ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 51901.13— 2005 (МЭК 61025:1990)

Менеджмент риска

АНАЛИЗ ДЕРЕВА НЕИСПРАВНОСТЕЙ

IEC 61025:1990
Fault Tree Analysis (FTA)
(MOD)

Издание официальное

БЗ 3—2004/33

Москва
Стандартинформ
2005

Предисловие

Задачи, основные принципы и правила проведения работ по государственной стандартизации в Российской Федерации установлены ГОСТ Р 1.0—92 «Государственная система стандартизации Российской Федерации. Основные положения» и ГОСТ Р 1.2—92 «Государственная система стандартизации Российской Федерации. Порядок разработки государственных стандартов»

Сведения о стандарте

1 ПОДГОТОВЛЕН Научно-исследовательским центром контроля и диагностики технических систем» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Научно-техническим управлением Госстандарта России

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 мая 2005 г. № 110-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 61025:1990 «Анализ дерева неисправностей (FTA)» (IEC 61025:1990 «Fault Tree Analysis (FTA)») путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ 1.5 (подраздел 3.6).

Изменения, введенные в настоящий стандарт по отношению к международному стандарту, обусловлены необходимостью наиболее полного достижения целей национальной стандартизации

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в указателе «Национальные стандарты», а текст изменений — в информационных указателях «Национальные стандарты». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе «Национальные стандарты»

размеров дерева неисправностей. Анализ дерева неисправностей позволяет выделять независимые ветви дерева неисправностей, которые могут исследоваться отдельно.

7.5.1.2 Булева редукция

Булеву редукцию применяют для оценки воздействия общих событий дерева неисправностей (идентичных событий, встречающихся в различных ветвях), когда местонахождение вершины событий не зависит от времени и последовательности событий. Булеву редукцию проводят путем решения булевых уравнений для дерева неисправностей.

7.5.1.3 Методы минимальных вырезок событий

Существует несколько методов определения минимальных вырезок событий, но их применение к большим деревьям может быть достаточно сложным. Рекомендуется использовать соответствующие компьютерные программы.

Набор вырезок — группа событий, которые при совместном появлении могут вызвать появление вершины событий. Минимальный набор вырезок — наименьшая группа событий, в которой для появления вершины событий все события должны произойти в надлежащей последовательности. Если любое из событий в минимальном наборе вырезок не происходит, это предотвращает появление вершины событий. Если события происходят в надлежащей последовательности, то расширяется определение минимальных наборов вырезок для дерева неисправностей, зависящих от последовательности событий. В этих случаях минимальный набор вырезок определяет группу событий, потенциально обеспечивающую появление вершины событий. Воздействие последовательности событий в этой группе может быть проанализировано с применением диаграммы установленных переходов, которая в настоящем стандарте не рассматривается.

7.5.2 Численный анализ

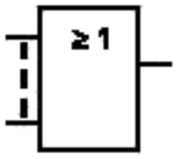
Цель численного анализа состоит в том, чтобы обеспечить количественную оценку вероятности появления вершины событий или выбранного набора событий. Численный анализ применяют также как дополнение к логическому анализу. Для численной оценки дерева неисправностей необходимы соответствующие вероятностные данные. Для определения количественных значений могут использоваться данные надежности, прогнозирования технического состояния, испытаний и эксплуатации.

7.5.3 Примеры использования булевой алгебры

7.5.3.1 Применение булевой алгебры к анализу дерева неисправностей

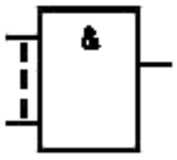
В деревьях неисправностей, которые состоят только из клапанов И, ИЛИ и НЕ, имеется взаимнооднозначное соответствие между выражением булевой алгебры и символами дерева неисправностей.

Символ дерева неисправностей



является клапаном ИЛИ, который представляет собой объединение входящих событий. Клапан ИЛИ эквивалентен булеву символу «+».

Символ дерева неисправностей



является клапаном И, который представляет собой пересечение входящих событий, приложенных к клапану. Клапан И эквивалентен булеву символу « · ».

