

УДК 681.5

ВЫБОР МЕТОДА ДЛЯ АНАЛИЗА НАДЁЖНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ АЭС В РАМКАХ НЕЗАВИСИМОЙ ОЦЕНКИ БЕЗОПАСНОСТИ

АКОЛОВИЧ А.В., КРЮК Ю.Е.

Государственное научное техническое учреждение «Центр по ядерной и радиационной безопасности»,

(Минск, Республика Беларусь)

Аннотация. В работе рассмотрен выбор метода для анализа надёжности автоматизированных систем управления технологическими процессами (АСУ ТП). Анализ надёжности предполагает использование различных методов, обусловленных определёнными критериями. В рамках выбранного метода выявляются наиболее уязвимые части и элементы энергоблока АЭС, ошибки персонала, которые требуют пристального внимания в рамках решения задачи повышения безопасности.

Ключевые слова: вероятностный анализ безопасности, анализ надёжности, деревья отказов, АСУ ТП.

SELECTION OF A METHOD FOR ANALYSIS OF RELIABILITY OF AUTOMATED PROCESS COMPUTER SYSTEMS NPP IN THE FRAMEWORK OF AN INDEPENDENT SAFETY ASSESSMENT

AKOLOVICH A.V., KRUK Y.E.

State Scientific Technical Institution "Center for Nuclear and Radiation Safety,

(Minsk, Republic of Belarus)

Abstract. The article considers the choice of a method for analyzing the reliability of automated process computer systems (APCS). Reliability analysis involves the use of various methods, conditioned by the established criteria. Whiting the chosen method, the most vulnerable parts and elements of the NPP, personal errors which require close attention to solving the problem of improving safety.

Keyword: probabilistic safety analysis, reliability analysis, fault tree, APCS.

Введение

Автоматизированные системы управления технологическим процессом (АСУ ТП) являются важной и в то же время сложной составной частью промышленного производства.

АСУ ТП – это комплекс систем, предназначенный для управления различными производственными процессами, включающий в себя работу человека и автоматизированный сбор и обработку информации. В отличие от автоматических систем, автоматизированная система управления предполагает активное участие человека. Применение АСУ ТП позволяет значительно увеличить производительность технологических процессов и их эффективность. Степень эффективности автоматизированных систем зависит от параметров и показателей АСУ ТП. Одним из существенных факторов, оказывающих влияние на эффективность управления АСУ ТП, является надёжность. Безопасность и безотказность систем характеризуется показателями надёжности. Следовательно, возникает потребность в проведении анализа надёжности АСУ ТП. Надёжность прямо влияет на такие свойства, как эффективность, живучесть и безопасность, так как отказы компонентов АСУ ТП приводят к ухудшению или потере способности обеспечивать поддержание данных свойств на должном уровне.

Целью работы является выбор метода для анализа надёжности АСУ ТП и обоснование его применения, как наилучшего метода для данного анализа.

Выбор метода анализа надёжности для АСУ ТП

Обеспечение необходимого уровня надёжности требует проведения специального комплекса работ, выполняемых на разных стадиях создания и эксплуатации АСУ ТП. В качестве показателей надёжности АСУ ТП используют показатели, характеризующие надёжность реализации функций системы и опасность возникновения аварийных ситуаций в самой системе [1].

При решении вопросов, связанных с обеспечением требуемого уровня надёжности АСУ, учитываются следующие особенности:

- каждая АСУ является многофункциональной системой, функции которой различны и, соответственно, характерны разным уровнем требований к надёжности;
- в функционировании АСУ участвует персонал, который может в той или иной степени влиять на уровень надёжности системы управления;
- в состав АСУ входит большое количество разнородных элементов. Один и тот же элемент может участвовать в выполнении нескольких функций системы или наоборот, в выполнении – одной функции АСУ участвует несколько различных элементов.

Основные используемые методы анализа надёжности, которые могут дать ответ на вопрос: будет ли система в состоянии выполнить возложенные на нее функции, следующие:

1. Анализ дерева отказов;
2. Марковский анализ;
3. Анализ видов и последствий отказов;
4. Метод логических блок-диаграмм

Выбор метода может быть упрощён при использовании следующих критериев [2]:

- сложность системы. Системы, включающие в себя резервирование, разнообразие и другие особенности, требуют более глубоко уровня анализа, чем простые.
- новизна системы. Вновь разрабатываемая система требует более детального и тщательного анализа, чем система, разработанная ранее и уже эксплуатирующая.
- необходимость количественного и качественного анализа.
- неисправности системы: единичные или многократные.
- зависимость системы от времени и последовательности иных событий.
- наличие зависимых событий.
- восходящий или нисходящий анализ.
- квалификация исполнителя анализа.
- проверка истинности результатов вручную.
- стандартизация.

Марковский анализ на практике используется очень редко из-за сложности систем дифференциальных уравнений, которые имеют место быть при анализе реальных систем.

Метод логических блок-диаграмм и анализ видов последствий и отказов применим лишь к простым системам, что не применимо к АСУ ТП.

Метод анализа дерева отказов (ДО) применяют для анализа видов, последствий и критичности отказов технической диагностики отказавшего элемента системы. Некоторые эксперты рассматривают данный метод как компромисс между простотой метода логических блок-диаграмм и полнотой Марковского анализа для вычисления уровня надёжности системы [3].

Применение анализа дерева отказов при замене элемента системы АСУ ТП позволит учесть известные неблагоприятные воздействия и рассчитать методом вероятностного анализа безопасности надёжность системы, и как следствие сделать вывод о влиянии на безопасность и пригодности использования данного элемента для АСУ ТП.

