УДК 621.039-78

СТРУКТУРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ БЕЛОРУССКОЙ АЭС С ТОЧКИ ЗРЕНИЯ БЕЗОПАСНОСТИ

Д.С. ТИМОХИН, С.Ю. ГРИЦЕНКО, К.П. АРТЕМЬЕВ

Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова
Сущевская, 22, Москва, 127055, Россия

Поступила в редакцию 2 февраля 2015

Как и любая современная автоматизированная система управления технологическими процессами (АСУ ТП), АСУ Белорусской АЭС состоит из достаточно большого числа подсистем. ФГУП «ВНИИА» является разработчиком и изготовителем оборудования для наиболее крупных частей АСУ ТП:

– система нормальной эксплуатации;

– управляющая система безопасности.

Система нормальной эксплуатации (СНЭ) выполняет функции, необходимые для повседневной работы АЭС, реализует автоматизированное управление технологическими процессами АЭС в целях выработки тепловой и электроэнергии.

Управляющая система безопасности (УСБ) предназначена для обеспечения ядерной безопасности АЭС. При этом необходимо обеспечить достаточную надежность УСБ и исключить выдачу ложных команд управления. На рис. 1 представлена укрупненная структурная схема АСУ ТП в соответствии с концепцией глубокоэшелонированной защиты (ГОСТ Р МЭК 61513-2011) для Белорусской АЭС.

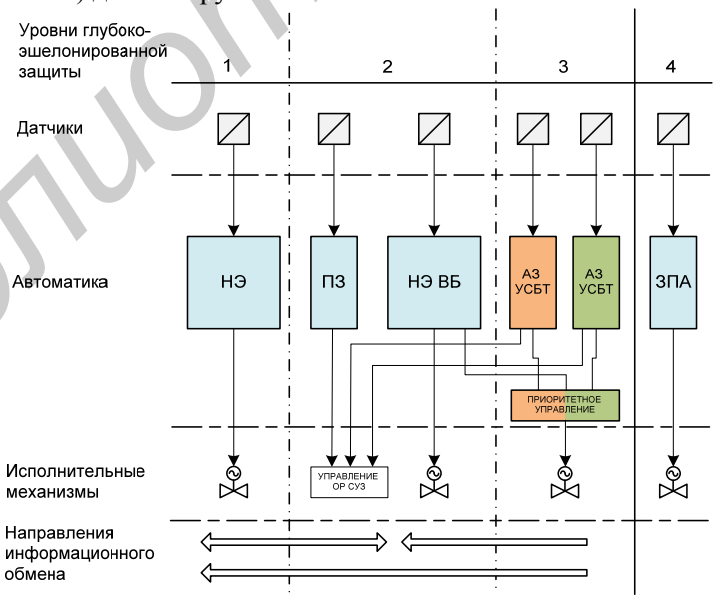

Рис. 1. Структурная схема АСУ ТП Белорусской АЭС

Уровень 1 – нормальная эксплуатация (НЭ) – направлен на безопасную и эффективную выработку электроэнергии. Уровень 2 содержит в себе системы нормальной эксплуатации важные для безопасности (НЭ ВБ), задачи которых сводятся к защите технологического оборудования, и предупредительные защиты (ПЗ), предназначенные для поддержания реактора

в подкритичном состоянии. Уровень 3 (далее по тексту – УСБ) спроектирован с учетом принципа разнообразия и отвечает за функции безопасности (аварийную защиту (АЗ) и управляющую систему безопасности технологическую (УСБТ)). Уровень 4 – управление запроектными авариями (ЗПА), его цель – это постававарийный мониторинг.

В проекте Белорусской АЭС для реализации функций СНЭ и УСБ предусмотрено применение аппаратуры ФГУП «ВНИИА»: для системы нормальной эксплуатации – ТПТС-НТ (уровни 1, 2, 4 на рис. 1), для управляющей системы безопасности – ТПТС-СБ (уровень 3 на рис. 1). Более подробно с информацией об аппаратуре ТПТС можно ознакомиться в статьях, посвященных КСА ТПТС-НТ и КСА ТПТС-СБ.

