ISSN 1561-8889. Космічна наука і технологія. 2002. Т 8. № 1. С. 55—60

УДК 621.039.5

Я. Е. Айзенберг[1], М. А. Ястребенецкий[2]

[1]Відкрите акціонерне товариство ХАРТРОН, Харків

[2]Державний науково-технічний центр ядерної і радіаційної безпеки Державного комітету ядерного регулювання України, Харків

Сопоставление принципов обеспечения безопасности систем управления ракетами-носителями и атомными электростанциями

Надійшла до редакції 20.11.2001

Розглянуто особливості двох найвідповідальніших (з точки зору безпеки) об'єктів керування — атомних електростанцій і ракет-носіїв. Виділено загальний напрямок розвитку систем керування (СК) цими об'єктами і порівнюються принципи забезпечення безпеки цих СК. Запропоновано деякі рекомендації для вдосконалення розробки СК.

Из всех возможных техногенных источников нарушения безопасности в глобальном масштабе атомные электростанции (АЭС) и ракеты-носители с ядерными боеголовками (РН) стоят вне конкуренции в худшем смысле этого слова и являются одними из наиболее опасных.

Авария на блоке 4 Чернобыльской АЭС стала катастрофой не только для СССР, но и для ряда стран Европы. Из аварий с ракетами можно вспомнить взрыв на полигоне Байконур РН без ядерного заряда, который привел к человеческим жертвам.

Системы управления (СУ) являются неотъемлемой частью как АЭС, так и РН. Развитие СУ АЭС и СУ РН, в принципе, подчиняется общим законам развития СУ любыми потенциально опасными объектами — военными или гражданскими. Однако СУ АЭС и СУ РН имеют ряд принципиальных различий, определяемых как особенностями объектов управления, так и сложившимися технологиями разработки и эксплуатации систем.

В нашей статье проведено сопоставление принципов обеспечения безопасности СУ АЭС и СУ РН. При этом мы основываемся на опыте двух организаций:

- НПО «Хартрон», создававшего в течение длительного времени различные типы СУ РН наземного базирования, а с 1992 г., в порядке конверсии, разрабатывающего также АСУ ТП АЭС для блоков ВВЭР-1000;
- Украинского Государственного научно-технического центра ядерной и радиационной безопасности, выполняющего работы по оценке безопасности новых СУ АЭС, разработанных как организациями Украины, так и фирмами «Вестингауз» (США), «Шкода» (Чехия), «Сименс» (Германия) и др. [4, 9].

Отметим, что в настоящее время Украина не имеет ракет-носителей с ядерными боеголовками. Однако анализ опыта создания их СУ представляет значительный интерес и может быть использован в иных отраслях техники, включая СУ АЭС, а также СУ ракет-носителей без ядерных боеголовок.

Сопоставление АЭС и РН как объектов управления, существенных с точки зрения обеспечения безопасности, сделано в табл. 1.

На основе опыта разработки СУ АЭС и СУ РН можно сформулировать некоторые общие направле-

Таблица 1. Особенности АЭС и РН как объектов управления, существенные с точки зрения обеспечения безопасности