Символы ИЛИ и И для булевой алгебры могут быть выражены другими символами, соответствующими используемым языкам компьютерных программ. В этом случае необходимо соблюдать логику символов.

Для дерева неисправностей, представленного на рисунке1, можно записать следующие логические выражения:

$$C = D + E,$$
$$A = B \cdot C = B \quad (D + E).$$

Применяя дистрибутивный закон, получаем выражение:

$$A = B \cdot D + B \quad E.$$

7.5.3.2 Применение булевой алгебры к минимальным вырезкам

Выражение для вершины событий может быть записано в терминах конечного числа минимальных вырезок p, которые являются уникальными для этой вершины событий.

Общая формула для описания вершины событий

$$T = M_1 + M_2 + \ldots + M_i + \ldots + M_p,$$

где T — вершина событий;

M_i — минимальные вырезки, каждая из которых состоит из комбинации определенных компонентов неисправностей. Общий минимальный набор вырезок можно записать в виде выражения

$$M = X_1 \cdot X_2 \cdot \ldots \cdot X_i \cdot \ldots \cdot X_c,$$

где X_i — основное событие дерева,

c — количество основных событий в минимальной вырезке M.

Рассмотрим дерево неисправностей, изображенное на рисунке 1. Минимальные наборы вырезок для вершины событий в этом случае — $B \cdot D$ и $B \cdot E$.

8 Идентификация и маркировка

Каждое событие в дереве неисправностей должно быть идентифицировано. События должны быть маркированы так, чтобы ссылки из дерева неисправностей к соответствующей проектной документации и обратно были понятны и легковыполнимы.

Вершина событий дерева неисправностей является нежелательным событием, которое является первичной причиной для проведения анализа дерева неисправностей. Необходимо отметить, что у каждого дерева неисправностей может быть только единственная вершина событий.

Если несколько событий в дереве неисправностей относятся к различным режимам отказа одного и того же элемента, то такие события должны быть маркированы так, чтобы их можно было различать, но должно быть ясно, что это — группа событий, связанных с одним и тем же элементом.

Если конкретное событие, например неспособность специфического клапана закрываться, имеется в нескольких местах дерева или в нескольких деревьях, то такие места должны иметь одинаковую маркировку. Однако события, которые являются подобными, но включают различные элементы, не должны быть одинаково идентифицированы.

Типичный код события должен содержать информацию, касающуюся идентификации системы, идентификации элемента и режима отказа.

Дерево неисправностей является диаграммой, в которой события связаны логическими клапанами. Каждый клапан имеет одно событие выхода, но одно или более входных событий.

Входные события указывают возможные причины и условия для событий выхода. Однако такая связь не обязательно определяет последовательные во времени отношения между событиями.

В основном дереве неисправностей используют клапаны И, ИЛИ и НЕ. Однако при анализе сложных систем могут потребоваться дополнительные символы для клапанов, что позволяет добиться максимальной простоты дерева неисправностей и обеспечить его читаемость. Очень важно определить и зафиксировать используемые символы, которые должны обеспечивать однозначное и непротиворечивое их применение при анализе конкретного дерева неисправностей. Это особенно важно, если анализ проводят автоматизированными методами.

При разработке дерева неисправностей аналитик должен использовать соответствующую символику и идентификацию, чтобы было ясно, что:

- событие или ветвь событий используются в другом месте дерева неисправностей;
- изображенная часть дерева включает события, используемые также в другой части дерева;
- событие общей причины, отраженное в одной части анализа, далее исследуется в другом месте.

Это необходимо для графического представления дерева неисправностей.

9 Отчет

Отчет об анализе дерева неисправностей должен включать, как минимум, перечисленные ниже основные пункты. Отчет может включать необходимую дополнительную информацию. Форма отчета в настоящем стандарте не устанавливается.

