МЕЖДУНАРОДНАЯ ИНФОРМАЦИЯ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕТРОСТАНЦИЙ
(Руководство по безопасности № NS-G-1.1; серия стандартов по безопасности; изд. МАГАТЭ, 2000)

Software for computer based systems important to safety in nuclear power plants.- IAEA Safety standards series. Safety Guide № NS-G-1.1; Ed. International Atomic Energy Agency, Vienna, 2000

Публикации МАГАТЭ по безопасности

В соответствии со ст. III своего Устава МАГАТЭ уполномочено устанавливать стандарты безопасности и обеспечивать применение их в ядерной деятельности для мирных целей.

Серия стандартов по безопасности охватывает ядерную безопасность, радиационную безопасность, транспортную безопасность, безопасность при обращении с отходами, а также общую безопасность (т.е. две или более областей).

Выпускаются три серии этих изданий:

Основы безопасности (обложка голубого цвета) устанавливают основные цели, концепции и принципы безопасности и защиты.

Требования безопасности (обложка красного цвета) устанавливают требования, которые должны быть выполнены для гарантии безопасности. Эти требования выражены в обязательной форме и соответствуют целям и принципам, представленным в Основах безопасности.

Руководства по безопасности (обложка зеленого цвета) рекомендуют действия, условия или процедуры для соответствия Требованиям безопасности.

Стандарты безопасности МАГАТЭ юридически не обязательны для государств-членов, но могут быть по их усмотрению приняты для использования в национальных регулирующих документах. Стандарты обязательны для МАГАТЭ в отношении его собственных действий и для государств-членов в отношении совместных действий с участием МАГАТЭ.

Содержание Руководства № NS-G-1.1

1. Введение
   - Основание
   - Цель
   - Область распространения
   - Структура
2. Техническое рассмотрение систем, выполненных на основе компьютерной техники
   - Характеристики систем
   - Процесс разработки
   - Аспекты безопасности и безотказности
   - Организационные и юридические аспекты
3. Требования к организации работ по важным для безопасности системам, выполненным на основе компьютерной техники
   - Требования к организации работ по безопасности
   - Проект и развитие деятельности
   - Организация работ и гарантии качества
   - Документация
4. Планирование проекта
   - Разработка плана
   - Гарантии качества
   - План верификации и валидации
   - План реализации конфигурации
   - План монтажа и ввода в эксплуатацию
5. Требования к компьютерной системе
   - Рекомендации
   - Документация

Далее все пункты с 6 по 15 разбиты аналогично пункту 5 на два подпункта “Рекомендации” и “Документация”

6. Проект компьютерной системы
7. Требования к программному обеспечению
8. Проект программного обеспечения
9. Выполнение программного обеспечения
10. Верификация и анализ
11. Интеграция компьютерной системы

12. Валидация компьютерной системы
13. Установка и ввод в эксплуатацию
14. Эксплуатация
15. Модификация после поставки

Ссылки

Приложения:

Использование и валидация предварительно разработанного программного обеспечения

Глоссарий

Вклад в проектирование и оценку

Органы надзора за соблюдением стандартов безопасности

В требования к организации работ по безопасности в качестве обязательных составляющих включаются: простота проекта; культура безопасности; равновесие между уменьшением риска и усилиями по разработке; защита в глубину; избыточность; критерий единичного отказа; разнопринципность; безопасный к отказам проект; надзор; отказоустойчивость; ремонтопригодность; полное представление эксплуатационных режимов; человеко-машинные интерфейсы и учет человеческих возможностей; доказуемость надежности; контролируемость.

При формулировании содержания проекта и деятельности по его разработке особое внимание следует уделять следующим разделам (§ 3.22 - 3.27 оригинала): управляемость процессом разработки шаг за шагом; рецензируемость; всестороннее испытание; использование автоматизированных инструментальных средств; отслеживание; соответствие стандартам.

Для надлежащей организации управления и гарантии качества требуются: четкое определение функций и квалификации персонала; наличие приемлемой практики; программа обеспечения качества; распределение обязанностей; оценка третьей стороной.

Документы, представляемые в регулирующие органы, должны быть идентичны тем, которые используются проектировщиком. Проектировщик должен быть информирован об этом на ранних стадиях проекта.

