Алпеев А.С.

НАДЕЖНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УПРАВЛЯЮЩИХ СИСТЕМ И БЕЗОПАСНОСТЬ АТОМНЫХ СТАНЦИЙ

В статье рассмотрены аспекты применимости программируемых управляющих систем на атомных станциях. Отмечены преимущества и недостатки этих систем. Основными недостатками этих систем названы: невозможность обоснования показателей надежности реализуемых функций управления и подверженность возможным кибератакам. Предложен метод выбора средств автоматизации для реализации управляющих систем на программируемых и не программируемых средствах автоматизации на основе проведения функционального анализа управляющих систем атомной станции.

Ключевые слова: *безопасность, управляющая система, атомная станция, надежность, безотказность, средства автоматизации, программное обеспечение, анализ, функция, функциональная группа, показатель.*

Проблема обоснования надежности программного обеспечения (ПО) с момента его применения в практической деятельности человека занимает одно из важных мест, поскольку использование ПО для достижения требуемых результатов стало необходимым при решении разнообразных сложных задач практически во всех областях науки и народного хозяйства. Особую важность приобретает доказательство характеристик надежности ПО при создании управляющих систем для ядерноопасных объектов, таких, например, как атомные станции (АС). Дело в том, что безаварийное функционирование атомной станции должно обеспечиваться в течение длительного времени, порядка 40 – 60 лет. Такая длительная безаварийная работа требует реализации управляющих систем с показателями надежности, реализация и демонстрация которых в настоящее время практически не достижима.

Поэтому исследованиями в данной области занимаются в разных странах различного рода коллективы уже не менее четырех – пяти десятков лет и пока необходимого результата не достигнуто. Конечно, решение этой проблемы насущно и необходимо, но задача по применению программируемых средств автоматизации должна решаться здесь и сейчас с теми исходными данными, которые доступны в настоящее время.

Как уже отмечалось, к надежности ПО, используемого в управляющих системах АС, для осуществления управления в режимах эксплуатации и при авариях предъявляются достаточно высокие требования, которые при современном состоянии программируемых средств автоматизации и системотехники не обеспечивают доказательства необходимой наработки на отказ реализуемых функций порядка 106 час. Такое состояние с разработкой управляющих систем является неудовлетворительным и требует принятия мер, которые гарантировали бы надлежащую надежность функционирования АС. Кроме того, появившаяся в настоящее время информация об успешных кибератаках на оборудование с управляющими программируемыми системами, связанными с ядерными установками

[1], значительно повысила интерес к решению проблем надежности управляющих систем в области ядерной энергетики.

Для начала рассуждений на предложенную тему рассмотрим современное состояние дел с имеющейся информацией по средствам и системам автоматизации. При этом следует учитывать, что «Количественная оценка безотказности цифровых программируемых систем из-за ряда недостатков более трудна, чем для непрограммируемых систем», как указывается в [2] п. 2.9. 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». Далее в [2], п. 2.13, также указывается, что «Количественное определение программной безотказности остается нерешенной проблемой. Испытание программного обеспечения имеет некоторые ограничения и поэтому количественное определение программной безотказности для компьютерных систем может быть трудно или невозможно демонстрировать».

Для последующих рассуждений предлагается все средства автоматизации разделить на две группы: 1 – программируемые средства автоматизации и 2 – не программируемые средства автоматизации. Управляющие системы могут быть реализованы как на средствах автоматизации первой группы, так и второй группы и такой опыт в мировой практике создания этих систем уже накоплен. Рассмотрим далее достоинства и недостатки управляющих систем реализованных на средствах автоматизации указанных ранее групп.

Сразу отметим, что в последнее время наблюдается расширяющееся применение управляющих систем, базирующихся на программируемых средствах автоматизации.

В частности, это связано с тем, что в этих системах достигается:

• улучшенный контроль параметров атомной станции, в том числе параметров, важных для безопасности;

• улучшенный интерфейс оператор-объект;

• обеспечение оперативных испытаний;

• самоконтроль средств автоматизации и функциональных групп;

• улучшенная диагностика;

• повышенная точность измерения;

• повышенная устойчивость функционирования;

• уменьшенная потребность в кабельных соединениях за счет применения мультиплексных структур (общих информационных шин);

• улучшенная модифицируемость управляющих систем под развивающиеся задачи эксплуатации.

Указанные преимущества программируемых управляющих систем не исключают имеющихся недостатков таких систем. Например, таких как:

• разработка и создание ПО представляет собой более высокоинтеллектуальный процесс, чем создание аналоговых средств, и поэтому имеет большую вероятность возникновения ошибок, выявление которых представляет собой достаточно сложную задачу;

• трудность демонстрации характеристики безотказности;

• реализация ПО, как правило, представляет собой дискретные логические модели реального мира, что имеет два типа последствий:

- программное обеспечение более чувствительно (т.е. менее терпимо) к «маленьким ошибкам»;

- методы интерполяции и экстраполяции полностью не пригодны, поскольку приводят к недостоверным результатам.