Основные пункты отчета:

- цель и область применения;
- описание системы:
  a) описание проекта,
  b) функционирование системы,

c) подробные определения границ системы;

- предположения:
  a) предположения, использованные в проекте системы,
  b) предположения, связанные с работой, обслуживанием, испытаниями и контролем,
  c) модельные предположения задач анализа надежности и эффективности;
- определение отказа системы и его критериев;
- анализ дерева неисправностей:
  a) анализ,
  b) данные,
  c) используемые символы;
- результаты и заключения.

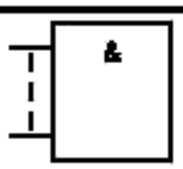
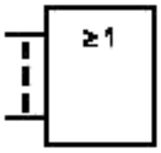
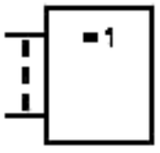
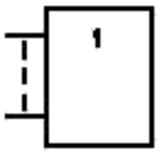
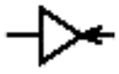
Дополнительные сведения, которые могут быть включены в отчет:

- графические изображения, схемы, чертежи;
- краткое описание данных надежности и ремонтопригодности и их источников;
- описание дерева неисправностей в читаемой компьютерной форме (для анализа сложных систем).

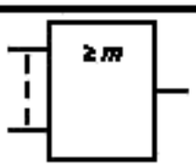
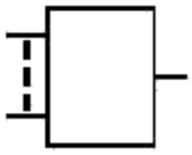
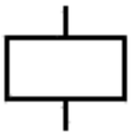
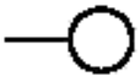
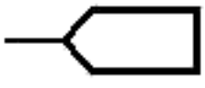
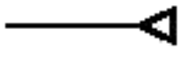
Приложение А
(обязательное)

Символы

Таблица А.1

Предпочтительный символ	Допустимый символ	Функция	Описание
		Клапан И	Событие происходит, если все входные события происходят одновременно
		Клапан ИЛИ	Событие происходит, если происходит любое из входных событий (или одно, или в любой комбинации)
		Клапан «исключительное ИЛИ»	Событие происходит, если происходит одно из входных событий (используется обычно с двумя входными событиями)
		Клапан НЕ	Событие представляет собой состояние, которое является инверсией состояния, определенного входным событием (событие, противоположное входному событию)
	—	Клапан ЗАПРЕЩЕНИЯ	Событие происходит, если происходит входное событие, приложенное справа, в то время как событие, указанное внутри символа и формирующее условия, выполняется. Если условие вызвано появлением другого события, клапан ЗАПРЕЩЕНИЯ подразумевает синхронизацию событий

Окончание таблицы А.1

Предпочтительный символ	Допустимый символ	Функция	Описание
		Избыточная структура	Событие происходит, если происходит по крайней мере *m* из *n* входных событий
		Клапан (общая форма)	Общий символ клапана, функция которого указывается внутри символа
	—	Блок описания события	Название или описание события, код события и вероятности появления (при необходимости) должны быть указаны внутри символа
	—	Основное событие	Событие, которое не может быть подразделено на составляющие события
	—	Неразработанное событие	Событие, дальнейшая разработка которого не была проведена (обычно потому, что это предполагалось нецелесообразным)
	—	Анализированное в другом месте событие	Событие, которое разработано в другом дереве неисправностей
	—	Дом	Событие, которое произошло или произойдет обязательно
	—	Нулевое событие	Событие, которое не может произойти
	—	«Переход в»	Событие, определенное в другом месте дерева неисправностей
	—	«Переход из»	Событие, переходящее из другого места дерева неисправностей

УДК 362:621.001:658.382.3:006.354 ОКС 13.110 Т58 ОКСТУ 0012

Ключевые слова: риск, надежность, вероятность отказа, система, элемент, отказ, дерево неисправностей, вершина событий

Редактор *Т.А. Леонова*
Технический редактор *Л.А. Гусева*
Корректор *М.С. Кабашова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 08.06.2005. Подписано в печать 29.06.2005. Формат 60×84 $^{1}/_{8}$. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 1,86. Уч.-изд. л. 1,40. Тираж 404 экз. Зак. 406. С 1457.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «Стандартинформ» на ПЭВМ
Отпечатано в филиале ФГУП «Стандартинформ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

