УДК 621.039.058

Л.Ю. ПАЦЕВА, Ю.Н. ХЛЕПЕТЬКО

ЗАО "СНПО "Импульс", Украина

АППАРАТУРА УПРАВЛЕНИЯ ОРГАНАМИ РЕГУЛИРОВАНИЯ ВВЭР-440. ОСНОВНЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Рассмотрены особенности построения и вопросы функциональной декомпозиции системы управления органами регулирования (СУОР-И). Освещены основные подходы к поэтапному тестированию (испытаниям) функций СУОР-И. Приведено описание имитационно-моделирующего испытательного стенда, использованного для функциональных испытаний в реальном масштабе времени.

функции безопасности, минимизация рисков, распределение ресурсов, устранение дефектов, подтверждение соответствия

Введение

В настоящее время очень остро и актуально стоит вопрос гарантированности функциональной безопасности критических и одновременно сложных систем управления, базирующихся на программируемых электронных компонентах. При этом под безопасностью систем понимается их работоспособное состояние и функционирование в соответствии с требованиями заказчика и технической документации, при которых отсутствуют опасные отказы и недопустимый ущерб [1]. Другими словами: безопасность системы – это качественное и надежное ее функционирование в части выполнения критических функций.

В рамках данной проблемы на первый план выдвигается безопасность технологии создания таких систем, которая гарантировала бы предотвращение большинства видов дефектов и ошибок при создании и модификации систем и их компонентов, обеспечивающих безопасность, а также уменьшила бы риск уязвимости от сбоев и отказов в процессе функционирования. Проблеме обеспечения функциональной безопасности критических систем посвящено не так уж много официальных документов, в основном это рекомендации МАГАТЭ и МЭК [2, 3]. Больше внимания уделяется вопросу обеспечения функциональной и информационной безопасности программных средств, что является не совсем справедливым и, на наш взгляд, однобоко представляет существующую проблему.

В статье изложены использованные для обеспечения функциональной безопасности концептуальные подходы при разработке программно-технических средств управления органами регулирования (СУОР-И) системы управления и защиты реактора ВВЭР-440.

В статье не рассматриваются проблемы, связанные с обеспечением аппаратной отказоустойчивости при воздействиях аномальных природных явлений и отклонениях условий эксплуатации, а также не рассматриваются нарушения и отказы, не влияющие на безопасность функционирования системы, на формирование управляющих воздействий объекту управления и на информацию, предоставляемую оперативному персоналу по управлению реакторной установкой.

Следует сразу сказать об основных аспектах, которые существовали на момент начала работ и которые повлияли на выбранные и использованные подходы к технологии разработки СУОР-И. Во-первых, – это сложность разрабатываемой системы, обусловленная технологическими особенностями объекта управления. Во-вторых, – это, к сожалению, ставшая уже нормой в современном мире, – ограниченность во временных ресурсах.

Технологические особенности объекта управления

Аппаратура управления органами регулирования СУОР-И представляет собой исполнительную часть СУЗ реакторной установки типа ВВЭР-440, предназначенную для регулирования, прекращения или замедления реакции деления в активной зоне реактора путем воздействия на приводы СУЗ в соответствии с принятыми извне (от подсистемы аварийной защиты, от автоматического регулятора мощности или от оператора БЩУ) и сформированными командами управления.

Исходя из назначения и характера выполняемых функций и в соответствии с классификацией по НП 306.5.02/3.035, СУОР-И относится к управляющим системам безопасности (УСБ), совмещающим функции систем нормальной эксплуатации (УСНЭ), а по влиянию на ядерную безопасность – к классу безопасности 2 (классификационное обозначение – 2НУ).

Исполнительными механизмами для управления реактивностью реакторной установки являются 37 приводов с низкооборотными электродвигателями (ЭД) синхронно-реактивного типа РД42-4РВ для перемещения кассет АРК и указателями положения типа ЛД-1 для определения положения кассет АРК в активной зоне реактора.