№ п/п	Наименование особенности	АЭС	РН
1	Определение понятия «безопасность»	Безопасность АЭС — свойство АЭС при нормальной эксплуатации и в случае аварий ограничивать радиационное воздействие на персонал, население и окружающую среду установленными пределами [3]	Безопасность РН — свойство систем и оборудования РН: — противодействовать применению РН без директивных указаний; — парировать действия, не предусмотренные документацией; — обеспечить невозможность подрыва заряда в составе РН или отдельно при эксплуатации, обслуживании, аварийном пуске и полете; — обеспечить невозможность пуска при неисправностях СУ и оборудования ракеты
2	Определение понятия «авария»	Авария — нарушение эксплуатации АЭС, при котором произошел выход радиоактивных продуктов и/или ионизирующих излучений за предусмотренные проектом при нормальной эксплуатации границы в количествах, превышающих установленные пределы безопасной эксплуатации [3]	Авария РН: — взрыв РН на пусковой установке или во время полета, а также аварийное выключение двигателя в полете из-за неисправностей СУ или оборудования РН; — выброс компонентов топлива за пределы пусковой установки; — разрушение заряда
3	Классификация аварий	— Проектная; — Запроектная	— Проектные аварии — аварийный полет с выключением двигателя; — запроектная авария — остальное (классификация условная)
4	Причина аварий	— Отказы оборудования; — ошибочные действия оперативного и обслуживающего персонала; — внешние воздействия (например, землетрясение); — диверсии	— Отказы оборудования; — ошибочные действия обслуживающего персонала; — диверсии
5	Наличие специальных систем, предназначенных только для предотвращения аварий или ограничения их последствий (и не участвующих в нормальной эксплуатации)	Имеются системы (называемые системами безопасности), включающие специальный вид СУ — управляющие системы безопасности [3]	Имеются: — специальные системы, прекращающие предстартовую подготовку РН при нарушении штатной циклограммы подготовки из-за неисправностей оборудования РН и пусковой установки; — система аварийного выключения двигателя, ограничивающая последствия при аномальном полете
6	Классификация СУ по влиянию на безопасность, что определяет требования к СУ	Все СУ делятся на относящиеся к системам, важным для безопасности, и остальные, не влияющие на безопасность	Классификации СУ по влиянию на безопасность нет. Оборудование, отказы которого могут привести к авариям, определяется в техническом задании на разработку СУ. Влияние отказов перечисленного оборудования учитывается при проектировании СУ
7	Наличие ряда уровней глубокоэшелонированной защиты безопасности	СУ участвуют в четырех из пяти уровней защиты АЭС: 1 — предотвращение нарушений нормальной эксплуатации; 2 — противодействие проектным авариям системами нормальной эксплуатации; 3 — противодействие авариям системами безопасности; 4 — управление запроектными авариями [3]	СУ РН обеспечивают: — предотвращение нарушений нормальной эксплуатации РН из-за отказов технических средств (ТС) или ошибок персонала с гарантией того, что они не приведут к опасным последствиям; — противодействие проектным авариям путем ограничения последствий аварии РН в полете с помощью выключения двигателя и электрических блокировок подрыва заряда
8	Разделение управления в сфере использования объекта и в сфере государственного регулирования безопасности	Принципы разделения имеют место во всех странах. В Украине управление использованием АЭС осуществляет Минэнерго через национальную энергетическую компанию (НАЭК) «Энергоатом». Государственное регулирование безопасности осуществляет государственный комитет ядерного регулирования [3]	Имеется последовательное разделение управления пуском РН между государственными ведомствами Нет организации, выполняющей государственное регулирование безопасности

Окончание табл. 1

№ п/п	Наименование особенности	АЭС	РН
9	Наличие международной организации, контролирующей безопасность	МАГАТЭ	Имеется только национальный контроль
10	Наличие развитой международной системы нормативных документов	Имеется множество документов МАГАТЭ различного назначения, в том числе непосредственно относящихся к СУ АЭС [5, 6], стандарты International Electrotechnical Commission [7, 8] и др.	Международной системы НТД, действующей в ракетной отрасли, нет. Есть система национальных нормативных документов
11	Соответствие срока службы объекта управления и СУ	Медленная смена поколений объекта по сравнению с поколениями СУ. Срок службы технологического оборудования АЭС — 30 лет. Срок службы СУ 8—10 лет. На АЭС функционирует технологическое оборудование, установленное при монтаже и пуске АЭС. Значительное число СУ заменяется новыми [7, 8]	Срок службы СУ превышает срок службы РН в целом. При этом гарантийные сроки СУ соответствуют сроку эксплуатации РН. Поколения РН и СУ практически всегда меняются одновременно
12	Временной режим работы	Непрерывный характер работы технологического оборудования и СУ в течение длительного времени (30—50 лет)	Непрерывное функционирование дежурных систем в течение всего срока эксплуатации и полная проверка исправности комплектующих РН технических и технологических систем при регламентных проверках
13	Участие человека в управлении	Управление АЭС — автоматизированное (с участием оперативного персонала в прямом контуре управления). Кроме того, имеется обслуживающий персонал	Управление РН в полете — автоматическое (без участия человека). Обслуживающий персонал участвует при проведении регламентных (периодических) проверок и выдаче команды на пуск РН