Содержание

Введение

Анализ дерева неисправностей является одним из методов идентификации опасностей и оценивания риска. Он представляет собой совокупность приемов идентификации опасности и анализа частот нежелательного события. Анализ дерева неисправностей позволяет выявить пути реализации опасного события, однако в первую очередь анализ дерева неисправностей используется при оценке риска для определения вероятностей или частот неисправностей и аварий. Общие рекомендации по применению анализа дерева неисправностей для оценки риска и обзор других возможных методов оценки риска приведены в ГОСТ Р 51901—2002 «Управление надежностью. Анализ риска технологических систем».

В настоящем стандарте метод анализа дерева неисправностей изложен применительно к анализу надежности. Для эффективного использования этого метода необходимо до его применения зафиксировать цель метода, а также определить, будет ли применяться метод анализа дерева неисправностей индивидуально или в комбинации с другими методами.

В отличие от применяемого международного стандарта в настоящий стандарт не включены ссылки на МЭК 60617-12:1983 «Графические символы для диаграмм. Часть 12. Элементы двоичной логики», которые нецелесообразно применять в национальном стандарте из-за отсутствия принятого гармонизированного национального стандарта. В соответствии с этим изменено содержание раздела 3.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

АНАЛИЗ ДЕРЕВА НЕИСПРАВНОСТЕЙ

Risk management.
Fault tree analysis

Дата введения — 2005—09—01

1 Область применения

Настоящий стандарт устанавливает метод анализа дерева неисправностей и содержит руководство по его применению. Метод анализа дерева неисправностей включает:

- определение основных принципов метода;
- выполнение необходимых этапов анализа,
- идентификацию соответствующих предположений, событий и режимов неисправностей;
- обеспечение выполнения идентификационных правил и символов.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ 27.002—89 Надежность в технике. Основные понятия. Термины и определения (МЭК 60050(191):1990 «Международный электротехнический словарь. Глава 191. Надежность и качество обслуживания», NEQ)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочного стандарта по указателю «Национальные стандарты», составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяют в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ 27.002.

4 Символы

Для графического представления дерева неисправностей необходимо, чтобы символы, идентификаторы и метки использовались непротиворечивым способом. Подробные правила идентификации и маркировки приведены в разделе 8 и приложении А.

5 Общие положения

5.1 Структура дерева неисправностей

Дерево неисправностей — организованное графическое представление условий или других факторов, вызывающих нежелательное событие, называемое вершиной событий. Представление приводят в форме, которая может быть понята, проанализирована и, по мере необходимости, перестроена таким образом, чтобы облегчить идентификацию:

- факторов, воздействующих на надежность и характеристики эффективности системы, например режимов неисправностей компонентов, ошибок оператора, условий окружающей среды, ошибок программного обеспечения;
- противоречивых требований или спецификаций, которые могут влиять на надежность и эффективность системы;
- общих событий, воздействующих более чем на один функциональный компонент, который может уменьшить преимущества резервирования.

Анализ дерева неисправностей является в основном дедуктивным (нисходящим) методом анализа, нацеленного на точное определение причины или комбинации причин, приводящих к вершине событий. Анализ, главным образом, качественный, но, в зависимости от некоторых условий, он может также быть количественным (см. 7.5.2).

5.2 Цели анализа

Имеется несколько оснований для проведения анализа дерева неисправностей независимо от других или вместе с другими исследованиями надежности. Такими основаниями являются:
- идентификация причин или комбинации причин, ведущих к вершине событий;
- определение соответствия уровня надежности системы установленным требованиям;
- демонстрация того, что предположения, сделанные в других исследованиях относительно независимости систем и нерелевантности неисправностей, не нарушены;
- определение факторов, которые наиболее сильно влияют на надежность системы, и изменений, необходимых для увеличения надежности;
- идентификация общих событий или общих причин неисправностей.

