Функциональная безопасность и человеческий фактор

А.С. Алпеев, к.т.н. (НТЦ ЯРБ)

Возрастающее внимание мировой общественности к проблемам безопасности в настоящее время приводит к более детальному изучению всех аспектов безопасности, их определению и классификации с целью формирования более корректных законодательных нормативных актов, содержащих положения, обязательные при создании и эксплуатации опасных технологий и производств. Результат такого изучения – появление новых аспектов безопасности.

Одним из них следует считать аспект, вводимый понятием "функциональная безопасность". Это понятие уже появилось в международных нормативных документах [1-2], регламентирующих положения, выполнение которых рекомендуется при создании и эксплуатации управляющих систем для автоматизации опасных технологий и производств, в частности, атомных станций. Так, например, в [1] изложены общие требования к функциональной безопасности объектов, которые определяют системы, важные для их безопасности (системы, связанные с безопасностью управляемых объектов). В [2] приводится определение термина "функциональная безопасность" и ряд терминов, выполненных на его основе. В частности:

> Функциональная безопасность – свойство систем, важных для безопасности (систем, связанных с безопасностью), выполнять действия, необходимые для достижения управляемым оборудованием безопасного состояния или поддержания безопасного состояния управляемого оборудования.

Для введения в отечественную практику указанное понятие требует рассмотрения на основе теории терминологии [3] и опыта отечественных нормативных документов с целью возможного применения этого термина с соответственно аргументированным определением в системе отечественных нормативных документов вместе с необходимым набором нормативных положений, регламентирующих обеспечение его практической реализации.

Какой аспект безопасности выделяет это новое понятие?

Проанализируем предложенное в [2] определение термина "функциональная безопасность" и укажем возможные некорректности этого понятия.

Как видно из предложенного определения, термин "функциональная безопасность" вводится как "свойство систем, важных для безопасности", а не как подкласс термина "безопасность", что в соответствии с теорией терминологии было бы логично и оправдано.

Поэтому первая некорректность с точки зрения теории терминологии в представленном понятии "функциональная безопасность" заключается в том, что определение не соответствует термину, поскольку в определении указывается не "функциональная безопасность" как таковая (как философское понятие), а конкретно: безопасность управляемого оборудования, обеспечиваемая свойством систем, важных для безопасности.

В отечественной терминологии совокупность управляемого оборудования (объекта управления) и управляющей системы принято называть системой управления. Кроме того, любой объект, предназначенный для производства какого-либо продукта, содержит управляемое оборудование и управляющую систему, т.е. представляет собой систему управления. В частности, атомная станция – это тоже система управления, или более точно, с точки зрения теории автоматизированных систем, автоматизированный технологический комплекс, предназначенный для выработки энергии. Как указывается в [4]:

> Безопасность атомной станции (АС) – свойство атомной станции, характеризуемое ее способностью предотвращать возникновение всех (возможных на АС) видов опасных воздействий на персонал, население и окружающую среду, или, если они

возникли, то ограничивать их воздействие установленными пределами.

С учетом этого понятия определение, представленное в [2], более соответствует термину "функциональная безопасность управляемого оборудования", чем термину "функциональная безопасность". Применительно к атомной станции, как к частному случаю, этот аспект логично представить термином "функциональная безопасность атомной станции", определение к которому может быть введено словосочетанием "часть безопасности атомной станции".

Подобные соображения позволяют сформировать следующие понятие:

Функциональная безопасность атомной станции – часть безопасности атомной станции, обеспечиваемая управляющими системами, важными для безопасности, атомной станции, которая определяет свойство этих систем: выполнять действия, необходимые для достижения управляемым оборудованием атомной станции безопасного состояния или поддержания безопасного состояния этого оборудования.

