ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 150— 2016

МЕНЕДЖМЕНТ РИСКА

Руководство по применению методов анализа надежности

(IEC 60300-3-1: 2003, NEQ)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 РАЗРАБОТАН Автономной некоммерческой организацией «Международный институт образования» (АНО «МИО»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 октября 2016 г. № 72-пнст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта МЭК 60300-3-1:2003 «Управление надежностью. Часть 3-1. Руководство по применению. Методы анализа надежности. Руководство по методологии» (IEC 60300-3-1:2003 «Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Март 2017 г.

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за четыре месяца до истечения срока его действия разработчику настоящего стандарта по адресу: Москва, Нахимовский пр-т, д. 31, корп. 2 и в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074, Москва, Китайгородский проезд, д. 7, стр. 1.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В настоящем предварительном стандарте приведено общее описание методов анализа надежности, применимых для оценки и анализа риска. Применение методов анализа надежности при оценке риска позволяет разработчикам требований в области менеджмента риска выделить этапы процесса менеджмента риска, где необходимо применение методов анализа надежности и четко сформулировать направленность применения этих методов для обеспечения безопасности и снижения риска.

Методы анализа надежности могут быть использованы для прогнозирования, исследования и улучшения надежности, работоспособности и ремонтопригодности объекта.

Исследования надежности проводят на стадиях концепции и определения, проектирования, разработки, эксплуатации и технического обслуживания. Методы могут быть использованы при определении допустимого риска и сопоставлении результатов анализа риска с установленными требованиями.

Для получения достоверных результатов анализа риска в процессе анализа риска должны быть рассмотрены все возможные воздействия на надежность системы со стороны: аппаратных средств, программного обеспечения, человеческого фактора и организационных действий.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ РИСКА

Руководство по применению методов анализа надежности

Risk management. Guide for application of analysis techniques for dependability

Срок действия — с 2017—01—01
по 2018—01—01

1 Область применения

Настоящий стандарт входит в группу стандартов в области менеджмента риска и дополняет ГОСТ Р ИСО 31010—2011.

В стандарте приведено общее описание методов анализа надежности, которые могут быть использованы при оценке и анализе риска, а также приведена необходимая информация для выбора соответствующего метода анализа надежности.

Настоящий стандарт не предназначен для целей оценки соответствия и использования в качестве обязательных или договорных требований.

Настоящий стандарт допускает использование других методов анализа надежности с учетом их применимости в конкретной ситуации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 31010—2011 Менеджмент риска. Методы оценки риска

ГОСТ Р 51897—2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения

ГОСТ 27.002—2015 Надежность в технике. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 51897—2011/Руководство ИСО 73:2009 и ГОСТ 27.002—2015.

Издание официальное

4 Методы анализа надежности при анализе и оценке риска

Отказ технической системы может привести к созданию опасной ситуации, способной вызвать кратковременные или долговременные неблагоприятные воздействия на персонал организации, экологию, население региона, социальную обстановку в обществе и т. п. Поэтому при анализе риска технических систем методы анализа надежности являются частью процесса анализа и оценки риска. Краткое описание процесса анализа надежности приведено в приложении А.

В соответствии с ГОСТ Р ИСО 31010—2011 методы оценки риска могут быть объединены в следующие группы:

- методы наблюдения (включая контрольные листы, предварительный анализ опасностей и др.);
- вспомогательные методы [включая структурированное интервью и мозговой штурм, метод Дельфи, структурированный анализ сценариев методом «что, если?», анализ влияния человеческого фактора (HRA[1)])];
- анализ сценариев [включая анализ первопричины, анализ сценариев, оценку токсикологического риска, анализ воздействия на бизнес, анализ дерева неисправностей, анализ причин и последствий, причинно-следственный анализ);
- функциональный анализ [включая анализ видов и последствий отказов (FMEA[2)]) и анализ критичности видов и последствий отказов (FMECA[3)]), техническое обслуживание, направленное на обеспечение надежности, анализ скрытых дефектов (анализ паразитных цепей), исследование опасности и работоспособности (HAZOP[4)]), анализ опасности и критических контрольных точек (HACCP[5)]), анализ уровней защиты (LOPA[6)]), анализ «галстук-бабочка»];
- статистические методы (Марковский анализ, моделирование методом Монте-Карло, Байесовский анализ).

