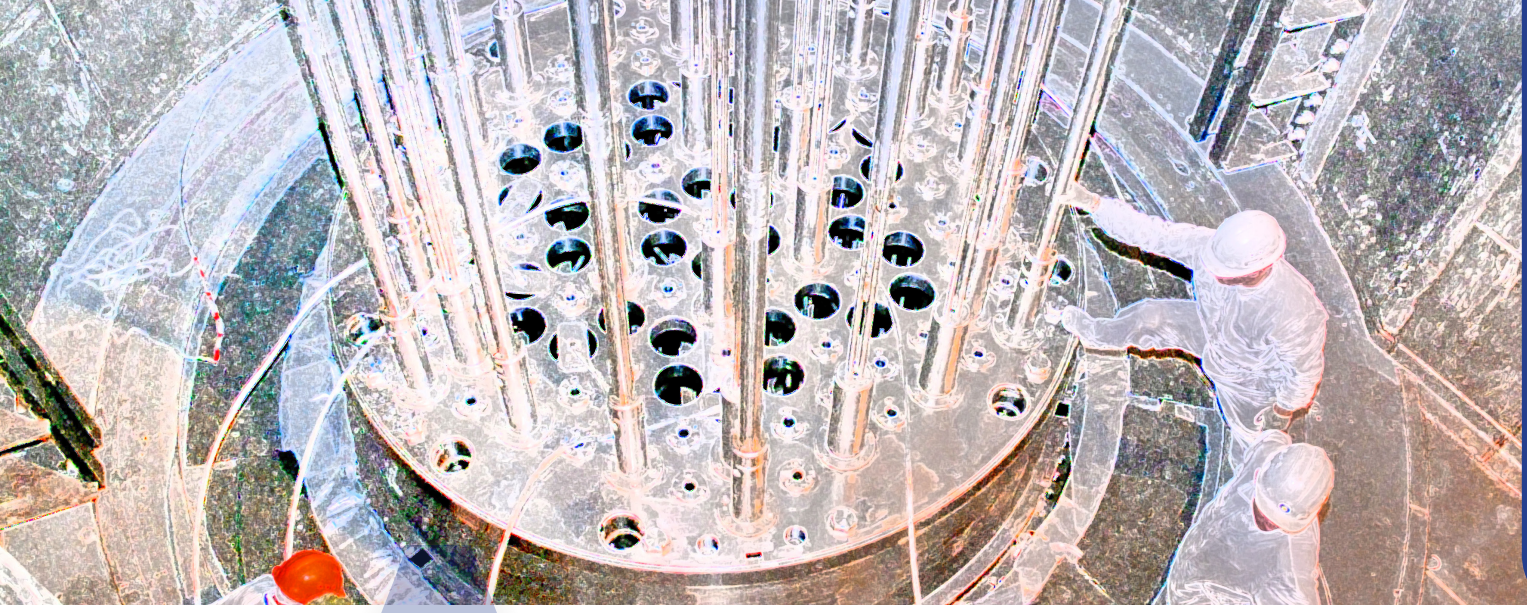

УДК: 621.039.50 + 621.3.015

ДИВЕРСНЫЕ ЗАЩИТЫ. ОБЕСПЕЧЕНИЕ РАЗНООБРАЗИЯ ПРИ ПРОЕКТИРОВАНИИ АВАРИЙНЫХ ЗАЩИТ АТОМНЫХ СТАНЦИЙ

Алпеев А.С. к.т.н. (ФБУ «НТЦ ЯРБ»)

В статье рассмотрены проблемы обеспечения разнообразия при проектировании аварийных защит атомных станций, виды и методы реализации разнообразия, их особенности. Отмечены недостатки и пробелы в нормативном обеспечении по этой проблеме. Определено понятие «диверсная защита» и даны рекомендации по применению.