5.3 Объекты применения

Дерево неисправностей используют для анализа сложных систем, включающих несколько функционально связанных или зависимых подсистем, что особенно удобно в случаях, когда системный проект требует сотрудничества нескольких специализированных групп проектировщиков. Примерами систем, к которым обычно применяют анализ дерева неисправностей, являются станции производства ядерной энергии, самолеты, системы связи, химические и другие промышленные процессы.

6 Принципы анализа

6.1 Общие положения

Построение дерева неисправностей должно начинаться на стадии проектирования системы. «Рост» дерева неисправностей должен отражать продвижение этапов проекта. В результате в процессе проектирования системы формируется более глубокое понимание режимов неисправностей. Анализ дерева неисправностей, проводимый параллельно с проектированием системы, позволяет на ранних этапах проектирования учитывать изменение проекта системы, поскольку основные режимы неисправностей идентифицированы. Часто итоговое дерево неисправностей является достаточно большим. В этом случае его обработку проводят при помощи компьютера. Особое внимание обращают на то, что события дерева неисправностей не ограничены исключительно ошибками программного обеспечения или аппаратными ошибками, но включают также все условия или другие факторы, которые обусловливают вершину событий для проектируемой системы.

Процедура анализа дерева неисправностей должна состоять из следующих этапов:
- определение области анализа;
- определение проекта, функций и действий системы;
- определение вершины событий;
- конструирование дерева неисправностей;
- анализ логики дерева неисправностей;
- составление отчетов о результатах анализа.

При проведении количественного анализа дерева неисправностей необходимо определить методику количественной оценки, выбрать необходимые данные и определить количественную оценку надежности.

6.2 Структура системы

Каждая система должна быть определена путем описания функции системы и идентификации системных интерфейсов. Такое определение должно включать:
- описание целей проекта;
- описание границ системы (электрические, механические и операционные интерфейсы). Такие границы формируются на основе взаимодействия с другими системами и должны быть описаны путем

идентификации специфических функций (например, электропитания) и частей (например, предохранителя), которые формируют интерфейсы;

- описание физической структуры системы;
- идентификацию рабочих режимов вместе с описанием работы системы и ожидаемой или приемлемой эффективности системы в каждом рабочем режиме;
- описание условий окружающей среды для системы и аспектов воздействия человеческого фактора и т. д.;
- список применяемых документов, например рисунков, спецификаций, рабочих инструкций, которые описывают детали оборудования и работы. Продолжительность выполнения задачи, интервал времени (периодичность) между испытаниями, а также время, необходимое для проведения корректирующих действий, должны быть установлены. Кроме того, должны быть установлены необходимое оборудование поддержки и задействованный персонал. Должна быть приведена также точная информация относительно предписанного действия в течение каждой стадии работы системы.

В дополнение к вышеупомянутому, рекомендуется подготовить список символов, идентификационных маркировок, условных обозначений и форматов для файлов данных при необходимости обмена между компьютерами данными о структуре дерева неисправностей и описании системы.

6.3 Рассматриваемые события

В дерево неисправностей должны включаться события, являющиеся следствием всех причин. Такие причины должны включать результаты воздействия всех условий окружающей среды или других условий, которые могут воздействовать на элемент, включая те, появление которых возможно в процессе работы, даже если они не предусмотрены в проектной спецификации.

При необходимости деревья неисправностей должны учитывать последствия ошибок и неточностей в программном обеспечении, включая случай, когда дерево неисправностей используется для контроля состояния и управления системой.

События, которые аналитики рассмотрели и исключили из дальнейшего анализа, должны быть зарегистрированы. Такие события в итоговое дерево неисправностей не включают.

Если дерево неисправностей выявляет проблему работоспособности системы, вызванную существующей ошибкой, то событие, описывающее эту неисправность, должно быть включено в дерево неисправностей. Оно должно быть отмечено как событие, которое уже существует. Это необходимо для того, чтобы учесть воздействие многократных ошибок.

6.4 Методология анализа

Развитие дерева неисправностей начинается с определения вершины событий. Вершина событий является следствием соответствующих входных событий, идентифицирующих возможные причины и условия появления вершины событий. Каждое входное событие в свою очередь может быть выходным событием более низкого уровня.

Если выходное событие определяет неспособность системы исполнять некую функцию, то соответствующими входными событиями могут быть неисправности оборудования или ограничения эффективности. Если выходное событие определяет неисправность оборудования, то соответствующими входными событиями могут быть неисправности оборудования, ошибки управления и нехватки необходимых ресурсов, если они не включены в дерево неисправностей как часть ограничений эффективности.

Развитие отдельной ветви дерева неисправностей заканчивается после того, как достигнуты события хотя бы одной из следующих групп:

- основные события — независимые события, для которых подходящие для их описания характеристики могут быть определены отличными от дерева неисправностей способами;
- события, которые не должны разрабатываться далее по решению аналитиков;
- события, которые были или будут рассмотрены в дальнейшем в другом дереве неисправностей.

Если событие исследовано, оно должно иметь ту же идентификацию, что и соответствующее событие в предыдущем дереве неисправностей так, чтобы последующее дерево эффективно формировало продолжение предыдущего.

7 Процедуры анализа

Анализ дерева неисправностей проводится «шагами». Определенная последовательность «шагов», выполняемая для конкретной системы, не может быть аналогична последовательности, установленной для другой системы. При исследовании любого дерева неисправностей должны быть проведены следующие основные «шаги».

7.1 Область применения анализа

Определение области применения должно включать определение анализируемой цели, глубины анализа и основных предположений. Эти предположения должны включать предположения, касающиеся ожидаемых действий, условий обслуживания и эффективности системы при всех возможных условиях ее использования.

7.2 Описание системы

Для успешного анализа дерева неисправностей необходимо детальное знание системы. Однако некоторые системы могут быть слишком сложны, чтобы быть полностью понятыми одним человеком. В этом случае получение необходимых специализированных знаний о системе должно включаться как соответствующий элемент анализа дерева неисправностей.

7.3 Идентификация вершины событий

Вершина событий является центром полного анализа. Вершина событий определяет начало или наличие опасного состояния или неспособности системы обеспечивать желательную эффективность.

Вершина событий должна определяться по возможности в измеримых единицах характеризующих ее параметров.

7.4 Построение дерева неисправностей

7.4.1 Формат дерева неисправностей

Деревья неисправностей могут быть изображены в вертикальном или горизонтальном расположении. Если используется вертикальное расположение, то вершина событий должна быть расположена наверху страницы, а основные события — внизу. Если используется горизонтальное расположение, то вершина событий может быть расположена слева или справа страницы.

Примеры

На рисунках 1, 2 изображены два примера дерева неисправностей. Символы, используемые в этих примерах, включают:

- **блок описания события;**
- **логические символы дерева неисправностей (клапаны);**
- **линию входа клапана;**
- **символ «переход из» (общий случай);**
- **символ «переход в»;**
- **символ завершения (например, основное событие).**

Событие *A* на рисунке 1 будет происходить только в случае, если произошли оба события *B* и *C*. Событие C произойдет в случае, если произошло событие *D* или *E*.

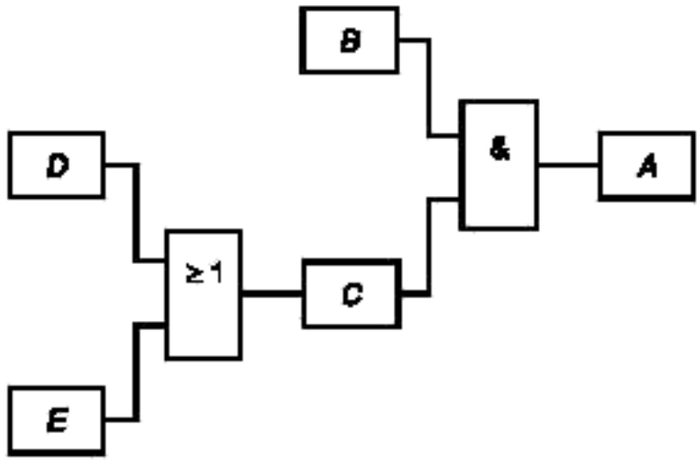


Рисунок 1 — Пример дерева неисправностей

Примечание — Для каждого события A, B и т. д. блок описания события должен включать следующую информацию:

