ГОСТ Р 27.302-2009

Группа Т59

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

АНАЛИЗ ДЕРЕВА НЕИСПРАВНОСТЕЙ

Dependability in technics. Fault tree analysis

ОКС 21.020

Дата введения 2010-09-01

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. N 184-ФЗ " О техническом регулировании", а правила применения национальных стандартов Российской Федерации - ГОСТ Р 1.0-2004 "Стандартизация в Российской Федерации. Основные положения"

Сведения о стандарте

1 РАЗРАБОТАН Федеральным государственным предприятием "Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении" (ВНИИНМАШ)

2 ВНЕСЕН Техническим комитетом по стандартизации N 119 "Надежность в технике"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. N 1249-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта МЭК 61025:2006* "Анализ дерева неисправностей" (IEC 61025:2006 "Fault tree analyses", NEQ)

_____

* Доступ к международным и зарубежным документам, упомянутым здесь и далее по тексту, можно получить, перейдя по ссылке. - Примечание изготовителя базы данных.

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе "Национальные стандарты", а текст изменений и поправок - в ежемесячно издаваемых информационных указателях "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Введение

Анализ дерева неисправностей заключается в определении и анализе условий и факторов, которые приводят или могут привести к возникновению негативных завершающих событий - полной или частичной утрате функций, деградации рабочих характеристик изделия, ухудшению безопасности или других важных рабочих свойств.

Анализ дерева неисправностей часто используют для анализа эксплуатационной безопасности транспортных систем, электростанций или других систем, для которых необходима оценка безопасности. Анализ дерева неисправностей может также использоваться для исследования свойств готовности и ремонтопригодности изделий различных видов. В настоящем стандарте анализ дерева неисправностей рассмотрен применительно к свойству безотказности.

Существуют два метода проведения анализа дерева неисправностей - качественный и количественный.

При качественном методе вероятности событий или частоту их возникновения не рассматривают. Это метод заключается в детальном анализе совокупности событий/неисправностей. Его применяют, когда необходимо выявить возможные причины неисправностей безотносительно реальной вероятности их возникновения. Иногда некоторые события, рассматриваемые при проведении качественного анализа, оценивают и количественно, но такие расчеты не связаны с попытками расчета общей безотказности.

При количественном методе в процессе детального анализа дерева неисправностей полностью моделируют изделие, процесс или систему и оценивают вероятности возникновения базисных событий, неисправностей или событий, выявленных в ходе анализа. В данном случае окончательный результат представляет собой вероятность появления завершающего события, свидетельствующего о вероятности возникновения неисправности или отказа.

1 Область применения

Настоящий стандарт распространяется на невосстанавливаемые изделия любых видов техники, для которых на стадии разработки проводят анализ и прогнозирование безотказности.

Настоящий стандарт представляет собой руководство по применению метода анализа дерева неисправностей и устанавливает:

- основные принципы анализа;
- описание математического моделирования, связанного с анализом дерева неисправностей;
- взаимосвязи анализа дерева неисправностей с другими методами прогнозирования безотказности;
- этапы выполнения анализа;
- события, виды неисправностей, допущения и предположения;
- описание обычно используемых символов.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий стандарт:

ГОСТ 27.002-89* Надежность в технике. Основные понятия. Термины и определения

_____

* На территории Российской Федерации документ не действует. Действует ГОСТ Р 27.009-2009, здесь и далее по тексту. - Примечание изготовителя базы данных.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 27.002*, а также следующие термины с соответствующими определениями:

_____

* Вероятно ошибка оригинала. Следует читать: ГОСТ 27.002. - Примечание изготовителя базы данных.

3 . 1 **итог:** Результат действий или входного воздействия; последствие причины.

Примечание - Итогом может быть событие или состояние. В пределах дерева неисправностей итог, как сочетание соответствующих входных событий, представляемых в виде логического элемента - вентиля, может быть либо промежуточным, либо завершающим событием.

3.2 **завершающее событие:** Итог сочетания всех входных событий.

Примечания

1 Завершающее событие часто называют конечным событием или конечным итогом. Для завершающего события строят дерево неисправностей.

2 Завершающее событие задано заранее и занимает верхнее положение в иерархии событий.

3 . 3 **конечное событие:** Конечный результат сочетания всех входных, промежуточных и базисных событий.

Примечание - Конечное событие является результатом входных событий или состояний (см. 3.2).

3 . 4 **завершающий итог:** Итог, изучаемый путем построения дерева неисправностей.

Примечание - Итог составного воздействия всех входных, промежуточных и базисных событий; результат итоговых событий или состояний (см. 3.2).

3.5 **вентиль:** Символ, используемый для обозначения связи между выходным событием и соответствующими входными воздействиями.

Примечание - Установленный символ вентиля отражает тип связи между входными событиями и итоговым событием, которое должно наступить.

3.6 **сечение:** Группа событий, которые в случае их совместного появления приводят к наступлению завершающего события.

3.7 **минимальное сечение:** Минимальный или наименьший набор событий, требуемых для наступления завершающего события.

Примечание - Если какое-либо событие из набора не состоится, завершающее событие не наступит.

3.8 **событие:** Появление состояния или действия.

3.9 **базисное событие:** Событие, которое не может (не будет) развиваться в дальнейшем.

3.10 **первичное событие:** Событие, расположенное в основании дерева неисправностей.

Примечание - В настоящем стандарте термин "первичное событие" может также означать базисное событие, которое не может развиваться, или событие, которое может развиваться где-то еще или не может совсем развиться (неразвиваемое событие), несмотря на то что является следствием воздействия группы событий.

3.11 **промежуточное событие:** Событие, которое не является итоговым или первичным.

Примечание - Это событие обычно является результатом одного или более первичных событий и/или других промежуточных событий.

3.12 **неразвиваемое событие:** Событие, не имеющее входных событий.

Примечание - При данном анализе событие не развивается по разным возможным причинам, например таким, как отсутствие более подробной информации, или если оно развивается в другом анализе, а в текущем анализе помечается как неразвиваемое. Примером неразвиваемых событий могут быть элементы перечня готовых к применению изделий коммерческого назначения или пакетов программного обеспечения.

3.13 **одиночный отказ:** Отказ, который приводит к отказу всей системы или который независимо от других событий или их сочетаний приводит к нежелательному завершающему событию (итогу).

3.14 **события, вызванные общей причиной:** Различные события системы или дерева неисправностей, имеющие общую причину их появления.

Примечание - Примером такого события может быть замыкание керамических конденсаторов вследствие изгиба печатной платы; даже если это разные конденсаторы, предназначенные для выполнения различных функций, причина их короткого замыкания одна - одинаковое итоговое событие.

3.15 **общая причина:** Причина появления многочисленных событий.

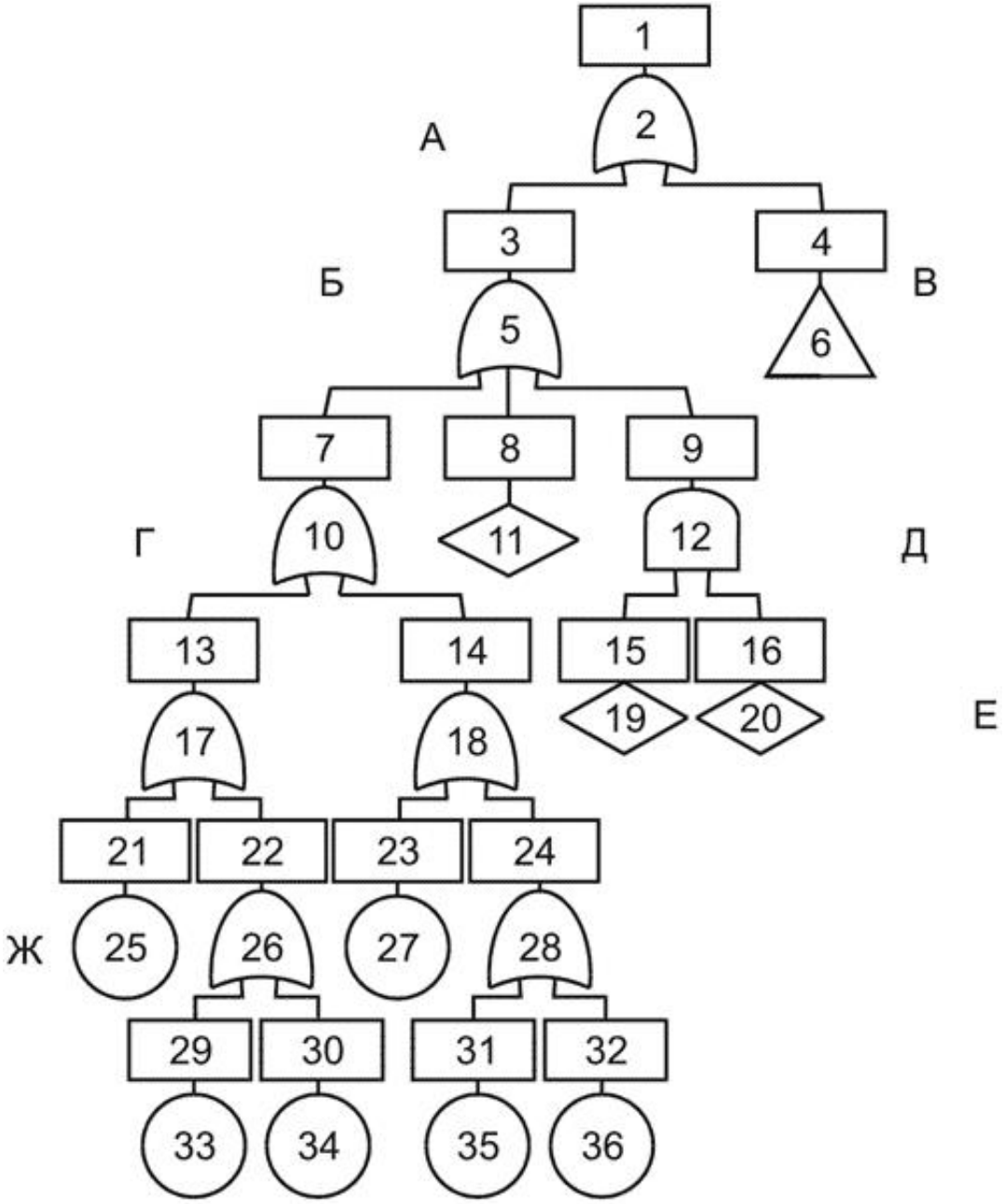
Примечание - В примере, приведенном в примечании к 3.14, общей причиной является изгиб платы, который сам по себе может быть промежуточным событием, являющимся следствием многих событий, таких как сотрясение, вызванное воздействием окружающей среды, вибрация или растрескивание печатной платы.

