Комплекс технических средств непрограммируемой логики (КТС НПЛ) для защиты ядерных реакторов АЭС

В статье представлено решение, разработанное для повышения надежности систем защиты ядерного реактора атомных электростанций: комплекс технических средств, построенный на базе непрограммируемой («жесткой») логики. Данное решение позволяет защитить реактор в случае возникновения в процессе эксплуатации ошибок в программном обеспечении управляющих систем, построенных на программируемых технических средствах, которые невозможно выявить на стадии испытаний и приемки.

ООО «Московский завод «ФИЗПРИБОР», г. Москва

Хотя «умные» устройства агрессивно захватывают мир, даря пользователям неслыханную прежде эффективность, легкость исполнения и выгоду, есть высокотехнологичные сферы, где им не доверяют и стараются ограничить их применение. Управляющие технологическим процессом системы, созданные на средствах программируемой логики, имеют свои уязвимые места, связанные с непрогнозируемой возможностью отказа по общей причине программного обеспечения. Это недопустимо при выполнении некоторых ответственных и опасных задач в системе защиты ядерного реактора на АЭС.

Применение в управляющих системах, важных для безопасности, решений, построенных на базе программируемой логики, оправданно для выполнения таких функций, как информирование и диагностика. В то же время выполнение с их помощью функций управления следует ограничивать по следующим причинам:

- во-первых, в программах могут быть ошибки, которые практически невозможно отследить и доказать их наличие. Надежность программного обеспечения непредсказуема, и ошибки могут проявить себя в критически важный момент;
- во-вторых, интегральные схемы «интеллектуальных» устройств очень сложны, а значит, их невозможно полностью проверить и проконтролировать действия, которые они выполняют.

Для обеспечения разнообразия в системах безопасности АЭС и исключения вероятного отказа оборудования из-за случайных или преднамеренных ошибок в программном обеспечении специалистами ООО «Московский завод «ФИЗПРИБОР» для нужд АО «Концерн Росэнергоатом» разработан комплекс технических средств непрограммируемой логики (КТС НПЛ).

Комплекс обеспечивает возможность построения диверсных систем защиты с ограниченными функциями в дополнение к существующим системам безопасности, построенным на программируемых технических средствах, а также применяется для создания полноценных каналов управляющих систем безопасности.

Функциональность КТС НПЛ

Комплекс технических средств непрограммируемой логики предназначен для формирования команд на запуск технологических систем безопасности, обесточивания приводов органов регулирования системы управления и защиты реактора в соответствии с алгоритмами, заданными проектом АЭС.

Комплекс обеспечивает:

- прием и обработку аналоговых и дискретных сигналов от первичных преобразователей (датчиков) и смежных систем на непрограммируемых средствах (без использования микроконтроллеров и программируемых логических интегральных схем – ПЛИС);
- реализацию функций защит на непрограммируемых средствах;
- выдачу информации о контролируемых параметрах и состоянии составных частей комплекса для предоставления на блочном и резервном пунктах управления, в системе верхнего блочного уровня (СВБУ) непрограммируемыми и программируемыми средствами;
- проверку технических средств, реализующих алгоритмы защиты,

и линий связи непрограммируемыми средствами.

Реализация функций защиты на непрограммируемых средствах позволяет:

- исключить из рассмотрения непредсказуемую надежность программного обеспечения;
- исключить влияние на функцию защиты аспектов информационной безопасности;
- проводить расчеты надежности, в том числе с учетом отказов по общей причине, что невозможно для программного обеспечения.

Инновационные решения, примененные при создании КТС НПЛ

- Алгоритмы защит реализованы на непрограммируемых средствах (логические вентили, счетчики, регистры) без использования микроконтроллеров и ПЛИС любой степени интеграции.
- Цифровая обработка аналоговых сигналов также выполняется непрограммируемыми средствами (преобразование шкал, фильтрация 50 Гц, демпфирование, линеаризация, компенсация температуры холодного спая, коррекция уровня), посредством табличной обработки на микросхемах энергонезависимой памяти.
- Непрограммируемыми средствами проводится и периодическая автоматизированная проверка (так называемое опробование) основной доли оборудования, включая проверку алгоритмов, внутрисистемных линий связи, а также линий связи с исполнительными механизмами.
- Обеспечено резервирование (работа по трехканальной или четырехканальной схеме) не только датчиков, но и аппаратных средств реализации алгоритмов для особо ответственных защит (разрывные защиты и др.). При этом опробование оборудования проводится без вывода его из эксплуатации и без потери функции защит на работающем энергоблоке.
- Передача информации о дискретных и аналоговых сигналах, срабатывании системы, состоянии технических средств комплекса в систему верхнего блочного уровня (СВБУ) реализовано с применением программируемых средств. На базе микроконтроллеров и процессорных модулей собственной разработки построены резервированная локальная сеть функциональных блоков и резервированная сеть связи с СВБУ. При этом обеспечено отсутствие влияния программируемых средств на работу средств «жесткой» логики, в том числе в случае отказа программируемых средств.

Построение системы и принцип ее работы

Технические средства КТС НПЛ в части реализации функций защиты выполнены на непрограммируемой элементной базе.

Узлы аналого-цифрового преобразования и гальванической развязки блоков сбора и обработки аналоговых сигналов выполнены на 24-разрядных аналого-цифровых преобразователях архитектуры «сигма-дельта» без встроенного микроконтроллера и на микросхемах цифровой гальванической развязки.