Методы анализа надежности обычно объединяют в две основные группы:

- основные методы анализа надежности [включая прогнозирование интенсивности отказов, анализ дерева неисправностей, анализ дерева событий, анализ структурной схемы надежности, Марковский анализ, анализ сети Петри, анализ видов и последствий отказов (FMEA), анализ критичности видов и последствий отказов (FMECA), исследование опасности и работоспособности (HAZOP), анализ влияния человеческого фактора (HRA), анализ прочности и напряжений, таблица истинности (анализ функциональной структуры) и др].
- общие технические методы (включая исследование ремонтопригодности, анализ скрытых дефектов (анализ паразитных цепей), анализ наихудшего случая, имитационное моделирование отклонений, анализ конечных элементов, ограничение допустимых значений и выбор частей, анализ Парето, диаграмму причин и следствий, анализ отчета об отказах и систему корректирующих действий и др).

Примечание — Общие технические методы могут быть использованы как вспомогательные при проведении анализа надежности, а также при проектировании надежности.

Также существуют методы анализа надежности, не выделенные как самостоятельные, включая анализ причин/следствий — комбинация ETA[7)] и FTA[8)], динамический FTA, функциональный анализ отказов, Булевы диаграммы решений и др.

Использование методов решения общих задач анализа надежности приведено в таблице 1. Характеристики методов приведены в таблице 2.

Применение единых методов оценки риска и методов анализа надежности обеспечивает тесное взаимодействие процессов оценки риска (см. ГОСТ Р ИСО 31010—2011, подраздел 5.1) и процессов анализа надежности (приложение А). Краткое описание большинства вышеприведенных методов анализа надежности приведено в ГОСТ Р ИСО 31010—2011.

---

1) HRA Human reliability analysis.

2) FMEA Failure mode and effects analysis.

3) FMECA Failure mode, effects and criticality analysis.

4) HAZOP — Hazard and operability study.

5) HACCP — Hazard Analysis and Critical Control Points.

6) LOPA — Layers Of Protection Analysis.

7) ETA Event tree analysis.

8) FTA Fault tree analysis.

Таблица 1 — Методы решения общих задач анализа надежности

Метод	Распределение требований/целей надежности	Качественный анализ	Количественный анализ	Рекомендации
Прогнозирование интенсивности отказов	Применим для последовательных систем без резервирования	Возможно применение для анализа стратегии технического обслуживания	Вычисление интенсивностей отказов и MTTF для электронных компонентов и оборудования	Поддержка
Анализ дерева неисправностей	Применим, если поведение системы зависит от времени или последовательности событий	Анализ комбинации неисправностей	Вычисление показателей безотказности работоспособности и относительного вклада подсистем в системы	Применим
Анализ дерева событий	Возможен	Анализ последовательности отказов	Вычисление интенсивностей отказов системы	Применим
Анализ структурной схемы надежности	Применим для систем, у которых можно выделить независимые блоки	Анализ путей работоспособности	Вычисление показателей безотказности и комплексных показателей надежности системы	Применим
Анализ Маркова	Применим	Анализ последовательности отказов	Вычисление показателей безотказности и комплексных показателей надежности системы	Применим
Анализ сети Петри	Применим	Анализ последовательности отказов	Подготовка описания системы для анализа Маркова	Применим
Анализ режимов и последствий (критичности) отказов FME(C) A	Применим для систем, у которых преобладают единичные отказы	Анализ воздействия отказов	Вычисление интенсивности отказов (и критичности) системы	Применим
Исследование HAZOR	Поддержка	Анализ причин и последствий отклонений	Не применим	Поддержка
Анализ человеческого фактора	Поддержка	Анализ воздействия действий эффективности человека на работу системы	Вычисление вероятностей ошибок человека	Поддержка
Анализ прочности и напряжений	Не применим	Применим как средство для предотвращения неисправности	Вычисление показателей безотказности для электромеханических компонентов	Поддержка
Таблица истинности (анализ функциональной структуры)	Не применим	Возможен	Вычисление показателей безотказности и комплексных показателей надежности системы	Поддержка
Статистические методы надежности	Возможен	Анализ воздействия неисправностей	Определение количественных оценок показателей безотказности с неопределенностью	Поддержка

Окончание таблицы 1

Примечание — Слова-обозначения, принятые в таблице:
«применим» означает, что метод рекомендован для решения задач;
«возможен» — метод допускается использовать для решения задач, учитывая, что он имеет некоторые недостатки по сравнению с другими методами;
«поддержка» — метод применим для некоторой части задач и может использоваться для решения задачи только в комбинации с другими методами;
«не применим» — метод не допускается для решения задач.