Исходя из вышесказанного, можно сделать следующий вывод, что оптимально подходящим методом для анализа надёжности систем, применим метод анализа дерева отказов, который является частью логического метода вероятностного анализа безопасности.

В таблице 1 приведён краткий обзор используемых методов анализа надёжности, их характеристики и особенности.

Таблица 1. Характеристики методов анализа надёжности [2]

Метод	Подходит для сложных систем	Подходит для новых проектов	Количественный анализ	Подходит для комбинаций неисправностей	Подходит для обработки с учётом значимости от времени	Учёт зависимых событий	Восходящий или нисходящий	Применимость и унифицированность	Проверка правоподобия результатов	Обозначение стандарта
Анализ дерева отказов (неисправностей)	Да	Да	Да	Да	Нет	Нет	Нисходящий	Высокая	Да	ГОСТ Р 27.009-2009
Марковский анализ	Да	Да	Да	Да	Да	Да	Нисходящий	Средняя	Нет	ГОСТ Р 51901.15
Анализ видов и последствий отказов	Только для простых систем	Только для простых систем	Да	Нет	Нет	Нет	Восходящий	Высокая	Да	ГОСТ 27.310
Метод логических блок-диаграмм	Только для простых систем	Только для простых систем	Да	Да	Нет	Нет	Нисходящий	Средняя	Да	ГОСТ Р 51901.14

Метод анализа дерева отказов для оценки анализа надёжности

Вероятностный анализ безопасности (ВАБ) представляет собой всесторонний, структурированный метод определения сценариев отказов, для получения численных оценок риска, в процессе которого разрабатываются вероятностные модели для определения конечных состояний системы с повреждением источников радиоактивного излучения [4]. Вероятностный анализ безопасности (ВАБ) содержит ответ на вопрос о частотах проявления переходных процессов, приводящих к конечным состояниям, характеризующийся нарушением пределов и условий безопасной эксплуатации.[5]. Основной целью ВАБ является оценка влияния инициирующих событий, возможных на энергоблоке АЭС, на безопасность этого энергоблока. Указанная цель может быть разделена на несколько отдельных целей ВАБ, достижение которых преследуется в зависимости от поставленных задач, например, оценка обеспечения достаточного уровня надёжности систем. Для данной цели и определения множества конечных состояний с повреждением оборудования, элементов и систем применяется логический метод дерева отказов (ДО).

Дерево отказов визуально представляет собой графическую схему, по которой определяются основные или вершинные события, заключающихся в отказе системы выполнить заданную функцию, вследствие комбинации элементарных или первичных событий, которые являются отказами отдельных элементов системы [5]. Анализ дерева отказов может использоваться для прогнозирования надёжности при проведении альтернативных исследований и на стадии проектирования систем. Данный метод предназначен для реализации заранее определённого нежелательного события, и позволяющий находить все возможные пути его достижения. Проводя соответствующий анализ системы, можно показать, что достигнуты заданные количественные или качественные показатели надёжности.

Этапы проведения анализа ДО для АСУ ТП:

- описание каждой части системы, входящий в состав АСУ ТП. Описание должно включать в себя технологические и структурные схемы с определением границ системы;
- выполнение декомпозицию системы, т.е. разделение ее на отдельные каналы или части, для которых будет разработано самостоятельное ДО;
- определение верхних событий в соответствующих ДО;
- определение для каждого элемента с учётом условий его функционирования присущие ему виды отказов. Каждый вид отказа должен быть определён показателем надёжности;
- выполнение анализа зависимостей от других систем и элементов;
- выполнение анализа ошибочных действий персонала;
- построение ДО по полученным результатам. Для оценки надёжности и работоспособности системы в методе анализа дерева отказов применяется Булева алгебра (математическая система позволяющая манипулировать с событиями). Основными исходными данными являются интенсивности отказов, вероятности появления неисправностей для элементов. Дерево отказов должно включать следующие компоненты: вершинное событие, логические операторы, разрабатываемые события, первичные события, ссылки на другие деревья отказов;
- определение множество минимальных сечений, представляющих собой логическое произведение первичных событий, являющиеся отказами системы, рассчитать параметры надёжности элементов.

Вывод

Автоматизированные системы управления являются сложными техническими системами, в процессе которых могут возникать отказы, имеющие негативные последствия для производственного цикла, персонала и инфраструктуры. Вероятность отказа определяется показателями надёжности системы в целом, а также ее элементов.

Для повышения надёжности АСУ применяют различные аналитические методы. Одним из таких методов является метод дерева отказов. Он учитывает сложные взаимодействия частей системы, моделируя их зависимые отказы, события, а также позволяет сформировать общее представление о системе.

При проектировании системы контроля и управления должен применяться подход, включающий набор технических средств, методов контроля и качества, которые должны учитывать принципы: разнообразия, единичного отказа, защиты от отказов по общей причине, резервирования, независимости, а также учёт человеческого фактора, качество, надёжность элементов, квалификацию оборудования.

Список литературы

1. ГОСТ 24.701-86 Надёжность автоматизированных систем управления. Основные положения, 2009 г. – 12 с.
2. ГОСТ Р 51901.5 Руководство по применению методов анализа надёжности, 2005 г. – 48 с.
3. Солонин В.И. Безопасность и надёжность реакторных установок. Учебное пособие по курсу «расчёты и проектирование ядерных установок». – М: Изд-во МГТУ им. Н.Э. Баумана, 1996. Т6– 80с.
4. Разработка и применение вероятностной оценки безопасности уровня 1 для атомных электростанций, Специальное руководство по безопасности МАГАТЭ, № SSG-3, 2014 г. – 243 с.
5. Швыряев Ю.В., Острейковский В.А. Безопасность атомных станций. Вероятностный анализ. – М.: ФИЗМАТЛИТ, 2008. – 352 с.