► ***Ключевые слова:*** *атомная станция, защита, разнообразие, безопасность, требование, функция, функциональная группа, надежность, безотказность, управляющая система, структура, кибератака.*

DIVERSITY PRINCIPLE IN PROTECTION. PROVISION OF DIVERSITY IN THE PROJECT EMERGENCY PROTECTION OF NUCLEAR POWER PLANTS

Alpeev A.S., Ph.D. (SEC NRS)

The article considers problems of species diversity in the design of emergency protection of nuclear power plants, the methods of implementation of diversity and their features. Are noted deficiencies and gaps in the regulatory provision on this problem. Is defined the concept of «diversity principle in protection» its features and the recommendations for use.

► ***Key words:*** *nuclear power plant, protection, diversity, safety, requirement, function, dependability, reliability, controlling system, structure, cyber attack.*

Аварийные защиты атомных станций играют первостепенную роль в обеспечении их безопасности при функционировании в режимах с нарушениями нормальной эксплуатации, в том числе при проектных авариях. В связи с этим к качеству реализации функций аварийных защит нормативными документами по безопасности атомных станций предъявляются достаточно жесткие технические требования. Так, например, в таблице приложения 1 документа [1] указаны следующие свойства функциональных групп управляющих систем, качество которых должно быть обосновано в проектной документации: разнообразие, многоканальность, независимость, надежность, контролепригодность, электромагнитная совместимость, стойкость к механическим воздействующим факторам, стойкость к климатическим факторам, пожаробезопасность, стойкость в полях ионизирующего излучения для элементов систем, расположенных в зоне этих полей, метрология и стойкость к химическим реагентам. Примененный термин «функциональная группа» определен в [1] следующим образом: «Функциональная группа (ФГ) – принятая в проекте часть управляющей системы, представляющая собой совокупность средств автоматизации, выполняющих заданную функцию управляющих систем». Этот перечень свойств ФГ дает наглядное представление об объеме обосновывающих материалов проекта управляющей системы (УС).

В настоящей статье в дальнейшем будет уделено внимание только двум свойствам ФГ УС: разнообразию и надежности.

В п. 4.1.6 отечественного нормативного документа [2] указывается, что «При проектировании АС должны быть рассмотрены и обоснованы меры по предупреждению или защите систем (элементов) от отказов по общей причине». Кроме того, в п. 4.4.5.7 того же документа указывается, что «…управляющие системы безопасности (УСБ) должны удовлетворять следующим принципам безопасности:

1) резервирование (избыточность);

2) независимость;

3) разнообразие.

Резервирование, независимость и разнообразие должны быть таковы, чтобы любые единичные отказы в УСБ не нарушали их работоспособность, а также обеспечивалась их защита от отказов по общей причине в соответствии с п. 4.1.6».

Как видно из приведенных требований, отечественные нормативные документы требуют соответствия проектных решений принципу разнообразия, но не указывают конкретные виды возможного разнообразия, которое нужно применять при проектировании систем аварийной защиты, а также возможные способы их реализации, оставляя решение проблемы проектировщикам этих систем. Необходимо также заметить, что отечественные нормативные документы не определяют само понятие «разнообразие», что, безусловно, является их недостатком.

В международных документах проблемы конкретных видов разнообразия и пути их реализации рассматриваются более детально, и начинается это рассмотрение с определения понятия «разнообразие».

Например, в глоссарии МАГАТЭ это понятие представлено так:

«Разнообразие – наличие двух или более резервных систем или компонентов, выполняющих определенную функцию, когда различные системы или компоненты имеют различные параметры, такие, которые уменьшают возможность отказа по общей причине.

Примерами таких параметров являются: различные условия эксплуатации, различные принципы работы или различные проектные группы (которые представляют функциональные разнообразие), различная конфигурация оборудования, различные производители и виды оборудования, которые используют различные методы обеспечения физического разнообразия».

Поскольку в разных документах, например в [3], предлагаются различные виды разнообразия, то целесообразно указать наиболее употребительные из них, которые уже нашли применение при проектировании. К ним относятся следующие виды:

- техническое (не программируемое) разно образие;
- функциональное разнообразие;
- параметрическое разнообразие;
- программное разнообразие;
- разнообразие, определяемое человеческим фактором;
- проектное разнообразие.

Все указанные виды разнообразия могут быть реализованы в проекте различным образом, например:

- техническое разнообразие – может быть реализовано выбором разных поставщиков средств автоматизации, изготовленных на разных заводах, разными производителями;
- функциональное разнообразие – может быть реализовано использованием различных

функций управления для реализации тех же самых целей управления;

- параметрическое разнообразие – может быть реализовано использованием для измерения разных технологических параметров, достижение установленных значений которых может служить моментом запуска защиты;
- программное разнообразие – может быть реализовано применением различных языков программирования, различных операционных систем, различной логики функционирования систем;
- разнообразие, определяемое человеческим фактором, – может быть реализовано привлечением различных исполнителей требуемых работ;
- проектное разнообразие – реализуется, как правило, применением различных конфигураций построения систем, в которых могут использоваться различные способы передачи информации, разные способы разделения информации, а также разнообразные алгоритмы функционирования систем в процессе работы.

Таким образом, при проектировании УС возникает ряд задач, которые связаны с выбором и реализацией способов обеспечения защиты этих систем от отказа по общей причине. При этом следует отметить (что особенно важно для безопасности) функционирование систем аварийной защиты должно обеспечиваться соответствующими показателями надежности, достижение которых является одной из главных задач при проектировании системы. Как указывается в п. 4.1.12 [2], «ООБ АС должен содержать данные о показателях надежности систем нормальной эксплуатации, важных для безопасности, и их элементов, отнесенных к классам безопасности 1 и 2, а также систем и элементов безопасности. Анализ надежности должен проводиться с учетом отказов по общей причине и ошибок персонала». Отчет по обоснованию безопасности атомной станции (ООБ АС), как правило, должен содержать результаты проведенного анализа и ссылку на материалы этого отчета, которыми можно воспользоваться, например, при проведении экспертизы проекта.

Следует отметить тот факт, что обязательность реализации соответствия системы защиты принципу разнообразия в настоящее время привела даже к появлению нового термина «диверсная защита», обязанного своим появлением английскому слову «diversity», которое переводится как «разнообразие».

Термин «диверсная защита» является термином, который определяет функцию, относящуюся к классу типов защит, его необходимо корректно раскрыть для последующего практического применения в проектной и эксплуатационной практике. Учитывая изложенное, можно предложить следующее определение для этого термина.

Диверсная защита – это защита, функциональная группа которой при проектировании реализована в соответствии с принципом разнообразия.

Применительно к проектированию диверсных защит можно рассматривать следующие приемлемые структуры функциональных групп выполнения аварийных защит (АЗ):

A. Два комплекта по «2 из 3» защит, выполненных на не программируемых средствах автоматизации, на разной элементной базе с формированием сигнала защиты по схеме «или»;

B. Один комплект по «2 из 3» защит, выполненных на программируемых средствах автоматизации, и один комплект по «2 из 3» защит, выполненных на не программируемых средствах автоматизации, с формированием сигнала защиты по схеме «или».

Варианты структуры АЗ, когда оба комплекта выполняются на одних и тех же средствах автоматизации, в данной статье не рассматриваются, как не соответствующие принципу разнообразия.

Наиболее приемлемым вариантом реализации структуры функциональной группы АЗ является вариант А. Однако в тех случаях, когда защиты уже реализованы на программируемых средствах, например при модернизации систем АЗ, следует применять вариант В.

Теперь вернемся к требованию п. 4.1.12 [2], в котором указывается обязательность данных о показателях надежности функциональных групп управляющих систем, важных для безопасности (ФГ УСВБ). Следует отметить, что для ФГ УСВБ должны устанавливаться, как минимум, следующие показатели надежности: безотказность и срок службы.