Таким образом, первая группа средств автоматизации позволяет создавать управляющие системы с повышенными показателями качества работы, однако эти системы не имеют достаточного обоснования по надежности выполнения требуемых функций и могут быть подвержены кибератакам. [1].

Вторая группа средств автоматизации имеет больший опыт промышленного применения, однако уступает первой группе по качеству реализации требуемых функций, более сложна в изготовлении, наладке и сервисном обслуживании. Но для управляющих систем, выполненных на средствах автоматизации 2-й группы достаточно хорошо обосновываются показатели надежности и они, как показывает опыт многолетней эксплуатации, не подвержены воздействию кибератак. При таком рассмотрении управляющих систем, реализованных на тех или иных средствах автоматизации, хорошо видны их преимущества и недостатки.

При этом, на мой взгляд, напрашивается рассмотрение возможного симбиоза систем на средствах автоматизации из двух названных ранее групп средств автоматизации с тем, чтобы использовать их положительные качества в полной мере и избежать проявления негативных моментов их применения.

Для этой цели необходимо проанализировать функциональные группы всех управляющих систем АС, чтобы выделить функциональные группы, для которых качество реализации представляется достаточно сложным и трудоемким, и функциональные группы, отказ которых приводит к аварии. В соответствии с [3] «Функциональная группа – принятая в проекте часть управляющей системы, представляющая собой совокупность средств автоматизации, выполняющих заданную функцию». В [3] п. 3.17, указывается, что в проектной документации управляющих систем важных для безопасности должны быть определены функциональные группы и их классификация по категориям безопасности. Проведение требуемого анализа необходимо учитывать не только классификацию функциональных групп по безопасно-

сти, но и целый ряд аспектов, важных для реализации управляющих систем.

Например, функциональные группы, реализующие защиты по одному параметру, как правило, представляют собой достаточно простую структуру: измеритель параметра защиты, сравнивающее устройство с величиной заданного параметра защиты, устройство, формирующее исполнительный сигнал в случае превышения измеренным параметром величины заданного параметра и исполнительное устройство. Алгоритм работы такой системы защиты достаточно прост и со временем не меняется. Режим работы стационарен и обычно хорошо диагностируем. Отказ системы защиты может приводить к значительным убыткам, т.е. достижение успешной кибератаки должно быть невозможно. Для таких функциональных групп, на мой взгляд, целесообразна ее реализация на средствах автоматизации, обозначенной ранее как группа – 2.

В случаях, когда функциональная группа реализует достаточно сложную функцию, например выравнивание поля энерговыделения активной зоны ядерного реактора, которая имеет достаточно сложный алгоритм реализации и зависит от множества постоянно меняющихся технологических параметров, то реализацию такой функциональной группы, на мой взгляд, следует выполнять на средствах автоматизации группы – 1. Эта группа обеспечит более высокое качество реализации требуемой задачи в автоматическом режиме, чем при автоматизированном управлении.

Применение для автоматизации средств первой группы целесообразно в случаях, когда требуется управление, связанное с координацией большой группы параметров и, в зависимости от меняющихся во времени технологических параметров, связанных, например, с выгоранием топлива или отказами технологического оборудования, при которых необходимо поддерживать непрерывность технологического процесса, оперативным вводом в работу резервного оборудования.

Таким образом, результаты функционального анализа управляющих систем АС являются основой для выбора средств автоматизации для создания соответствующих управляющих систем.

Следует отметить, что системы диагностики, особенно управляющих систем, важных для безопасности, по которым формируются сигналы аварийной защиты, также должны формироваться на основе не программируемых средств автоматизации, чтобы не подвергаться воздействию кибератак и иметь расчетное обоснование надежности.

Как указывается в [4], п. 4.1.12, «Отчет по обоснованию безопасности 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».

Таким образом, все функциональные группы управляющих систем классов безопасности 1 и 2 будут иметь обоснованные расчетом показатели надежности, поскольку будут выполнены на средствах автоматизации группы 2. Функциональные группы класса 3, выполненные на программируемых средствах автоматизации, будут достигать наработки на отказ до 104 час, что в настоящее время является допустимым значением.

Автор выражает надежду на то, что предложенный метод выбора средств автоматизации и соответствующее построение управляющих систем для атомных станций будут обеспечены более аргументированными показателями надежности функционирования.

Литература

1. Армейский вестник от 04.09.2012г. «Мировые кибервойны».

2. Программное обеспечение систем важных для безопасности, выполненных на основе компьютерной техники для атомных энергетических станций. NS-G-1.1. МАГАТЭ 2000.

3. Требования к управляющим системам, важным для безопасности атомных станций. НП-026-04.

4. Общие положения обеспечения безопасности атомных станций. НП-001-97.