ОГЛАВЛЕНИЕ

Предисловие....5
Список принятых сокращений....9
Введение....10
1. Информационно-управляющие системы — класс сложных технических систем....13
   1.1 Сложные технические системы, основные понятия, целевые функции и структуры....13
   1.2 Классификация ИУС....20
   1.3 Стадии и этапы жизненного цикла ИУС....22
   1.4 Принципы проектирования и архитектура ИУС....32
   1.5 Основные проблемы при создании ИУС и способы их решения....38
2. Стратегия оценивания и контроля надежности и безопасности....43
   2.1. Основные понятия надежности и безопасности....43
   2.2. Показатели надежности и безопасности....51
   2.3. Концепция оценивания надежности и безопасности....57
   2.4. Классификация методов оценивания....59
   2.5. Методы объединения информации....63
3. Методы оценивания надежности и безопасности....74
   3.1. Расчетные методы....74
   3.2. Экспериментальные методы....95
   3.3. Расчетно-экспериментальные методы....108
   3.4. Ускоренные испытания....113
   3.5. Испытательное оборудование....120
   3.6. Эквивалентные испытания....125
   3.7. Оценивание остаточного ресурса....138
4. Методы контроля показателей надежности и безопасности....146
   4.1 Классификация методов контроля....146
   4.2 Метод одноступенчатого контроля....147
   4.3 Последовательный контроль....149
   4.4 Контроль методом доверительных границ....152
5. Оценивание завершенности экспериментальной отработки ИУС....155
   5.1 Основные задачи и модели экспериментальной отработки....155
   5.2 Показатели завершенности экспериментальной отработки....159
   5.3 Прогнозирование уровня экспериментальной отработки....163
   5.4 Оценивание уровня экспериментальной отработки....167
   5.5 Экспериментальная отработка программного обеспечения....172
Приложение А. Методика контроля качества программных средств ИУС....186
Приложение Б....198
   Б. 1. Анализ структуры и принципов функционирования комплексной информационно-управляющей системы обеспечения безопасности движением поездов метрополитена....198
   Б. 2. Расчет показателей надежности стационарной аппаратуры станций и перегонов комплексной системы обеспечения безопасности движения и автоматизированного управления движением поездов метрополитена....201

Приложение В. Расчет показателей безопасности и безотказности поездной аппаратуры комплексной системы «Движение» метрополитена 223
Приложение Г. Расчетно-экспериментальная методика и анализ результатов ускоренных испытаний теплоизоляционных блоков трубопроводов атомных электростанций 249
Приложение Д. Коэффициенты форсирования для назначения режимов автономных (предварительных) испытаний системы безопасности РН и датчиков системы ликвидации информации КА 259
Статьи, опубликованные в средствах массовой информации по прикладным вопросам надежности и безопасности ИУС 262
Литература 343

ПРЕДИСЛОВИЕ

Развитие техники на современном этапе характеризуется широким внедрением в научную и производственную деятельность системных подходов, что потребовало кардинального изменения идеологии и принципов проведения исследовательских и проектных работ, обусловленных ростом сложности создаваемых изделий, жесткими требованиями к их безопасности и надежности. Опыт, накопленный в мире, существенные результаты, достигнутые в теориях проектирования, испытаний и эксплуатации сложных систем в нашей стране, пока не могут обеспечить полного решения проблем в областях надежности и безопасности. Множество публикаций, потоков руководящих документов и методических указаний, разработанных различными авторскими коллективами, имеют часто нечеткие, а иногда и противоречивые формулировки понятий и определений, использующихся в указанных областях современной науки. Данное обстоятельство приводит к трудностям поиска рациональных путей решения прикладных задач по надежности и безопасности не только начинающими специалистами, но и опытными разработчиками и испытателями.

Особенно сложные проблемы встречаются при исследовании параметров безопасности информационно-управляющих систем, которые интенсивно внедряются в современные разработки больших технических систем. Развитие данного направления в научной и проектной деятельности приобретает особую актуальность в связи с трагическими последствиями аварий и катастроф, происходящих в мире и в нашей стране при эксплуатации объектов повышенной опасности. К числу таких объектов относятся:

- стационарные и подвижные ядерные реакторы атомных тепловых и электрических станций, включая космические ядерные энергоустановки, а также реакторы кораблей и подводных лодок;
- авиационные средства и ракетно-космические комплексы;
- автоматизированные системы управления движением железнодорожного транспорта (наземного и подземного);
- объекты химической промышленности;
- государственные автоматизированные системы электроснабжения, имеющие в своем составе мощные тепловые и гидроэлектростанции, и многие другие.