ния развития СУ в части обеспечения безопасности. К ним относятся:

- широкое применение программного обеспечения и современной компьютерной техники;
- применение высоконадежной элементной базы;
- обеспечение самоконтроля и самодиагностики (с заданной глубиной и достоверностью);
- использование распределенной структуры построения СУ;
- защита от действий, не предусмотренных документацией, направленная на парирование попыток изменить штатные связи в технических средствах и программном обеспечении систем безопасности с представлением информации обслуживающему персоналу в реальном масштабе времени и архивированием таких действий;
- исключение влияния ошибочных действий операторов на правильность функционирования систем защиты и невозможность выведения их из строя в результате таких действий;
- разработка на всех этапах жизненного цикла СУ программ обеспечения качества и комплексной программы экспериментальной отработки систем на этапах проектирования, поставки и ввода в эксплуатацию;
- верификация ПО и валидация системы с участием представителей независимых контролирующих организаций;
- экспертиза со стороны независимых организаций этапов разработки и отработки СУ в темпе их выполнения, а не по окончании разработки и поставки оборудования.

Сопоставим далее принципы обеспечения безопасности СУ АЭС и СУ РН на различных стадиях их жизненного цикла (табл. 2).

На основе опыта создания СУ РН можно предложить некоторые рекомендации по совершенствованию разработки СУ АЭС.

1. Выпуск программы экспериментальной отработки на начальной стадии выполнения заказа позволит заранее определить объем испытаний, место их проведения, требуемое время, состав технических средств и испытательного оборудования, обеспечивающего планируемую отработку, формы отчетных материалов, финансовые затраты.

2. Должны быть приняты технические и программные меры, препятствующие несанкционированному их отключению, изменению/нарушению электрических схем и программного обеспечения. В част ности, необходимо предусматривать:

Таблица 2. Принципы обеспечения безопасности на различных стадиях жизненного цикла СУ АЭС и РН

Принцип обеспечения безопасности	АЭС [1, 3]	РН
	РАЗРАБОТКА СИСТЕМЫ	
Принцип единичного отказа	Управляющие системы должны выполнять заданные функции при любом требующем их работы исходном событии и при независимом от исходного события отказе одного из элементов системы	Требование выполнения функций СУ при одной возможной неисправности является обязательным и задается в ТЗ на разработку СУ
Принцип резервирования	В управляющих системах безопасности должен быть использован принцип повышения надежности путем применения структурной, функциональной, информационной и/или временной избыточности по отношению к минимально необходимому и достаточному для выполнения системой заданных функций объему	Вычислительный комплекс выполняется с глубоким резервированием (внутренние мажоритарные элементы). Релейно-коммутационная аппаратура выполняется двух- или трехканальной
Принцип независимости	В управляющих системах безопасности требуется, чтобы отказы одной СУ не приводили к отказам другой СУ и отказы каналов в СУ не приводили к отказам каналов в этой же СУ. Принцип независимости реализуется: — функциональным разделением, которое должно использоваться для уменьшения вероятности неблагоприятного взаимодействия между элементами СУ с резервированием или взаимосвязанных СУ в результате нормальной или аномальной эксплуатации, или отказа какого-либо элемента систем; — физическим разделением и размещением компонентов СУ, которые должно использоваться для уменьшения вероятности отказов по общей причине	В СУ РН реализуется принцип независимости отказов, при котором: — отказ элементов резервированного канала какой-либо подсистемы не приводит к отказам в сопряженной подсистеме; — физическим разделением и размещением компонентов СУ уменьшается вероятность отказов по общей причине (раздельное размещение резервированных каналов в приборах, раздельное исполнение и прокладка силового электропитания и т.д.)
Принцип разнообразия (диверсности)	Используется в наиболее ответственных системах безопасности (например, аварийных защитах). Принцип реализуется: — функциональным разнообразием, при котором в СУ используются различные алгоритмы реализации одной и той же функции; — разнообразием технических средств, при котором для реализации одной и той же функции с одним и тем же алгоритмом используются различные технические средства (например, полученные от различных поставщиков); — программным разнообразием, при котором используются различные варианты (версии) программного обеспечения, соответствующие одной спецификации (например, созданные с использованием разных языков, разных средств программирования, разными разработчиками и т.д.)	В СУ РН не используется
Консервативный подход	Консервативный подход — при котором для параметров и характеристик принимаются значения и пределы, заведомо приводящие к более неблагоприятным результатам	Консервативный подход — при котором в ходе проектирования предусматривается выполнение заданных функций при граничных значениях входных параметров, предельных значениях напряжения питания и внешних воздействующих факторов
Жесткие требования к поведению СУ при внешних воздействиях	СУ должна удовлетворять требованиям устойчивости к воздействиям окружающей среды (землетрясение, температура, электромагнитные помехи и др.) и воздействиям, вызванным авариями технологического оборудования АЭС (например, разрывом трубопроводов)	СУ выполняется устойчивой к: — внешним воздействиям и их комбинациям; — транспортировке в штатной таре и в составе РН; — хранению в штатной таре и в составе РН

Окончание табл. 2

Принцип обеспечения безопасности	АЭС [1, 3]	РН
Защита от несанкционированного доступа	Охрана АЭС и блочного щита, исключение возможности несанкционированного доступа к программам, данным, настройкам, сигнализация о доступе	Охрана периметра района расположения пусковой установки РН, физическая защита линий связи и помещений с аппаратурой от проникновения посторонних лиц, постоянный электрический контроль стыковки разъемов цепей управления пуском с сигнализацией о НСД
	ПРОВЕРКА И ИСПЫТАНИЯ	
Верификация ПО	Для систем безопасности должна выполняться независимой от разработчика организацией	Представительство заказчика осуществляет контроль разработки на соответствие НТД и техническому заданию от начала разработки и до сдачи РН в эксплуатацию с выдачей этапных заключений по результатам анализа документации и совместных с разработчиком отработочных испытаний, в том числе верификации ПО и валидации системы в целом
Приемка представителем заказчика	Специальная приемка для АЭС (введенная после аварии на Чернобыльской АЭС)	Все комплектующие изделия, технические средства и ПО принимаются службой технического контроля поставщика, а затем представительством заказчика с оформлением протоколов качества (формуляров)
Многоступенчатые испытания	Испытания СУ включают в себя (см. [2]) — предварительные (автономные и комплексные) — опытную эксплуатацию — приемочные	Планирование испытаний осуществляется на начальном этапе разработки путем выпуска программ экспериментальной отработки. Выполнение программы контролируется представительством заказчика. Испытания СУ включают в себя: — испытания программно-алгоритмического обеспечения (ПАО) в схеме исследовательских стендов, — лабораторно-отработочные и совместные с представительством заказчика автономные и комплексные испытания аппаратуры и ПАО, — испытания на контрольно-испытательной станции РН, — испытания на технической и стартовой позициях. Завершающий этап испытаний — летные испытания штатных РН в реальных условиях эксплуатации
Испытания компонентов и СУ в целом при тяжелых условиях	Технические средства управляющих систем безопасности должны испытываться при всех установленных требованиях в любых предусмотренных проектом условий эксплуатации (включая проектные аварии и послеаварийный режим)	Программой экспериментальной отработки предусматриваются автономные испытания всех компонентов и СУ в целом во всех заданных ТЗ условиях и их комбинациях, с искусственным внесением неисправностей в резервированные каналы