5 Классификация методов анализа надежности

Методы анализа надежности классифицируют в соответствии с их основной целью по следующим категориям:

а) методы, направленные на предотвращение отказов (например, анализ прочности и напряжений);

б) методы анализа архитектуры системы и распределения надежности, включая следующие основные методы (перечень может быть дополнен):

- восходящий метод (главным образом, направленный на исследование последствий единичных отказов, например, ETA, FMEA, HAZOP).

Начальным этапом любого восходящего метода является идентификация режимов отказов на соответствующем уровне. Для каждого режима отказа определяют его влияние на эффективность системы. Восходящий метод анализа надежности позволяет четко идентифицировать все режимы одиночных отказов, поскольку он опирается на перечень составных частей системы или другие контрольные списки. На начальных этапах разработки анализ может быть качественным и исследовать функциональные отказы. Затем может быть применен количественный анализ;

- нисходящие методы (исследующие последствия комбинаций отказов, например, FTA, Марковский анализ, анализ сети Петри, анализ функциональной структуры, анализ структурной схемы надежности).

На начальном этапе нисходящего метода определяют одиночное неблагоприятное событие или событие, обеспечивающее успех системы на самом высоком уровне (вершина событий). Затем идентифицируют и анализируют причины этого события на всех уровнях.

Нисходящий метод начинают с самого высокого уровня, т. е. с анализа надежности системы или подсистемы в целом и последовательно спускаются на более низкий уровень. Затем анализ проводят на следующем более низком уровне декомпозиции системы, идентифицируют все отказы и соответствующие последствия. Для каждого из отказов этого уровня анализ повторяют путем прослеживания функциональных отказов в отношении следующего более низкого уровня системы. Этот процесс продолжают до тех пор, пока не достигнут самого низкого уровня.

Нисходящий метод используют для оценки многократных отказов, включая последовательные зависимые отказы, при наличии отказов общей причины, а также для сложных систем;

- методы оценки характеристик основных событий (например, прогнозирование интенсивности отказов, HRA, статистические методы надежности, SRE[1]).

Методы анализа надежности различают по зависимости и независимости анализируемых событий.

Результаты классификации перечисленных методов приведены на рисунке 1.

Последовательность зависимых событий	Анализ дерева событий	Марковский анализ, анализ сети Петри, таблица истинности
Последовательность независимых событий	FMEA, HAZOR	FTA, RBD[2]
	Восходящий (одиночные отказы)	Нисходящий (многократные отказы)

Рисунок 1 — Классификация методов зависимости(независимости) анализируемых событий

[1] SRE — Software reliability engineering.

[2] RDB — Reliability block diagrams.

Эти методы применимы как для оценки качественных характеристик, так и для определения оценок количественных характеристик при прогнозировании показателей системы при эксплуатации. Следует отметить, что достоверность результата зависит от точности и правильности данных об основных событиях.

Однако ни один метод анализа надежности не может быть использован для всестороннего анализа реально существующих систем (аппаратных средств и программного обеспечения, систем со сложной функциональной структурой, систем с различными технологиями ремонта и технического обслуживания и т. д.). Для проведения анализа надежности сложных или многофункциональных систем, как правило, необходимо применять несколько дополнительных методов анализа.

В таблице 2 приведен краткий обзор различных методов анализа надежности, их характеристик и особенностей. Для полного анализа системы, как правило, применяют несколько методов.