3.16 **повторное событие:** Событие, которое является входным для более чем одного события более высокого уровня.

Примечание - Это событие может быть общей причиной или видом неисправности компонента, присущим более чем одной части конструкции.

3.17 Иллюстрация некоторых из приведенных выше определений приведена на рисунке 1. Для лучшего объяснения практического применения дерева неисправностей под рисунком приведены ссылки и описания событий. На рисунке не приведено графическое представление минимального завершающего сечения и других завершающих сечений.

Рисунок 1 - Термины, используемые в ДН


1
2
А
3
4
Б
В
5
6
7
8
9
Г
10
11
12
Д
13
14
15
16
19
20
Е
17
18
21
22
23
24
Ж
25
26
27
28
29
30
31
32
33
34
35
36

1 - система, не соответствующая спецификации или неработающая; А - завершающее событие; конечное событие; завершающий итог; 2 - отказ системы; 3 - отсутствие напряжения или неправильное напряжение; 4 - нет обработки данных или их неправильная обработка; Б - промежуточное событие; причина события следующего уровня; входное событие для события следующего уровня; итоговое событие, вызванное его входными воздействиями; В - событие, возникшее в другом месте дерева неисправностей; представлено графически вентилем переноса; 5 - источник питания; 6 - микропроцессор; 7 - нет питания от батареи; 8 - нет фильтрации питания от батареи; 9 - на выходе системы нет ни одного из двух сигналов; Г - вентиль ИЛИ как символ обозначает сочетание входных событий: появление того или иного события или состояния, вызывающего следующее событие или состояние; 10 - подача питания от батареи; 11 - фильтрация напряжения; 12 - выходы; Д - вентиль И как символ обозначает сочетание входных событий: появление обоих событий вызывает следующее событие; существование обоих состояний приводит к появлению итогового состояния; 13 - обрыв входного элемента индуктивности; 14 - сглаживающий конденсатор замыкает батарею на землю; 15 - нет сигнала на выходе 1; 16 - нет сигнала на выходе 2; 19 - выход 1; 20 - выход 2; Е - неразвиваемое событие; развито в другом АДН или осталось неразвитым из-за отсутствия информации или необходимости получения дополнительных данных; 17 - обрыв входной катушки индуктивности; 18 - короткое замыкание сглаживающего конденсатора; 21 - обрыв катушки индуктивности вызван ее случайным отказом; 22 - обрыв в схеме вызван производственным дефектом; 23 - короткое замыкание конденсатора вызвано его случайным отказом; 24 - короткое замыкание обусловлено производственным дефектом; Ж - базисное событие; 25 - обрыв компонента $L1$; 26 - обрыв $L1$, вызванный производственным дефектом; 27 - короткое замыкание; 28 - короткое замыкание $C1$, вызванное производственным дефектом; 29 - недостаток припоя вызвал обрыв соединения; 30 - катушка индуктивности повреждена при сборке; 31 - избыток припоя привел к замыканию контактов; 32 - компонент поврежден при сборке - короткое замыкание; 33 - припой $L1$; 34 - повреждение $L1$; 35 - короткое замыкание $C1$, вызванное припоем; 36 - повреждение $C1$

Рисунок 1 - Термины, используемые в ДН

Примечание - Графические представления ДН на рисунках настоящего стандарта следует рассматривать только как примеры.

4 Обозначения и сокращения

4.1 Символы, обозначающие события дерева неисправностей, зависят от предпочтения пользователя и используемого программного обеспечения. Общие обозначения приведены в приложении А.

Другие обозначения, используемые в настоящем стандарте, представляют собой типовые математические символы, например F - вероятность события, или символы суммы, произведения и т.п. Поэтому их отдельный перечень не приводится.

4.2 В настоящем стандарте применены следующие сокращения:

АДН - анализ дерева неисправностей;

ДН - дерево неисправностей

5 Общие положения

5.1 Описание и структура дерева неисправностей

5.1.1 АДН является одним из ряда методов анализа надежности. Цель каждого метода и возможность его применения, отдельно или совместно с другими, должны быть рассмотрены до начала проведения АДН. Следует обратить внимание на достоинства и недостатки каждого метода и на получаемые результаты, на данные, требуемые для выполнения анализа, сложность анализа, а также на другие факторы, приведенные в настоящем стандарте.

5.1.2 ДН - систематизированное графическое представление условий и факторов, вызывающих или способствующих появлению ожидаемого итога - завершающего события.

АДН представляет собой дедуктивный (сверху вниз) метод анализа. Анализ может быть качественным (метод А) или количественным (метод В), в зависимости от целей и возможностей анализа.

В случае, если вероятность развития основных событий нельзя определить, для исследования причин возможных нежелательных итогов проводят качественный АДН с указанием неколичественной вероятности развития события, например "весьма высокая вероятность", "высокая вероятность", "средняя вероятность", "низкая вероятность" и т.п. Первичная цель качественного АДН - определить минимальное сечение для того, чтобы установить, как базисные или первичные события влияют на завершающее событие.

Количественный АДН проводят в том случае, если известны вероятности развития первичных событий. Вероятности развития всех промежуточных событий и завершающего события (итога) могут быть рассчитаны в соответствии с используемой моделью.

АДН также можно использовать при анализе систем, для которых характерны сложные взаимоотношения между подсистемами, в том числе взаимодействие программных/аппаратных средств.

5.2 Цели

АДН проводят независимо или совместно с другими методами анализа безотказности. АДН позволяет:

- установить причины или сочетание причин, приводящих к завершающему событию;
- определить соответствие безотказности конкретной системы заданным требованиям;
- определить виды возможных отказов или факторов, вносящих наибольший вклад в вероятность отказа системы или в вероятность ее неготовности (в случае восстанавливаемой системы) для выявления возможности улучшения безотказности системы;
- сравнить различные варианты конструкции для улучшения безотказности системы;
- доказать правомерность допущений, принятых при анализе другими методами, такими как марковский анализ или анализ возможных причин и последствий отказов;
- определить возможные виды отказов, которые могут влиять на безопасность системы, оценить соответствующие вероятности их появления и возможности их уменьшения;
- идентифицировать общие события;
- найти события или сочетания событий, которые наиболее вероятно вызовут развитие завершающего события;
- оценить влияние первичного события на вероятность завершающего события;
- рассчитать вероятности событий, готовность системы и интенсивности отказов ее компонентов, представленных ДН (при наличии необходимых данных).

5.3 Применение

5.3.1 АДН особенно подходит для систем, содержащих несколько функционально связанных или зависимых подсистем. Преимущества АДН наглядно проявляются, когда система разрабатывается несколькими независимыми специализированными группами разработчиков и отдельные ДН связывают друг с другом. АДН обычно проводят при проектировании атомных электростанций, транспортных систем, средств связи, химических и других промышленных процессов, медицинского оборудования, вычислительных систем и т.п. АДН также играет важную роль при оценке систем, содержащих различные типы взаимодействующих компонентов (механических, электронных и программных), которые трудно моделировать с помощью других методов, и систем, для которых важны последовательность и сочетание событий.

5.3.2 АДН находит разнообразное применение в качестве инструментального средства, в том числе для:

- определения подходящей логической комбинации событий, ведущих к завершающему событию и, возможно, назначения приоритетности событий или комбинаций;
- оценки разрабатываемой системы, предупреждения и предотвращения или ослабления потенциальных причин появления нежелательных событий;
- анализа системы, определения ее безотказности, установления факторов, вносящих основной вклад в ее ненадежность, и оценки изменений проекта;
- содействия оценке вероятностного показателя риска.

5.3.3 АДН может быть использован в качестве контролирующего способа для определения возможных проблем при разработке новых изделий или при модификации изделий, в том числе на ранних этапах проектирования, когда мало подробностей о схемных решениях. Эти ранние работы могут расширяться по мере получения дополнительной информации. АДН также определяет возможные проблемы, которые могут быть вызваны конструкцией изделия, воздействием окружающей среды или рабочих нагрузок, нарушением технологии изготовления изделия и влиянием условий эксплуатации, содержания и технического обслуживания.

5.4 Сочетание с другими методами анализа безотказности

5.4.1 Сочетание АДН с анализом причин и последствий отказов

Такое сочетание имеет следующие преимущества:

- АДН представляет собой метод анализа сверху вниз, а анализ причин и последствий отказов - метод анализа снизу вверх, и как дедуктивные, так и индуктивные умозаключения являются хорошим аргументом для достижения полноты анализа;

- анализ причин и последствий отказов полезен для определения основных событий или угроз, в то время как АДН представляет собой метод анализа причин нежелательных событий.

Взаимосвязь методов анализа причин и последствий отказов и АДН выражается в следующем:

- любой единичный отказ, приводящий к появлению в ДН завершающего события и определенный методом анализа причин и последствий отказов, должен также отражаться как одиночный отказ в минимальном сечении.