- ***код события;***
- ***вероятность появления события (если требуется);***
- ***наименование или описание события.***

Случай, когда событие представляет общую причину, показан в дереве неисправностей как набор событий. Эти события связаны с любыми событиями, с которыми они взаимодействуют. Все общие события в наборе должны иметь один и тот же код и должны быть отмечены символом «переход в», кроме случая, когда они расположены на самом низком уровне в наборе, отмеченном символом «переход из».

Если дерево неисправностей представлено в нескольких частях, то событие, представляющее общую причину, которая появляется в двух или более частях, должно обрабатываться следующим образом:

- событие должно быть отмечено символом завершения или, если происходит дальнейшее развитие события, символом «переход из» только в одной из частей;
- в части, где используется символ завершения, местонахождение общего события в других частях должно обозначаться символом «переход в».

Пример — Дерево неисправностей, демонстрирующее рассмотрение общей причины, изображено на рисунке 2. Событие *B* — событие общей причины, которое анализируется далее в другом дереве неисправностей. Событие *D* — основное событие.

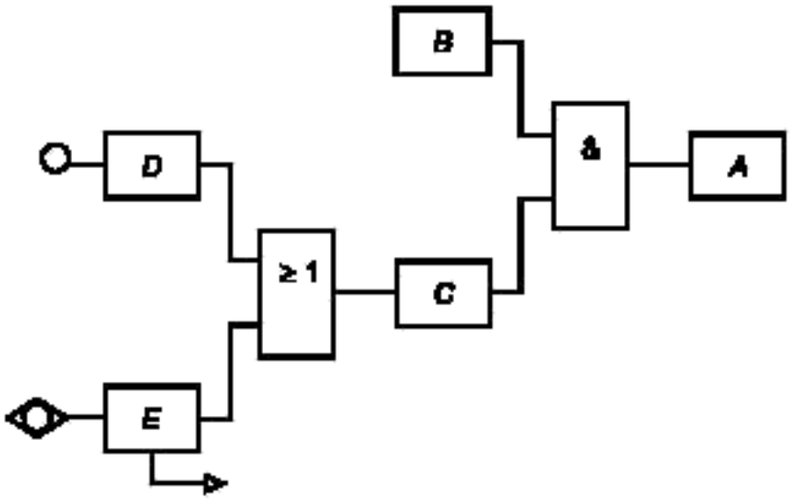


Рисунок 2 — Пример рассмотрения общей причины

Примечание — Для каждого события A, B и т. д. блок события должен включать следующую информацию:

- ***код события;***
- ***вероятность появления (при необходимости);***
- ***наименование или описание события.***

7.4.2 Процедура построения дерева неисправностей

Результаты анализа надежности должны быть документально оформлены таким способом, чтобы при необходимости была обеспечена возможность их рассмотрения и внесения необходимых корректировок, отражающих изменения в проекте, рабочих процедурах или для более глубокого понимания физики отказа. Для этого необходимо проводить систематическое исследование конструкции системы. При проведении таких исследований необходимо последовательно использовать две концепции: «непосредственная причина» и «основной элемент».

При использовании концепции «непосредственная причина» необходимо, чтобы аналитик определил непосредственные необходимые и достаточные причины для появления вершины событий, которые не являются основными причинами события, но являются непосредственными причинами или механизмами для появления события.

Таким образом, непосредственные необходимые и достаточные причины, обусловливающие появление вершины событий, теперь трактуются как события, предшествующие высшему событию, а аналитик продолжает определять уже для таких событий непосредственные необходимые и достаточные причины.

