УДК 519.71

В.П. Пошивалов, Ю.Ф. Даниев, Л.В. Резниченнко

СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ НАДЁЖНОСТИ СЛОЖНЫХ СИСТЕМ

Аннотация. Рассмотрен системный подход к обеспечению надёжности. Приведены основные принципы современной методологии обеспечения надежности сложных систем на всех этапах жизненного цикла
Показана перспективность использования метода активного резервирования с перестраиваемым восстанавливающим элементом в задачах обеспечения надежности.
Ключевые слова: сложная система, системный анализ, обеспечение надёжности, программное обеспечение.

Постановка проблемы. При решении проблемы надежности сложных систем (СС) условно можно выделить два направления: расчёт надёжности и её обеспечение. Первое направление основывается в основном на применении специальных математических методов, а второе связано с решением традиционных конструкторских и технологических задач по созданию высококачественных систем и правильной их эксплуатации. В процессе становления науки и практики в области надёжности СС стало понятно, что отдельно взятыми расчётными, конструкторскими или одними организационными методами проблему надёжности не решить. Поэтому постепенно ситуация изменилась в пользу разумного сочетания методов расчёта надёжности и организационно-технического обеспечения надёжности систем с помощью нормирования, конструкторских решений и экспериментальной отработки. Непрерывный рост сложности систем ставит перед разработчиками ряд проблем, связанных с обеспечением высокой надежности, так как недостаточно высокий ее уровень, как показывает практика их эксплуатации, приводит к большому числу аварий. Поэтому на современном этапе, учитывая накопленную информацию в части надежности сложных систем, актуальным является разработка новых подходов и методов по обеспечению надежности на этапах от проектирования до снятия системы с эксплуатации.

Целью работы является разработка системного подхода к обеспечению надёжности сложных систем.

Основная часть. На основе анализа различных источников можно выделить следующие принципы современной методологии обеспечения надежности:

– системный подход к обеспечению надежности;

– использование вероятностных показателей надежности, включаемых в контракты с заказчиком;

– всесторонние отработочные испытания в условиях, максимально приближенных к эксплуатационным;

– использование на стадиях опытно-конструкторских работ систем автоматизированного проектирования, позволяющих сократить сроки разработки, избежать конструкторских ошибок, проводить сравнение различных вариантов построения систем, оптимизировать проекты по критериям стоимости и надежности, оптимальных весовых показателей и габаритов;

– использование на стадии производства автоматических и автоматизированных технологических процессов, контрольных систем и средств неразрушающего контроля;

– создание экспериментальной базы, позволяющей проводить отработку элементов систем на этапе испытаний;

– создание отказоустойчивой аппаратуры.

В [1-10] отмечены следующие направления работ по обеспечению надежности на всех этапах жизненного цикла:

– обеспечение безопасности;

– разработка нормативов и сертификаций, методических документов в области надёжности;

– создание физических основ надёжности;

– программное обеспечение работ по надёжности и безопасности.

В качестве основы обеспечения надежности СС целесообразно использовать методы системного подхода. Этот подход к проектированию любого объекта дает определенную гарантию получения качественного проектного решения и позволит объективно оценить уровень надежности на всех этапах жизненного цикла системы. Системный подход отличается от традиционного подхода предположением, что целое обладает такими качествами (свойствами), каких нет у его

частей. Наличием этих качеств целое, собственно, и отличается от своих частей. Данная связь между целыми и его частями была положена в основу первых определений системы, например такого: «система - это совокупность связанных между собой частей» [3].

Системы являются сложными многоуровневыми и многокомпонентными образованиями. В целях адекватной информации и определения причинных связей элементы системы конкретизируются. Такой подход позволяет однозначно определить опасности и опасные состояния системы. Он обеспечивается декомпозицией систем - расчленением иерархии и организации системы на взаимосвязанные составные части (подсистемы, элементы), последующим исследованием их независимо друг от друга и координацией локальных решений. Этот метод представляет, по существу, разложение сложных систем на простые с применением теорем об условных вероятностях и условных распределениях. При этом вначале вычисляются показатели надежности более простых подсистем, а затем полученные результаты группируются с целью получения характеристик всей системы в целом. Рассматриваемый метод может быть использован для упрощения, как пространства состояний, так и конфигурации системы. Эффективность метода зависит от выбора ведущего элемента, т.е. элемента, используемого при декомпозиции системы. Если этот элемент выбран неудачно, то, несмотря на идентичность конечного результата, вычисления окажутся значительно более громоздкими. В случае сравнительно сложных систем правильный выбор главных элементов для создания простой конфигурации может оказаться сложной задачей.