Формализованное описание должно поддерживаться объяснениями на естественном языке. Каждое описание или требование должно иметь только одну интерпретацию.

Подтверждение правильности и безопасности системы требует ряда действий по верификации и валидации. В жизненном цикле компьютерной системы с помощью верификации контролируется результат на выходе предшествующего этапа, а валидация контролирует результат требований к системе в целом и достижение целей более высокого уровня.

Верификацию надлежит выполнять для результатов следующих этапов разработки:

Проект компьютерной системы
Требования к программному обеспечению
Проект программного обеспечения
Выполнение программного обеспечения

Отчеты должны быть доступны третьей стороне для ревизии и обзора.

Системные интерфейсы следует проектировать с целью облегчить оператору участие в защитных действиях, таких, как ручное резервирование, вмешательство и ручной аварийный останов реактора. Входные данные и команды пользователя необходимо повторно подтверждать для операторов и автоматически подвергать валидации системой прежде их обработки.

Системные интерфейсы также следует проектировать с учетом выполнения инспекций и при этом так, чтобы не вызывать ложные срабатывания систем защиты. Одновременно не должны нарушаться другие защитные функции, выполняемые внешними системами. Следует рассматривать совместимость систем безопасности с другими системами на станции и защиту от распространения отказов в системах, не влияющих на безопасность.

А. Алпеев

АСПЕКТЫ БЕЗОПАСНОСТИ ПРИ ПРОДЛЕНИИ СРОКА СЛУЖБЫ АЭС

Safety aspects in life extension of NPPS.- Working material, ed. IAEA, Vienna, Austria, 2002, 32 p.

Во многих странах продление срока службы АЭС рассматривается как экономически привлекательная стратегия, совместимая с безопасной эксплуатацией станций. Некоторые страны-члены МАГАТЭ уже разрабатывают нормативные документы по продлению срока службы либо на основе периодического обзора безопасности - Periodic Safety Review (PSR), либо в процессе непрерывной модернизации станции и проведения мониторинга. Причем мониторинг сосредоточен на проблемах старения, а технические аспекты управления старением в рамках PSR регулируются Руководством по безопасности № 50-SG-012.

Применение PSR (хотя и весьма дорогостоящее) очень полезно на ранних стадиях реализации программ продления срока службы и представляет собой приемлемый путь восстановления лицензионной основы, когда это необходимо. А непрерывный регулирующий контроль на основе лицензирования представляется наилучшей стратегией в долгосрочном плане.

Таким образом, можно констатировать отсутствие консенсуса между странами-членами по поводу стратегического курса, которого следует придерживаться, чтобы программа могла гарантировать безопасную долгосрочную эксплуатацию станции - Long-term safe operation of plant (LTO).

Продление срока эксплуатации (в английской терминологии - жизни) - это не особый процесс, описываемый в устоявшихся терминах, согласованных странами-членами МАГАТЭ. И хотя термины Plant life extension (PLEX) и Plant life management (PLIM) употребляются повсеместно, они зависят от специфики законодательства каждой страны.

PSR главным образом относится непосредственно к процессу регулирования. Назначение PSR - гарантировать текущую эксплуатационную безопасность АЭС с перспективой на 10 лет, что признается нормальным уровнем консерватизма.

Но необходимо отметить, что сама концепция PSR была разработана как часть процесса обычного регулирования или мониторинга безопасности и специально не предназначалась для подтверждения возможности долгосрочной эксплуатации станции.

Обеспечение LTO не должно дублировать работы, которые необходимо выполнять как часть нормальной эксплуатации, и подразумевается, что станция должна модернизироваться по мере необходимости.

Вместо программы обеспечения LTO некоторые страны, где законодательством предусмотрено периодическое возобновление лицензии, используют непрерывную программу PLIM или (под другим названием) программу управления сроком службы станции - Life management program (LMP), функции которой включены в организацию нормальной эксплуатации АЭС. В целом поддержание условий безопасности при долгосрочной эксплуатации должно включать четыре основных элемента: тщательное управление и обслуживание; разработанную стратегию замены оборудования; технические модификации критически важных систем; сглаживание выявленных эффектов старения. Трудность такого подхода заключается в поддержании баланса между упомянутыми четырьмя элементами.