Электродвигатель служит для создания крутящего момента с целью перемещения рейки с кассетой АРК и удержания их в пределах рабочего хода. Низкая частота питающего напряжения, подаваемая на ЭД, обусловлена малым передаточным отношением редуктора, при котором нужно обеспечить приемлемую для безопасности скорость перемещения кассеты АРК и, следовательно, скорость изменения положительной реактивности. В тормозном режиме (частота питающего напряжения на двигателе равна 0) двигатель удерживает рейку с приводом в заданном положении по высоте активной зоны. Ход вниз, вверх определяется чередованием фаз питающего напряжения ЭД.

Вращательное движение двигателя преобразуется в поступательное движение гайки-шунта в датчике положения типа ЛД-1. Внутри корпуса ЛД-1 установлены индукционные катушки, изменение напряжения во вторичной обмотке которых пропорционально положению привода.

Основные подходы при разработке

Из всех этапов разработки любой системы, важной для безопасности, критичными являются как начальные этапы, на которых определяются основные функции и их свойства в части безопасности и качества, а также принимаются концептуальные системные решения по структуре и распределению задач (функций) между компонентами, так и завершающие этапы, на которые возлагается кропотливая задача экспериментального подтверждения характеристик, показателей назначения, требований к безопасности.

Поэтому для определения основных функций СУОР-И и требований к ним части безопасности и качества были тщательно изучены:

1) специфика объекта управления (принципы работы датчика ЛД-1 и электродвигателя РД42-4РВ) путем проведения экспериментальных исследований;

2) принципы работы действующей системы управления и взаимосвязь со смежными системами энергоблока посредством тщательного изучения всей эксплуатационной документации;

3) регламент эксплуатации модернизируемой системы, а также особенности технического обслуживания;

4) современные требования нормативных документов Украины, МАГАТЭ, МЭК к системам, важным для безопасной работы АЭС;

5) существующие аналоги разработки других фирм.

Для разработки общих требований к основным функциям были проанализированы все доступные

ресурсы для их реализации с учетом допустимого ущерба (рисков вследствие отказов при неполном выполнении требований), определены и оценены факторы уязвимости, возможные оказать влияние на основные характеристики качества и безопасности, а также на суммарный риск [4]. К основным факторам уязвимости можно отнести [1]:

1) технические отказы внешней аппаратуры и искажения исходной информации от объектов внешней среды и от потребителей систем и обработанной информации;

2) случайные отказы, сбои и физические разрушения элементов и компонентов аппаратных средств вычислительных комплексов и средств коммуникации;

3) ошибки оператора по управлению реакторной установкой и ошибки обслуживающего персонала;

4) дефекты и ошибки в комплексах программ обработки информации и в данных;

5) пробелы и недостатки в средствах обнаружения опасных отказов и оперативного восстановления работоспособного состояния систем, программ и данных.

Для минимизации рисков при любых внутренних и внешних негативных воздействиях и обеспечения равнопрочной защиты безопасности функционирования разработка структуры СУОР-И и распределение ресурсов и задач между компонентами выполнены исходя из следующих основных принципов:

1) обеспечение выполнения функции аварийной защиты 1 рода при любом количестве отказов;

2) обеспечение выполнения управляющих и информационных функций при любом единичном отказе;

3) равномерное распределение задач функционирования и мер по защите между аппаратными и программными средствами с обеспечением избыточности по ресурсам (структурной, временной, информационной);

4) обеспечение защиты на всех уровнях (измерения, ввода, обработки и вывода);

5) модульное построение технических и программных средств;

6) глубокоэшелонированное техническое диагностирование;

7) обеспечение регистрации всех нештатных ситуаций для последующего анализа и устранения дефектов.

Обеспечение высокого качества выполнения всего процесса проектирования, разработки и изготовления технических средств (ТС) и программного обеспечения (ПО) достигнуто применением стандартизированных процедур и технологий, соответствующих международным стандартам обеспечения безопасности и качества. Рассмотрим особенности поэтапного функционального тестирования и испытаний компонент и СУОР-И в целом.