В целях безопасной эксплуатации АСУ ТП с технологической точки зрения необходимо обеспечить условия эксплуатации оборудования в соответствии с требованиями заводов-изготовителей. Эти функции выполняет система контроля и управления нормальной эксплуатации, управляя и ограничивая в проектных пределах технологические параметры с помощью регуляторов и блокировок. Если значения параметров, тем не менее, достигают неприемлемых для оборудования пределов, то исполнительные механизмы переводятся в безопасное состояние (насосы отключаются, сбрасывается давление или прекращается подача пара на турбину, обесточивается электрооборудование и т.п.). Таким образом, помимо предотвращения поломки оборудования, СКУ НЭ позволяет избежать и более серьезных последствий, таких как пожар в помещениях АЭС.

Еще более ответственными являются мероприятия по обеспечению ядерной безопасности энергоблока. Функции УСБ направлены на предотвращение проектных аварий, ограничение их последствий и обеспечение безопасности при любом из учитываемых проектом исходном событии с наложением, в соответствии с принципом единичного отказа, одного, независимого от исходного события, отказа элементов или одной, независимой от исходного события, ошибки оператора.

АСУ ТП должна быть построена таким образом, чтобы максимально учитывать требования нормативных документов, сохраняя в то же время эффективность работы АЭС. Важнейшими из требований, направленных на обеспечение ядерной безопасности, являются требования по применению в УСБ принципов резервирования, независимости и разнообразия (в соответствии с рекомендацией NUREG/CR-7007). Структурная схема УСБ показана на рис. 2.

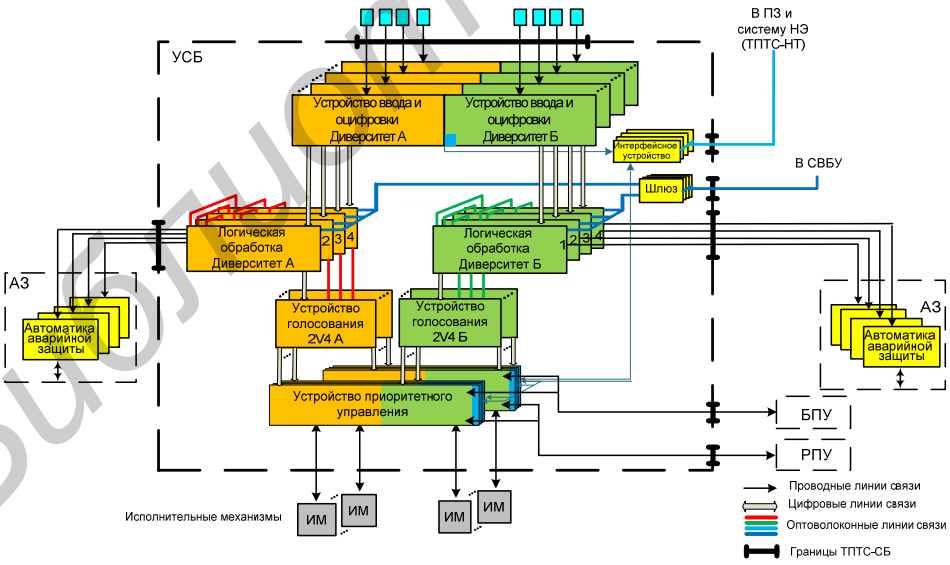

Рис. 2. Структурная схема УСБ Белорусской АЭС

Необходимый уровень резервирования достигается путем создания многоканальной УСБ (в Белорусской АЭС этих каналов четыре, см. рис. 2). При этом каждый канал УСБ должен быть способен выполнить каждую из функций безопасности. Для этих целей каждый канал комплектуется выделенным КИП (по одному датчику на параметр для каждого канала) и исполнительными механизмами. Для того, чтобы при отказе оборудования не выдавались ложные команды, предусмотрено голосование по логике «2 из 4», в котором помимо