Целью представленной монографии является обобщение мирового опыта по оцениванию и контролю показателей надежности и безопасности, отвечающего современным требованиям к информационно-управляющим системам, функционирование которых сопряжено с риском аварий и катастроф, а также по систематизации практически используемых методов и средств анализа надежности и безопасности систем, относящихся к категории объектов повышенной опасности. Актуальность настоящей работы обусловлена необходимостью систематического изложения подходов к оцениванию и контролю показателей надежности и безопасности аппаратно-программных средств информационно-управляющих систем, позволивших объединить в

единую концепцию методы, применяемые при теоретическом анализе на различных стадиях жизненного цикла информационно-управляющих систем, и результаты, полученные на практике с их использованием.

В материалах, представленных в книге, выполнено дальнейшее развитие теории безопасности, что подтверждает научную и практическую ценность результатов изложенных исследований. Учитывая тенденцию к интеграции отечественных образцов промышленного производства в мировую экономику, в монографии учтены основные положения международных стандартов в сфере безопасности и надежности.

Материалы, изложенные в монографии, имеют следующее содержание: введение, пять разделов, пять приложений и список литературы.

Во ***введении*** приведено изложение проблем и целей, решению которых посвящены исследования.

В ***первом разделе*** приведены основы, признаки и свойства сложных технических систем, дается общая характеристика информационно-управляющих систем, предназначенных для выполнения ответственных функций управления большими техническими объектами и обладающих определенной опасностью при их эксплуатации, хранении, транспортировке, подготовке к применению и других этапах жизненного цикла. Логика изложения и материал, описывающий системные подходы к формированию проблем, позволяют глубоко осознать и быстро освоить основные понятия и структурные построения информационно-управляющих систем, правильно сформулировать главные задачи, требующие решения с помощью информационно-управляющих систем, и обосновать состав обобщенной ИУС.

Кроме того, приведена новая классификация информационно-управляющих систем, разработка которой продиктована тем, что впервые предложенные методы оценивания и контроля надежности и безопасности информационно-управляющих систем рассматриваются с учетом их конструктивных и схемных особенностей, значимости и ответственности решаемых проблем, условий эксплуатации, а также последствий возможных отказов и ошибок обслуживающего персонала.

В разделе изложены новые общие и частные принципы проектирования информационно-управляющих систем, разработка которых обусловлена их особенностями, а именно тем, что рассматриваемые в монографии информационно-управляющие системы предназначены для управления объектами, которые относятся к категории повышенной опасности и представляют собой сложные программно-аппаратные комплексы с иерархической организацией. Указанные принципы были использованы при впервые осуществленной разработке и практической реализации вариантов архитектуры аппаратных и программных средств двухуровневой иерархии.

Второй раздел посвящен описанию разработанной впервые стратегии оценивания показателей надежности и безопасности информационно-управляющих систем. Даны определения основных терминов в области надежности и безопасности, которые в настоящее время широко используются в литературных публикациях. Формулировки имеют понятный и ясный смысл, который удобен при решении теоретических и практических задач оценивания и контроля показателей надежности и безопасности на всех этапах жизненного цикла информационно-управляющих систем, а именно в процессе разработки технического задания, создания, испытаний, приемки и эксплуатации системы.

Важно отметить, что указанные работы не противоречат международным стандартам.

В данном разделе приведена оригинальная концепция оценивания и контроля показателей надежности и безопасности информационно-управляющих систем. Концепция разработана с учетом ограничений материальных ресурсов, сроков создания и целесообразности сохранения или восстановления работоспособного состояния информационно-управляющих систем после проведения всех видов необходимых испытаний. Главным требованием при разработке концепции явилось условие ее непротиворечивости комплексу нормативных документов в области надежности технических систем.

Положения, позволяющие уточнить область применения концепции, определяются спецификой классификации эмпирической базы, используемой для оценивания показателей надежности, безопасности и завершенности отработки информационно-управляющих систем на различных стадиях и этапах ее жизненного цикла. В этом разделе представлена общая характеристика и область применения методов оценивания показателей надежности и безопасности, а также приведена их классификация. Изложены не имеющие аналогов методы интегрирования информации, которые созданы с целью повышения точности оценок на ранних этапах проектирования информационно-управляющих систем, а также оценивания показателей надежности и безопасности информационно-управляющих систем, выпускаемых небольшими сериями или являющихся уникальными.