Применение системного подхода при анализе элементов СС дает возможность формально оценить ее структуру. Используемые в ходе анализа характеристики СС могут служить объективной (относительной) мерой его структурного совершенства. Если в качестве примера СС рассмотреть, стартовый комплекс, то в том случае проведение анализа возможно, если выполнен синтез структуры его технологического оборудования, и функций, им реализуемых, а также приняты технические решения по разработке средств обеспечения безопасности каждого из агрегатов и систем оборудования. Такой анализ позволяет принимать окончательное решение при формировании облика стартового комплекса даже в случае использования при его по-

строении принципиально новых, ранее не опробованных, технических решений.

Анализ структуры СС проводится с использованием теории графов. Вершинам графов соответствуют агрегаты, а ребрам (дугам) – технологические операции. В качестве одной из важных характеристик структур СС является сложность, которая характеризует структуру оборудования СС и позволяет оценивать однородность оборудования.

Сложность определяется соотношением

$$U = E \log_a n , \qquad (1)$$

где e_i – связи графа (дуги или ребра);

$E = \sum_{i=1}^{m} e_i$ – количество дуг и ребер графа;

n – число агрегатов;

m – число технологических операций;

a – произвольное число, значение которого выбирается в диапазоне

$$1 < a < \sqrt{n} . \qquad (2)$$

Для обеспечения безопасности функционирования СС ее сложность должна быть по возможности минимальной.

При разработке системного подхода к обеспечению надежности сложных систем необходимо найти взаимосвязь между конструкторскими, технологическими, экономическими, эксплуатационными и эргономическими факторами, определяющими конкурентоспособность системы. В этом отношении важно установить влияние функционально-стоимостного анализа указанных факторов на обеспечение надежности системы. Решение этой задачи чрезвычайно сложно и многовариантно, а также требует оптимизации всех факторов.

Обычно системный подход к обеспечению надежности систем увязывают с оптимизацией лишь конструкторских и технологических факторов, проводя их функционально-стоимостный анализ, включающий две процедуры: функционально-стоимостную диагностику процесса; поиск и выбор оптимального варианта конструкции или технологического процесса, исходя из целей анализа. При выполнении функционально-стоимостного анализа конструкторских и технологических решений необходимо предусмотреть следующие этапы: подготовительный, аналитический, творческий, исследовательский,

 ISSN 1562-9945

рекомендательный, внедрения. Решение этих проблем на этапе проектирования в значительной мере зависит от выбора надежных схемно-конструкторских решений, введения различных видов избыточности, обеспечения определенных запасов работоспособности.

Одним из методов обеспечения надёжности СС является резервирование. При этом определяется основной показатель надежности СС – безотказность в течение требуемого времени. При анализе вероятности безотказной работы рассматривают структурные схемы надежности, образованные из конечного набора последовательных и параллельных блоков определенного типа. Трудности, возникающие при рассмотрении сложных систем, можно уменьшить, используя метод преобразования. Он состоит в последовательном упрощении систем с последовательным и параллельным соединением элементов путем преобразования их в эквивалентные схемы. Подобная процедура выполняется до тех пор, пока вся система не будет сведена к одному-двум элементам. При этом обычно делается допущение о независимости отказов.

Соединения элементов в структурной схеме надёжности СС может включать различные виды последовательного и параллельного соединения элементов (цепей). В настоящее время наибольшее распространение получили математические модели расчета надежности СС и ее комплектующих (функциональных устройств, блоков, цепей), которые могут находиться в активном режиме или в пассивном (ненагруженном) состоянии. При этом зачастую применяется экспоненциальный закон распределения времени безотказной работы.

Для расчета надежности $P(t)$ СС с такими комплектующими можно использовать следующие соотношения:

– резервированный по схеме m/n „блок со всеми блоками в активном (нагруженном) режиме”

$$P(t) = \sum_{i=1}^{n-m} C_n^i \left(1 - e^{-\lambda t}\right)^i \left(e^{-\lambda t}\right)^{n-i}; \qquad (3)$$

– резервированный по схеме m/n „блок с наличием блоков в ненагруженном режиме”

$$P(t) = e^{-m\lambda t}\left[1 + \sum_{i=1}^{n-m} \frac{\left(1 - e^{-\lambda_{xp} t}\right)}{i!} \prod_{j=0}^{i-1}\left(j + m\frac{\lambda}{\lambda_{xp}}\right)\right], \qquad (4)$$

где t – время работы блока;

λ – интенсивность отказов в активном режиме;

$\lambda_{хр}$ – интенсивность отказов блока в режиме хранения ($\lambda_{хр} = \lambda/10$;

n – количество одинаковых параллельных блоков;

m – количество работающих блоков, определяющих работоспособность схемы, и тех, которые зарезервированы остальными $n-m$ блоками.

Вероятность безотказной работы системы при общем резервировании с постоянно включенным резервом при кратности резервирования m вычисляется по формуле

$$P_c(t) = 1 - \left[\left(1 - P_o(t)\right)\right]^m, \tag{5}$$

где $P_o(t)$ – вероятность безотказной работы исходной нерезервированной системы.