параметров, выработанных (измеренных или вычисленных) внутри каждого канала УСБ, используется информация из трех других каналов. Голосование происходит на двух уровнях: первый – на уровне технологических параметров, формируя, таким образом, достоверный и пригодный для дальнейшей обработки сигнал в каждом канале; второй – на уровне ввода команд в стойки приборные приоритетного управления, где пресекается таким образом выдача ложной команды на исполнительные механизмы, а так же, в случае отказа в данном канале УСБ (процессор ПА-СБ или тракт передачи команд), выдача команд на исполнительные механизмы по мажорированным командам других каналов УСБ. Данные подходы обеспечивают при единичных отказах – в части аварийных защит принцип «безопасного» отказа, а в части управления исполнительными механизмами УСБТ защиту от выдачи ложной команды. Таким образом, выполняется защита от отказа на требование.

Принцип независимости реализуется проектным путем. Оборудование каналов УСБ размещается в отдельных помещениях, разнесенных в пространстве. Питание осуществляется от независимых (дублированных) источников с применением в качестве резервного питания отдельных аккумуляторных батарей. Как уже упоминалось ранее, каждый канал имеет собственный контрольно-измерительный прибор (КИП) и собственные исполнительные механизмы. Необходимые цифровые связи между каналами выполнены в виде выделенных (точка-точка) оптических линий связи, обеспечивающих гальваническую развязку каналов УСБ. Связь с аппаратурой системы нормальной эксплуатации (СНЭ) также реализована оптическими каналами системной шины EN. Каждый канал УСБ, в свою очередь, содержит два независимых комплекта аппаратуры. Комплекты А и В реализованы различными техническими средствами и никак не связаны между собой. Каждый комплект имеет собственный набор КИП. Объединяются эти комплекты только в стойке приборной приоритетного управления с использованием элементов жесткой логики. Фактически каждый комплект (А и В, которые обмениваются информацией с одноименными комплектами других каналов УСБ) представляет собой целый канал УСБ. Внутри каждого комплекта для связи между стойками приборными широко используются оптические линии связи. Для функционирования СНЭ требуется информация от КИП УСБ – эти связи также оптические, каналы связи УСБ-СНЭ не связаны с межканальными шинами УСБ и имеют другой протокол обмена. Кроме того, однонаправленность канала связи из УСБ в СНЭ (и не наоборот) обеспечивается аппаратными средствами УСБ. Как видно, принцип независимости, при том, что он должен выполняться, вполне может сочетаться с наличием информационных связей, как между каналами, так и между УСБ и СНЭ. Только таким образом, разумно сочетая независимость и интеграцию, можно достичь весьма значительных успехов по минимизации объема оборудования АСУ ТП для Белорусской АЭС.

Переходя к описанию использованного в УСБ АСУ ТП Белорусской АЭС принципа разнообразия, следует отметить, что принципы резервирования, независимости и разнообразия не самоцель. Данные принципы являются основой для построения УСБ, в которой снижена до приемлемого и разумного минимума вероятность отказа по общей причине в системе безопасности при любых проектных воздействиях, а также при ошибочном действии персонала при эксплуатации и ремонте. Помимо единичных случайных отказов в оборудовании систем безопасности АЭС, устойчивость к которым безусловно необходима, в соответствии с современными нормами должна быть обеспечена устойчивость к отказу по общей причине. Под отказом понимается невыполнение любой функции безопасности в момент аварии (отказ на требование), а также выдача ложной команды на оборудование, обеспечивающее безопасность тогда, когда аварии нет. Под отказом по общей причине понимается групповой отказ однотипного или одноприципного оборудования (например одного и того же звена в каждом из каналов безопасности), приводящий к невыполнению требуемой функции во время ядерной аварии всей системы в целом.

Возможность возникновения отказа по общей причине может быть вызвана различными причинами: внешнее воздействие (сейсмика, пожар, наводнение, падение самолета и т.п.), ошибка персонала, недостаток проекта, скрытая ошибка в программном обеспечении. Все эти причины обусловлены наличием скрытых дефектов в оборудовании или проекте системы безопасности.