Независимое функциональное тестирование и испытания являются основным методом устранения дефектов, измерения и определения реальных характеристик функций на любых этапах их жизненного цикла и должны устанавливать, что все функции действительно демонстрируют свойства безопасности, необходимые для удовлетворения требований спецификаций [4].

Для обеспечения вышеуказанных целей, задач функционального тестирования и испытаний в реальном масштабе времени такой сложной как СУОР-И системы необходимо было создание комплексного имитационно-моделирующего испытательного стенда, который бы обеспечил:

1) поэтапную проверку «снизу-вверх», начиная от функций каждой подсистемы, сопряжений между подсистемами и заканчивая функциями СУОР-И;

2) проверку методом «черного ящика», исключая любое вмешательство в функционирование компонент;

3) распределение имитирующих воздействий по реальных физическим каналам и временным тактовым интервалам, равным 20 ms;

4) имитацию динамических изменений, соответствующих как нормальным режимам функционирования, так и различным нарушениям, отказам;

5) управление моделируемыми данными в соответствии с предопределенными сценариями;

6) регистрацию результатов работы испытуемого компонента для последующего анализа;

7) возможность сопровождения разработанного комплекса СУОР-И на последующих этапах жизненного цикла.

В связи с ограниченными временными ресурсами на разработку и тестирование были приняты следующие основные концептуальные решения по созданию комплексного имитационно-моделирующего испытательного стенда:

1) разработать и изготовить физические имиторы основных устройств: датчиков положения привода ЛД-1 и электродвигателей (в части имитации нагрузки);

2) в качестве технических средств использовать унифицированный комплекс МСКУ 3, являющийся базовым для центральной подсистемы СУОР-И – подсистемы группового управления. Такой выбор обеспечил имитацию 74 устройств, подключенных через радиальные линии связи приема-передачи, 80 входных и 48 выходных дискретных сигналов;

3) функционирование имитационных моделей обеспечить программными средствами, размещенными в шкафу технологическом и на инструментальной ПЭВМ.

Следует отметить, что в связи со сложностью модели поведения разработанный имитационно-моделирующий испытательный стенд не мог обеспечить автоматическое сравнение фактических результатов с эталонными в реальном времени и оценку их приемлемости (правильности) с формированием заключения.

Эта задача выполнялась, как отдельная процедура, группой экспертов.

Далее в разделах изложены основные решения по затронутым выше вопросам обеспечения функциональной безопасности СУОР-И.

Состав и характеристики функций СУОР-И

СУОР-И обеспечивает выполнение основных (управляющих и информационных) и вспомогательных функций.

К основным **управляющим функциям** относятся:

1) автоматическое управление перемещением АРК по сигналам аварийных защит;

2) автоматическое управление перемещением АРК в режиме регулирования по сигналам от АРМ;

3) дистанционное управление перемещением АРК по командам оператора.

К **информационным функциям** относятся:

1) индикация текущего положения и состояния АРК на БЩУ и РЩУ;

2) сигнализация нарушений в работе оборудования;

3) обеспечение информацией смежные подсистемы АСУТП энергоблока (ИВС, СВРК).

К **вспомогательным функциям** относятся:

1) контроль работоспособности и правильности функционирования собственных программных и технических средств, а также состояния внешних линий связи;

2) регистрация и визуализация параметров, их изменений и нарушений.

Основные качественные характеристики СУОР-И:

1) время прохождения сигнала АЗ-1 - не более 100 ms;

2) точность позиционирования кассеты АРК – не более 15 mm.

В таблице 1 приведены основные структурные решения по реализации функций СУОР-И для обеспечения ее функциональной безопасности.

Таблица 1

Основные структурные решения

Функция	Диверсность	Резервирование	Независимость
Управление перемещением АРК	Для АЗ-1	2 из 3D и 1 из 2D	Есть
Индикация положения и состояния АРК	Есть	1 из 2D	Есть
Обеспечение данными смежные подсистемы СУЗ	Нет	1 из 2D	Есть
Электропитание	Нет	1 из 2D	Есть
Регистрация и визуализация результатов контроля	Нет	1 из 2D	Есть

Состав и характеристики функциональных подсистем СУОР-И

Структурная декомпозиция позволяет выделить из всей совокупности предполагаемых функций СУОР-И ряд функциональных подсистем, представляющих собой совокупность технических и программных средств, объединенных по признаку участия в выполнении однородных функций [5]:

1) подсистема контроля и управления приводами АРК (ПКУП);

2) подсистема группового управления приводами АРК (ПГУ);

3) подсистема электропитания (ПЭ);

4) подсистема взаимодействия с оператором (ПВО);

5) подсистема контроля и диагностирования состояния технических и программных средств (ПКД).

Подсистема контроля и управления приводами ПКУП предназначена для управления электродвигателями по командам подсистемы группового управления, определения зоны положения кассет АРК по сигналам от датчиков типа ЛД-1 и представления ее на индивидуальных индикаторах положения (на БЩУ и РЩУ).

Подсистема ПКУП состоит из 37 независимых каналов силового управления, каждый из которых управляет одним своим приводом АРК, с независимым электропитанием каждого устройства каждого канала.

Аппаратура каждого канала силового управления движением каждой кассеты реализована с применением структурной избыточности, обеспечивающей облегченное (теплое) резервирование методом замещения. Кратность резервирования – 1.

Отказ нерезервированного устройства определения положения не приведет к потере информации о положении кассеты АРК (в случае ее не падения), поскольку в СУОР-И реализован диверсный способ определения положения АРК по текущей фазе, формируемой на электродвигатель.

Подсистема группового управления ПГУ предназначена для принятия решения и формирования (в соответствии с алгоритмами управления и текущими положениями приводов) управляющих воздействий (команд) в подсистему контроля и управления приводами:

1) по сигналам от АРМ и органов ручного управления оператора БЩУ,

2) по командам аварийных защит от внешних подсистем СУЗ.

ПГУ также обеспечивает расчет точного положения приводов в миллиметрах, динамический контроль перемещения кассет АРК.

ПГУ реализована с применением структурной избыточности, обеспечивающей нагруженное (горячее) постоянное резервирование методом голосования. Кратность резервирования – 2.

Каждый из трех независимых каналов (с независимым электропитанием и отсутствием «горизонтальных» информационных связей) выдает по радиальным линиям связи в ПКУП команды управления на движение АРК.

Команды поступают на вход соответствующего канала силового управления, где происходит их выбор по мажоритарному принципу 2 из 3 применительно к трем каналам ПГУ.

Подсистема электропитания ПЭ предназначена для обеспечения электропитания силовой аппаратуры напряжением 220 V постоянного тока, а также питания части технических средств СУОР-И, аппаратуры РОМ и АРМ трехфазным напряжением переменного тока 220/380 V частотой 50 Hz.

ПЭ реализована с применением структурной избыточности, обеспечивающей общее облегченное (теплое) постоянное резервирование. Кратность резервирования – 1.

Каждый из двух независимых полукомплектов ПЭ обеспечивает гарантированное электропитание линий 1L, 3L и 2L, 4L соответственно. Подача электропитания к каждому устройству обеспечивается индивидуальными линиями с защитой от перегрузки по току и короткого замыкания.

Подсистема взаимодействия с оператором ПВО предназначена для обеспечения ручного управления органами регулирования, представления в графическом и цифровом виде информации о текущем положении и состоянии кассет АРК, формирования предупреждений и сигнализации нарушений на мониторе пульта оперативного наблюдения БЩУ. ПВО также обеспечивает автоматизацию выполнения тестовых операций «Эксперимент» и «Осциллографирование».

ПВО реализована методом раздельного (горячего) резервирования следующих элементов:

1) контактных групп кнопок и переключателей с кратностью 2;

2) линий связи пульта оперативного наблюдения с кратностью 1.

ПВО реализована с учетом принципов независимости и разнообразия:

1) сигналы на движение АРК от ключей управления БРУ передаются независимо в каждый канал ПГУ посредством прямых кабельных линий связи;

2) устройства индикации, участвующие в функции индикации положения каждой кассеты АРК, полностью независимы и сгруппированы в два комплекта – для БЩУ и РЩУ. Каждый индикатор соединен радиальной линией связи с устройством определения положения по сигналам от ЛД-1 для получения данных и электропитания;

3) на мониторе пульта оперативного наблюдения отображаются положения кассет АРК, сформированные двумя независимыми способами: по сигналам от датчика положения ЛД-1 (по зонам) и по текущей фазе питания электродвигателя (в mm). Пульт не только резервирует информацию о текущем положении кассет АРК, индицируемую на табло индикации положения ТИП, но и представляет ее в удобной для оператора форме (в виде гистограмм, графиков, цветовой сигнализации нарушений).

Подсистема контроля и диагностирования ПКД предназначена для выполнения контроля работоспособности и правильности функционирования технических и программных средств СУОР-И, включения сигнализации на БЩУ при обнаружении неисправностей или отказов в работе аппаратуры, а также для регулярного сбора, регистрации и представления в графическом и текстовом видах параметров функционирования СУОР-И. ПКД также реализует функцию передачи (посредством цифровых сообщений) информации о точном положении кассет АРК в систему внутриреакторного контроля (СВРК).

ПКД реализована с применением структурной избыточности, обеспечивающей нагруженное (горячее) постоянное резервирование по функциям обработки данных и резервирование замещением по функциям визуализации. Кратность резервирования – 1.

ПКД реализована с учетом принципа независимости:

1) информационные функции визуализации, регистрации и сигнализации реализованы в двух независимых шкафах;

2) функции контроля и диагностирования отделены от функций управления физически и не влияют на их выполнение;

3) обмен данными с СВРК реализован по индивидуальным оптоволоконным каналам передачи информации.

Для обеспечения функциональной живучести и детерминированности информационное взаимодействие между подсистемами реализовано в виде двухуровневой локальной сети с «радиальной» организацией потоков данных (термин «сеть» подразумевает организованную совокупность абонентов, взаимодействующих по предопределенным правилам, называемым «протоколом»).

Все компоненты СУОР-И соединены между собой радиальными линиями связи и обеспечивают информационное и электрическое соединение по принципу «точка-точка». Все информационные и электрические связи между компонентами ПТК СУОР-И имеют гальваническое разделение.

Для каждого компонента, участвующего в двунаправленном обмене данными, процессы обслуживания канала приема и передачи являются независимыми друг от друга. Выход из строя какого либо канала обмена не влияет на работу остальных каналов и на СУОР-И в целом. Команда управления передается регулярно посредством структурированного сообщения предопределенной длины и с контрольной суммой.

Локальная сеть нижнего уровня ЛСНУ функционально разделена на:

1) локальную управляющую сеть для передачи команд управления и данных, обеспечивающих функционирование СУОР-И;

2) локальную информационную сеть для сбора диагностической информации составных частей СУОР-И.

Локальная сеть верхнего уровня ЛСВУ по своим функциям является информационной сетью, предназначенной для обеспечения СВРК и внешних систем энергоблока оперативными данными результатов функционирования, контроля и диагностирования СУОР-И. В основу прикладного протокола обмена для ЛСВУ легли требования документа «Техническая спецификация сопряжения ИВС «КОМПЛЕКС АЭС» с локальными системами энергоблока».

Состав и характеристики испытательного стенда

Имитационный испытательный стенд (ИИС) представляет собой совокупность средств испытываемой системы СУОР-И, одного реального электродвигателя РД42-4РВ и одного линейного датчика ЛД-1, физических имитаторов внешних устройств, программно-технических средств моделирования основных компонентов СУОР-И, комплекса программ имитации внешних сигналов, визуализации и регистрации результатов работы испытываемых компонент.

Разработанный физический имитатор датчика положения привода ЛД-1 по состоянию и чередованию фаз, формируемых устройством силового питания на ЭД, определяет текущее грубое положение АРК и формирует соответствующие напряжения, имитирующие сигналы с катушек ЛД-1. Физический имитатор ЛД-1 обеспечивает возможность имитации обрыва любой из катушек датчика, а также «застревание» привода.

Разработанный физический имитатор электродвигателя обеспечивает имитацию нагрузки РД42-4РВ в каждой из фаз А, В, С.

Проверка правильности функционирования физических имитаторов проводилась экспериментально путем сравнительного анализа работы канала управления приводом с реальными электродвигателем РД42-4РВ и датчиком ЛД-1 и канала управления приводом с имитаторами основных устройств.

Программно-технические средства моделирования основных компонент СУОР-И скомплексированы из устройств унифицированного комплекса МСКУ 3 и специализированного программного обеспечения в технологическом шкафу и обеспечивают следующие режимы работы:

1) имитацию подсистемы группового управления в части формирования команд управления – при проверке функций канала ПКУП;

2) имитацию подсистемы контроля и управления приводами и внешних устройств (датчика ЛД-1 и электродвигателя) – при проверке функций канала ПГУ, подсистемы контроля и диагностирования, подсистемы взаимодействия с оператором;

3) имитацию подсистемы электропитания в части формирования сигналов состояния оборудования – при проверке функций контроля электропитания.

Комплекс программ имитации внешних сигналов, визуализации и регистрации результатов работы испытываемых компонент, функционирующий на инструментальной ПЭВМ, обеспечил тестирование компонент СУОР-И в следующих режимах:

1) ручном с заданием набора исходных данных в диалоговом окне;

2) пакетном с формированием нескольких наборов исходных данных (сценария тестирования) и соответствующего временного расписания смены наборов, и одновременным ведением архивирования всех результатов;

3) автоматическом с выбором предопределенного набора тестовых данных и получением результатов проверки. Предопределенные внешние воздействия формировались в виде сценариев в файле формата Excel, куда же заносились полученные от проверяемых компонент СУОР-И результаты их работы. Анализ выполненных проверок осуществлялся визуально экспертами.

Разработанный испытательный стенд обеспечил имитацию динамических изменений предопределенных внешних воздействий (с дискретностью 20 ms), соответствующих как нормальным режимам функционирования, так и различным нарушениям, отказам, что позволило проверить внутреннюю непротиворечивость и полноту реализации функциональных требований, требований к безопасности, а также временных характеристик.

Заключение

Изложенные в статье концептуальные подходы, использованные при разработке программно-технических средств, позволили гарантировать высокую вероятность обеспечения функциональной безопасности системы управления органами регулирования СУОР-И.

Разработанная аппаратура системы управления органами регулирования СУОР-И позволяет повысить безопасность эксплуатации реакторной установки и вывести на более высокий уровень надежности за счет существенного расширения функциональных возможностей аппаратуры, направленных на своевременное обнаружение дефицита безопасности, уменьшение времени на его устранение и значительное повышение информативности средств визуального наблюдения оперативного персонала щитов управления.

Литература

1. Липаев В.В. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств. – М.: Jet Info. № 08.2004.

2. Серия норм МАГАТЭ по безопасности.

3. IEC 61508:1-6: 1998. Функциональная безопасность электрических / электронных / программируемых электронных систем безопасности.

4. Липаев В.В. Функциональная безопасность программных средств. – М.: Jet Info. № 08.2004.

5. Системы контроля и управления технологическими процессами: Сб. научн. ст. / Под общ. ред. В.В. Елисеева. – Луганск: Світлиця, 2006. – 440 с.

Поступила в редакцию 1.03.2007

Рецензент: д-р техн. наук, проф. М.А. Ястребенецкий, Государственный научно-технический центр по ядерной и радиационной безопасности, Харьков.