Из (5) получаем следующее выражение кратности резервирования:

$$m = \frac{\ln\left[1 - P_c\right]}{\ln\left[1 - P_o(t)\right]} - 1. \tag{6}$$

Вероятность безотказной работы системы при общем резервировании замещением при кратности резервирования m вычисляется по формуле

$$P_c(t) = P_o(t) \sum_{i=0}^{m} \frac{\left[-\ln P_o\right]^i}{i!}. \tag{7}$$

Здесь выражение для кратности резервирования m получить в явном виде нельзя.

В настоящее время одним из эффективных методов обеспечения надёжности является метод активного резервирования с перестраиваемым восстанавливающим элементом (ВЭ) способном обеспечить непрерывность работы системы при возникновении неисправностей в резервируемых блоках. Это необходимо для обеспечения требуемой эксплуатационной надежности СС ответственного применения.

Другая не менее важная задача - обеспечение надежности СС с использованием выбранного метода активного резервирования с ВЭ - также является проблематичной. Выигрыш в надежности при применении того или иного метода активного резервирования с ВЭ всегда

сопровождается ухудшением ряда других характеристик системы, таких как масса, габариты, потребляемая мощность, стоимость. Для систем с различным функциональным составом и характером функционирования возникают проблемы выбора оптимального состава средств восстановления. Поэтому важно решение этой задачи с учетом минимизации структурной избыточности. При этом необходимо решать эти задачи с учетом использования современных комплектующих элементов и новых подходов в технологии испытаний.

Применение программного обеспечения (ПО) в сложных системах требует изучения вопроса повышения его надежности. Каждая ошибка в ПО, применяемом в системах важных для безопасности опасных производственных объектов (таких как система внутриреакторного контроля, система контроля и управления, автоматизированная система контроля радиационной обстановки), может привести к серьезным последствиям и даже аварийным ситуациям. При увеличение сложности и все более широкое распространение программных систем, сжатость сроков разработки, ограниченность в людских и финансовых ресурсах часто не позволяет достичь требуемых показателей надежности ПО. Основная причина ошибок в ПО – сложность. Для борьбы со сложностью выделяются две концепции:

– независимость;

– иерархическая структура.

Необходимо выработать рекомендации по созданию надежного ПО, прогнозированию характеристик ПО в условиях ограниченных ресурсов и достижению требуемых показателей надежности ПО.

В этом плане целесообразно выделить следующие способы обеспечения и повышения надежности ПО:

– усовершенствование технологии программирования;

– выбор алгоритмов, не чувствительных к различного рода нарушениям вычислительного процесса (использование алгоритмической избыточности);

– резервирование программ;

– верификация и валидация программ с последующей коррекцией.

Выводы

– Рассмотрен системный подход к обеспечению надёжности.

– Приведены основные принципы современной методологии обеспечения надежности сложных систем на всех этапах жизненного цикла.

– Отмечено перспективность использования метода активного резервирования с перестраиваемым восстанавливающим элементом в задачах обеспечения надежности.

ЛИТЕРАТУРА

1. Тимошенков С. П. Основы теории надежности / С. П. Тимошенков, Б. Н. Симонов, В.Н. Горошко. – М.: Издательство Юрай,2015.– 445с.
2. Лазуков В.Л. Способы обеспечения надёжности технических систем // Фундаментальные исследования. – 2009. – № 1 – стр. 33-33
3. Месарович М., Мако Д., Такахара И Теория иерархических многоуровневых систем: Пер. с англ. – М.: Мир, 1973. — 344 с.
4. Непомнящий В.М., Рякин О.М. Прикладные методы верификации программ. - М.:Радио и связь, 1988.-256 с.
5. Атлас Д., Миллер Г., Новак М. Практическое руководство по экстремальному программированию. - М.: Вильяме, 2002. - 318 с.
6. Гэйн К, Сарсон Т. Структурный системный анализ: средства и методы. - М: ЭЙТЕКС, 1993. - ч. 1 и т. 2 -188 с. и 214 с.
7. Бек К. Экстремальное программирование. - М.: Питер, 2002. - 220 с
8. Пальчун Б.П., Юсупов Р.М. Оценка надежности программного обеспечения. - СПб: Наука, 1994. - 84 с.
9. Смагин В.А. Метод оценивания и обеспечения надежности сложных программных комплексов. УДК 681.3.06 - http://www.bezpeka.com/library/sci/smaginl.html. 2000.
10. ШтрикА.А., ОсовецкийЛ.Г., Мессих И.Г. Структурное проектирование надежных программ встроенных ЭВМ. - Л. Машиностроение, 1989. - 296 с.

 ISSN 1562-9945