— использование кодов, не разрешающих отключение систем безопасности и изменения ПО, а также отключение сигнализации о попытках действий с ТС и ПО, не предусмотренных документацией;
— программные блокировки несанкционированного изменения ПО с сигнализацией и архивированием таких попыток;
— электрический контроль стыковки разъемов и линий связи ТС (по возможности) с немедленным включением сигнализации (индикационной, звуковой) при нарушениях.

3. Для обеспечения поддержания СУ в работоспособном состоянии при штатной эксплуатации должна быть разработана структура построения ЗИП (одиночный, групповой и т. д.) и предусмотрена обязательная его поставка комплектно с техническими средствами СУ. Обязательность комплектной поставки ТС и ЗИП к ним должны быть оговорены государственной нормативной документацией.

4. Увеличение глубины и достоверности системы диагностики (до конструктивно-съемных единиц) и предоставление информации оператору о месте неисправности в темпе ее появления.

На основе опыта создания СУ АЭС можно предложить некоторые рекомендации совершенствования разработки СУ РН (без ядерных боеголовок).

- Использование принципа разнообразия в резервированных каналах за счет различия алгоритмов выполнения одной и той же функции и/или программ, реализующих один и тот же алгоритм (использование разных языков, раз-

ных инструментальных средств программирования и т. п.).

- Классификация компонентов СУ РН по критериям безопасности.
- Разработка документов, устанавливающих требования по безопасности СУ РН и методику оценки безопасности СУРН в рамках системы нормативных документов, регламентирующих общие технические требования к РН.

В заключение отметим, что опыт обеспечения СУ РН может быть использован не только для СУ АЭС, но и для СУ объектов различного назначения, критических с точки зрения безопасности (газопроводов, химических производств и др.).

1. Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій. — Київ: Державна адміністрація ядерного регулювання України, 2000.—(НП 306.5.02/3.035-2000).
2. ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем.
3. Загальні положення забезпечення безпеки атомних станцій. — Київ: Державна адміністрація ядерного регулювання України, 2000.—(НП 306.1.02/1.034-2000).
4. Ястребенецкий М. А. Системы контроля и управления энергоблоков АЭС Украины: вчера, сегодня, завтра // Ядерная и радиационная безопасность.— 1998.—№ 1.— С. 58—65.
5. International Atomic Energy Agency. Modern instrumentation and control for nuclear power plants: a guidelook. — Vienna, 1999.—(Technical Report Ser. № 387).
6. International Atomic Energy Agency. Specifications of requirements for upgrades using digital instrumentation and control system. — Vienna, 1999.—(IAEA TECDOC-1066).
7. International Electrotechnical Commission. Software for computers in the safety systems of nuclear power stations // IEC.—1986.—IEC 60880-86.
8. International Electrotechnical Commission. Nuclear power plants. Instrumentation and control systems important for safety. Classification // IEC.—1993.—IEC 61226-93.
9. Yastrebenetsky M. Modernization of he Ukrainian NPP Instrumentation and Control Systems // Modernization of instrument and control in nuclear power plants. — Vienna, 1998.— P. 165—173.—(IAEA TECDOC-1016).

COMPARISON OF THE SAFETY PRINCIPLES FOR THE CONTROL SYSTEMS FOR LAUNCHERS AND ATOMIC POWER STATIONS

Ya. E. Aizenberg and M. A. Yastrebenetskii

We discuss the peculiarities of the control of two most important (from the safety point of view) objects — atomic power stations and launchers. We determine a general trend in the development of the control systems for these objects and compare the basic principles in providing their safety. Some recommendations are proposed for improving the gesign of the control systems.