Таблица 2 — Характеристики выбранных методов анализа надежности

Метод	Для сложных систем	Для новых проектов	Количественный анализ	Для комбинаций неисправностей	Для обработки с учетом последовательности и зависимости событий	Для зависимых событий	Восходящий или нисходящий	Для распределения надежности	Квалификация исполнителя	Применимость и унифицированность	Потребность в инструментах поддержки	Проверка правдоподобия результатов	Пригодность инструментальных средств	Обозначение стандарта IEC
Прогнозирование интенсивности отказов	Нет	Да	Да	Нет	Нет	Нет	BU	Да	H	B	C	Да	B	61709
Анализ дерева неисправностей (FTA)	Да	Да	Да	Да	Нет	Нет	TD	Да	C	B	C	Да	B	61025
Анализ дерева событий (FTA)	NR	NR	Да	NR	Да	Да	BU	NR	B	C	C	Да	C	
Анализ структурной схемы надежности (RBD)	NR	NR	Да	Да	Нет	Нет	TD	Да	H	C	C	Да	C	61078
Марковский метод	Да	Да	Да	Да	Да	Да	TD	Да	B	C	B	Нет	C	61165
Анализ сети Петри	Да	Да	Да	Да	Да	Да	TD	Да	B	H	B	Нет	H	
Анализ видов и последствий отказов (FMEA)	NR	NR	Да	Нет	Нет	Нет	BU	NR	H	B	H	Да	B	60812
Исследование HAZOP	Да	Да	Нет	Нет	Нет	Нет	BU	Нет	H	C	H	Да	C	61882
Анализ надежности человеческого фактора	Да	Да	Да	Да	Да	Да	BU	Нет	B	B	C	Да	C	
Анализ нагрузок и напряжений	NA	NA	Да	NA	NA	Нет	NA	Нет	B	C	B	Да	C	
Таблица истинности	Нет	Да	Да	Да	Нет	Нет	NA	Да	B	C	B	Нет	H	
Статистические методы надежности	Да	Да	Да	Да	Да	Да	NA	NR	B	C	B	C	H	60300-3-5

NR — может использоваться для анализа простых систем. Не рекомендуется использовать как автономный метод, только совместно с другими методами.
TD — нисходящий метод анализа.
BU — восходящий метод анализа.
H — критерий не применим для этого метода.
B — высокий.
C — средний.
H — низкий.

6 Выбор метода анализа надежности

Выбор метода анализа является очень индивидуальным и обычно осуществляется объединенными усилиями экспертов по надежности и эксплуатации системы. Выбор должен быть сделан на ранних этапах разработки программы и исследован на применимость.

При использовании следующих критериев выбор методов может быть упрощен:

а) Сложность системы: сложные системы, например, включающие резервирование или другие особенности, обычно требуют более глубокого уровня анализа, чем простые системы.

б) Новизна системы: вновь разрабатываемая система требует более тщательного анализа, чем разработанная ранее;

в) Качественный или количественный анализ: действительно ли количественный анализ необходим?

г) Единичные или многократные неисправности: существенно ли влияние комбинации неисправностей или ими можно пренебречь?

д) Поведение системы зависит от времени или последовательности событий: имеет ли значение для анализа последовательность событий (например, система отказывает только в случае, если событию А предшествует событие Б, а не наоборот) или поведение системы зависит от времени (например, ухудшение режимов работы после отказа или выполнения функции)?

е) Возможность использования метода для зависимых событий: зависят ли характеристики отказа или восстановления отдельного элемента системы от состояния системы в целом?

ж) Восходящий или нисходящий анализ: обычно применение восходящих методов является более простым. Применение нисходящих методов требует осмысления и творческого подхода и имеет больше возможностей для ошибок.

и) Распределение требований надежности: может ли метод быть приспособлен к количественному распределению требований надежности?

к) Квалификация исполнителя: какой требуется уровень образования или опыта для правильного применения метода?

л) Применимость. Например, регулирующая сторона или заказчик обычно применяет метод?

м) Необходимость инструментальной поддержки: нуждается ли метод в компьютерной поддержке или он может быть выполнен вручную?

н) Проверки правдоподобия: можно ли проверить правдоподобие результатов вручную? Если нет, являются ли инструментальные средства доступными?

п) Доступность инструментальных средств: действительно ли инструментальные средства доступны? Имеют ли эти инструментальные средства общий интерфейс с другими инструментальными средствами анализа, чтобы результаты могли многократно использоваться или передаваться?