В ***третьем разделе*** монографии представлены методы определения показателей надежности и безопасности информационно-управляющих систем. Приведенные методы согласуются с разработанной стратегией и разделены на три группы: расчетные, экспериментальные и расчетно-экспериментальные. Наряду с известными в практике проектирования информационно-управляющих систем методами особое внимание при выполнении исследований уделено оригинальным методам, актуальность создания которых диктуется потребностью разработки исключительно сложных по своей структуре и алгоритму функционирования систем.

Приводятся описания теоретических и прикладных задач, решаемых при проведении ускоренных испытаний. Актуальность их использования заключается в существенном сокращении материальных и временны□х затрат, необходимых для оценивания и контроля информационно-управляющих систем с повышенными требованиями по надежности и безопасности.

Дается описание предложенных способов проведения ускоренных испытаний, методики оценивания интенсивности отказов электрорадиоизделий по результатам этих испытаний, а также типового комплекса для их проведения. Комплекс используется при осуществлении выборочного контроля в соответствии с требованиями международных стандартов. Раздел содержит обзор отдельных видов испытательного оборудования, которое, как правило, входит в состав испытательных и сертификационных центров.

В этом разделе изложена сущность эквивалентных испытаний информационно-управляющих систем, которые проводятся при отсутствии возможности обеспечить испытания в условиях полномасштабных динамических воздействий. В связи с исключительной важностью и актуальностью решения проблемы рационального использования материальных средств, вложенных в разработку, изготовление и техническое обслуживание находящихся в эксплуатации

информационно-управляющих систем, в отдельный подраздел вынесены способы оценивания их остаточного ресурса.

Методы, представленные в этом разделе, являются достаточно универсальными, что обеспечивает возможность их широкого применения на практике.

В ***четвертом разделе*** помещено описание сравнительного анализа методов контроля показателей надежности и безопасности, разработанных в соответствии с заданными к ним требованиями при проектировании современных информационно-управляющих систем. Сравнение осуществляется по критерию, согласно которому количество всех отказов, зарегистрированных в ходе испытаний, должно быть равно нулю. Данное обстоятельство ограничивает использование результатов выполненных исследований только областью контроля составных частей и критичных элементов информационно-управляющих систем.

В ***пятом разделе*** приведены методы оценивания надежности и безопасности информационно-управляющих систем, при проведении которой значительная роль отведена экспериментальной отработке. Основными проблемами, возникающими при выполнении оценивания, являются отладка и контроль завершенности отработки программного обеспечения, представляющие собой важную часть информационно-управляющих систем.

В приложениях дается описание результатов следующих научных исследований:

• методики контроля качества программных средств информационно-управляющих систем;

• моделей, методики и результатов расчета показателей надежности стационарной аппаратуры станций и перегонов комплексной системы обеспечения безопасности движения и автоматизированного управления движением поездов метрополитена, которые выполнены с помощью аналитико-табличного метода;

• примера расчета аналитико-статистическим методом показателей безопасности и безотказности поездной аппаратуры комплексной системы «Движение»;

• расчетно-экспериментальной методики и анализа результатов ускоренных испытаний теплоизоляционных блоков атомных электростанций;

• коэффициентов форсирования, использованных для назначения режимов автономных (предварительных) испытаний системы безопасности ракет-носителей и датчиков системы ликвидации информации космических аппаратов.

Представленные в Приложениях Б и В обозначения устройств широко используются в нормативной документации информационно-управляющих систем железнодорожного транспорта и в данном издании приведены в сокращенном виде.

Материал монографии основан на результатах опытно-конструкторских работ, выполненных под научным руководством и при личном участи автора в ОАО «НИИ точной механики» и ФГУП «КБ ″Арсенал″ имени М.В. Фрунзе», связанных с разработкой и сертификацией современных информационно-управляющих систем, а также на материалах курса лекций, который в течение ряда лет автор читал в Военно-космической академии имени А.Ф. Можайского. Изложенные в монографии научные положения, подходы и пути разрешения практических проблем предназначены для специалистов в области обоснования технических требований, проектирования, испытаний и эксплуатации

информационно-управляющих систем, отказы которых способны нанести вред жизни и здоровью людей, причинить материальный и экологический ущерб. Материал монографии может быть полезен научным сотрудникам, аспирантам и студентам, в сферу научных интересов которых входят вопросы анализа надежности и безопасности.

Основные результаты исследований, приведенные в монографии, являются новыми. В частности, обобщенные сведения о путях и способах решения отдельных аспектов теории безопасности, методах оценивания показателей надежности информационно-управляющих систем потенциально опасных объектов на различных этапах их жизненного цикла опубликованы впервые.

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АВПКО — анализ видов последствий и критичности отказов
БТС — большая техническая система
БЦВМ — блок цифровой вычислительной машины, бортовая цифровая вычислительная машина
ВОЛС — волоконно-оптическая линия связи
ВС — вычислительная система
ЖЦ — жизненный цикл
ЗИП — запасные части, инструменты и принадлежности
ИСО — Международная организация по стандартизации (ISO — International Standard Organization)
ИУС — информационно-управляющая система
КА — космический аппарат
КСД — комплексная система обеспечения безопасности движения и автоматизированного управления движением поездов метрополитена
КТС — комплекс технических средств
ЛКИ — летно-конструкторские испытания
ЛПД — линия передачи данных
МЦМ — микропроцессорная централизация метрополитена
МЭК — Международная электротехническая комиссия
НИР — научно-исследовательская работа
ОКР — опытно-конструкторские работы
ОС — операционная система
ПА — поездная аппаратура
ПЛИС — программируемые логические интегральные схемы
ПО — программное обеспечение
ПОД — подсистема обмена данных
ПУ — подсистема управления
РН — ракета-носитель
СА — станционная аппаратура
СЗ — средство защиты
СУД — система управления движением
СКОП — специализированный комплекс отладки программ
СТС — сложная техническая система
ТЗ — техническое задание
ТС — техническая система
ТУ — технические условия
ЦДП — центральный диспетчерский пост
ЭРИ — электрорадиоизделия

ВВЕДЕНИЕ

Последнее десятилетие характеризуется не только радикальным изменением социально-экономической среды, в которой функционируют российские предприятия и организации всех форм собственности, но и устойчивой тенденцией развития информационных процессов управления, выполняемых с помощью информационно-управляющих систем (ИУС).

Информационно-управляющая система представляет собой совокупность статистических данных, экономико-математических методов, технических, программных и других технологических средств, предназначенных для обработки информации и принятия управленческих решений.

Следует отметить, что вопросы надежности и безопасности в настоящее время приобретают особую актуальность. Основное внимание уделяется вопросам обеспечения надежности и безопасности таких систем управления объектами, которые являются потенциально опасными, т. е. относятся к системам с требованиями по безопасности. Свойство безопасности занимает центральное место вследствие возрастающей сложности технических систем управления промышленного назначения. Такими промышленными объектами являются атомная энергетика, ракетно-космическая техника и ее испытательные полигоны, все виды транспорта, государственные и региональные системы электроснабжения и многие другие. Сложные системы управления при определенных ситуациях могут стать источниками опасности для населения и окружающей природной среды, сопрягаемых объектов и обслуживающего персонала. Поэтому разработка и внедрение научных и практических основ теории безопасности, методологии формирования математического аппарата, позволяющего оценивать и контролировать выбранные показатели управляющих систем, являются перспективным направлением повышения конкурентоспособности российских систем управления потенциально опасными объектами, основой инвестиционной привлекательности наукоемких технологий их создания. Главную проблему, возникающую при создании данных систем, обусловливает необходимость обеспечения повышенных требований по надежности и безопасности современных многофункциональных информационно-управляющих систем при наличии жестких ограничений на сроки разработки и материальные ресурсы. Это делает разработку методологии оценивания и контроля показателей надежности и безопасности одним из важных и востребованных научных направлений.

Разработчикам систем управления необходимо понимать определение термина «безопасность», а также представлять, что понимается под угрозой, каковы источники ее происхождения, каким образом оцениваются и контролируются безопасность и эффективность средств защиты от различного рода угроз.

В Федеральном законе «О техническом регулировании» указано, что безопасность — это «состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу, …, окружающей среде…». Практическое применение систем управления опасными

объектами возможно при условии, что сами эти системы являются безопасными, т. е. обладают свойством безопасности.

В международном стандарте (МС) ЕН 292-1:1991 «Безопасность машин. Основные понятия, общие принципы конструирования. Часть 1. Основная терминология, методология», аутентичным переводом которого является применяемый в нашей стране ГОСТ Р 51333–99, а также в МС Международной организации по стандартизации ИСО 12100-1:1992 «Безопасность машин. Основные концепции, общие принципы проектирования. Часть 1. Основная терминология, методология» термин «безопасность» зафиксирован как свойство системы (объекта).