Таким образом, аналитик достигает нижнего уровня дерева неисправностей, перемещая внимание от механизма к режимам и непрерывно приближаясь к более высокой разрешающей способности механизма и режимов, пока не будет достигнут предел разрешающей способности дерева неисправностей.

Строгое соблюдение концепции «непосредственная причина» является гарантией того, что режимы неисправностей не будут пропущены.

Концепцию «основной элемент» используют для сохранения усилий аналитика по построению схемы дерева неисправностей. В этом случае основной элемент обрабатывают как единичный элемент или компонент или рассматривают отдельно.

Для того чтобы элемент рассматривался как «основной», необходимо и достаточно, чтобы он соответствовал следующим требованиям:

- функциональные и физические границы элемента должны быть четко определены;
- работа элемента не должна зависеть от функций поддержки. В противном случае все события, имеющие отношение к элементу, должны быть представлены в схеме дерева неисправностей клапаном, отмеченным знаком ИЛИ, у которого один вход представляет отказ элемента, а другие входы — невозможность выполнения соответствующих функций поддержки;
- отсутствуют события, связанные с элементом, который появляется в другой части дерева неисправностей.

7.4.3 Характеристики неисправностей

Аналитик должен внимательно изучить причины отказов элемента, особенно для категорий независимых и зависимых отказов, следующих за независимыми и зависимыми неисправностями.

При проведении классификации отказа должны быть рассмотрены рабочие и внешние напряжения в сравнении с максимальными напряжениями, для которых элемент предназначен.

7.5 Анализ дерева неисправностей

Основные цели логического (качественного) и численного (количественного) анализа системы:

- идентификация событий, которые могут непосредственно вызвать неисправность системы, и оценка вероятности таких событий;
- оценка отказоустойчивости системы (способность системы функционировать даже после того, как произошло указанное количество неисправностей более низкого уровня или событий, способствующих появлению неисправности системы);
- проверка независимости неисправностей систем, подсистем или компонентов;
- оценка данных для определения места расположения критических компонентов и неисправных механизмов;
- идентификация устройств диагностики неисправностей, входов для ремонта и обслуживания, и т. д.

Оценка отказоустойчивости системы включает определение степени избыточности в системе и проверку того, что избыточность не снижается под воздействием общих событий (общих причин событий). Хотя главная часть оценки отказоустойчивости не требует использования числовых данных, они необходимы для оценки наиболее вероятных комбинаций событий, вызывающих неисправность системы.

7.5.1 Логический анализ

Логический анализ проводят тремя основными методами: исследованием, булевой редукцией и определением минимальных вырезок событий.

7.5.1.1 Исследование

Исследование включает обзор структуры дерева неисправностей, идентификацию общих событий и поиск независимых ветвей. Этот метод обеспечивает аналитика важной информацией, которая в некоторых случаях позволяет отказаться от дальнейших исследований. Во всех других случаях проводят исследования для принятия правильного решения о типе и глубине дальнейших исследований. Непосредственное визуальное исследование графического изображения дерева возможно только для маленьких деревьев, не превышающих приблизительно 70 событий. Исследование больших деревьев, являющихся результатом анализа реально существующих систем, требует соответствующего компьютерного инструментария, но в целом подход остается тем же самым.

Исследование начинают с обзора структуры дерева неисправностей. Все события, которые связаны с вершиной событий через непрерывную цепочку клапанов ИЛИ, являются событиями, которые вызывают вершину событий. Поэтому, если дерево неисправностей состоит только из клапанов ИЛИ, дальнейший анализ не требуется. Если дерево неисправностей включает другие типы клапанов, то анализируемая система представляет собой некоторый вид избыточности или других особенностей предотвращения неисправностей, реализации которых могут помешать общие причины событий. Исследование должно идентифицировать общие причины событий, но не должно предполагать, что их присутствие является благоприятным. Такие заключения могут быть сделаны только после полного анализа дерева неисправностей с использованием булевой редукции или определения минимальных вырезок событий. Существенную трудность составляет быстрое увеличение объема анализа с ростом