Примечание - Одиночный отказ - отказ любого компонента, вызывающий отказ всей системы;

- любой выявленный АДН одиночный отказ должен также выявляться и при анализе причин и последствий отказов.

Если методы анализа выполняются отдельно и независимо друг от друга, значение анализа в целом усиливается. Это особенно важно при анализе эксплуатационной безопасности.

5.4.2 Объединение АДН и анализа дерева событий

С помощью АДН можно проанализировать любое событие. Однако в некоторых случаях такой анализ может оказаться затруднительным или даже неприемлемым по следующим причинам:

- иногда легче определить не взаимосвязь причин, а последовательность событий;
- получаемое дерево может быть очень большим;
- в различных видах анализа могут использоваться разные термины.

Чтобы найти практически полезную процедуру, зачастую нужно в первую очередь определять не завершающее нежелательное событие, а возможные нежелательные события на границе функционального и технического аспектов.

Например, катастрофическим завершающим событием программы космического полета является потеря экипажа или летательного аппарата. Вместо того чтобы строить большое дерево неисправностей на основе этого завершающего события, в качестве завершающих событий можно определять промежуточные события, такие как неисправность системы зажигания или отказ реактивного двигателя и др. и проводить их анализ с помощью отдельных ДН. Затем эти завершающие события низкого уровня будут в свою очередь использованы как входные воздействия для ДН при анализе последствий работы системы в целом.

Сочетание АДН и анализа дерева событий иногда называют последовательным анализом причин.

5.4.3 Сочетание АДН и метода марковского анализа

АДН, рассматривающий только сочетания статических событий, обычно касается систем, в которых последовательность событий является независимой (статические вентили не рассматривают и не моделируют упорядоченные по времени сочетания событий). Однако можно расширить АДН, задав дополнительные вентили, представляющие марковские модели. Эти вентили называют "динамическими" вентилями, к которым относят "вентиль И с приоритетом", "последовательный вентиль" и "дополнительный вентиль". Для таких вентилей следует оценивать вероятность отказа в момент t, используя соответствующую марковскую модель или моделирование. После оценки динамический вентиль и его входные воздействия могут быть заменены единичным первичным событием, вероятность развития которого определяют марковским анализом. Существующие программные средства позволяют моделировать динамические вентили и рассчитывать вероятность развития события, которое они представляют.

Как статические, так и динамические вентили ДН используют при допущении независимости отдельных событий (если они не заданы как общие). При этом необходимо внимательно проверять независимость событий, входящих в марковскую модель и ДН.

5.4.4 Сочетание АДН и бинарной диаграммы решений

При расчете вероятности появления завершающего события ДН со многими сечениями необходимо рассчитать вероятности для всех комбинаций сечений. Так как такой расчет является очень сложным, его часто приходится упрощать.

На основе АДН можно рекурсивно построить бинарную диаграмму решений, что позволяет получить эффективный метод точного расчета. Метод полезен в тех случаях, когда упрощение расчетов вероятности сечений приводит либо к неприемлемой потере точности, либо к слишком большой затрате времени на завершение АДН, особенно когда модель содержит большое число высоковероятных событий.

5.4.5 Сочетание АДН с блок-схемой расчета безотказности

Блок-схема расчета безотказности состоит из блоков или модулей, представляющих собой группу компонентов или видов отказов. Эти модули обычно формируют в соответствии с функциональной блок-схемой изделия, системы или процесса. Для этих модулей либо задана интенсивность отказов, либо рассчитывается их вероятность безотказной работы или вероятность отказа для данного применения или графика изменения состояния в процессе эксплуатации. Как правило, интенсивность отказов модулей равна сумме интенсивности отказов отдельных компонентов. В этом случае функциональное взаимодействие компонентов модуля не учитывают.

Чтобы усилить корректность функционального моделирования в пределах какого-либо модуля (программные/аппаратные средства, взаимодействие механических деталей), его безотказность можно моделировать с помощью АДН, а затем присвоить полученную в итоге информацию о вероятности его отказа в блок-схеме расчета безотказности. При таком подходе можно получить более реальный прогноз.

6 Разработка и оценка

6.1.1 Сочетания событий и состояний

ДН описывает состояния и события. Состояние характеризуется вероятностью его существования в момент времени t, а событие - интенсивностью отказов (частотой появления отказов) либо вероятностью появления события за время t.

Сочетания событий и состояний в АДН должны соответствовать итогу. Например, входы вентиля ИЛИ, выход которого, либо состояние, либо событие, могут быть состоянием или событием. Все входы вентиля И, на выходе которого представлено событие, также должны быть событиями, и наоборот, если на его выходе представлено состояние, то и все входы должны также представлять состояния.

6.1.2 ДН для анализа неисправностей, вызывающих другие неисправности или события

Построение и оценка ДН для такого анализа описана в разделе 7 с учетом того, что итог характеризуется вероятностью существования неисправности или ее развития и не связан с безотказностью анализируемого изделия или системы.

При таком анализе базисные или любые другие события могут не иметь никакой реальной вероятности и используются лишь для рассмотрения события, которое, вероятно, может состояться (метод А). В этом случае их можно представлять описанием вероятности - высокая, средняя или низкая, и оценивать как возможные события, способствующие появлению завершающего события или неисправности. ДН такого типа часто используют для определения основной неисправности или события, представляющего собой единственную или основную причину появления завершающего события.

6.1.3 Использование АДН для оценки безотказности и внесения исправлений в процессе разработки изделия

В этом случае применяют метод Б.

ДН может полностью моделировать все изделие или моделировать части изделия, которые могут представлять риск для его безопасной эксплуатации. Вероятности определяют обычным способом, таким как анализ неисправности или события изделия, влияющего на его безопасность, или детальный анализ возможного отказа изделия в определенный период времени, который позволяет получить значение вероятности отказа для представляющего интерес периода времени. При таком применении метод ДН следует принципам анализа причин и последствий отказов сверху-вниз, когда каждый возможный вид отказа может привести к развитию события или неисправностей, вызывающих отказ изделия.

В этом случае АДН отражает динамику событий, происходящих в изделии, взаимодействие программных/аппаратных средств, а также взаимосвязь между неисправностями или событиями, представляющими возможные виды отказов. Такую взаимосвязь нельзя получить с помощью обычного анализа причин и последствий отказов и трудно моделировать с помощью блок-схем расчета безотказности. К тому же оценка безотказности изделия является более реальной, поскольку рассматривают только те виды отказов, которые приводят к отказу изделия.

Примечание - Большие ДН требуют применения программных средств. Имеется много программ АДН, существенно отличающихся друг от друга.

При проведении количественного анализа, когда вероятности появления некоторых событий нельзя определить, такие события и их функциональные (логические) сочетания должны быть учтены. Их не учитывают при прогнозировании безотказности (или вероятности отказа), но присутствие таких событий следует принимать во внимание при округлении окончательных результатов.

Процедура АДН должна включать в себя следующие этапы:

- определение программы анализа;
- изучение проекта, функций и работы системы;
- установление завершающего события;
- создание ДН;
- проведение АДН;
- отчет о результатах анализа;
- оценка улучшения безотказности и принятых решений.

АДН должен проводить подготовленный персонал, который знаком с системой, ее конструктивными особенностями и работой, а также обучен методу проведения АДН и другим методам моделирования безотказности.

6.2 Информация о системе

Требуемой информацией являются:

- краткое изложение назначения проекта;
- определение критериев отказа системы;
- функциональная структура системы, обычно представляемая функциональной блок-схемой;
- физическая структура системы, отличающаяся от функциональной структуры;
- границы системы, например электрические, механические и рабочие интерфейсы;
- перечень рабочих режимов системы с описанием работы системы и ожидаемых допустимых рабочих характеристик для каждого рабочего режима;
- описание изменения состояния системы в процессе эксплуатации;
- описание условий окружающей среды и важных человеческих факторов (уровень квалификации операторов и персонала, проводящего техническое обслуживание и ремонт);
- перечень необходимых документов: чертежей, спецификаций, руководства по эксплуатации, описывающих детали конструкции и работы системы.

Должны быть определены продолжительность выполнения задачи, время, необходимое для обслуживания системы и внесения исправлений. Необходимо иметь представление о вспомогательном оборудовании и о персонале, имеющем отношение к работе системы.

6.3 Графическое описание и структура дерева неисправностей

ДН содержит следующие компоненты:

вентили - символы, показывающие логическую связь входных событий, выходных событий и завершающего события, в том числе:

- статические вентили (выход не зависит от порядка появления входных данных);
- динамические вентили (выход зависит от порядка появления входных данных).

Обычно используемые символы событий и их определения приведены в таблице А.1 приложения А.

В ДН используют следующие графические элементы:

а) логические символы дерева неисправностей (вентили);

б) линии, соединяющие входы и выходы вентилей;

в) символы, описывающие промежуточные события;

г) символы входа и выхода из блока;

д) символы основных событий.

Все важные события должны быть включены в ДН. В том числе к ним относят воздействия окружающей среды, нагрузки, вызывающие непредусмотренные напряжения в изделии, в том числе в программных средствах, устройствах управления и проверки состояния изделия; нагрузки, которые могут возникнуть при работе, даже если они не указаны в техническом задании на разработку.

Учтенные события, исключенные из последующего АДН как неприемлемые, должны быть указаны в отчете.

Если при проведении АДН выявлены две или более проблем в работе системы, вызываемые одной возникающей неисправностью, то событие, описывающее эту неисправность, должно быть включено в несколько мест ДН. Это событие также должно быть помечено как общее событие. При количественном анализе общее событие учитывают в расчетах только один раз. Чтобы исключить дополнительное использование общих событий в многочисленных расчетах, следует определить и применять обозначения, присвоенные таким событиям. Обозначения должны быть постоянными.