Понятие функциональной безопасности введено Международной электротехнической комиссией (МЭК), опубликовавшей серию базовых стандартов IEC 61069: Industrial-process measurement and control. Evaluation of system properties for the purpose of system assessment[1]. Согласно указанным документам под функциональной безопасностью понимается способность системы надежно и достоверно выполнять заданные функции, обеспечивающие безопасную работу потенциально опасных объектов. В этой серии стандартов, а также в других международных и национальных стандартах, нормативных и руководящих документах, монографиях и учебниках свойства надежности и безопасности часто путаются. Между терминами «надежность» и «безопасность» в некоторых публикациях отсутствуют границы, а используемые определения имеют нечеткий характер.

Для оценивания и контроля надежности и безопасности при решении многих практических задач требуются научно обоснованные терминологические и методические определения.

Защита человеческой жизни, минимизация материальных потерь, предотвращение вреда окружающей среде являются значительными проблемами. Кроме того, создание методических основ расчета и нормирования безопасности осложняется возрастанием функциональных требований к системам управления, обусловленным, в свою очередь, бурным развитием элементной базы. Например, применяемые в настоящее время электронные компоненты промышленных систем управления имеют среднюю наработку до отказа от сотен тысяч до нескольких миллионов часов. При использовании таких компонентов в достаточно объемной и сложной системе достижимой является ее наработка до отказа 50–100 тыс. ч. Высокие, на первый взгляд, показатели надежности, тем не менее, не дают представления о реальной безопасности системы, ибо если не принять специальные меры, то даже единичный отказ составной части или отдельного элемента может оказаться «опасным», т. е. или реально, или потенциально приведет либо к жертвам, либо к серьезным экономическим, экологическим и другим последствиям.

Данная проблема привела к возникновению и утверждению на уровне национальных и отраслевых стандартов кроме численного нормирования — «философии» построения безопасных систем, формированию специфических требований: для систем управления на базе микропроцессорной техники это, как правило, требования использования мажоритарных схем («схем с голосованием»)

[1] МЭК 61069. Контроль и управление промышленными процессами. Оценка свойств системы для целей ее аттестации.

типа «два из двух», «два из трех», «три из четырех» и т. п., а также схем с безопасными оконечными устройствами или иначе — со схемами с «несимметричными отказами». Под схемами с несимметричными отказами понимаются собственно схемы и их реальные физические компоненты, обеспечивающие при любых однократных внутренних повреждениях или сбоях перевод системы в безопасное («защитное») состояние путем выдачи соответствующего управляющего воздействия. Описанная «философия» распространяется на схемы выдачи потенциально опасных команд и схемы выдачи команд перевода системы в «защитное» состояние при аппаратных повреждениях или программных сбоях. Причем перевод в «защитное» состояние должен выполняться во всех случаях появления повреждений или сбоев элементов системы, поскольку следующий, даже крайне маловероятный отказ может быть «опасным». Действие последнего правила распространяется и на схемы систем с неконтролируемыми (не выявляемыми самой системой в процессе эксплуатации) отказами компонентов, т. е. априори считается, что если в системе такие компоненты есть, то может произойти накопление их отказов в произвольном количестве и порядке.

Представим себе на уровне логичных рассуждений, например, двух-трехуровневую иерархическую систему управления, в которой на каждом уровне, как по входу, так и по выходу, используются мажоритарные схемы «два из трех», а для приема и выдачи сигналов и команд управления на исполнительные устройства используются дублированные схемы с «несимметричными отказами». Если, кроме того, вся система взаимодействует с подсистемами контроля, диагностики и восстановления (отключения) поврежденных компонентов и имеет несколько резервированных автоматизированных рабочих мест, а также определенную модель технического обслуживания, то ясно, что создание методики и проведение расчетов показателей безопасности и надежности такой системы является чрезвычайно сложной проблемой.

В этой связи понятно, что конкретные наработки по созданию сложных многофункциональных систем управления с требованиями по безопасности и проведение расчетов соответствующих показателей с использованием стохастических и других методов являются актуальными не только для понимания проблемы обеспечения надежности и безопасности разрабатываемой системы, но и для адекватного и взвешенного подхода к формированию нормативных требований общего применения.