Основные составляющие программы

Организация работ по программе будет зависеть главным образом от выбора подхода к продлению срока службы станции. Применение PSR потребует большей численности персонала в течение нескольких лет, в то время как использование PLIM потребует меньшего числа специалистов, занятых составлением отчетов, но большей численности сотрудников, работающих на постоянной основе. В любом случае особое внимание должно быть уделено следующим аспектам:

- Обеспечение того, чтобы законодательные и регулирующие требования, касающиеся долгосрочной эксплуатации, были согласованными и удобопонятными;
- Обеспечение доступности необходимых ресурсов (финансовых и кадровых);
- Распределение ответственности персонала предприятия и регулирующего органа должно быть четко очерчено и подкреплено соответствующими тренировками;
- Наличие эффективных коммуникаций между предприятием и регулирующим органом;
- Определение временных рамок проекта и составление соответствующих планов его реализации;
- Обеспечение связи с общественностью в тех случаях, когда это требуется национальным законодательством или заказчиком.

Ключевым элементом при принятии решения о продлении срока эксплуатации АЭС является Заключительный отчет о проведении анализа безопасности - Final safety analysis review (FSAR). Он должен отражать современную конфигурацию станции и текущее состояние ее безопасности. Уточнения, относящиеся к долгосрочной эксплуатации, как правило, касаются всех частей станции, подверженных старению. Текущую документальную основу лицензирования, то есть технические спецификации, FSAR и отчет о влиянии на окружающую среду - Report of Environmental Impact Assessment (EIA), в идеале следовало бы пополнять свежей информацией непрерывно в течение эксплуатации и периодически представлять в виде отчета как часть нормального процесса регулирования.

FSAR и сопутствующая документация должны содержать всю информацию об основах проекта станции. С точки зрения долгосрочной эксплуатации наиболее существенны:

- заложенная в проект информация, относящаяся к условиям эксплуатации; начальные события; внутренние и внешние риски;
- проистекающие отсюда нагрузки, их комбинации, циклические нагрузки, условия окружающей среды;
- выбор материалов, заложенные в проект предположения об их старении, проектные предписания, касающиеся ремонта.

Также существенными могут быть консервативный подход и допуски на вводимые данные, оценка граничных условий анализа, валидация используемых методов и моделей. Станция должна иметь валидацию FSAR, согласуемую с ее современной конфигурацией.

Программа управления старением - Aging management program (AMP) должна разрабатываться до принятия решения о продлении срока службы станции. Ее содержание может быть сгруппировано в два основные раздела:

1. Все относящиеся к безопасности системы, конструкции и компоненты должны с уверенностью обеспечивать выполнение следующих функций:

a) Целостность контура охлаждения реактора;

b) Возможность аварийного останова реактора с обеспечением безопасности его обслуживания;

c) Возможность предотвращения или смягчения последствий аварий, способных приводить к радиационному облучению за пределами площадки.

2. Все не относящиеся к безопасности системы, конструкции и компоненты, отказ которых может воспрепятствовать удовлетворительному исполнению любой из вышеперечисленных функций.

Иные важные для безопасности системы, конструкции и компоненты можно включать или не включать в эти два раздела, но и они подлежат рассмотрению в случае продления срока службы. Сюда относятся противопожарное оборудование; элементы, подвергающиеся термогидравлическому удару и участвующие в переходных процессах; все системы управления тяжелыми авариями; все оборудование, действующее при полной потере внешнего электроснабжения.

Оценка старения

Старение - это непрерывный процесс. Начинаясь на ранних стадиях, оно может ускоряться в ходе эксплуатации. Его главной причиной является деградация материала под влиянием разнообразных условий окружающей среды - температуры, влажности, радиационного облучения, а также усталости металла. Исследование каждого из механизмов деградации для всех конструкций и компонентов АЭС применительно к продлению срока ее эксплуатации потребовало бы слишком много времени и было бы непрактичным. Вместо этого целесообразнее сосредоточить внимание на результатах старения. Например, коррозия приводит к потере материала. Потеря материала может быть оценена, отслежена, ею можно управлять, например, применительно к трубопроводам и сосудам, работающим под давлением. А при растрескивании бетона с помощью соответствующей программы можно измерять и отслеживать ширину раскрытия трещин и возможное коррозионное повреждение стальной арматуры. Любая приемлемая программа управления старением должна иметь следующие атрибуты:

- Формулировка цели программы;
- Предупреждающие действия;
- Параметры, подлежащие отслеживанию или проверкам;
- Выявление эффектов старения;
- Мониторинг и выявление тенденций;
- Критерии приемлемости;
- Корректирующие и подкрепляющие действия;
- Административное управление;
- Накопление и учет эксплуатационного опыта.

