

АНАЛИЗ ДИНАМИЧЕСКОГО ДЕРЕВА ОТКАЗОВ

Статью представил д.т.н., проф. Бочков К. А.

Введение

Анализ дерева отказов (Fault Tree Analysis – ФТА) – один из распространенных методов моделирования надежности технических систем и технологических процессов на стадии проектирования [1]. Он заключается в построении и анализе дерева отказов – ациклического ориентированного графа, определяющего причинно-следственные связи отказа системы с отказами ее подсистем и элементов, а также другими событиями и воздействиями (рис. 1).

Дерево отказов (ДО) получают в результате последовательной детализации событий, связанных с отказами системы, ее подсистем и элементов от «следствия» к

«причине» (т.е. «сверху вниз»), для того чтобы отыскать возможные причины их возникновения [1, 2].

Целью работы является разработка модели динамического дерева отказов, которая обобщает традиционные деревья отказов: события дерева характеризуются временем до наступления с некоторой функцией распределения. Показать способ вычисления функции распределения времени до наступления результирующего события (функции отказа системы) по известным функциям распределения времени до наступления базовых событий, что позволит непосредственно определять все показатели безотказности невосстанавливаемых объектов.

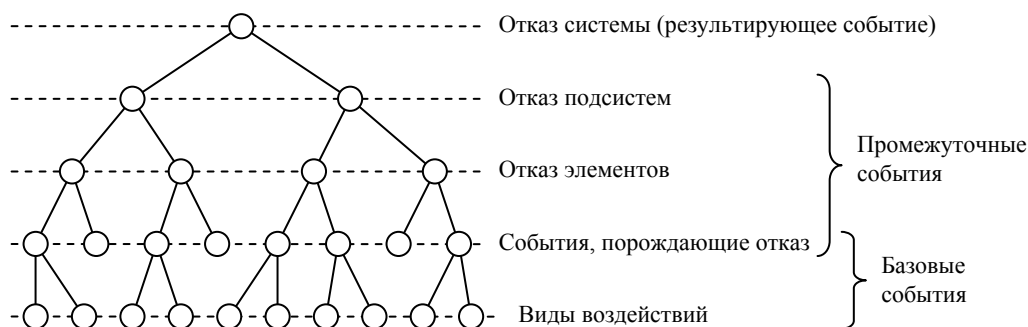


Рис. 1. Схематическое изображение дерева отказов

Возможности метода ФТА

По информативности описания условий работоспособности системы, которая включает логическую полноту средств графического представления булевых функций и задания условий работоспособности системы через состояния ее элементов, ДО занимает промежуточное положение между структурной схемой надежности и графом состояний [1, 2]. Несмотря на это, метод ФТА традиционно используется лишь для качественной оценки безотказности сис-

тем [1, 2, 3], в том числе, для анализа минимальных сечений отказов (реализован в программных комплексах RAM Commander, Risk Spectrum, FaultTree [4, 5]). Количественный анализ показателей надежности в основном ограничивается определением следующих показателей безотказности невосстанавливаемых систем с независимыми отказами элементов:

- вероятность отказа (пакеты RAM Commander, Risk Spectrum, FaultTree);
- частота отказов (пакеты RAM Commander, Risk Spectrum);

- значимость исходных событий (пакет RAM Commander) и аварийных сочетаний по различным критериям (пакет FaultTree);
- анализ Парето (пакеты FaultTree, RAM Commander).

Вместе с тем, в [6] рассматриваются перспективы использования ФТА для определения показателей надежности систем

- с восстанавливаемыми элементами;
- с учетом последовательности отказов;
- с учетом зависимости между отказами (и другими событиями);
- с учетом частичных и множественных отказов.

Модель и метод количественного анализа динамического дерева отказов

Большинство проблем количественного анализа показателей надежности методом ФТА обусловлены тем, что существующие подходы оперируют статической моделью ДО. При этом предполагается, что некоторые события (воздействия, отказы) могут иметь место в течение некоторой наработки с известной вероятностью, а время и последовательность их наступления не учитываются.

Главной особенностью предлагаемой модификации метода ФТА является рассмотрение ДО в динамике. Для этого предусматривается учет не вероятностей на-

ступления событий, а функций распределения времени до наступления каждого из базовых, промежуточных и результирующего события в системе. Информация о функции распределения времени до наступления результирующего события (отказа системы) позволяет непосредственно определять среднюю и гамма-процентную наработку системы до отказа, все другие показатели безотказности невосстанавливаемых систем [1, 2]. В частном случае, задаваясь некоторой наработкой, можно прийти к традиционному подходу определения вероятности отказа системы.

В соответствии с выбранной моделью и операциями над событиями [3], представим способ определения вероятностных характеристик промежуточных и результирующего события. Для этого определим следующие функции и величины.

Пусть ξ_1 – время до наступления первого события-причины, описываемое функцией распределения $F_1(x)$; ξ_2 – время до наступления второго события-причины, описываемое функцией $F_2(x)$. Тогда η – время до наступления события-следствия, описываемое функцией распределения $F(x)$ (рис. 2). Укажем способ определения функции распределения $F(x)$ времени до наступления события-следствия для различных вариантов взаимосвязей событий-причин.

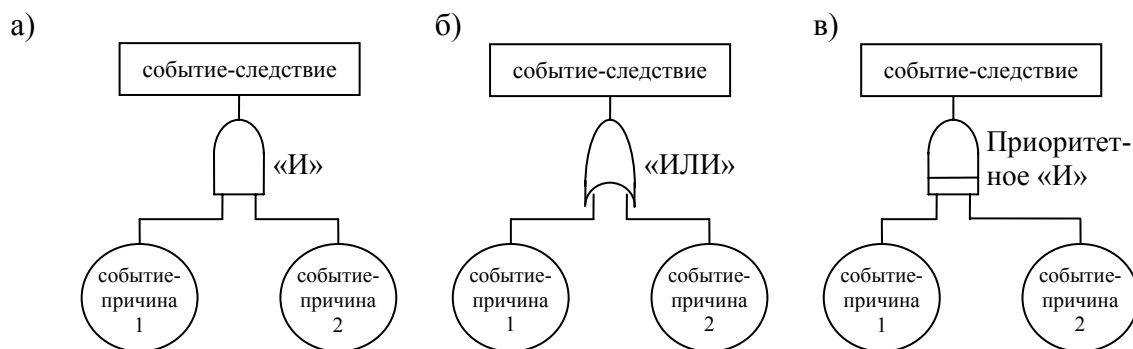


Рис. 2. Примеры используемых логических операций над событиями

Моделирование причинно-следственной связи «И»

Рассмотрим вариант, когда событие-следствие связано с событиями-причинами логическим символом «И» (рис. 2, а). В

этом случае величина η определяется величинами ξ_1 и ξ_2 следующим выражением:

$$\eta = \max\{\xi_1, \xi_2\}, \quad (1)$$

а ее функция распределения:

$$\begin{aligned}
F(x) &= P(\eta < x) = P(\{\xi_1 < x\} \cap \{\xi_2 < x\}) = \\
&= P(\xi_1 < x) P(\xi_2 < x | \xi_1 < x) = F_1(x) \times \\
&\times F_2(x | \xi_1 < x)
\end{aligned} \quad (2)$$

Предполагая, что события-причины независимы,

$$F(x) = F_1(x) F_2(x). \quad (3)$$

Моделирование причинно-следственной связи «ИЛИ»

Рассмотрим вариант, когда событие-следствие связано с событиями-причинами логическим символом «ИЛИ» (рис. 2, б). В этом случае:

$$\eta = \min\{\xi_1, \xi_2\}, \quad (4)$$

а ее функция распределения (для независимых событий-причин):

$$\begin{aligned}
F(x) &= P(\eta < x) = P(\{\xi_1 < x\} \cup \{\xi_2 < x\}) = \\
&= P(\xi_1 < x) + P(\xi_2 < x) - P(\xi_1 < x) \times \\
&\times P(\xi_2 < x) = F_1(x) + F_2(x) - F_1(x) F_2(x).
\end{aligned} \quad (5)$$

Моделирование причинно-следственной связи «приоритетное И»

Рассмотрим вариант, когда событие-следствие связано с событиями-причинами символом «приоритетное И» (рис. 2, в). В этом случае, как и в случае логического «И» величина η определяется величинами ξ_1 и ξ_2 выражением

$$\eta = \begin{cases} \xi_2, & \text{если } \xi_1 < \xi_2; \\ \infty, & \text{если } \xi_1 \geq \xi_2. \end{cases} \quad (6)$$

а ее функция распределения:

$$F(x) = P(\eta < x) = \begin{cases} P(\xi_2 < x), & \text{если } \xi_1 < \xi_2; \\ 0, & \text{если } \xi_1 \geq \xi_2. \end{cases} \quad (7)$$

Рассматривая события $\{\xi_1 < \xi_2\}$ и $\{\xi_1 \geq \xi_2\}$ как гипотезы и применяя к (7) формулу полной вероятности,

$$\begin{aligned}
F(x) &= P(\eta < x) = P(\xi_1 < \xi_2) \times \\
&\times P(\xi_2 < x | \xi_1 < \xi_2) + P(\xi_1 \geq \xi_2) \cdot 0 = \\
&= P(\xi_1 < \xi_2) P(\xi_2 < x | \xi_1 < \xi_2)
\end{aligned} \quad (8)$$

или, применяя к событиям $\{\xi_1 < \xi_2\}$ и $\{\xi_2 \leq x\}$ теорему умножения вероятностей,

$$F(x) = P(\eta < x) = P(\xi_2 < x) P(\xi_1 < \xi_2 | \xi_2 < x). \quad (9)$$

Рассмотрим вспомогательную случайную величину ξ^* , полученную из ξ_2 усечением справа в точке x . Ее функция плотности определяется выражением [7]

$$f^*(y) = \begin{cases} \frac{1}{P(\xi_2 < x)} f_2(y), & y < x; \\ 0, & y \geq x. \end{cases} \quad (10)$$

Событие $\{\xi_1 < \xi_2 | \xi_2 < x\}$ тождественно событию $\{\xi_1 < \xi^*\}$. Тогда выражение (9) преобразуется в выражение

$$F(x) = P(\eta < x) = P(\xi_2 < x) P(\xi_1 < \xi^*). \quad (11)$$

В свою очередь, вероятность $P(\xi_1 < \xi^*)$ определим формулой [8, с. 145]

$$P(\xi_1 < \xi^*) = \int_{-\infty}^{\infty} f^*(y) F_1(y) dy. \quad (12)$$

Учитывая связь величин ξ^* и ξ_2 выражение (12) преобразуется в

$$\begin{aligned}
P(\xi_1 < \xi^*) &= \int_{-\infty}^{\infty} f^*(y) F_1(y) dy = \\
&= \frac{1}{P(\xi_2 < x)} \int_{-\infty}^x f_2(y) F_1(y) dy
\end{aligned} \quad (13)$$

Подставляя (13) в (11) и учитывая, что $\xi_1 > 0$ и $\xi_2 > 0$, получим

$$F(x) = \int_0^x f_2(y) F_1(y) dy. \quad (14)$$

Таким образом, выражение (14) вычисляет функцию распределения времени до наступления события-следствия, определяемого двумя событиями-причинами, связанными логическим символом «приоритетное И».

Компьютерная реализация предлагаемого метода анализа динамического ДО

Количественный анализ динамического ДО заключается в рекуррентном использо-

вании выражений (3), (5) и (14). При этом, по заданным функциям распределения времени до наступления базовых событий (отказов элементов, воздействий на систему) «снизу вверх» определяется функция распределения времени до наступления результирующего события (функция отказа системы). В дальнейшем по известной функции отказа системы можно определить все показатели безотказности невосстанавливаемых объектов по ГОСТ 27.002-89 [1, 2].

Для автоматизации расчета показателей безотказности систем методом анализа динамического ДО был разработан специализированный программный комплекс FDiTA (Fault Dinamic Tree Analysis). Поскольку реализация сложных математических преобразований (символьное интегрирование и дифференцирование) непосредственно в разрабатываемом программном обеспечении не представляется целесообразной из-за высокой трудоемкости, вместо этого рассматривалась возможность

а) использования свободно распространяемых бесплатных библиотек математических функций;

б) интеграции с современными пакетами компьютерной математики.

Несмотря на финансовые затраты, связанные с приобретением лицензионного программного обеспечения, второй подход имеет ряд преимуществ: алгоритмы пакетов компьютерной математики имеют, как правило, более высокую вероятность получения верного результата; они сопровождаются и постоянно дорабатываются; могут использоваться для решения других инженерных и научных задач.

Начиная с версии 9 разработчики пакета компьютерной математики Maple (компания Waterloo Maple Inc.) реализовали возможность использования функций ядра внешними программами. Данная технология, называемая OpenMaple, представляет собой набор интерфейсных функций и заголовочных файлов с описанием используемых Maple-структур для обмена данными, в том числе с программами, написанными с использованием компиляторов с языка программирования C++.

Апробация метода анализа динамического ДО

Продемонстрируем некоторые возможности использования пакета FDiTA на тестовом примере системы, заданной ДО (рис. 3, а). Будем предполагать, что базовые события (отказы элементов или воздействия на систему) независимы, а время до наступления каждого из них подчиняется экспоненциальному закону распределения с математическими ожиданиями 3, 4, 1, 2 тыс. часов, соответственно.

На рис. 3, б представлено ДО исследуемой системы в пакете FDiTA, на рис. 4, а – исходная информация о свойствах одного из базовых событий ДО, а на рис. 4, б – расчетные вероятностные показатели результирующего события.

Иллюстрация функции распределения времени до наступления результирующего события (функция отказа системы) в пакете FDiTA приведена на рис. 5. Результаты анализа ДО документируются в панели сообщений FDiTA и в текстовом файле Microsoft Word.

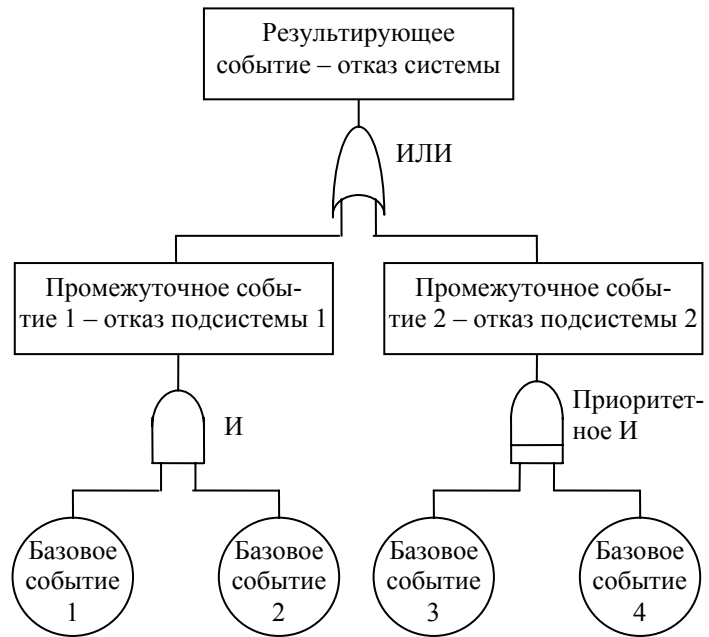
Выводы

В работе предложена модель динамического ДО, которая обобщает традиционные ДО: события динамического ДО характеризуются не только вероятностью, но и временем до наступления с некоторой функцией распределения. Такой подход позволяет дополнительно учитывать последовательность наступления событий.

Показан способ вычисления функции распределения времени до наступления результирующего события (функции отказа системы) по известным функциям распределения времени до наступления базовых событий. Информация о функции отказов системы позволяет непосредственно определять все показатели безотказности невосстанавливаемых объектов по ГОСТ 27.002-89, что не предусмотрено существующими стандартами и программными средствами анализа ДО.

Предлагаемый метод анализа динамического ДО реализован и апробирован в компьютерном пакете FDiTA

а



б

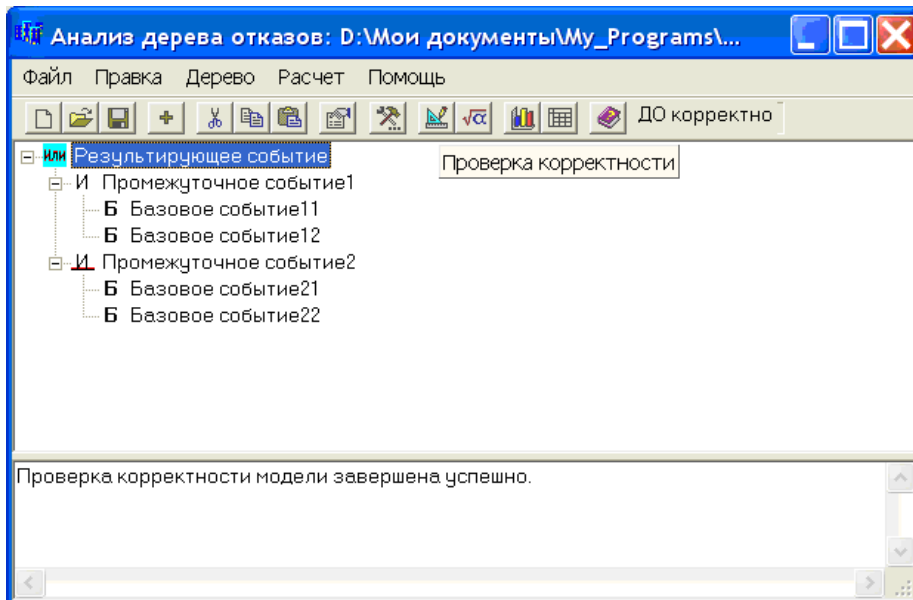


Рис. 3. Дерево отказов: исходное (а), в пакете FDiTA (б)

а

Свойства события: Базовое событие11

Название: Базовое событие11

Примечание: Отсутствует

Функция распределения времени до наступления: $1 - \exp(-1/3000 \cdot x)$

Вероятность наступления в течение заданной наработки, час: 2

Гамма-процентное время до наступления (час) для гамма, %: 95

Математическое ожидание времени до наступления, час: []

Мода времени до наступления, час: []

Стандартное отклонение времени до наступления, час: []

Медиана времени до наступления, час: []

Условие наступления события-следствия в зависимости от наступления событий-причин: Базовое событие

Список событий-причин: Отсутствуют

OK Cancel Отображать F(t) на диаграмме

б

Свойства события: Результирующее событие

Название: Результирующее событие

Примечание: Отсутствует

Функция распределения времени до наступления: $1 - 1/3 \cdot \exp(-1/4000 \cdot x) - \exp(-3/4000 \cdot x) + 1/3 \cdot \exp(-7/4000 \cdot x) - 1/3 \cdot \exp(-1/3000 \cdot x) - \exp(-1/1200 \cdot x) + 1/3 \cdot \exp(-1/11 \cdot x)$

Вероятность наступления в течение заданной наработки, час: $.13323e-5$

Гамма-процентное время до наступления (час) для гамма, %: 95

Математическое ожидание времени до наступления, час: 3159.866800

Мода времени до наступления, час: 0.

Стандартное отклонение времени до наступления, час: 3031.782340

Медиана времени до наступления, час: 2249.062541

Условие наступления события-следствия в зависимости от наступления событий-причин: ИЛИ

Список событий-причин: Промежуточное событие1

OK Cancel Отображать F(t) на диаграмме

Рис. 4. Окно свойств событий в пакете FDiTA: исходная информация (а), результаты анализа (б)

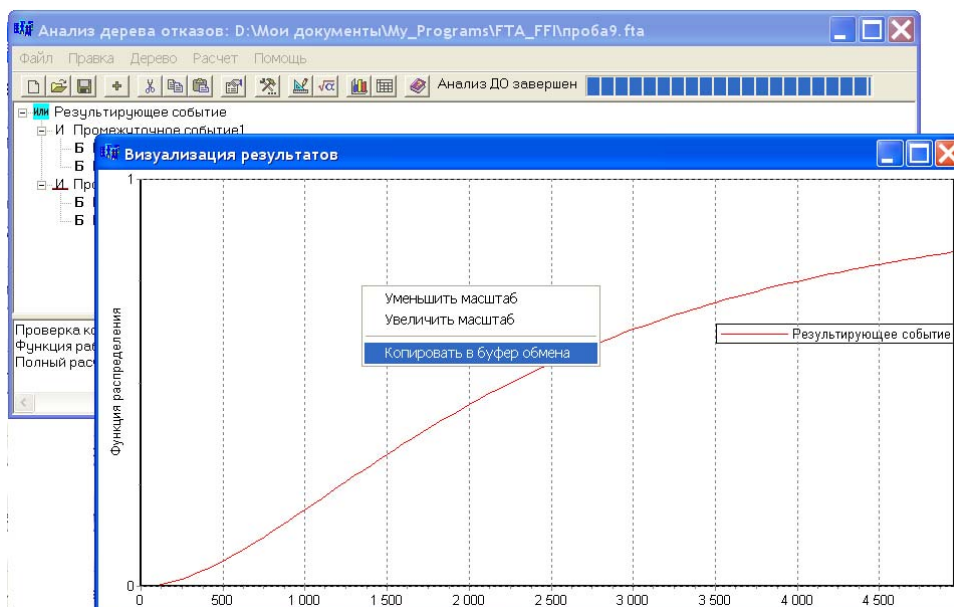


Рис. 5. Функция распределения времени до наступления результирующего события

Библиографический список

1. ГОСТ 27.301-95. Надежность в технике. Расчет надежности. Основные положения. – М.: Издательство стандартов, 1997. – 15 с.

2. Патрушев, В. И. Надежность и эффективность в технике. Проектный анализ надежности [Текст]: справочник В. И. Патрушев, А. И. Рембеза. – М.: Машиностроение, 1988. – 316 с.

3. Fault tree-analysis (FTA) IEC 1025: 1990. Стандарт МЭК Анализ дерева неполадок, 1990 [Текст] / перевод с франц., СИФ НТЦ ПБ-707. (ГОСТ Р 51901.13-2005 (МЭК 61025:1990). Менеджмент риска. Анализ дерева неисправностей).

4. Строгонов, А. Обзор программных комплексов по расчету надежности сложных технических систем [Текст] / А. Строгонов, В. В. Жаднов, С. Н. Полесский // Компоненты и технологии, – 2007. – №5. – С. 183–190.

5. Зильбербург, К. Л. Программные средства для анализа последствий отказов и обеспечения надежности изделий [Текст] / К. Л. Зильбербург, Е. В. Мекрюкова // Ра-

циональное управление предприятием. – 2007. – № 5. – С. 54–58.

6. Диллон, Б. Инженерные методы обеспечения надежности систем [Текст] / Б. Диллон, Ч. Сингх. Пер. с англ. – М.: Мир, 1984. – 318 с.

7. Крамер, Г. Математические методы статистики [Текст] / Г. Крамер. – М.: Мир, 1975. – 648 с.

8. Капур, К. Надежность и проектирование систем [Текст] / К. Капур, Л. Ламберсон – М.: Мир, 1980. – 606 с.

Ключевые слова: динамическое дерево отказов, функция распределения времени, результирующее событие.

Ключові слова: динамічне дерево відмов, функція розподілу часу, результуюча подія.

Key words: dynamic fault free, function of time allocation, result event.

Поступила в редколлегию 16.03.2011.

Принята к печати 17.03.2011.