Возможная реакция оборудования системы безопасности при воздействии внешних факторов достаточно четко может и должна быть проверена в процессе ее создания прямыми испытаниями на стойкость по утвержденным методикам на соответствие требованиям проекта.

При этом в техническое задание на аппаратуру именно эти требования вносятся как обязательные для выполнения. Таким образом, подтверждается работоспособность аппаратуры во всем проектном диапазоне внешних воздействующих факторов, в том числе и при протекании ядерных аварий. Следовательно, коль скоро при внешних воздействиях вероятность возникновения единичных отказов не повышается, то и нет предмета анализа вероятности возникновения отказов по общей причине.

Гораздо более сложной является задача разработки программного обеспечения (системных и базовых функций, управление работой элементов и т.п.). При ее решении используются инструментальные средства, корректность работы которых подтверждена опытом эксплуатации, однако строго доказать отсутствие несоответствий, которые могут привести к отказу по общей причине, практически невозможно.

Система безопасности должна формировать автоматические управляющие воздействия в течение ограниченного времени и только при возникновении аварии, а корректная логическая обработка входных сигналов и готовность выдать управляющие воздействия должна гарантироваться в течение всего времени ее работы. В том случае, если отказ УСБ не связан с состоянием объекта управления, совпадение двух событий – аварии на энергоблоке АЭС и отказа управляющей системы безопасности – представляется событием маловероятным.

При разработке процессорных модулей автоматизации для разных диверситетов были выбраны существенно различные микропроцессоры. Для каждой из платформ производители предоставляют собственные средства разработки. При этом из-за отсутствия совместимости даже на уровне языка представления алгоритмов, а также абсолютно различных аппаратных особенностях микропроцессоров нет физической возможности скопировать решения, принятые в одном диверситете в другой и таким образом растиражировать допущенные ошибки. Исходя из такого же принципа выбраны различные производители программируемых логических интегральных схем (ПЛИС).

Нельзя утверждать, что программный код не содержит скрытых ошибок, но благодаря разнообразию средств разработки и различным аппаратным спецификациям можно утверждать, что возникающие (при достаточно редких комбинациях внешних и внутренних сигналов, чтобы не быть зафиксированными при испытаниях) отказы будут возникать в разных диверситетах в разное время. Таким образом, в момент возникновения ядерной аварии какой-либо (или оба) из диверситетов будет готов выполнить запрос и выдать необходимые защитные команды.

Поскольку мы постулируем возможность отказа по общей причине программируемой системы, необходимо оценить, какова вероятность наложения этого события на аварию на энергоблоке. Такая оценка может быть получена при следующих предположениях:

– отказ обнаруживается и устраняется в течение времени τ после его возникновения;

– автоматические защитные действия выполняются в течение времени t после выявления аварии, по истечении этого времени защитные действия выполняет оперативный персонал, используя дистанционное управление;

– отказ программно-технического комплекса, связанный с постулируемой ошибкой в программе, причинно не связан с аварией на энергоблоке АЭС.

В этих предположениях вероятность отказа на требование выполнить автоматические действия, связанного с ошибкой в программном обеспечении, можно оценить как:

$\theta = \frac{\tau + t}{T}$, где T – среднее время работы программ, входящих в состав УСБТ, до их отказа. Оценочно, $(\tau+t)=(1\ldots10)$ ч, т.о., для получения разумно малого значения $\Theta \le (10^{-5}\ldots\ 10^{-7})$, необходимо подтвердить, что $T \ge 10^5 \ldots 10^8$ ч. Наиболее простой способ подтвердить значение вероятности – прямые испытания, однако их продолжительность оказывается неразумно большой. Для сокращения продолжительности работы по подтверждению надежности введен внутренний диверситет в каждый канал управляющей системы безопасности (рис. 2). Вероятность отказа можно оценить соотношением: $\frac{\theta_1 = (\tau + t)^2}{T_1 \times T_2}$, где T_1 и T_2, соответственно, среднее время работы до отказа программ, входящих в состав первого и второго подканала УСБТ. Оценочно, необходимо подтвердить, что: T_1 и $T_2 \ge (0{,}3\ldots3)10^4$ ч. Такая продолжительность испытаний представляется практически реализуемой для подтверждения

малой вероятности отказа программируемой УСБ по общей причине. При этом возможно параллельное проведение испытаний нескольких комплектов аппаратуры ТПТС-СБ, доводя, таким образом, длительность испытаний до вполне приемлемой. Сложные электронные компоненты для реализации схем диверситетов А и Б проиллюстрированы в таблице.