Как видно из предложенного понятия, термин и определение, его образующие, семантически сбалансированы. Понятие "функциональная безопасность АС" выделяет подкласс аспектов безопасности АС, обеспечиваемых только управляющими системами, важными для безопасности, атомной станции, в том числе и части таких известных аспектов безопасности атомной станции, как ядерная безопасность АС, радиационная безопасность АС, пожарная безопасность АС, химическая безопасность АС и др.

Теперь необходимо определить существо термина "функциональная безопасность" и тем самым пояснить, на основании чего приписывается такое свойство управляющим системам, важным для безопасности.

Как раз вторая некорректность с точки зрения теории терминологии в представленном понятии "функциональная безопасность" [2] заключается в том, что термин "функциональная безопасность" в представленном понятии не соответствует определению. Это связано с тем, что родовым словом для определения указанного термина в соответствии с теорией терминологии должно быть слово "безопасность", поскольку определяемый термин претендует на выделение из класса понятий, связанных с термином "безопасность", подкласса понятий, связанных только с аспектом функциональной безопасности.

Как показано в [4], наиболее корректным родовым словом для системообразующего термина "безопасность" служит слово "наука", а также следующая структура определения:

Безопасность – наука, изучающая…, с целью выявления…и формирования законов и других нормативных актов, устанавливающих понятия, нормы, требования, рекомендации и методики, выполнение которых должно гарантировать …

Согласно теории терминологии, все последующие термины, образованные на основе термина "безопасность" (например, "экологическая безопасность", "пожарная безопасность", "радиационная безопасность" и др.), следует определять по аналогии, в том числе и термин "функциональная безопасность". Таким образом, термины, характеризующие различные аспекты безопасности, должны вводиться родовым словом "раздел безопасности" с сохранением примерно той же структуры определения, но с учетом конкретных особенностей выделяемого аспекта.

Для корректного определения термина "функциональная безопасность" следует еще уточнить предмет изучения, цели изучения и далее аспекты защищенности, обеспечиваемые в каждом конкретном случае, например, защищенность личности, общества и принадлежащего им имущества.

По информации из [1-2], предметом изучения раздела безопасности "функциональная безопасность" служат функции управляющих систем, важных для безопасности, которые должны обеспечивать безопасное состояние управляемого обо-

рудования во всех режимах его работы. Вполне понятно, что нарушение безопасного состояния управляемого оборудования может происходить при его отказах и при отказах управляющих этим оборудованием систем. В случае указанных отказов управляющая система должна в соответствии с определением выполнять действия, необходимые для достижения управляемым оборудованием безопасного состояния или поддержания безопасного состояния управляемого оборудования.

В соответствии с изложенными соображениями первый шаг изучения подкласса "функциональная безопасность" какого-либо объекта управления – изучение отказов управляющих систем и управляемого оборудования с целью классификации их на отказы, приводящие к нарушению безопасности управляемого оборудования, и отказы, не влияющие на безопасность указанного оборудования.

Второй шаг, выполняемый на основе результатов изучения, – формирование нормативных положений, определяющих понятия, требования и правила, выполнение которых обязательно при создании и эксплуатации управляющих систем, важных для безопасности. Создание управляющих систем, важных для безопасности, которые соответствуют положениям обязательных нормативных документов по безопасности управляемых объектов, и есть то основание, позволяющее приписать управляющим системам свойство выполнять действия по обеспечению безопасности управляемого оборудования.

Таким образом, понятие "функциональная безопасность" можно предложить в следующей редакции:

> **Функциональная безопасность – раздел безопасности, занимающийся изучением отказов управляющих систем и управляемого оборудования, важных для безопасности, с целью:**

- **выявления опасных отказов, которые могут привести к нарушению безопасного состояния управляемого оборудования;**
- **формирования нормативных документов, регламентирующих положения, выполнение которых при создании и эксплуатации опасных технологий или производств обеспечивает свойство управляющих систем, важных для безопасности, выполнять действия, необходимые для достижения управляемым оборудованием безопасного состояния или поддержания безопасного состояния управляемого оборудования.**

Представленное определение термина "функциональная безопасность" однозначно указывает, на основе какого изучения формируется концепция функциональной безопасности рассматриваемого объекта управления (системы управления или автоматизированного технологического комплекса), а также приписывается указанное свойство управляющим системам, важным для безопасности:

> "выполнять действия, необходимые для достижения управляемым оборудованием безопасного состояния или поддержания безопасного состояния управляемого оборудования" [2].