Некоторые из этих атрибутов взаимозависимы, в особенности частота замеров, число и места расположения датчиков измерительных приборов, которые зависят от опыта, накопленного в ходе предшествующей эксплуатации. С учетом опыта их можно изменять в ту или иную сторону.

Другая существенная часть оценки старения - выявление тех конструкций и компонентов, для которых время их возможной деградации, вызываемое, например, усталостью металла, потерей натяжения предварительно напряженной арматуры, тепловым и радиационным охрупчиванием, закладывается в проект.

Оператор станции может продемонстрировать, что для продления срока эксплуатации станции:

1. Первоначальный анализ остается действительным.

2. Анализ может быть распространен вплоть до конца намеченного срока продления эксплуатации.

3. Эффект старения и его влияние на выполнение одной или нескольких предназначенных функций будут адекватно учтены и восприняты системами управления.

Компетентность и профессиональная культура при долгосрочной эксплуатации станции требуются от всех, кто к этому причастен. Способности и интеллектуальный потенциал специалистов, выдающих лицензии, администрации регулирующего органа и сотрудников служб технической поддержки должны обеспечивать понимание и выполнение требований безопасности.

Средний возраст персонала АЭС и служб технической поддержки заметно приближается к пятидесяти годам. Для долгосрочной эксплуатации станций необходима разработка кадровой стратегии, чтобы обеспечить квалифицированными сотрудниками новое поколение эксплуатационников. Опыт и знания, накопленные операторами, следует сохранять и передавать следующему поколению операторов.

СТРУКТУРНАЯ РЕОРГАНИЗАЦИЯ РЕГУЛИРУЮЩИХ ОРГАНОВ ФРАНЦИИ

J.Richardson. Launching the new French regulatory agency.-
Nuclear Engineering International, May 2002, vol. 47, № 574, p. 12-13

Во Франции проведена структурная перестройка системы регулирующих органов в сфере ядерной безопасности и здравоохранения. С 22 февраля 2002 г. Генеральная дирекция по ядерной безопасности и радиационной защите - Direction Generale de la Surete Nucleaire et de la Radioprotection (DGSNR) преобразована из Дирекции по безопасности ядерных установок - Direction de la Surete des Installations Nucleaires (DSIN) посредством объединения с тремя другими организациями: с радиационным

отделом Генеральной дирекции по здравоохранению - Direction Generale de la Sante (DGS); частью отдела радиационной инспекции Управления защиты от ионизирующего излучения - Office de Protection contre les Rayonnements Ionisants (OPRI) и частью Постоянного секретариата межминистерской комиссии по искусственным радиоизотопам - Permanent Secretariat de la Commission Interministerielle des Radioelements Artificiels (CIREA).

Управление по ядерной безопасности - Autorite de Surete Nucleaire (ASN) входит в состав DGSNR и его региональные отделения. ASN получает техническую поддержку от Института радиационной защиты и ядерной безопасности - Institut de Radioprotection et de Surete Nucleaire (IRSN).

Одновременно приняты решения об укреплении ядерной безопасности по линии Министерства обороны Франции за счет развертывания зенитных батарей и истребителей-перехватчиков для улучшения охраны критически важных ядерных установок.

Директор DGSNR г-н Лакост сформулировал главные направления, которым должно уделяться повышенное внимание властей для обеспечения ядерной безопасности.

После реорганизации на DGSNR возложена ответственность за все технологическое обеспечение ядерной безопасности (реакторы, контейнмент, трубопроводы, клапаны), а также за внешние связи (взаимодействие с производителями оборудования и другими поставщиками, местной администрацией, населением, профсоюзами, профессиональные контакты за рубежом).