Аппаратное разнообразие

Средства, обеспечивающие аппаратное разнообразие модулей		
Тип модуля	Диверситет А	Диверситет Б
Модуль ввода унифицированных сигналов тока	ПЛИС Altera	Микроконтроллер STM
Модуль ввода сигналов термоэлектрических преобразователей и термопреобразователей сопротивления		
Модуль приоритетного управления	ПЛИС Altera	ПЛИС Xilinx
Модуль ввода аппаратных дискретных сигналов	ПЛИС Altera	ПЛИС Xilinx
Процессорный модуль автоматизации	Микропроцессор Freescale (PPC) + ПЛИС Altera + микроконтроллер Hilscher NetX	Микропроцессор Xilinx (ARM) + ПЛИС Xilinx
Модуль-размножитель 4-канальный	ПЛИС Altera	ПЛИС Xilinx
Преобразователь интерфейсов крейта	ПЛИС Altera	ПЛИС Xilinx
Модуль-коммутатор голосования	ПЛИС Altera	ПЛИС Xilinx
Модуль голосования	ПЛИС Altera	ПЛИС Xilinx

Для обеспечения независимости поведения программного обеспечения от внешних инициирующих факторов, возникающих при авариях, при разработке применялся принцип детерминизма. Это значит, что в любой момент времени можно предсказать интенсивность потоков данных между элементами системы безопасности. Более того, эта интенсивность постоянна и не зависит от времени и состояния внешнего оборудования (КИП, приводов, смежных систем) и идентична той, которая была зафиксирована при сдаче системы в промышленную эксплуатацию. Достигается такой эффект за счет исключения использования прерываний – вся обработка и пересылка сигналов происходит циклически. Таким образом, система безопасности, построенная на базе средств ТПТС-СБ, является системой реального времени.

Для обеспечения устойчивости к отказам по общей причине, связанных с ведением времени в системе, решено отказаться от поддержания системного времени в аппаратуре диверситетов А и Б. Время ведется и синхронизируется с временем АСУ ТП только в узлах нормальной эксплуатации, служащих для передачи информации из аппаратуры диверситетов А и Б в систему нормальной эксплуатации и СВУ, которые не взаимодействуют с узлами системы безопасности и не влияют на их работу.

В целях повышения устойчивости системы безопасности на базе средств ТПТС-СБ к кибератакам на передней панели процессорного модуля предусмотрен физический ключ, запрещающий или разрешающий запись прикладного программного обеспечения со стороны инжиниринговых средств – САПР GET-R1, а также изменение настроечных параметров прикладного программного обеспечения с помощью сервисных средств ТПТС.

В завершение следует отметить, что АСУ ТП Белорусской АЭС, построенная на базе средств ТПТС-НТ в СНЭ (уровни 1, 2, 4) и ТПТС-СБ в УСБ (уровень 3) полностью отвечает всем требованиям по разнообразию, независимости, резервированию. Реализован принцип глубокоэшелонированной защиты. Цифровая система безопасности на базе ТПТС-СБ, применяя впервые в мире встроенный программный и аппаратный диверситет на каждом этапе выполнения функций УСБ, гарантирует выполнение функции как при единичном отказе, так и при отказе по общей причине, в том числе и программного обеспечения. Применение ТПТС-СБ для построения АСУ ТП АЭС в сочетании с ТПТС-НТ позволяет создать гармоничную АСУ ТП с оптимизированными связями безопасности и нормальной эксплуатации, а также с блочным и резервным пунктами управления, что обеспечит эффективное и безопасное управление энергоблоком.