Если для оценок, получаемых с помощью ДН, применяют компьютерные программы, следует использовать подходящие условные обозначения и установочные параметры. При построении ДН они могут быть вертикальными, надстраиваемыми сверху вниз, или горизонтальными - слева направо.

7 Построение и оценка дерева неисправностей

7.1 Общее положение

Построение ДН начинают с определения и задания завершающего события и проводят до намеченного уровня ДН. Результатом построения является графическое представление всех событий, которые сами по себе или в сочетании с другими событиями приводят к появлению завершающего события.

7.2 Границы анализа

Задание границ анализа должно предусматривать описание анализируемой системы, цели и объема анализа, основных принимаемых допущений. Эти допущения должны включать в себя допущения, относящиеся к рабочим характеристикам системы при всех возможных условиях ее эксплуатации, а также к условиям технического обслуживания и ремонта данной системы.

АДН может предоставить информацию, касающуюся:

- анализа безотказности системы в тех случаях, когда известны вероятности появления основных событий;

- основных причин получения нежелательного итога, который может потребовать внесения соответствующих изменений.

При необходимости определения появления завершающего события сложной системы в АДН, в отличие от других аналитических методов моделирования безотказности и прогнозирования, могут быть включены только те виды неисправностей или возможных событий, которые влияют на работу системы и имеют отношение к появлению завершающего события. Это приводит к более сфокусированной оценке системы.

7.3 Ознакомление с системой

Для успешного выполнения АДН необходимо иметь точное представление о системе. Некоторые системы могут быть слишком сложными для полного понимания их работы. В этом случае необходимые разъяснения о работе системы должна предоставить группа разработчиков.

7.4 Построение дерева неисправностей

Построение ДН начинают с точного определения завершающего события или нежелательного итога. Таким событием может быть существование или формирование опасного состояния или невыполнение системой требуемых функций.

Если событие на выходе вентиля указывает на невозможность выполнения функции, то входные события должны представлять собой соответствующие причины, например отказ вследствие неисправности аппаратных или программных средств, рабочих ограничений, неправильных команд (отказ системы управления) и ошибок человека.

Построение конкретных ветвей ДН заканчивают после определения одного или более из следующих событий:

- первичных событий, т.е. независимых событий, необходимые характеристики которых могут быть определены методами без построения ДН;
- событий, которые, по мнению разработчика, можно не развивать дальше;
- событий, которые были или будут развиваться при перемещении в другое ДН. Если событие развивается дальше, то оно должно иметь то же описание, что и соответствующее событие в другом ДН, чтобы это дерево было эффективным продолжением предыдущего.

7.5 Примеры построения дерева неисправностей

7.5.1 Формат дерева неисправностей

ДН могут быть расположены вертикально или горизонтально. При вертикальном расположении завершающее событие должно находиться наверху страницы, а базисные события - внизу. При использовании горизонтального расположения завершающее событие располагают на левой стороне страницы.

Примечание - Приведенные в настоящем стандарте примеры иллюстрируют построение и представление ДН.

7.5.2 Применение количественного АДН (метод В) для улучшения безотказности проектируемой системы или изделия

7.5.2.1 Общие положения

Основное различие между АДН и другими методами моделирования и анализа безотказности заключается в том, что при АДН учитывают только события, имеющие отношение к появлению завершающего события, и моделируют сочетание их функций и возможное динамическое взаимодействие и взаимозависимость. Другие методы рассматривают интенсивность или вероятность отказов компонентов (а не вероятность вида неисправности компонента) в предположении независимости отказа. Так конденсатор, используемый в схеме фильтра напряжения, может оказаться разомкнутым (причина примерно 35% отказов конденсаторов данного вида), короткозамкнутым (причина приблизительно 55% отказов) или, возможно, изменилась его емкость (оставшиеся 10% его отказов), но только один вид неисправности - короткое замыкание приведет к отказу изделия. В этом случае будут учтены лишь 55% вероятностей отказов конденсаторов, что позволит точно определить виды неисправностей или их причины, требующие внимания разработчика.

При построении моделей вентилей важно помнить, что значения вероятности относятся только к видам отказов и факторам, способствующим их появлению, или являются значениями вероятности статических или динамических комбинаций видов отказов, приводящих к потере функции и отказу системы.

7.5.2.2 Конфигурация последовательной системы

При анализе безотказности методом блок-схемы расчета безотказности блоки или компоненты в системе соединены последовательно, и отказ любого из них приведет к отказу системы.

Соответствующая модель ДН будет такой, в которой блоки (вентили или события) представлены вентилем ИЛИ.

Математическое выражение безотказности системы, содержащей n независимых блоков, имеет вид

$$R_S(t) = R_1(t)R_2(t)\ldots R_i(t)\ldots R_n(t). \quad (1)$$

Это выражение в терминах безотказности означает, что для обеспечения работоспособности системы все блоки должны быть работоспособными.

При АДН отказ наступает в результате отказа компонента 1 или компонента 2 и так далее. Поэтому последовательная система или ее конфигурация представлена вентилем ИЛИ.

Математическое выражение для вентиля ИЛИ такое же, как и для последовательной системы, за исключением того, что в нем используется вероятность отказа $F(t)$, вместо вероятности безотказной работы.

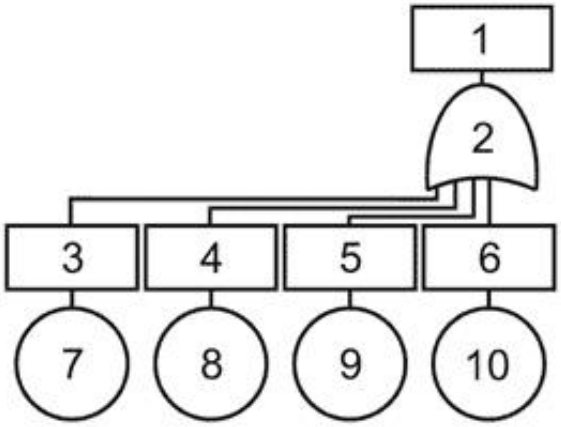
$$F(t) = 1 - R(t). \quad (2)$$

Вероятность нежелательного итога для вентиля ИЛИ (системы), содержащего n независимых вентилей или входящих событий имеет вид

$$F_S(t) = 1 - (1 - F_1(t))(1 - F_2(t))\ldots(1 - F_i(t))\ldots(1 - F_n(t)). \quad (3)$$

Отказ системы наступает при отказе любого компонента (блока). Пример вентиля ИЛИ приведен на рисунке 2. На этом и всех последующих рисунках в настоящем разделе соответствующий вид отказа компонента представляет собой вид отказа, который как входящее событие вызывает появление выходного события.

Рисунок 2 - Представление последовательной системы в виде ДН



1 - неисправности системы в результате отказа любого компонента; 2 - отказ системы или появление завершающего события; 3 - компонент 1: неисправность из-за соответствующего вида отказа; 4 - компонент 2: неисправность из-за соответствующего вида отказа; 5 - компонент i: неисправность из-за соответствующего вида отказа; 6 - компонент n: неисправность из-за соответствующего вида отказа; 7 - событие 1; 8 - событие 2; 9 - событие i; 10 - событие n.

Рисунок 2 - Представление последовательной системы в виде ДН

7.5.2.3 Конфигурации параллельной системы и системы с резервированием

Нагруженный резерв

Предполагается, что каждый вход в блок нагруженного резерва является независимым.

Если завершающее событие появляется только в случае, когда происходят все независимые способствующие его появлению события, то эти события могут быть описаны вентилем И. Такая конфигурация может быть резервной. При анализе безотказности ее также называют параллельной системой, несмотря на то, что ее физическая конфигурация может быть другой.

Требование независимости выполняется тогда, когда вероятность входного события является постоянной и не зависит от состояния других входных воздействий.

Соответствующее математическое выражение безотказности выводят исходя из того, что система остается в работоспособном состоянии, если, по крайней мере, хотя бы один из компонентов 1 или 2, или любой другой компонент системы остается в работоспособном состоянии, т.е. отказ системы наступает тогда, когда отказывают все компоненты.

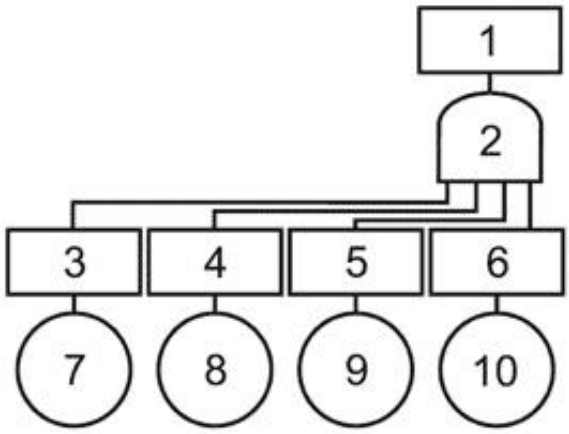
$$R_S(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) . \quad (4)$$

При АДН это условие представлено вентилем И, число входных вентилей или событий равно n. Смысл заключается в том, что отказ системы наступает тогда, когда компонент 1 и компонент 2 и остальные компоненты откажут. В этом случае вероятность отказа определяют по формуле

$$F_S(t) = \prod_{i=1}^{n} F_i(t) . \quad (5)$$

Представление АДН параллельного резервирования, когда для успешной работы системы достаточно нахождение в работоспособном состоянии только одного компонента или когда отказ системы наступает в случае отказа всех компонентов, приведено на рисунке 3.

Рисунок 3 - Представление параллельной системы в виде ДН



1 - неисправности системы в результате отказа всех компонентов; 2 - отказ системы или появление завершающего события; 3 - компонент 1: неисправность из-за соответствующего вида отказа; 4 - компонент 2: неисправность из-за соответствующего вида отказа; 5 - компонент i: неисправность из-за соответствующего вида отказа; 6 - компонент n: неисправность из-за соответствующего вида отказа; 7 - событие 1; 8 - событие 2; 9 - событие i; 10 - событие n

Рисунок 3 - Представление параллельной системы в виде ДН

Резервные компоненты могут работать в режиме распределения нагрузки между параллельно работающими устройствами (например, генераторов электрической сети). Вероятность развития события, приводящего к отказу компонента, сохранившего работоспособность, с каждым отказом возрастает. Такие изменения вероятности события не отвечают требованию независимости, которое должен обеспечивать простой вентиль И.

Если итог должен появляться только в случае развития всех событий, способствующих его появлению, а входные события зависят друг от друга, вентиль И применять нельзя. В этом случае необходимо использовать динамический вентиль.

В общем случае резервирования k из n одинаковых блоков при АДН можно использовать следующее математическое выражение, описывающее вероятность безотказной работы

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} [R_0(t)]^i [1 - R_0(t)]^{n-i}$$

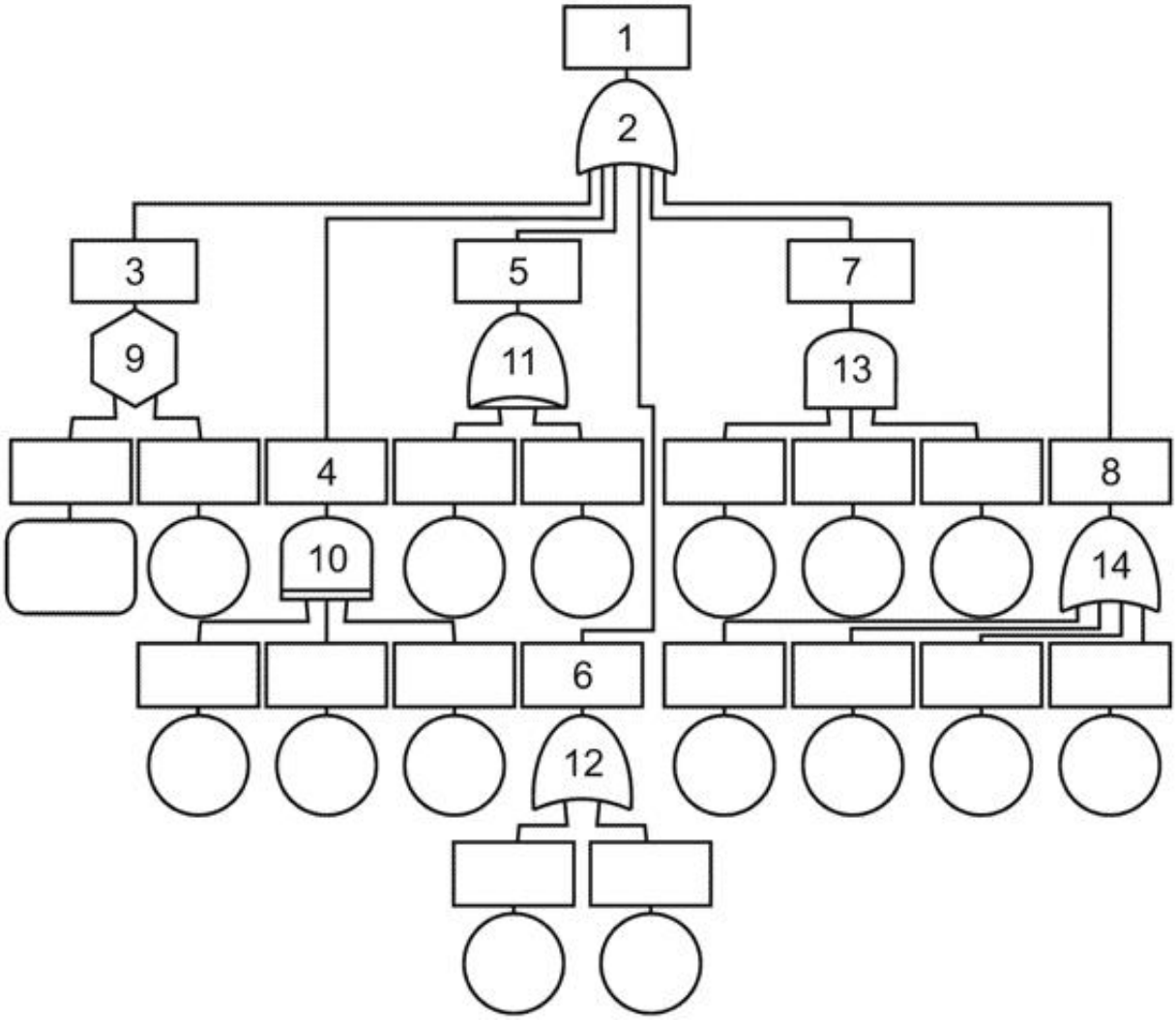
или

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} [1 - F_0(t)]^i [F_0(t)]^{n-i} . \quad (6)$$

При АДН это сочетание событий представлено основным мажоритарным вентилем, при этом критическое число $m = n - k + 1$ и символ соответствующего вентиля m означает, сколько событий должно было произойти для дальнейшего развития события в дереве. Так, если требуемое резервирование замещением составляет 3 из 6, то критическое число событий равно 4, поскольку появление четырех входных событий приведет к тому, что останутся только два работоспособных компонента. Это означает, что отказ системы наступит в том случае, если из шести компонентов работоспособными останутся три.

Мажоритарный вентиль, а также другие примеры вентилей, используемых при моделировании безотказности, приведены на рисунке 4.

Рисунок 4 - Пример ДН с различными типами вентилей



1 - отказ системы вследствие появления любого входного события; 2 - отказ системы или появление завершающего события; 3 - событие наступает, если наступают оба входных события; 4 - событие наступает, если наступают все входные события по порядку; 5 - событие наступает, если наступает одно, но не другое входное событие; 6 - событие наступает, если наступают некоторые входные события; 7 - событие наступает, если наступают все входные события; 8 - событие наступает, если наступают три входных события; 9 - вентиль запрета; 10 - вентиль И с приоритетом; 11 - вентиль ИСКЛЮЧАЮЩЕЕ ИЛИ; 12 - вентиль ИЛИ; 13 - вентиль И; 14 - мажоритарный вентиль с критическим числом 3; непронумерованные прямоугольники - неисправности компонентов соответствующих видов отказов; непронумерованные окружности - компоненты

Рисунок 4 - Пример ДН с различными типами вентилей

Ненагруженный резерв

При ненагруженном резерве активными являются только компоненты, необходимые для работы системы, и в случае отказа одного или более из этих компонентов активируется один или более запасной заменяющий компонент для того, чтобы выполнить функции отказавших компонентов. Отказ системы определяется как событие, в результате развития которого общее число функционирующих компонентов меньше числа компонентов, требуемых для работы системы.

Ненагруженный резерв нельзя представить статическими вентилями. Однако можно использовать символ запасного вентиля. Для оценки этого вентиля проводят марковский анализ.

Ненагруженный резерв хорошо описывается динамическими вентилями. В этом случае запасной вентиль используется для резервируемых систем, вероятность событий которых меняется.

7.5.2.4 Представление условной вероятности повторяющихся событий с общей причиной

К условной вероятности относится вероятность развития события в зависимости от появления другого события, при этом второе событие происходит только в том случае, если развивается первое.

Условную вероятность описывают в терминах динамических вентилей, таких как вентили И с приоритетом. Для анализа их состояния используют марковский анализ.

Пример условной вероятности приведен на рисунке 4.

7.5.2.5 Графическое представление ДН

ДН имеют различные графические представления в зависимости от предпочтений и принятых в различных странах обозначений, а также от области их применения. В некоторых представлениях используют прямоугольники с размещенными в них символами, такими как & для вентиля И и $\geq$ для вентиля ИЛИ. В этом случае нулевой вентиль также классифицируют как вентиль ИЛИ, за исключением того, что данный вентиль ИЛИ имеет только одно входное событие, поскольку нулевой вентиль представляет завершающее событие, вызываемое только одним входным событием.

Представление вентилей и событий в виде прямоугольников приведено на рисунке 5, на котором событие A наступит, если появятся оба события B и C. Событие C наступит, если появятся события D или E.

Рисунок 5 - Представление вентилей и событий в виде прямоугольников

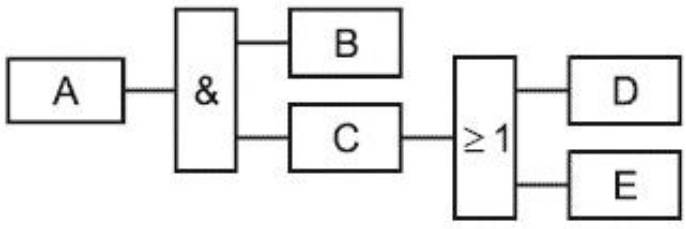
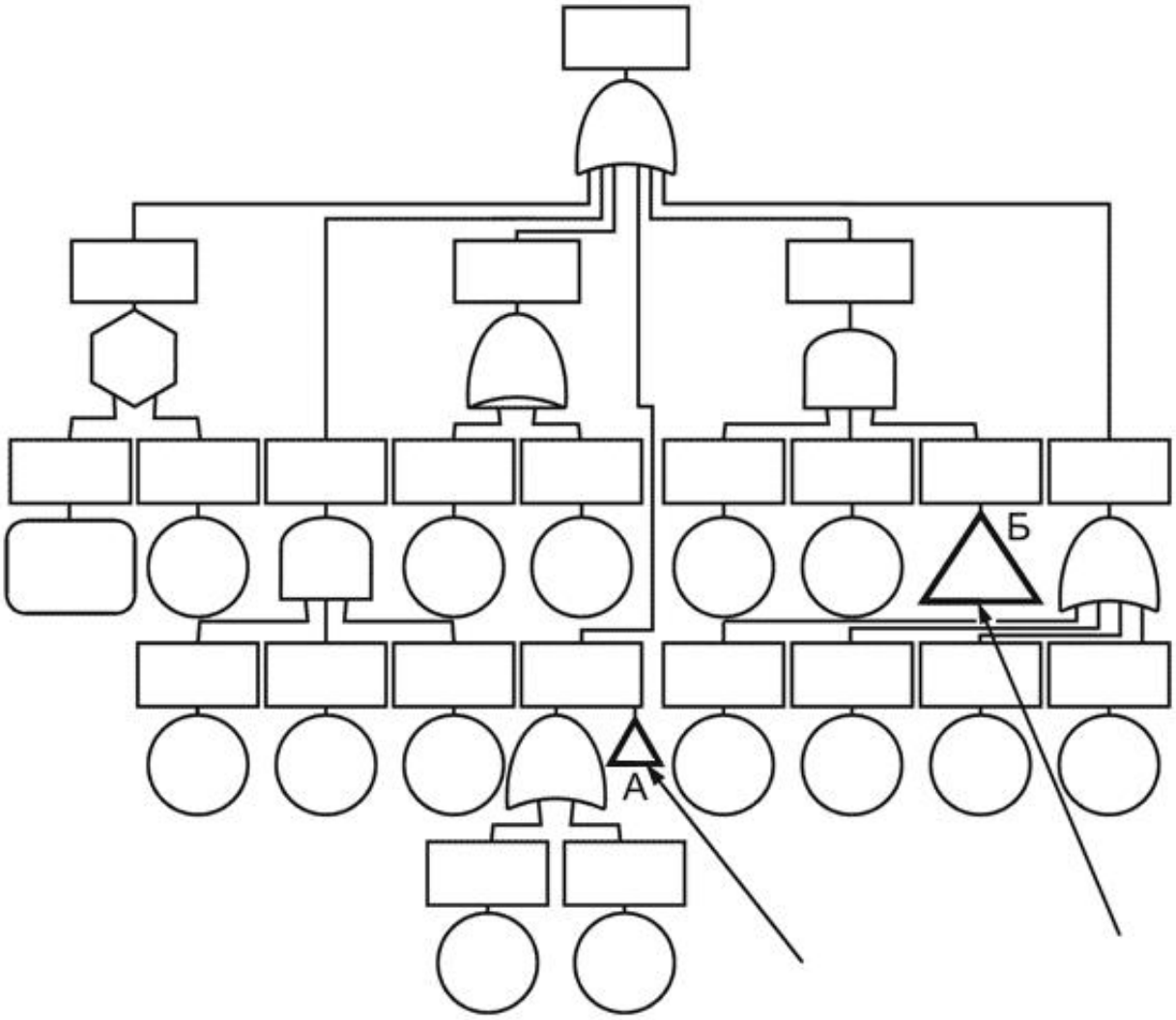


Рисунок 5 - Представление вентилей и событий в виде прямоугольников

Если событие представляет собой повторяющееся событие или событие, вызываемое общей причиной, его изображают в ДН повторно, но с отметкой, которая показывает его как входное событие по отношению к другим событиям ДН. Все повторяющиеся события или события, вызываемые общей причиной, в совокупности имеют в ДН одинаковый код и обозначаются символом включения или символом, обычно используемым в ДН. Это правило относится ко всем повторяющимся событиям или событиям, вызываемым общей причиной, за исключением события самого низкого уровня, который обозначают символом переноса.

На рисунке 6 приведен пример графического представления, в котором повторяющееся событие, описываемое вентилем ИЛИ и имеющее флаг с номером страницы, можно найти в другом месте ДН, где оно представляет собой первичное событие для другого события более высокого уровня. Это событие может появиться в двух или более местах ДН. Примером такого события может быть повышенная температура или влажность, вызывающая появление в системе двух различных событий. В этом случае каждое событие разобщают (преобразуют с целью исключения общих элементов). На рисунке 6 также показан вентиль переноса, указывающий на то, что данное событие возникло в другом месте или на другой странице ДН. Обычно это происходит, когда сложное событие является входным событием для события более высокого уровня и, следовательно, далее его следует приводить на отдельном листе. Вентиль И с приоритетом, показанный на рисунке 6, следует использовать в тех случаях, когда завершающее событие зависит от порядка входных событий.

Рисунок 6 - Пример ДН, содержащего повторяющееся и перемещаемое события



А - событие, приведенное на другой странице АДН (должен быть указан номер страницы); Б - повторяющееся событие, приведенное на другой странице АДН (должен быть указан номер страницы)

Примечание - Остальные элементы ДН идентичны приведенным на рисунке 4.

Рисунок 6 - Пример ДН, содержащего повторяющееся и перемещаемое события

Пример ДН с прямоугольными обозначениями повторяющегося и перемещаемого вовне события или события, вызываемого общими причинами, приведен на рисунке 7. Событие B представляет собой событие, которое будет анализироваться дальше на ДН. Событие D является базисным событием.

Рисунок 7 - Пример событий, вызванных общими причинами и изображенных в виде прямоугольных вентилей

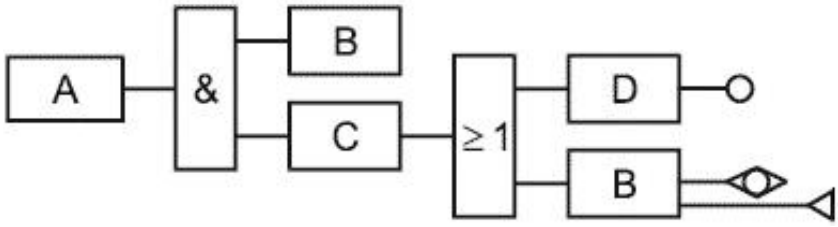


Рисунок 7 - Пример событий, вызванных общими причинами и изображенных в виде прямоугольных вентилей

7.5.3 Процедура построения

Первые шаги построения ДН заключаются в установлении завершающего события, рамок и задач ДН, границ системы или объекта и глубины анализа.

При использовании АДН для улучшения безотказности системы завершающим событием является отказ системы, и цель анализа заключается в определении факторов, способствующих появлению этого события, и выявлении недостатков разработки или ненадежных компонентов.

Для того чтобы виды отказов не были пропущены из-за предположения, что они были рассмотрены ранее, необходимо следовать принципу "непосредственная причина".

Принцип "базовые элементы" можно использовать для освобождения разработчика от построения диаграмм ДН, не предоставляющих новой или полезной информации. Базовый элемент в дальнейшем не развивается. Его рассматривают как единичный элемент или компонент или как элемент, обрабатываемый отдельно.

Чтобы элемент или событие рассматривались в качестве первичных, необходимо и достаточно, чтобы выполнялись следующие три требования:

- функциональные и физические границы четко определены;

- работа элемента не зависит от какой-либо вспомогательной функции или все события, связанные с элементом, описаны одним вентилем ИЛИ, один из входов которого соответствует неисправности элемента, а оставшиеся входы - неспособности выполнить соответствующие вспомогательные функции;

- причины появления данного события непосредственно не определены.

Перечень обозначений, используемых в ДН, должен быть стандартизован для того, чтобы минимизировать несоответствия, четко обозначить и объяснить, какие события представлены в систематизированном виде.

Фактически построение ДН следует аналитической логике потока событий:

- принцип "непосредственная причина" требует, чтобы были определены необходимые и достаточные непосредственные причины появления завершающего события. Следует отметить, что это не базовые причины завершающего события, а прямые причины или прямые механизмы, вызывающие появление завершающего события. Это могут быть события нижнего или промежуточного уровня;

- необходимые и достаточные непосредственные причины завершающего события рассматривают как промежуточные события и продолжают анализ;

- построение ДН вниз продолжают, причем внимание переключают с механизмов на виды неисправностей, постепенно приближаясь к более низкому уровню до окончательного достижения соответствующего или заданного уровня глубины анализа. Отдельные базовые события или первичные события нижнего уровня - это события, представляющие отдельные причины возможных отказов или неисправностей.

7.5.4 Оценивание АДН

7.5.4.1 Исследование и анализ

Исследование заключается в экспертизе структуры ДН путем сравнения с имеющейся информацией, такой как схемы, графики, функциональные диаграммы, команды, реализуемые программными средствами, идентификация общих событий и поиск независимых ветвей. Исследование должно выявить события, вызываемые общими причинами. Выводы могут быть сделаны только после всестороннего анализа с применением булевого преобразования или определения минимальных сечений, когда присутствуют статические вентили, поскольку сечения не обозначают динамическими вентилями (если не предполагается допущение, игнорирующее упорядочение). По мере усложнения анализа с увеличением размера ДН следует установить, какие ветви ДН являются независимыми и, при необходимости, их следует анализировать отдельно.

Процесс анализа следует документировать так, чтобы были понятны результаты анализа и любые изменения конструкции, рабочих процедур или поясняющие природу отказа.

Основные задачи логического (качественного) и численного (количественного) анализов системы можно обобщить следующим образом:

- идентификация событий или неисправностей, способных непосредственно вызвать отказ системы и повлиять на вероятность появления таких событий;
- подавление неисправностей, которые могут стать возможной угрозой безопасности;
- оценка отказоустойчивости системы (способности функционировать даже после того, как появилось определенное число неисправностей или событий более низкого уровня, приводящих к отказу системы);
- оценка информации для установления критических компонентов и механизмов отказа;
- проведение диагностики отказа, действий по стратегии технического обслуживания и ремонта и т.п.

Оценка отказоустойчивости системы предусматривает определение степени резервирования, используемого в системе. Оценка отказоустойчивости большей частью не требует численных данных, однако такие данные необходимы при оценке наиболее вероятных сочетаний событий, приводящих к отказу системы.

7.5.4.2 Логический анализ

Основа анализа

При логическом анализе применяют, как правило, булево преобразование и определение минимального сечения. Основа логического анализа - моделирование, приводящее к построению ДН, представляющего собой структуру системы - функциональную, архитектурную или одновременно и ту, и другую. Правильное моделирование предусматривает представление функций или компонентов системы так, чтобы можно было установить их взаимосвязи, зависимости, прямые причины нежелательных итогов и т.п.

Булево преобразование

Булево преобразование применяют для оценки влияния общих событий ДН (одинаковых событий, развивающихся в различных ветвях дерева), в котором появление завершающего события не зависит от согласованности событий во времени или от их последовательности. Булево преобразование выполняют путем решения булевых уравнений для ДН. Булево преобразование можно также применять для определения минимальных сечений.

Определение минимальных сечений

Существует несколько методов определения минимальных сечений, но для больших деревьев эти методы являются трудными и несовершенными. Для реализации этих методов разработаны разнообразные компьютерные программы.

Сечение представляет собой группу событий, которые при совместном появлении вызывают развитие завершающего события. Минимальное сечение - наименьшая группа, все события которой должны появиться для развития завершающего события. Если любые события минимального сечения не развиваются, завершающее событие не появится. Определение можно расширить для ДН, зависящих от последовательности событий. В таких случаях минимальное сечение представляет собой группу событий, которые, возможно, смогут вызвать завершающее событие. Если появление завершающего события зависит от порядка исходных событий, событие анализируют с помощью марковских методов.

7.5.4.3 Численный анализ

Задача численного анализа - дать количественную оценку вероятности появления завершающего события или отобранного набора событий. Численный анализ используют для поддержки и дополнения логического анализа.

7.5.5 Примеры оценки аппаратных средств с помощью булева алгоритма и его представление в дереве неисправностей

7.5.5.1 Пример мостовой схемы

ДН с применением булевой алгебры может существенно упростить анализ безотказности. Как показано в примере, сложные математические выражения, которые нужно использовать при анализе с использованием блок-схемы расчета безотказности, заменяют значительно более простой булевой алгеброй. АДН особенно пригоден для наиболее сложных схем, программные и аппаратные средства которых являются независимыми, и анализ проводят с использованием одного из многих пакетов прикладных программ.

Мостовая схема приведена на рисунке 8.

Рисунок 8 - Пример мостовой схемы, анализируемой с

помощью ДН

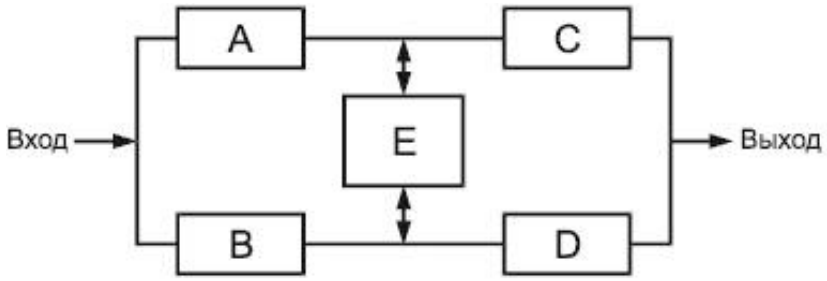


Рисунок 8 - Пример мостовой схемы, анализируемой с помощью ДН

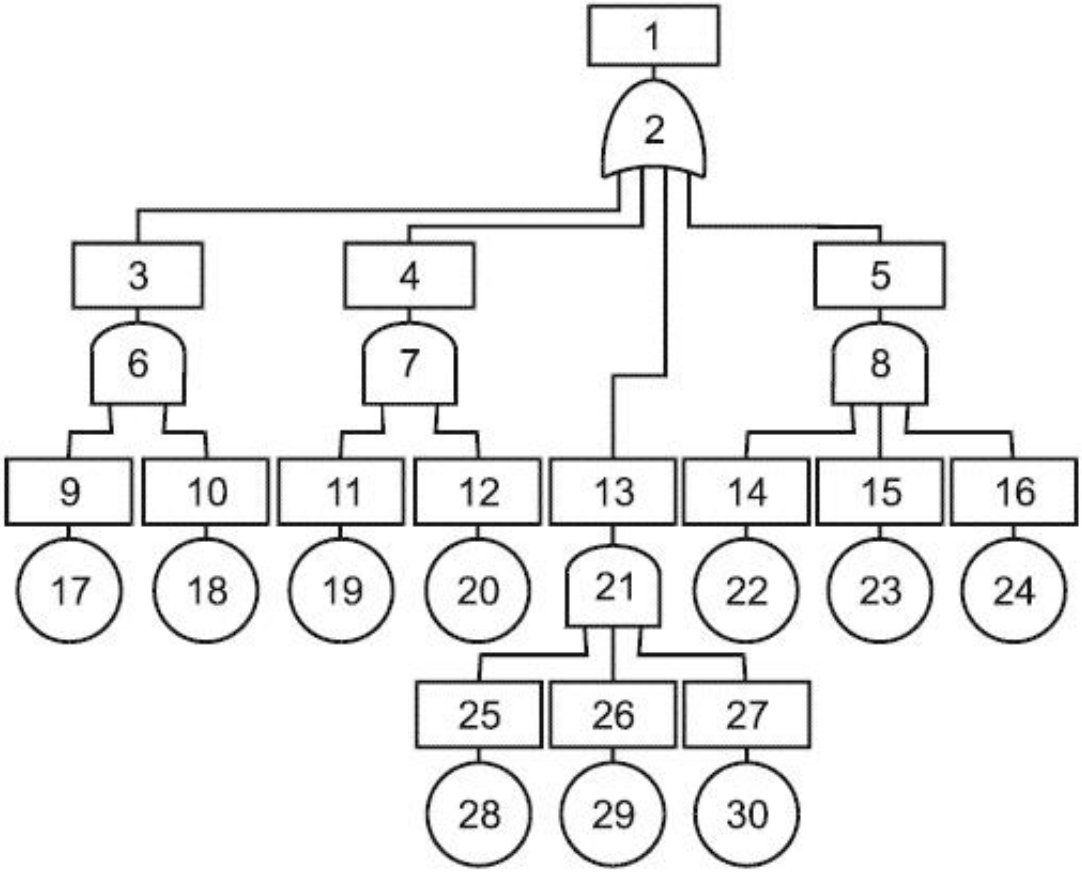
В мостовой схеме, изображенной на рисунке 8, сигнал проходит от "Входа" к "Выходу". Он может пройти через блок E в двух направлениях. Анализ можно провести путем моделирования системы для двух возможных условий, первое из которых предполагает, что блок E исправен, а второе - что блок неисправен. В первом случае сигнал пройдет через блоки A или B и C или D, при условии, что они включены параллельно. Если блок E неисправен (состояние блока E - отказ), блоки A и C включены последовательно и параллельно блокам B и D, которые также включены последовательно. Это может быть представлено в виде следующего уравнения:

$$R_S = (R_A + R_B - R_A R_B)(R_C + R_D - R_C R_D)R_E + \\ + (R_A R_C + R_B R_D - R_A R_B R_C R_D)(1 - R_E). \quad (7)$$

Если положить, что $R_A = 0{,}78$; $R_B = 0{,}30$; $R_C = 0{,}15$; $R_D = 0{,}50$; $R_E = 0{,}40$, то $R_S = 0{,}344$; вероятность отказа $F_S = 0{,}656$.

Представление мостовой схемы в виде ДН приведено на рисунке 9.

Рисунок 9 - Представление мостовой схемы в виде ДН



1 - вероятность отказа мостовой схемы; 2 - мостовая схема; 3 - прерывание сигнала блоками A и B; 4 - прерывание сигнала блоками C и D; 5 - прерывание сигнала блоками B, E и C; 6 - блоки A и B; 7 - блоки C и D; 8 - блоки B, E и C; 9 - событие отказа блока A; 10 - событие отказа блока B; 11 - событие отказа блока C; 12 - событие отказа блока D; 13 - прерывание сигнала блоками A, E и D; 14 - событие отказа блока B; 15 - событие отказа блока E; 16 - событие отказа блока C; 17 - блок A; 18 - блок B; 19 - блок C; 20 - блок D; 21 - блоки A, E и D; 22 - блок B; 23 - блок E; 24 - блок C; 25 - событие отказа блока A; 26 - событие отказа блока E; 27 - событие отказа блока D; 28 - блок A; 29 - блок E; 30 - блок D

Рисунок 9 - Представление мостовой схемы в виде ДН

С помощью булевой алгебры и минимального сечения систему, изображенную на рисунке 9, можно преобразовать следующим образом.

Сечения системы представляют собой сочетания следующих событий, приводящих к блокированию сигнала:

- A и B ($c_1 = F_A F_B = ab$);

- C и D ($c_2 = cd$);

- A, E и D ($c_3 = aed$);

- B, E и C ($c_4 = bec$).

При использовании булевой алгебры вероятность отказа системы будет равна

$$F_S = \Pr(c_1 \cup c_2 \cup c_3 \cup c_4). \qquad (8)$$

Вероятности появления сечений

$$\Pr(c_1) = F_A F_B = (1 - R_A)(1 - R_B);$$

$$\Pr(c_2) = F_C F_D = (1 - R_C)(1 - R_D);$$

$$\Pr(c_3) = F_A F_E F_D = (1 - R_A)(1 - R_E)(1 - R_D);$$

$$\Pr(c_4) = F_B F_E F_C = (1 - R_B)(1 - R_E)(1 - R_C). \quad (9)$$

7.5.5.2 Разобщение

Разобщение представляет собой серию алгебраических операций, выполняемых для того, чтобы общую ветвь (или общую причину отказа) при расчетах не рассматривать повторно.

Для больших ДН процедуры разобщения следует выполнять с помощью компьютерной программы.

Расчет вероятности появления завершающего события мостовой схемы при использовании метода разобщения дает следующие результаты:

2 - мостовая схема $F = 0{,}6557$;

6 - блоки A и B: $F = 0{,}1540$;

7 - блоки C и D: $F = 0{,}4250$;

8 - блоки B, E и C: $F = 0{,}3570$;

17 - блок A: $F = 0{,}2200$;

18 - блок B: $F = 0{,}7000$;

19 - блок C: $F = 0{,}8500$;

20 - блок D: $F = 0{,}5000$;

21 - блоки A, E и D: $F = 0{,}0660$;

22 - блок B: $F = 0{,}7000$;

23 - блок E: $F = 0{,}6000$;

24 - блок C: $F = 0{,}8500$;

28 - блок A: $F = 0{,}2200$;

29 - блок E: $F = 0{,}6000$;

30 - блок D: $F = 0{,}5000$.

Примечание - Номера соответствуют приведенным на рисунке 9.

Расчет не привязан к конкретной программе, поскольку настоящий стандарт не отдает предпочтение каким-либо определенным программным средствам. Это решает пользователь в соответствии со своими конкретными задачами.

Из расчета видно, что при определении безотказности системы или дополнительного показателя вероятность появления завершающего события является такой же, как и при расчете с помощью уравнения для первой модели безотказности.

7.6 Интенсивность отказов при анализе дерева неисправностей

Во многих случаях при АДН вместо вероятности отказа можно рассматривать интенсивность отказов. В этом случае применяют распределения Пуассона для описания появления событий, а также постоянство связанной с этими событиями интенсивности отказов. Используемые в данном случае алгебраические выражения приняты при обычном моделировании надежности, и алгоритмы расчета интенсивности отказов завершающих событий будут такими же, как и при моделировании с помощью блок-схемы расчета надежности.

Можно строить ДН с разными значениями интенсивности отказов и вероятностями отказов, присвоенных различным событиям. Простейший способ АДН такого типа заключается в преобразовании интенсивностей отказов в соответствующие вероятности появления события и применении стандартных методов АДН.

8 Идентификация и классификация элементов дерева неисправностей

Каждое событие ДН должно быть однозначно идентифицировано. События должны быть классифицированы, чтобы обеспечить простые перекрестные ссылки между ДН и соответствующей проектной документацией.

Завершающее событие ДН - нежелательное итоговое событие, являющееся основным фактором, стимулирующим проведение АДН. Одно ДН может иметь только одно завершающее событие.

Если несколько событий ДН относятся к разным видам неисправностей одного и того же элемента, такие события следует классифицировать так, чтобы их можно было различать. Вместе с тем должно быть понятно, что они представляют собой группу событий, относящихся к одному и тому же элементу.

Если определенное событие, например неспособность отключить конкретный затвор, происходит в нескольких местах ДН, все появления такого события следует называть одинаково (с помощью программ одно и то же входное событие может быть добавлено в различные места ДН с тем же именем). При этом одинаковые события, присущие различным элементам, не следует классифицировать одинаково.

Важно, чтобы было обеспечено одинаковое и постоянное применение кодов и имен на протяжении конкретного АДН. Это особенно важно при использовании компьютерных расчетов.

Постоянство кода особенно важно в том случае, когда программы АДН позволяют импортировать расчетные значения вероятности появления базисных или первичных событий в крупномасштабные таблицы, содержащие перечни используемых материалов, компонентов, виды неисправностей компонентов и данные, характеризующие эксплуатацию системы.

9 Отчет

Отчет АДН должен содержать следующие основные разделы:

- цель и область действия;
- описание системы и указание ее границ;
- все виды допущений, касающиеся конструкции системы, эксплуатации, технического обслуживания и ремонта, тестирования и проверки, моделирования безотказности и др.;
- определение и критерии завершающего события;
- ссылки на базисные события, неразвитые события и события, которые анализировались за пределами ДН;
- данные, используемые символы и, при необходимости, отказы, вызванные общими причинами, минимальные сечения;
- результаты, выводы, рекомендации;
- данные о сотрудниках, проводивших анализ.

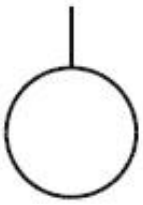
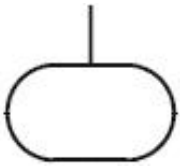
Дополнительными данными, которые могут быть включены в отчет, являются:

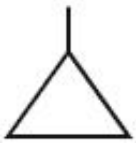
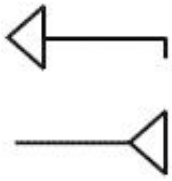
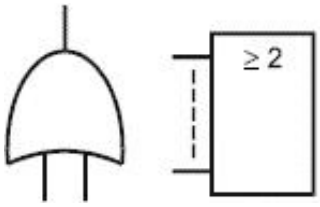
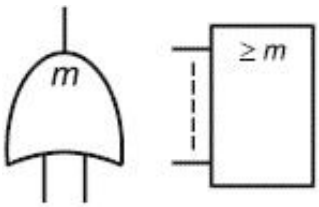
- блок-схема или схема системы;
- краткая сводка данных, касающихся безотказности, технического обслуживания и ремонта, а также такие источники, как базы данных, информация изготовителей, файлы и т.д.;
- анализ вида и последствий отказов/анализ вида, последствий и критичности отказов или ссылка на анализ.

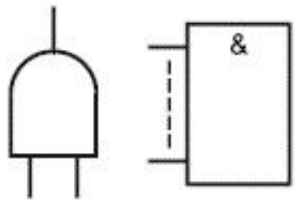
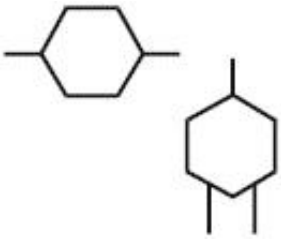
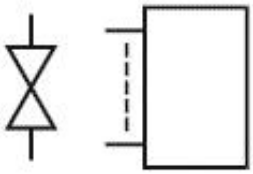
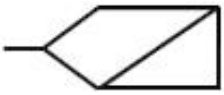
Приложение А (справочное). Символы

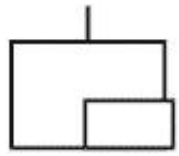
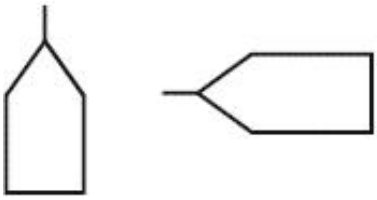
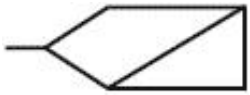
Приложение А
(справочное)

Таблица А.1 - Символы, наиболее часто используемые в процессе АДН

Символ	Наимено-вание	Описание	Отношение к безотказности	Число входных событий
	Базисное событие	Событие самого низкого уровня, для которого имеются данные, касающиеся вероятности его появления	Вид неисправности компонента или причина вида неисправности	0
	Условное событие	Событие, которое является результатом появления другого события, при этом для развития завершающего события должны состояться оба события	Появление события, которое должно появиться для развития другого события. Условная вероятность	0
	Скрытое событие	Первичное событие, отображающее скрытый отказ; событие, которое нельзя обнаружить сразу, но которое, возможно, будет обнаружено при дополнительной проверке или анализе	Скрытый вид отказа компонента или скрытая причина отказа	0

	Неразвитое событие	Первичное событие, относящееся к неразработанной части системы	Событие, вносящее вклад в вероятность отказа. Структура части системы не определена	0
	Вентиль переноса	Вентиль, указывающий на то, что данная часть системы разрабатывается в другой части страницы или диаграммы	Частичная диаграмма дерева неисправностей, приведенная в другом месте диаграммы системы.	0
Перенос из (OUT) 			IN означает, что развиваемый вентиль находится в другом месте, OUT - что вентиль будет перенесен в другое место	
Перенос в (IN) 				
	Вентиль ИЛИ	Выходное событие наступает, если наступает любое из входных событий	Отказ наступает, если любая часть системы отказывает (последовательная система)	≥ 2
	Мажоритар-ный вентиль	Выходное событие наступает, если наступают m или более входных событий из общего числа n	Резервирование k элементов из общего числа n, где $m = n - k - 1$	≥ 3

	Вентиль И	Выходное событие наступает, если наступают все входные события	Параллельное резервирование из n одинаковых или различных ветвей	≥ 2
	Вентиль И с приоритетом	Выходное событие наступает, если входные события наступают последовательно слева направо	Пригоден для представления вторичных отказов или для описания последовательности событий	≥ 2
	Вентиль запрета	Выходное событие наступает, если наступают оба входных события, одно из которых условное	Условная вероятность появления выходного события	2
	Вентиль НЕ	Выходное событие наступает, если не наступает входное событие	Несовместные (взаимоисключающие) события	1
	Вентиль очередности	Завершающее событие наступает, если все исходные события наступают поочередно слева направо. Этот вентиль идентичен вентилю И с приоритетом, если число входов вентиля И с приоритетом не менее двух	Используют для представления последовательно возникающих (цепных) отказов. Также используют для представления последовательности нагрузок, способных вызвать развитие события или отказа. Следует применять марковский анализ	≥ 3

	Вентиль резерва	Завершающее событие наступает, если число запасных компонентов меньше требуемого числа	Представление нагруженного, ненагруженного и частично нагруженного запасных компонентов	≥ 1
	Собственное событие	Событие, которое произошло или обязательно произойдет	-	-
	Нулевое событие	Событие, которое не может произойти	-	-

Электронный текст документа
подготовлен ЗАО "Кодекс" и сверен по:
официальное издание
М.: Стандартинформ, 2011