая система безопасности инициирующая |
| УСБТ | управляющая система безопасности технологическая |
| УСНЭ | управляющая система нормальной эксплуатации |

## Список литературы


1) Ю.В. Швыряев, А.Ф. Барсуков, А.А. Деревянкин, В.Б. Морозов, Г.В. Токмачев, Л.М. Векслер. Вероятностный анализ безопасности атомных станций. Методика выполнения. Ядерное общество СССР. Москва, 1992.

2) RISK SPECTRUM, User's Manual, Yersion 2.1, Relkon Teknik AB, Box 1288, S – 172 25 Sundbyberg, Sweden, April 1994.

3) Component Reliability Data for Use in Probabilistic Safety Assessment, МАГАТЭ, IAEA-TECDOC-478, 1988 год

4) Общие положения обеспечения безопасности атомных станций. ОПБ-88/97. ПНАЭ Г-01-011-97. Госатомнадзор России, Москва, 1997.

5) Проект NOVISA. Руководство по Анализу Надежности Персонала. NPG-7. Нововоронежская АЭС, декабрь 1998.