Сформированное понятие "функциональная безопасность" и понятие "функциональная безопасность атомный станции", как пример определения подкласса родового термина, позволяют ввести в отечественную практику нормативной терминологии указанные понятия, а также методологию формирования других подклассов, связанных с конкретными объектами изучения.

Теперь необходимо определить, какую новизну внесут сформированные таким образом понятия в теорию и практику создания и эксплуатации управляющих систем, важных для безопасности.

Как показывает накопленный опыт создания и эксплуатации управляющих систем, важных для безопасности, атомных станций, указанный предмет изучения и вытекающие из него аспекты не являются чем-то новым и неизвестным. Расчеты надежности функционирования оборудования и управляющих систем всегда были и остаются основой для оценки безопасности атомной станции. Тот факт, что функции управляющих систем, важных для безопасности, играют определяющую роль

в обеспечении безопасности объектов управления, закреплено введением нормативного документа [5]. В нем указывается, что элементом управляющих систем при их классификации по влиянию на безопасность должна быть "функциональная группа". Этот термин определяет понятие:

> Функциональная группа – принятая в проекте часть управляющей системы, представляющая собой совокупность средств автоматизации, выполняющих заданную функцию управляющей системы [5].

Таким образом, в управляющих системах, важных для безопасности, атомных станций при анализе безопасности выделяются и анализируются все функциональные группы, реализующие функции, важные для безопасности. Этот же документ содержит требования к составу свойств функциональных групп, обеспечивающих необходимое качество их функционирования.

Изложенные факты и рассмотрение международных нормативных документов, в частности [1, 2], позволяют считать, что отечественные нормативные документы в основном хорошо отражают рекомендательные положения международных документов, касающиеся аспекта "функциональной безопасности".

Тем не менее следует отметить, что в состав управляющих систем, важных для безопасности управляемых объектов, входит персонал управления, т.е. это автоматизированные системы, управляющие технологическим процессом и оборудованием. Таким образом, человеческий фактор представляет собой неотъемлемую часть изучения при определении функциональной безопасности любого объекта.

Как показывает опыт эксплуатации [6], доля аварий, например, на энергоблоках атомных станций, связанных с ошибками в деятельности операторов, по оценкам из различных источников, составляет примерно 30 – 40 % от общего числа аварий. Столь большой негативный вклад, естественно, не остается без пристального внимания со стороны общественности, фирм- создателей и фирм, эксплуатирующих атомные станции.

Проблема человеческого фактора в [6] подразделяется на две части:

- профессиональный отбор, подготовка, проверка и повышение квалификации операторов;
- создание гармоничной рабочей среды для операторов, которая обеспечивает ему психологическую уверенность в своих действиях.

Если по проблеме отбора и обучения операторов уже накоплен большой положительный опыт, то по второй проблеме еще идут с переменным успехом поисковые и экспериментальные работы.

Стержень проблемы формирования требуемой рабочей среды для операторов – обоснованность разделения функций между средствами автоматизации и оператором с той точки зрения, чтобы все задачи, решаемые оператором, соответствовали его знаниям, физиологическим и психологическим возможностям [7]. В частности, при разделении функций между средствами автоматизации и оператором должны соблюдаться следующие ограничения, связанные с физиологическими возможностями оператора:

- оператору трудно реагировать на требования по управлению в течение очень коротких промежутков времени (от нескольких секунд до минуты). Это необходимо компенсировать подсистемами автоматической поддержки реализации функций, например, типа защит и блокировок;
- оператору трудно длительное время (от десятков минут и более) удерживать какой-либо параметр (мощность, температуру и др.) в допустимых пределах. Это следует компенсировать подсистемами автоматической поддержки типа автоматических стабилизаторов параметров технологического процесса;
- оператору трудно осуществлять переходные процессы с требуемыми параметрами в течение длительного времени. Это следует компенсировать подсистемами автоматической поддержки типа логических автоматов или программируемых регуляторов;
- оператору трудно постоянно работать в режиме ожидания для отработки каких-

либо возмущений. Это также необходимо компенсировать подсистемами автоматической поддержки типа автоматических регуляторов;

- оператор не в состоянии выполнять самостоятельно сложные преобразования с отображаемой ему информацией для оперативного управления. Это необходимо компенсировать подсистемами вычислительной поддержки;
- оператор не запоминает с необходимой степенью подробности предысторию сложившейся ситуации или ее аналогов на протяжении больших промежутков времени.

Кроме того, как указывается в [7], современную концепцию деятельности оператора следует базировать на принципах психологической уверенности: достоверности, доступности, санкционированности и контролируемости, реализуемых с помощью подсистем поддержки оператора. Концепция деятельности оператора должна содержать основные решения об его участии в процессе управления и обоснованность его ответственности за безопасность функционирования АС. Последнее утверждение подразумевает подконтрольность операторам энергоблока атомной станции всех режимов работы его технологического оборудования и средств автоматизации, а также диагностику их состояния.

Следует особо обратить внимание на то, что для оператора следует планировать различную степень участия в управлении. Диапазон участия оператора распространяется от непосредственной пошаговой реализации требуемого алгоритма управления с помощью специально предусмотренных органов управления до инициации этого алгоритма управления на реализацию, выполняемую автоматически с одновременным получением оператором информации о пошаговой реализации всего алгоритма. Кроме того, есть супервизорный режим работы оператора, когда он управляет процессом через задание конечной цели управления и наблюдает реализацию достижения заданной цели на средствах отображения информации.

Как показывает практика, супервизорный режим работы оператора наиболее предпочтителен для деятельности операторов, поскольку обеспечивает наиболее благоприятную психологическую обстановку. Оператор формирует параметры цели управления, задает эту цель на автоматическое исполнение и наблюдает за реализацией процесса достижения цели. Если некоторые события будут мешать достижению цели, то оператор должен иметь возможность вмешаться в процесс управления.

Реализация концепции на основе супервизорного режима работы оператора и принципов его психологической уверенности отвечает современным представлениям о деятельности оператора и, как следствие, повышает уверенность в безопасной реализации технологических процессов. Однако внедрение рассмотренной концепции на атомной станции связано с жесткими требованиями к наблюдаемости и управляемости технологического оборудования и технологического процесса.

Следовательно, введение понятия "функциональная безопасность" позволяет более точно очертить те аспекты безопасности рассматриваемого объекта управления, за которые отвечают управляющие системы.

Список литературы

1. МЭК 61508-1 Функциональная безопасность. Системы электрические/электронные/программируемые электронные, связанные с безопасностью. Общие требования.
2. МЭК 61508-4 Функциональная безопасность. Системы электрические/ электронные/программируемые электронные, связанные с безопасностью. Определения и аббревиатуры терминов.
3. Волкова И.Н. Стандартизация научно-технической терминологии. – М.; Изд-во стандартов, 1984.

4. Алпеев А.С. Основные понятия безопасности // Надежность и контроль качества, серия "Надежность". - 1994.- № 7.
5. НП-026-01. Требования к управляющим системам, важным для безопасности, атомных станций.
6. Алпеев А.С. Принципы психологической уверенности операторов атомных станций // Атомная энергия. - 1994.-Т.77. - Вып.1.
7. Алпеев А.С. Автоматизированное управление и безопасность атомных станций // Атомная энергия. -2001.- Т.90. - Вып.2.