А. Е. Александрович, В. О. Чуканов, В. А. Шурыгин

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

При создании информационно-вычислительных систем (ИВС) ответственного целевого назначения встает проблема обеспечения их функциональной безопасности в рамках заданных системных спецификаций и требований. Определим функциональную безопасность ИВС как надежность выполнения ее базовых функций. На протяжении многих лет методика проектирования высоконадежных ИВС включала в себя важный этап моделирования надежности проектируемой системы. При этом для получения общей оценки надежности первоначально при ее проектировании использовалось аналитическое моделирование надежности на основе теоретико-вероятностных формул и соотношений. Для более полного учета временных и технических параметров системы применялось имитационное моделирование, особенно если разрабатывалась система реального времени. Таким образом, главными этапами надежностного проектирования (которое всегда происходило параллельно с общим процессом проектирования продукта) являлись

- анализ требований и выработка системных спецификаций (пунктов технического задания, связанных с требованиями к надежности ИВС);
- построение аналитической модели надежности проектируемой системы;
- построение имитационной модели надежности системы;
- создание системного прототипа и верификация полученных ранее оценок;
- реализация системы и проверка адекватности разработанных ранее моделей надежности.

Данная работа посвящена анализу современной ситуации в области проектирования ИВС ответственного целевого назначения и разработке методики надежностного проектирования современных систем с учетом их специфики и особенностей их разработки.

На основе анализа доступной проектной информации можно выделить следующие особенности процесса проектирования современных ИВС:

- рост масштаба и сложности проектируемой системы;
- наличие сетевых линий и коммуникационных каналов практически в каждой разработке;
- возрастание требований к надежности проектируемой системы обусловлено не только ответственностью целевого приложения, но и чисто коммерческими факторами и причинами, например, недопустимостью перерывов в работе системы, которые могут приводить к серьезным финансовым потерям;
- при анализе надежности всей системы необходимо учитывать не только безотказность оборудования (аппаратной части системы), но и надежность ее программного обеспечения.

Сложность системы. Данная особенность существенно влияет на процесс проектирования ИВС. Усложнение разработки предполагает многоэтапную процедуру моделирования надежности системы. Иерархия построения надежностной модели сложной системы может быть представлена следующим образом:

- Построение приближенной аналитической модели на ранних этапах проектирования ИВС.
- Разработка детализированной аналитической модели надежности отдельных звеньев (функциональных подсистем, коммуникационных каналов) системы; на этом этапе обычно используются традиционные теоретико-вероятностные методы анализа: метод перебора состояний, методы максимальных путей и минимальных сечений системы и т. д. [1].
- Структурное имитационное моделирование отдельных звеньев системы; на этом этапе целесообразно использовать универсальный язык структурного моделирования GPSS [2], в качестве альтернативы можно рассмотреть систему AnyLogic [3].
- Функционально-логическое моделирование отдельных устройств системы (при необходимости разработка специализированных компонентов и схем); на этом этапе в настоящее время целесообразно использовать язык VHDL [4].

Если говорить об особенностях проектирования современных ИВС, то нельзя не упомянуть о жесткости сроков их разработки и реализации. В сочетании с ростом их масштабов и сложности это приводит к тому, что:

- разработка общей имитационной модели надежности всей системы становится нецелесообразна, поскольку из-за ее сложности время ее разработки и верификации слишком велико;
- разработку аналитических и имитационных моделей надежности отдельных звеньев системы приходится вести параллельно с созданием системного прототипа и даже реализацией системы.

Следует отметить, что такой параллельный режим разработки как самой системы, так и ее моделей надежности обеспечивает возможность непрерывной калибровки (уточнения) разрабатываемых моделей надежности, поскольку собираемая статистика по системным отказам позволяет все время получать более точные значения исходных параметров, в частности, интенсивности отказов системных компонентов (аппаратных и программных), среднего времени их восстановления и т. д.

Результатом проведенных исследований является методика надежностного проектирования современных высоконадежных ИВС, учитывающая все вышеприведенные факторы и особенности процессов разработки. Методика использована при проектировании трех конкретных информационно-управляющих систем ответственного целевого назначения. Первая система предназначена для информационного обеспечения и управления мобильными объектами, соединенными с центром управления с помощью каналов радиосвязи. Вторая система обеспечивает мониторинг ряда важных технологических объектов. Система имеет звездообразную конфигурацию, в центре которой находится управляющая станция, соединенная несколькими коммуникационными каналами с важными технологическими объектами. Третья система представляет собой типовую архитектуру корпоративной IP-телефонии.

СПИСОК ЛИТЕРАТУРЫ:

1. *Половко А. М., Гуров С. В.* Основы теории надежности. СПб.: БХВ-Петербург, 2006.
2. *Жданова Е. Г., Томашевский В. Н.* Имитационное моделирование в среде GPSS. М.: Бестселлер, 2003.
3. *Карпов Ю. Г.* Имитационное моделирование систем. Введение в моделирование с AnyLogic 5. СПб.: БХВ-Петербург, 2006.
4. *Армстронг Дж. Р.* Моделирование цифровых систем на языке VHDL / Пер. с англ. М.: Мир, 1992.