Показатели безотказности ФГ УСВБ, в зависимости от выполняемой функции, могут приниматься следующими [4]:

- по функциям АЗ – средняя наработка на отказ не менее $1 \cdot 10^6$ час;
- по функциям управления всех родов средняя наработка на отказ не менее $2 \cdot 10^5$ часов.
- Показатели надежности ФГ УСВБ по информационным функциям и функциям диагностики должны быть такими, чтобы обеспечить по информационным функциям наработку на отказ не менее $2 \cdot 10^4$ час.

Назначенный срок службы ФГ УСВБ (долговечность) должен быть не менее 30 лет; средств автоматизации, входящих в состав ФГ УСВБ, – не менее 15 лет.

Наиболее важный показатель надежности для ФГ защиты – ее безотказность, обоснование которого является для современных УСБ, выполненных на программируемых средствах автоматизации, проблемным моментом. Этот факт отмечен неоднократно в рекомендуемых для использования документах МАГАТЭ. Например, в п.1.6 [5] отмечается: «Так как в настоящее время безотказность компьютерной системы не может быть предсказана на единой основе или обоснована в процессе проектирования, то трудно определить и согласиться с систематически появляющимися послаблениями в руководствах по применению программного обеспечения систем, связанных с безопасностью». В п. 2.9 этого же документа указывается, что «Количественная оценка безотказности цифровых программируемых систем из-за ряда недостатков более трудна, чем для непрограммируемых систем. Это может вызывать определенные трудности в демонстрации ожидаемой безопасности системы, выполненной на основе компьютерной техники. В настоящее время требования высокой программной безотказности не доказуемы. Следовательно, проекты, базирующиеся на единственной системе, выполненной на основе компьютерной техники и достигающей вероятности отказа на требование более низкой, чем 10^{-4} для программного обеспечения, должны реализовываться с предосторожностью».

Два этих положения содержат следующие базовые аргументы:

- безотказность компьютерной системы не может быть предсказана или обоснована в процессе проектирования;
- в настоящее время требования высокой программной безотказности не доказуемы.

Таким образом, применение только программируемых средств автоматизации для выполнения функций, важных для безопасности АС, в первую очередь защит, в настоящее время представляется невозможным из-за отсутствия доказательств требуемой безотказности их выполнения.

Кроме того, в связи с появившимися случаями успешных кибератак [6] на подобные системы возникает озабоченность возникновения аварий из-за действий диверсионной направленности, связанных с нарушением функционирования АС.

Эта ситуация предполагает либо необходимое изменение проектов АС в части АЗ, либо установку дополнительных защит, которые бы некоторым образом компенсировали эти пробелы в проектировании. При этом ясно следующее: эти дополнительные защиты не должны реализовываться на программируемых средствах автоматизации таким образом, чтобы они обеспечивали соответствие функциональной группы защиты принципу разнообразия. Это позволит получить расчетное обоснование надежности и защиту от отказов по общей причине.

Автор выражает надежду на то, что эта статья будет представлять интерес не только проектировщикам аварийных защит, но и разработчикам нормативных документов.

Список литературы

1. Требования к системам важным для безопасности атомных станций. НП-026-04. М., НТЦ ЯРБ, 2010.
2. Общие положения обеспечения безопасности атомных станций. НП-001-97. М., НТЦ ЯРБ, 2010.
3. Метод реализации разнообразия и защиты в глубину. Анализ защит реактора NUREG/CR-6303.
4. Системы контроля нейтронного потока для управления и защиты ядерных реакторов. Общие технические требования. ГОСТ 27445-87.
5. Программное обеспечение систем, важных для безопасности, выполненных на основе компьютерной техники для атомных энергетических станций. NS-G-1.1.
6. Армейский вестник от 04.09.2012. «Мировые кибервойны».