Новая организация ответственна перед тремя министерствами: финансов (с подключением в ряде случаев Министерства промышленности и торговли); труда (с подключением Министерства здравоохранения) регионального планирования и охраны окружающей среды. При реальном возникновении чрезвычайных обстоятельств DGSNR обращается непосредственно к премьер-министру. По своей активности французские экологи не выдерживают сравнения с “зелеными” в большинстве других стран. Ядерные риски (особенно, когда это касается транспорта и хранения отходов) вызывают у них быстрый и заметный для всех протест. Власти полагают, что эта часть электората способна перешагивать ведомственные границы.

Два инцидента, случившиеся в 2001 г., заслуживают внимания. Ошибка при перегрузке топлива на блоке Dampierre-4 при других обстоятельствах могла привести к неконтролируемой ядерной реакции. Большое число топливных стержней на блоке Cattenom-3 оказались поврежденными. И хотя ситуация, по официальному мнению, не представляла существенной опасности, возникает вопрос, как это могло произойти и что нужно сделать для улучшения контроля за такими нарушениями.

Проводя политику прозрачности, ASN стремится непрерывно повышать профессиональную компетентность сотрудников, строгость соблюдения норм, открытость для населения (уделяя внимание его опасениям); поддерживает сбалансированные отношения с парламентом; постоянно пополняет информацию о безопасности, размещаемую на правительственном сайте в Интернете (www.asn.gouv.fr) и в журнале Minitel, оказывает содействие общественности, публикуя подробные отчеты о технических инспекциях, проводимых на ядерных предприятиях.

Достигнут прогресс и в рационализации топливного цикла. В стремлении улучшить экономические показатели эксплуатируемых реакторов один из подходов, применяемых во Франции и других странах, - повышение глубины выгорания топлива. Примером служит использование программы CYCLADES на старейших блоках 900 MWe в Bugey и Fessenheim или программы GEMMES на блоках 1300 MWe. Electricite de France выражает готовность продолжить эти работы, а ASN намерено уделять большее внимание режимам использования топлива в период 2000-2010 гг.

Проводя исследования в топливном секторе, французские инженеры еще в 80-х годах обнаружили, что сейсмические толчки на площадке АЭС Cadarache вблизи Средиземноморского побережья могут вызывать повреждения и нарушения, поэтому конструкции нуждаются в усилении, особенно при планируемом производстве MOX-топлива в этом районе. Совместно с фирмой Cogema на Cadarache завершаются работы с MOX-топливом с последующей передачей его на расположенную поблизости фирму Melox к началу 2003 г. или позже. Г-н Лакост заявил, что передача производства MOX-топлива фирме Melox потребует общественного одобрения, а обсуждение вопроса о закрытии АС Cadarache никак не повлияет на принятие решения об увеличении производственной мощности Melox.

Американские события в сентябре 2001 г. и катастрофа с человеческими жертвами на химическом предприятии в Тулузе оказали большое влияние на реорганизацию системы ядерной безопасности во Франции, особенно на “кризисное управление”. Тренировки на АЭС Gravelines (на берегу Ламанша) в течение 2001 г. позволили впервые получить информацию, проанализированную в соответствии с международными соглашениями по процедурам, принятым уже после катастрофы. Анализ показал важность продолжения тренировок: обогащается опыт действий персонала в аварийных условиях, возрастает эффективность обеспечения безопасности.

В качестве заключительного ключевого элемента г-н Лакост выделил гармонизацию различных подходов к ядерной безопасности, используемых Западноевропейской ассоциацией органов ядерного регулирования - Western European Nuclear Regulator’s Association (WENDRA), с принятыми в странах Европейского Союза нормами мониторинга ядерной безопасности и стандартными уставками приборов. Этим охватываются следующие страны: Бельгия, Великобритания, Финляндия, Италия Нидерланды, Испания, Швеция, Швейцария (хотя она и не член ЕС), а также Франция, которая в настоящее время председательствует в ЕС. Две главные цели, преследуемые WENDRA в ЕС: первая - независимость анализа и оценки проблем ядерной безопасности и ее регулирования в странах-кандидатах на вступление в члены ЕС и вторая - развитие общего подхода к ядерной безопасности и ее регулированию применительно к собственным проблемам Европейского Союза.

Бюджет DGSNR составил 80 миллионов евро в 2002 г.

Раздел подготовил В.Цукерник