Узлы обработки сигналов и сравнения с уставкой во всех блоках вы-

Рис. 1. Комплекс технических средств диверсной системы защиты

полнены на микросхемах энергонезависимой памяти EEPROM (200 лет хранения, не менее 1,2 млн циклов перезаписи, встроенная коррекция ошибок) и микросхемах дискретной логики (вентили И, ИЛИ, НЕ и их сочетания, счетчики, триггеры, мультиплексоры, дешифраторы, регистры). Следует отметить, что в микросхемах памяти хранятся только таблицы данных, но не команды, поскольку устройства, способные выполнять команды (микроконтроллеры, процессоры) при реализации функций защиты не применяются.

Узлы мажоритарной обработки в блоках управления исполнительными механизмами выполнены по схеме шести ключей на оптических реле. Электромагнитные реле в блоках, обеспечивающих реализацию функций защиты, не применяются.

Структура комплекса предусматривает резервирование (работа по трехканальной или четырехканальной схеме) 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 АЭС.

Основу комплекса составляют блоки сбора сигналов и блоки логической обработки.

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 индивидуально для каждого входа блока в диапазоне 50 мс – 10 с);
- 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 уровня;
- 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, встроенных в функциональные блоки, и процессорных модулей (концентраторов).

Логическая обработка сигналов предусматривает:

- мажоритарную обработку по логике «2 из 3» («2 из 4»);
- обработку на логических элементах типа И, ИЛИ, НЕ, триггер;
- выдержку времени.

Принцип работы комплекса можно рассмотреть на примере диверсной системы защиты (ДСЗ) по обесточиванию органов регулирования системы управления и защиты реактора.

Каждый из аналоговых сигналов вводится от трех или четырех одноименных датчиков в три шкафа ДСЗ (рис. 1). В шкафах ДСЗ (в блоках сбора и обработки унифицированных сигналов тока) 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» (в блоках мажоритарной логики «2 из 3») и логической обработке (в блоках логической обработки, 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».

Линии связи с источниками сигналов контролируются непрерывно, аналого-цифровые преобразователи блоков – косвенно, через вычисление процессорными модулями (концентраторами) аналогового рассогласования.

Периодически (при опробовании) контролируются:

- дискретная логика всех блоков, включая внутришкафные и межшкафные линии связи между ними;
- логика аналоговых блоков от выхода аналого-цифрового преобразователя;
- срабатывание (замыкание) каждого из силовых ключей в отдельности.

Преимущества КТС НПЛ

Сбор аналоговых и дискретных сигналов с технических средств комплекса и их выдачу в резервированную локальную сеть осуществляют микроконтроллеры, встроенные в функциональные блоки. Кроме того, микроконтроллеры независимо от опробования осуществляют непрерывную пассивную диагностику (без воздействия на непрограммируемые средства) отдельных узлов функциональных блоков, в частности контроль сигналов АЦП, содержимого памяти, прохождения дискретных сигналов.

Отсутствие влияния программируемых средств на непрограммируемые достигается следующим образом:

- цепи питания основной (непрограммируемой) и программируемой схем разделены: для питания каждой из схем используется отдельный стабилизатор напряжения, каждая из цепей питания защищена отдельным самовосстанавливающимся предохранителем;
- сигналы из основной схемы выдаются через однонаправленные буферы (усилители). Выход буфера защищается резистором, что предотвращает его перегрузку или выход из строя при неисправностях в программируемой схеме (при коротких замыканиях, пробое на шину питания и т. п.);
- каждая из схем с помощью своих средств диагностики формирует сигнал исправности в виде замкнутого «сухого» контакта. «Сухие» контакты соединяются последовательно, формируя линию контроля блока. Линии контроля блоков шкафа также соединяются последовательно, формируя общую линию (обобщенный сигнал) исправности шкафа.

При реализации функций защиты принципиально не использова-

лись программируемые логические интегральные схемы, в том числе ПЛИС малой степени интеграции, по следующим соображениям:

- в ПЛИС высокой степени интеграции можно с помощью загруженных соединений реализовать ядро микроконтроллера (соответствующие прошивки предоставляются производителями ПЛИС), при этом подтверждение отсутствия загруженного ядра требует проведения верификации прошивки ПЛИС;
- для подготовки и загрузки прошивки в ПЛИС используются программные продукты (САПР), которые также требуют верификации и отсутствие критических ошибок в которых практически недоказуемо;
- отказ в ПЛИС может привести не только к потере отдельных ячеек ПЛИС, но и подключению к схеме ранее не использовавшихся ячеек и образованию ранее отсутствовавших связей, что приводит к непредсказуемому поведению ПЛИС при отказе;
- схема на ПЛИС, в которой доступны только входы и выходы, трудно проверяема уже на этапе разработки. В случае наличия в схеме большого количества входов и выходов становится затруднительным перебрать все сочетания входных сигналов. В случае использования в схеме триггеров в качестве элементов памяти или каскадов счетчиков (что практически всегда бывает при реализации реальных алгоритмов) проверка схемы еще более осложняется, поскольку состояние выходов в текущий момент времени определяется не только текущим состоянием, но и предыдущими состояниями входов.

Срок службы системы, построенной на базе КТС НПЛ, с учетом ремонта и восстановительных работ – не менее 30 лет.

Вероятность невыполнения управляющей функции на требование на интервале один год – не более 10^{-6}.

Комплекс технических средств непрограммируемой логики (КТС НПЛ) – это решение, ставящее во главу угла надежность работы, максимальную защищенность от киберугроз и отвечающее наиболее строгим требованиям к отказоустойчивости систем, важных для безопасности атомных станций.

С.И. Сафонов, первый заместитель генерального директора по техническим вопросам, производству и качеству,
ООО «Московский завод «ФИЗПРИБОР»,
г. Москва,
тел.: +7 (495) 228-6019,
e-mail: info@fizpribor.ru,
сайт: www.fizpribor.ru