р) Стандартизация: существует ли стандарт по применяемому методу и унификации его результатов?

Приложение А
(справочное)

Процесс анализа надежности

Процесс анализа надежности представлен на рисунке А.1 и состоит из следующих этапов:

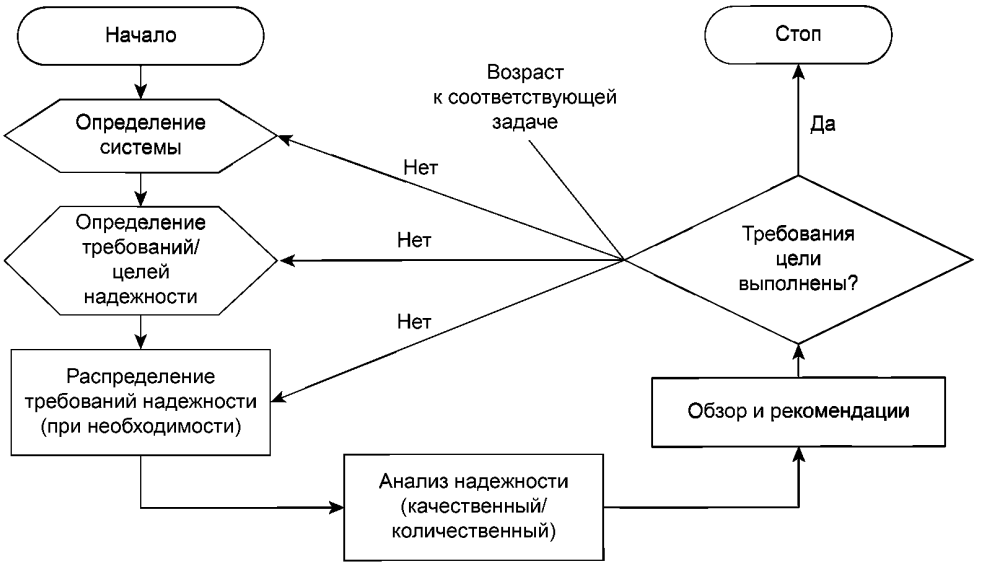

Рисунок А.1 — Процесс анализа надежности

а) определение системы.

Определение исследуемой системы, режимов и условий ее работы, функциональных связей, включая процессы и интерфейсы, а также оценку риска. Обычно результаты определения системы являются входом в процесс разработки системы;

б) определение требований и целей в области надежности.

Определение всех требований или целей в области надежности и работоспособности системы, а также характеристик и особенностей системы, режимов ее эксплуатации, условий окружающей среды и требований обслуживания. Определение отказа системы, критериев отказов и условий, основанных на функциональной спецификации системы, ожидаемой продолжительности и условий эксплуатации;

в) распределение требований надежности.

Распределение требований или целей надежности системы по различным подсистемам на этапе проектирования (при необходимости);

г) проверка соответствия установленным требованиям.

Качественный и/или количественный анализ системы на основе методов анализа надежности и соответствующих данных об оценке их эффективности;

д) исследования и рекомендации.

Анализ выполнения требований в области надежности для рассматриваемого объекта и возможности их выполнения может включать оценку повышения надежности системы по результатам проектирования и производства (например, резервирование, снижение нагрузок, снижение риска, улучшение технического обслуживания системы, контроль технологических процессов и системы менеджмента качества).

УДК 658:562.014:006.354 ОКС 13.180

Ключевые слова: менеджмент риска, анализ надежности, показатели надежности, прогнозирование интенсивности отказов, анализ дерева неисправностей (FTA), анализ дерева событий (FTA), анализ структурной схемы надежности, Марковский анализ, сетевой анализ Петри, анализ видов и последствий отказов (FMEA), исследование HAZOP, анализ человеческого фактора, анализ нагрузок и напряжений, таблица истинности, статистические методы надежности

Редактор *М.И. Максимова*
Технический редактор *В.Ю. Фотиева*
Корректор *О.В. Лазарева*
Компьютерная верстка *Л.А. Круговой*

Подписано в печать 22.03.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,10. Тираж 6 экз. Зак. 561.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru