ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.015— 2019 (МЭК 60300-3-15: 2009)

Надежность в технике

УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ

Руководство по проектированию надежности систем

(IEC 60300-3-15:2009, Dependability management — Part 3-15: Application guide — Engineering of system dependability, MOD)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Закрытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ЗАО «НИЦ КД») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 119 «Надежность в технике»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 ноября 2019 г. № 1275-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 60300-3-15:2009 «Менеджмент надежности. Часть 3-15. Руководство по применению. Проектирование надежности системы» (IEC 60300-3-15:2009 «Dependability management — Part 3-15: Application guide — Engineering of system dependability», MOD) путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

Международный стандарт разработан Техническим комитетом по стандартизации ТС 56 Международной электротехнической комиссии (МЭК).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (www.gost.ru)

Содержание

Введение

В современных условиях системы становятся все более сложными. Надежность является важным атрибутом системы, который влияет на бизнес-стратегии, связанные с приобретением системы и соотношением стоимость—результат при функционировании системы. Надежность системы в целом является результатом сложного взаимодействия элементов системы, условий эксплуатации, интерфейсов «человек—машина», служб поддержки и других влияющих факторов.

В настоящем стандарте приведены рекомендации по проектированию системы в целом для достижения целей в области надежности. В стандарте представлены приемы проектирования, основанные на применении научных знаний и соответствующих технических дисциплин для достижения требуемой надежности системы.

Рассмотрены четыре основных аспекта проектирования надежности:

- процесс,
- достижение цели,
- оценка,
- измерение.

Методы проектирования охватывают технические процессы, которые применяют на различных стадиях жизненного цикла системы. Методы проектирования, описанные в настоящем стандарте, представлены последовательностью действий, обеспечивающих достижение целей на каждой стадии жизненного цикла системы.

Настоящий стандарт применим к системам, включающим аппаратное обеспечение, программное обеспечение и человека. Во многих случаях функция может быть реализована путем использования приобретаемых готовых составных частей и комплектующих. Система может быть связана с другими системами в форме сети. Границы, отделяющие систему от других объектов и от сети, можно выделить на основе определения их применения. Например, приобретаемый цифровой таймер может быть использован для синхронизации работы компьютера, компьютер как система может быть связан с другими компьютерами в бизнес-офисе в локальной сети. Условия использования применимы ко всем видам систем. Примерами таких систем являются системы управления при производстве электроэнергии, отказоустойчивые вычислительные системы и системы технического обслуживания.

Руководство по проектированию надежности разработано для универсальных систем, без выделения систем по видам их применения. Большая часть систем, как правило, являются восстанавливаемыми на всех стадиях жизненного цикла в соответствии с экономической целесообразностью и особенностями применения. Невосстанавливаемые системы, такие как спутники связи, оборудование дистанционного зондирования и мониторинга и устройства для одноразового использования, рассматривают в качестве специальных систем. Они требуют идентификации области применения, условий эксплуатации и дополнительной информации о специальных характеристиках для выполнения задачи системы. Невосстанавливаемые подсистемы и компоненты рассмотрены как элементы одноразового использования. Выбор применимого способа проектирования надежности конкретной системы осуществляется через процесс отработки проекта в системе менеджмента надежности.

Настоящий стандарт является одним из стандартов на системы надежности (см. *ГОСТ Р МЭК 60300-1* и *ГОСТ Р 51901.3*). В настоящем стандарте приведены ссылки на применимые к системам действия управления проектом. Они включают в себя определение надежности элементов, задачи, относящиеся к системе и руководящие принципы анализа менеджмента надежности и отработки проекта в части надежности.

В настоящем стандарте ссылки на международные стандарты заменены ссылками на национальные стандарты.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ

Руководство по проектированию надежности систем

Dependability in technics. Dependability management.
Guide for engineering of system dependability

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт представляет собой руководство по проектированию системы, устанавливающее процесс обеспечения надежности системы на стадиях жизненного цикла.

Настоящий стандарт применим при разработке новой системы и для усовершенствования существующих систем, включающих взаимодействия аппаратных средств, программного обеспечения и человека.

Настоящий стандарт также применим к поставщикам подсистем и комплектующих, которые изучают информацию о системе и критерии интеграции системы. В стандарте приведены методы оценки надежности системы и проверки результатов достижения целей в области надежности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 27.002—2015 Надежность в технике. Термины и определения

ГОСТ IEC 61508-3 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 27.014 Надежность в технике. Управление надежностью. Руководство по установлению требований к надежности систем

ГОСТ Р 27.301 Надежность в технике. Управление надежностью. Техника анализа безотказности. Основные положения

ГОСТ Р 27.606 Надежность в технике. Управление надежностью. Техническое обслуживание, ориентированное на безотказность

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.3 Менеджмент риска. Руководство по менеджменту надежности

ГОСТ Р 51901.6 (МЭК 61014:2003) Менеджмент риска. Программа повышения надежности

ГОСТ Р 51901.16 (МЭК 61164:2004) Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки

ГОСТ Р 53392 Интегрированная логистическая поддержка. Анализ логистической поддержки. Основные положения

ГОСТ Р 53613 (МЭК 60721-2-2:1988) Воздействие природных внешних условий на технические изделия. Общая характеристика. Осадки и ветер

ГОСТ Р 53614 (МЭК 60721-2-3:1987) Воздействие природных внешних условий на технические изделия. Общая характеристика. Давление воздуха

Издание официальное

ГОСТ Р 53615 (МЭК 60721-2-4:1987) Воздействие природных внешних условий на технические изделия. Общая характеристика. Солнечное излучение и температура

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

ГОСТ Р ИСО 10007 Менеджмент организации. Руководящие указания по управлению конфигурацией

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 15026 Информационная технология. Уровни целостности систем и программных средств

ГОСТ Р МЭК 60300-1 Менеджмент риска. Руководство по применению менеджмента надежности

ГОСТ Р МЭК 61508-1 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

ГОСТ Р МЭК 61508-4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61508-5 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 61508-6 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

ГОСТ Р МЭК 61508-7 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ГОСТ ИСО/МЭК ТО 15271 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии 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 дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

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

3.1 **система** (system): Набор взаимосвязанных объектов, рассматриваемый для определенной цели как единое целое, отделенный от других объектов[1)].

Примечания

1 Систему, как правило, оформляют в виде набора выполняемых ею функций.

2 Систему рассматривают отделенной воображаемой поверхностью, которая пересекает связи системы с окружающей средой и другими внешними системами.

3 Для работы системы могут требоваться внешние ресурсы (т.е. ресурсы, находящиеся вне границ системы).

4 Структура системы может быть иерархической, например система, подсистемы, компоненты и т. д.

[1)] Приведенное определение несколько отличается от стандартизованного (см. 3.1.3 ГОСТ 27.002—2015).

3.2 **подсистема** (subsystem): Система, которая является частью более сложной системы[1)].

3.3 **рабочий профиль** (operating profile): Полный набор задач, выполнение которых необходимо для достижения цели эксплуатации системы.

Примечания

1 Конфигурации и сценарии эксплуатации системы влияют на режимы эксплуатации системы.

2 Рабочий профиль является последовательностью необходимых задач, которые должны быть выполнены системой для достижения цели ее эксплуатации. Рабочий профиль представляет конкретные сценарии работы системы в эксплуатации.

3.4 **функция** (function): Элементарное действие, выполняемое системой, которое в сочетании с другими элементарными действиями (функциями системы) позволяет системе выполнить задачу.

3.5 **элемент** (element): Комбинация компонентов, которые составляют базовый блок, необходимый для выполнения отдельной функции[2)].

Примечания

1 Элемент может включать компоненты аппаратного и/или программного обеспечения, информацию и/или человека.

2 Для некоторых систем информация и данные являются важной частью работы системы.

3.6 **целостность** (integrity): Способность системы поддерживать свою форму, сохранять стабильность и работоспособное состояние при работе и использовании.

4 Обеспечение надежности системы при проектировании

4.1 Общие сведения

Надежностью называют свойство системы сохранять во времени способность выполнять требуемые функции в соответствии с заданными целями и условиями применения (см. также *3.1.5 ГОСТ 27.002—2015*). Свойства системы описывают показатели надежности (готовность, безотказность, ремонтопригодность, долговечность и др.), а также такие характеристики, как отказоустойчивость, восстанавливаемость, целостность, безопасность и обеспеченность техническим обслуживанием. Надежность системы означает, что система способна выполнять по запросу требуемые функции и удовлетворять потребности пользователя. Цель, структура, свойства системы и условия, влияющие на надежность системы, описаны в *ГОСТ Р 27.014,* в котором приведено руководство по определению соответствующих функций системы для установления требований к надежности системы.

Существует четыре основных аспекта проектирования надежности систем:

a) процесс обеспечения надежности — устанавливает технические процессы разработки системы, позволяющие обеспечить выполнение требований к надежности системы. Этот процесс состоит из разработки последовательности действий, осуществляемых на каждой стадии жизненного цикла для достижения установленных целей надежности системы. Процесс обеспечения надежности должен быть полностью интегрирован в процессы проектирования и управления;

b) достижение целей надежности — использование эффективных методов проектирования и экспериментальных знаний применительно к стадиям жизненного цикла системы. Целью является достижение целей надежности в отношении компонент и функций системы на уровне подсистем, пригодных для реализации и интеграции системы (повышение безотказности);

c) анализ показателей надежности и характеристик системы — определение показателей надежности и других характеристик системы и анализ достижения целей эксплуатации системой с такими показателями и характеристиками. Этот процесс определяет конкретные свойства надежности и характеристики системы для удовлетворения требований проекта, определяет методологию и дает обоснование определения этих показателей и характеристик;

d) оценка (измерение) показателей надежности и характеристик системы — количественное определение показателей надежности и других характеристик системы для включения в контракты, спецификации. Этот процесс состоит в присвоении количественного значения или числа целевому по-

---

1) Приведенное определение несколько отличается от стандартизованного (см. 3.1.4 ГОСТ 27.002—2015).

2) Внутреннюю структуру элемента не учитывают, рассматривая его как неделимый объект (см. 3.1.2 ГОСТ 27.002—2015).

казателю надежности или характеристике системы. Целью является составление заявления о намерениях в виде количественных величин для облегчения взаимного понимания проблемы при подготовке и выполнении договоров.

4.2 Свойства, показатели надежности и характеристики системы

Надежность и особенности системы представляют набором конкретных свойств и зависящих от времени параметров, присущих системе в соответствии с конструкцией. Некоторые характеристики системы, такие как параметры производительности, могут быть количественными и измеримыми. Другие характеристики, которые не могут быть описаны количественно, могут представлять собой некоторую величину или полезную информацию относительно свойств системы. Такие характеристики могут быть описаны качественно для определения их субъективной оценки. Как количественные, так и неколичественные показатели имеют важное значение для описания надежности и других свойств системы. Примеры неколичественных характеристик включают значение бренда, доброжелательное отношение пользователя и информативность инструкции. Примеры количественных показателей включают продолжительность безотказной работы, частоту простоев, среднее время между отказами и время восстановления системы до работоспособного состояния.

Важными свойствами надежности и характеристиками системы являются следующие:

a) готовность: свойство системы быть в состоянии выполнять требуемые функции в соответствии с заданными требованиями к системе. Показателями готовности являются процент продолжительности работоспособного состояния системы в соответствии с требованиями и продолжительность неработоспособного состояния;

b) безотказность: свойство системы непрерывно выполнять требуемые функции в течение данного периода времени, в заданных условиях. Показателями безотказности, которые можно измерить, являются среднее время между отказами и продолжительность безотказной работы;

c) ремонтопригодность: свойство системы, заключающееся в его приспособленности к поддержанию и восстановлению состояния, в котором она способна выполнять требуемые функции, путем технического обслуживания и ремонта. Измеримыми показателями ремонтопригодности являются такие, как среднее время до восстановления и время восстановления;

d) обеспеченность технического обслуживания и ремонта: свойство организации технического обслуживания в заданных условиях по запросу обеспечивать объект ресурсами, требуемыми для технического обслуживания. Измеримыми показателями данного свойства являются: коэффициент использования ресурсов для технического обслуживания и ремонта, необходимость обучения, возможность применения инструментов и оборудования, продолжительность логистических простоев обслуживания и время оборота запасов запчастей.

Существуют другие свойства системы, характеризующие ее работу для конкретных применений. Они включают, но не ограничиваются следующими:

e) восстанавливаемость: свойство системы, заключающееся в ее способности восстановления в состояние, в котором она может выполнять необходимые функции, после отказа без ремонта аппаратного или программного обеспечения. Измеримым показателем этого свойства является среднее время восстановления;

f) тестируемость: свойство системы быть протестированной на определенных уровнях технического обслуживания (по выполнению действий по замене/ремонту) для определения зоны неисправности. Измеримым показателем является процент тестового покрытия;

g) доступность услуги: способность услуги быть полученной в пределах заданных границ и других условий по запросу пользователя. Измеримым показателем является вероятность доступности услуги;

h) сохранение услуги: свойство услуги однажды полученной пользователем быть непрерывно поддерживаемой в заданных условиях в течение требуемого периода. Измеримым показателем является вероятность сохранения услуги в течение заданного периода времени.

Показатель восстанавливаемости зависит от конструкции системы, ее отказоустойчивости и способности к самовосстановлению. Показатели функционирования системы зависят от свойств оборудования системы, ее конструкции, а также структуры распределения ресурсов. Свойства системы полностью зависят от ее конструкции. Показатели функционирования системы определяют на основе возможностей системы и ее надежности.

Показатели надежности системы определяют на основе измерений времени (наработки) и параметров, характеризующих инцидент. Инцидент — это нежелательное или непредвиденное событие, наблюдаемое в процессе испытаний или эксплуатации системы. Следует документировать и расследо-

вать все инциденты. Это необходимо для определения причин возникновения инцидента (отказ системы, ошибка человека или ошибка наблюдений). Отказ[1)] элементов системы может привести к отклонению параметров функционирования системы от требуемых значений. Однако это не всегда приводит к полному прекращению выполнения всех функций системы, а может лишь ухудшить работу системы. Для измерений следует определить состояние системы, классифицируемое как отказ системы в целом.

5 Менеджмент надежности системы

5.1 Менеджмент надежности

Надежность является технической дисциплиной и основана на инженерных принципах и практике. *ГОСТ Р МЭК 60300-1* и *ГОСТ Р 51901.3* использованы в настоящем стандарте для построения стратегий менеджмента надежности и общего применения технических подходов для решения задач надежности и обеспечения надежности элементов. Кроме того, для достижения конкретных целей менеджмента введены процессы менеджмента надежности. Менеджмент надежности включает в себя планирование работ по проектированию, распределению ресурсов, определению задач надежности, мониторингу и обеспечению надежности, измерению результатов, анализу данных и постоянному улучшению. Деятельность в области надежности следует сочетать с действиями в области других технических дисциплин. Это позволяет улучшить результаты разработки проекта. Необходима отработка проекта для обеспечения рентабельного менеджмента проекта системы. Там, где это применимо, следует использовать анализ стоимости жизненного цикла для распределения ресурсов и оптимизации оценки стоимости проекта.

5.2 Обеспечение надежности системы при проектировании

Надежность является ключевым фактором при принятии решений в области управления проектом. Надежность влияет на стоимость реализации проекта. Деятельность в области надежности направлена на получение эффективных решений задач надежности при проектировании. Надежность оказывает большое влияние на результаты проектирования в отношении удовлетворения ожиданий потребителей. С инженерной точки зрения обеспечение надежности системы является важным вопросом, который требует полной интеграции разработки и проектирования с процессами принятия решений. Управление устареванием, оценка риска, принятие компромиссных технических решений, оценка стоимости жизненного цикла, координация аутсорсинга и цепи поставок являются некоторыми примерами деятельности при разработке системы.

Не все проекты предусматривают разработку абсолютно новой системы. Большая часть систем создана путем интеграции подсистем и применения приобретенных существующих объектов для реализации функций системы. В основном в разработке или совершенствовании системы участвует несколько разработчиков подсистем и субподрядчиков по снабжению и оказанию услуг для своевременного завершения работ по проектированию системы. В этой связи менеджмент проекта имеет важное значение для координации различных действий по разработке проекта. Проектирование системы с заданной надежностью может включать конкретные действия:

a) использование новых технологий;

b) разработка требований к надежности системы и ее подсистем;

c) оценка надежности приобретаемых составных частей для использования при обеспечении выполнения функций системы;

d) оценка возможностей поставщиков для выполнения требований надежности;

e) гарантии надежности для приемки системы.

Действия в области обеспечения надежности системы могут быть предусмотрены на любой стадии жизненного цикла системы. Решение некоторых задач надежности может потребовать специальных навыков и подготовки в области конкретных технических дисциплин, таких как разработка программного обеспечения, материально-технической поддержки и надежности человеческого фактора.

5.3 Учет требований проекта

Обеспечение надежности системы направлено на решение конкретных вопросов надежности системы. Учет требований проекта необходим для управления распределением доступных ресурсов и

[1)] См. 3.4.1 ГОСТ 27.002—2015.

выбора методов эффективного решения задач проектирования. Примеры действий по обеспечению надежности системы с учетом требований проекта:

a) бюджетное планирование распределения ресурсов надежности в соответствии с целями проекта;

b) оценка альтернативных технологий для приобретения высоконадежных комплектующих;

c) применение аутсорсинга при разработке подсистем в соответствии со строгими критериями требований к программному обеспечению, где это имеет решающее значение;

d) обучение в течение необходимого времени для получения достаточного опыта использования новых методов анализа надежности;

e) выбор субподрядчиков по обеспечению технического обслуживания критически важных систем с высокой готовностью без запланированных простоев.

Руководящие принципы учета требований проектирования описаны в *ГОСТ Р 51901.3*.

5.4 Мероприятия, гарантирующие обеспечение надежности

Мероприятия менеджмента надежности должны быть частью процесса менеджмента качества при проектировании системы. Это необходимо для обеспечения того, что все спланированные и систематические действия выполнены в соответствии с системой менеджмента качества и продемонстрировали по мере необходимости достаточную уверенность в том, что требования к качеству системы и приобретаемых объектов выполнены. Основные действия включают: планирование, распределение ответственности в технической и организационной сфере, верификацию результатов оценки надежности, валидацию данных о надежности системы, мониторинг результативности процесса менеджмента надежности, ведение записей об отказах и анализ данных для оперативных корректирующих и предупреждающих действий, документирование соответствующей информации о надежности и ведение протоколов испытаний для поддержки объективных свидетельств и анализа со стороны руководства для инициирования процесса улучшения. В *ГОСТ Р 51901.3* приведена дополнительная информация по выбору элементов программы надежности и задач обеспечения надежности системы.

6 Выполнение обеспечения надежности системы

6.1 Процесс обеспечения надежности

6.1.1 Цель процесса

Установление процесса обеспечения надежности имеет важное значение для успешного управления задачами проекта и координации деятельности. Процесс должен быть интегрирован в технические процессы для облегчения проектирования системы. Процесс обеспечения надежности при проектировании снабжает исходными данными основные точки принятия решений на этапах жизненного цикла системы для облегчения реализации проекта. Эти основные точки принятия решений возникают при завершении критических этапов выполнения проекта: идентификации рынка, разработки системы, реализации продукции, приемки, эксплуатации, модернизации и утилизации системы. Информация о надежности имеет в этих точках решающее значение для обоснования инвестиций.

6.1.2 Жизненный цикл системы и процессы

Отправная точка обеспечения надежности системы находится на самой ранней стадии жизненного цикла системы. На этой стадии жизненного цикла необходимо применять результативный процесс проектирования.

Описание стадий жизненного цикла системы можно рассматривать с точки зрения конструирования систем. Существуют также и другие описания жизненного цикла системы. В *ГОСТ Р 51901.3* стадии жизненного цикла объекта описаны с точки зрения управления проектом. В *ГОСТ Р 57193* приведено аналогичное описание стадий жизненного цикла системы с точки зрения информационных технологий и разработки программного обеспечения. Рекомендации настоящего стандарта основаны на концепции стадий жизненного цикла системы в соответствии с описанием, приведенным на рисунке 1. Завершение каждой стадии жизненного цикла системы является точкой перехода на другую стадию жизненного цикла, тогда как этапы проекта могут перекрываться (по решению руководства) для достижения основных целей бизнеса. Менеджмент риска в соответствии с *ГОСТ Р 51901.3* применяют на протяжении всего жизненного цикла системы.

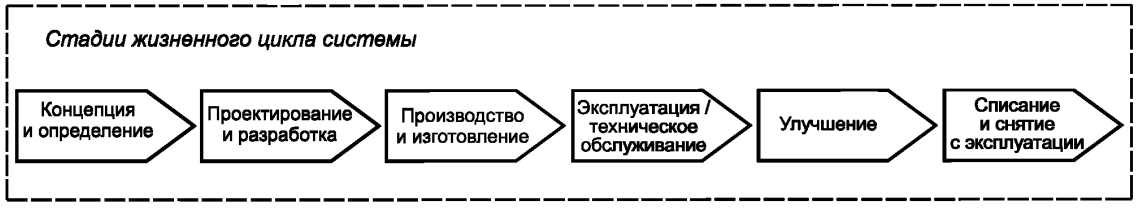

Рисунок 1 — Стадии жизненного цикла системы

Технические процессы проектирования состоят из последовательности действий, выполняемых на каждом этапе жизненного цикла, предназначенных для достижения целей функционирования и надежности системы. Обеспечение надежности системы не совершается в изоляции. Его выполняют совместно с другими техническими действиями (например, проектированием структуры системы) и вспомогательными мероприятиями (например, по обеспечению качества) для реализации функций системы в соответствии с их предполагаемым применением. В приложении А описана типовая последовательность процессов жизненного цикла системы.

Ключевыми действиями процесса жизненного цикла системы являются следующие:

a) определение требований, идентифицирующее требования пользователей и ограничения в области применения системы;

b) анализ требований, преобразующий представление пользователей о применении системы в технические требования к проектированию системы и включающий в себя разработку рабочего профиля, продолжительности эксплуатации и проекта системы в соответствии с ее целевой задачей;

c) разработка структуры, синтезирующей решение, удовлетворяющее требованиям к системе в соответствии со сценариями ее эксплуатации, с выделением функций аппаратного, программного обеспечения и человеческого фактора;

d) проектирование и оценка функций, определяющие практические средства реализации функций для облегчения поиска компромиссов и оптимизации;

e) создание системы проектной документации, охватывающей сведения о системе, включая данные о надежности проектируемой системы;

f) проектирование системы и подсистем, обеспечивающее выполнение требуемых функций системы и подсистем;

g) создание элементов системы и подсистем в форме аппаратного и программного обеспечения;

h) интеграция системы и подсистем в соответствии со структурой, предусмотренной проектом;

i) верификация системы, подтверждающая, что установленные требования к конструкции выполнены;

j) установка (монтаж), обеспечивающая системе возможность работать с требуемой производительностью в заданных условиях;

k) валидация и ввод в эксплуатацию, обеспечивающие объективные свидетельства того, что система соответствует функциональным требованиям;

l) эксплуатация системы, обеспечивающая оказание системой соответствующих услуг;

m) техническое обслуживание, обеспечивающее возможность эксплуатации системы;

n) улучшение функционирования системы, обеспечивающее ее дополнительными возможностями;

p) вывод из эксплуатации и демонтаж системы, завершающие существование системы.

6.1.3 Применение процесса на протяжении жизненного цикла системы

Процесс — это интегрированный набор взаимосвязанных и взаимодействующих действий, которые преобразуют входы в выходы. Процессы используют в качестве моделей для организации функций [например, системы менеджмента качества (СМК), менеджмента проекта)], коммерческих операций (например, соглашение о поставках, цепочка поставок), технического планирования и разработки (например, разработка продукции, оценка системы). В настоящем стандарте рассмотрены технические процессы обеспечения надежности систем.

На рисунке 2 приведен пример модели процесса. В контексте проектирования первичные входы обычно предоставляют собой набор требований или формализованных ожиданий потребителя. Выходы могут состоять из технических данных, описывающих желаемое решение, такое как спецификация, изготовление продукции или предоставление услуг. Существуют другие входы, связанные с процессом

контроля и реализации цели. Процесс трансформирует или конвертирует первичные входы в желаемые выходы. Это преобразование зависит от условий, устанавливаемых соответствующими механизмами и влияющими факторами. Некоторые влияющие факторы являются контролируемыми (например рабочие процедуры для активации процесса), другие могут быть неконтролируемыми, (например погодные условия или неожиданные климатические изменения). Для осуществления преобразований необходимы механизмы в виде методов и инструментов. Ниже приведена модель процесса, используемая для описания технических процессов в настоящем стандарте.

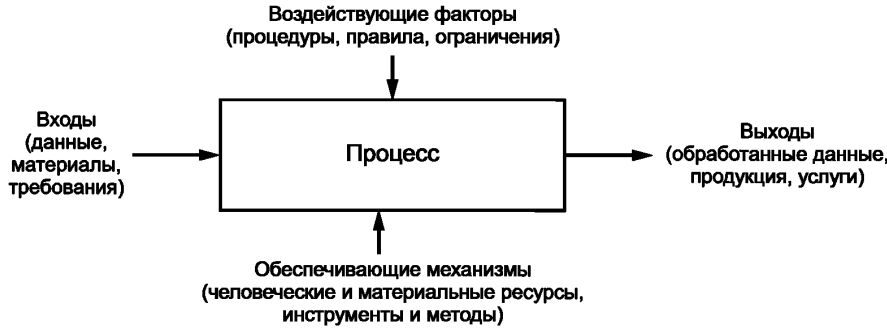

Рисунок 2 — Пример модели процесса

Технические процессы используют для двух целей:

a) выполнение конструкторских задач и проведение реконструкций в процессе создания концепции и разработки системы;

b) выполнение действий эксплуатации, технического обслуживания и распоряжения в отношении системы.

Применение технических процессов является одновременно рекурсивным и итеративным до достижения желаемого решения. Это относится ко всем стадиям жизненного цикла системы. Взаимодействие технических процессов не зависит от размера системы и ее структуры. Действия процесса, такие как определение требований, анализ требований и проектирование структуры системы являются техническими подходами «сверху вниз» для получения желаемого решения (т. е. декомпозиции системы вплоть до ее составляющих элементов); вместе с тем интеграция и верификация являются подходами «снизу вверх» к разработке конфигурации системы и валидации ее работоспособности (т. е. создание сначала элементов, а затем системы в целом). Переход от подхода «сверху вниз» к подходу «снизу вверх» происходит при завершении установки системы в начале ввода ее в эксплуатацию. Это называют моделью «V» в инженерной практике, она описана в *ГОСТ Р 57193.*

Примечание — Для получения дополнительной информации о модели «V» см. *ГОСТ Р ИСО/МЭК ТО 15271.*

В *ГОСТ Р ИСО/МЭК 12207* установлены границы процессов жизненного цикла программного обеспечения. Приведено описание процессов, действий и задач, которые могут быть применены при приобретении программного продукта или услуги и при установке, разработке, эксплуатации, техническом обслуживании и распоряжении программных продуктов. Этот документ может быть использован самостоятельно или вместе с *ГОСТ Р 57193.*

Типовые примеры применения процесса на каждой стадии жизненного цикла системы приведены в приложении А. Знание типа системы и среды ее применения имеет важное значение для использования процессов на стадиях жизненного цикла соответствующей системы и в соответствии с установленными требованиями к проекту.

6.2 Достижение надежности системы

6.2.1 Цель

Достижение надежности — это действие, направленное на выполнение цели в области надежности и отражает результаты успешного решения задачи. Действия, необходимые для достижения надеж-

ности системы, могут быть выполнены с помощью эффективных инженерных усилий, знаний и опыта, примененных на соответствующих стадиях жизненного цикла системы. Целью является обеспечение необходимого уровня надежности для каждой функции системы. Достижение надежности системы является важной целью проектирования, требует координации и демонстрации при приемке системы. Приемка системы обычно предусмотрена конкретным соглашением и представляет собой проверку выполнения требований потребителя. Конечной целью является удовлетворение ожиданий пользователей системы.

6.2.2 Критерии достижения надежности системы

Необходимой надежности системы достигают путем создания системы с соответствующими свойствами и показателями надежности. Критерии достижения надежности системы должны отражать:

a) четкое понимание целей работы системы;

b) глубокое понимание условий эксплуатации;

c) результативное выполнение принципов надежности в рабочей структуре;

d) условия использования;

e) применение соответствующих процессов при изготовлении системы;

f) использование знаний и опыта для экономически эффективного внедрения системы.

Эти критерии могут быть выполнены путем концентрации на ключевых факторах, влияющих на надежность системы. Важными критериями являются критерии, связанные с процессом применения системы и реализацией целей системы. Для пояснения значения надежности системы необходимы соответствующие обоснования. Критерии следует рассматривать при планировании и выполнении проекта. Пользователь должен адаптировать соответствующие действия в области надежности для обеспечения соответствия системы требованиям проекта с точки зрения жизненного цикла системы.

1) Политика менеджмента надежности. Данный критерий влияет на рабочую инфраструктуру, распределение соответствующих ресурсов, распределение ответственности и лидерство надежности проекта. Значение политики в области надежности отражает ориентацию потребителя на стратегию и обязательства, совместные усилия и систематический процессный подход для эффективного применения принципов менеджмента надежности, описанных с *ГОСТ Р МЭК 60300-1.* Политику менеджмента надежности в соответствии с *ГОСТ Р МЭК 60300-1* применяют ко всем техническим процессам, описанным в настоящем стандарте;

2) база знаний в области надежности. Данный критерий влияет на точность интерпретации потребностей рынка, адекватность соответствующей информации, необходимой для инициирования проекта, применение имеющихся стандартов, спецификаций и конкурентных факторов при заключении контрактов и обоснование надежности для представления объективных свидетельств. Значение базы знаний в области надежности определяет конкурентные преимущества и технологическое лидерство при работе с новыми вызовами в вопросах надежности систем;

3) структура конструкции. Данный критерий влияет на использование технологий применения системы, подбор оборудования, программного обеспечения и человеческих ресурсов для реализации функций системы, интеграции системы, ее работы, обеспечения улучшения и обновления системы. Проектирование структуры системы устанавливает взаимосвязанную и конструктивную схему интеграции и реализации системы. Это облегчает возможность улучшения, расширения возможностей экономически эффективной работы и обеспечения качества услуг. Соответствующее использование технологий позволяет находить компромиссные решения путем придания системе дополнительных свойств и расширения технических ограничений применения системы;

4) координация цепочки поставок. Данный критерий влияет на решения о закупках, аутсорсинге и привлечении субподрядчиков, верификацию и валидацию процедур и документов, процессы мониторинга и гарантии. Значимость менеджмента поставок основана на сотрудничестве покупателя и поставщика и обмене между ними соответствующей информацией в процессе закупок и приобретения. Цепочка поставок обеспечивает необходимую связь для отслеживания важной информации. Координация цепочки поставок способствует улучшению административного процесса, сокращению затрат на снабжение и стимулирует поставки качественных продукции и услуг;

5) вспомогательные системы. Данный критерий связан с использованием методов и инструментов, целесообразностью проектной производительности, потребностями в профессиональной подготовке, введением новой продукции и разработкой стратегий технического обслуживания и материально-технического обеспечения системы. Значение вспомогательных систем видят в улучшении процессов проектирования и поставки и эффективном использовании методов и средств ускорения решения про-

блем. Вспомогательные системы не всегда являются технически сложными, требующими специальных навыков для их понимания и использования. Некоторые из методологий представляют собой просто контрольные перечни и инструкции по принятию решений для операторов и специалистов по техническому обслуживанию при эксплуатации системы. Дополнительная информация о вспомогательных системах приведена в *ГОСТ Р 57193*;

б) обратная связь с потребителем и управление информацией. Данный критерий влияет на отношения потребителя в части удовлетворенности и лояльности, обеспечение потребителя качественными услугами, на точность записей об инцидентах, выбор данных для анализа, результативное выполнение корректирующих и предупреждающих действий, установление тенденции изменения производительности системы и хронологических записей о показателях надежности системы. Значение информации об обратной связи состоит в возможности установления тенденций в работе системы, определении областей, требующих внимания и обеспечении объективных свидетельств для верификации и валидации.

6.2.3 Методология обеспечения надежности системы

Выбор методов можно начать с совершенствования критериев и понимания их значения для обеспечения надежности системы. Цель заключается в использовании методов обеспечения надежности системы при ее создании. Обеспечение надежности направлено на придание соответствующей надежности функциям системы.

Существует два подхода к обеспечению надежности функций системы:

a) нисходящий подход к синтезу надежности системы на основе установленных требований к системе и рыночной информации для разработки структуры системы;

b) восходящий подход обеспечения надежности функций системы, основанный на правилах проектирования надежности, отказоустойчивости, снижения риска.

Оба подхода включают определение свойств надежности и определение значений соответствующих показателей. Свойства надежности являются основополагающими для оценки и достижения целевой надежности системы.

Свойства надежности, которые имеют отношение к функционированию системы, зависят от времени. Они могут быть количественно определены и выведены на основе данных наблюдений соответствующих инциденту. Примеры включают процент продолжительности работоспособного состояния системы, вероятность успешного выполнения функции системы в эксплуатации с продолжительностью работы без отказов для демонстрации безотказности и завершение восстановления системы в рамках запланированного простоя, чтобы показать целесообразность действий технического обслуживания.

Однако не все свойства надежности можно легко продемонстрировать в силу временны́х и стоимостных ограничений, технических ограничений или по другим причинам, связанным с проектом. Примеры включают сложные системы с высокой безотказностью, новые системы при ограниченных данных эксплуатации, программные системы для использования в новых условиях применения и некоторые приобретаемые объекты, без данных эксплуатации о безотказности. В этих случаях необходимо применять другие методы для обеспечения уверенности при использовании и гарантии надежности. Следует отметить, что данные наблюдений о надежности системы являются стохастическими. Они могут включать косвенные оценки других свойств, кроме оцениваемых, которые могут быть получены непосредственно на основе измерений. Типичные методы включают исследования безотказности, ремонтопригодности, моделирование тестовых случаев, модели зрелости и программы повышения надежности.

Количественные значения часто нуждаются в интерпретации. Определение интенсивности отказов по результатам измерений может быть непонятно без объяснения соответствующих условий. В то время как интенсивность отказов может быть использована (как показатель) для сопоставления альтернативных проектных решений, при этом использованные предположения крайне важны для объяснения и обоснования полученных результатов. Это позволяет применить статистические методы для определения предположительных и доверительных границ возможных рисков. В примере из бизнеса среднее время между отказами копировального аппарата может быть не слишком значимым для владельца бизнеса, но количество некачественных копий за месяц использования аппарата будет сказываться на финансовых потерях.

В приложении В приведены примеры применимых методов обеспечения надежности системы. Для выбора соответствующих методов необходимо знание рабочих функций системы и условий применения, описанных в приложении С. Для эффективного применения методов следует сосредоточиться на критических вопросах решения технических задач. Ограничения этих методов при их конкретном применении следует учитывать для правильной интерпретации результатов.

6.2.4 Реализация функций системы

Функции системы могут быть реализованы с использованием аппаратного и программного обеспечения, человеческого фактора или любой их комбинации, обеспечивающей выполнение целей функционирования системы. Ниже описаны общие вопросы, касающиеся выбора и применения этих элементов для успешного обеспечения надежности.

a) Аппаратное обеспечение представляет собой оборудование, широко используемое в конструкции системы. Оно может состоять из механических, электрических, электронных, оптических и других физических компонентов. Они используются в различных конфигурациях для реализации функций аппаратного обеспечения. Бóльшая часть электронной продукции включает в себя элементы аппаратного обеспечения, которые являются относительно изученными при применении. Правила разработки четко установлены. Электронная продукция демонстрирует работоспособность в контролируемых условиях процесса производства. Качество и надежность продукции могут быть установлены соответствующими программами гарантии. Также имеется достаточно большое количество баз данных об испытании и эксплуатации электронной продукции, включающей аппаратные средства, полезные для обеспечения безотказности системы. Однако некоторые виды продукции с активными электронными компонентами чувствительны к различным условиям применения. Физические свойства таких компонентов доминируют среди отказов элементов аппаратного обеспечения, а также причин феномена детской смертности. Конструкция, упаковка и проверка, соответствующие надлежащей безотказности, могут помочь значительно снизить количество отказов. Некоторые элементы аппаратного обеспечения могут изнашиваться в процессе эксплуатации или использования, в то время как другие могут иметь ограниченный срок хранения. Эти проблемы обеспечения безотказности могут быть решены путем осуществления профилактического планового технического обслуживания. Структура аппаратных систем является иерархической. Стратегия технического обслуживания может быть разработана собственными силами на основе функционального проектирования и представлять собой стратегию замены простейших сборочных элементов. Это облегчает техническое обслуживание конструкции и логистическое обеспечение системы и способствует улучшению показателей готовности системы;

b) программное обеспечение состоит из закодированных инструкций, компьютерных программ, установленных правил и процедур работы системы. Закодированные команды используются в программном обеспечении, осуществляющем управление выполнением функций системы. Программные коды трудно проверить на наличие ошибок кодирования без фактического выполнения компьютерных операций. Сбой программного обеспечения, приводящий к отказу системы, обусловлен активацией скрытой ошибки в программном обеспечении. Аккуратность при создании программного обеспечения необходима для минимизации возможного проявления непреднамеренных ошибок в разработке. Используемые подходы включают предотвращение отказов, устранение отказов и обеспечение отказоустойчивости. Они являются формализованными методами создания программного обеспечения. Хотя программное обеспечение не изнашивается, его функции могут ухудшаться вследствие введенных изменений. Поскольку программное обеспечение создается при участии человека, контроль за его созданием сосредоточен на условиях разработки программного обеспечения. Использование методологии «моделей зрелости» как основы для разработки программного обеспечения может быть способом обеспечения надежности функций программного обеспечения. Вопросы программного обеспечения и версии для его обновления должны быть под контролем процесса управления конфигурацией системы для поддержания совместимости функций и повышения надежности системы в эксплуатации;

c) человеческий фактор (взаимодействие человека с функционирующей системой) можно рассматривать как часть функций системы или как функции конечного пользователя системы. Роль человека в работе системы может быть полезна вследствие способности человека смягчать текущую ситуацию или управлять ею. Однако бóльшая часть промышленных инцидентов и изученных крупных аварий может быть следствием ошибок человека как первичной причины неисправности системы или нарушения ее работы. Системы, разработанные для работы человека или использующие труд человека, должны включать человеческий фактор в проект системы, чтобы минимизировать риск возникновения критических отказов, потери свойств, нарушения безопасности или появления угроз для безопасности. Надежность может быть обеспечена путем учета человеческого фактора в правилах проектирования и упрощения задач, выполняемых человеком при работе. Изучение человеческого фактора включает сбор междисциплинарной информации о возможностях и ограничениях человека для применений, включающих взаимодействия «человек—система». Инженерные аспекты состоят в применении информации о человеческом факторе при проектировании инструментов, машин, систем, задач, производственных заданий и окружающей среды для безопасного, комфортного и результативного использования чело-

веком. Обучение и образование человека являются важными обязательными требованиями для функционирования любой системы, требующей взаимодействия с человеком. Стандартизация в вопросах, связанных с человеческим фактором, облегчает интеграцию системы, повышает функциональную совместимость элементов системы и улучшает работоспособность и надежность в целом.

Бóльшая часть функций системы в существующей электронной продукции использует комбинацию программных и аппаратных элементов в конструкции системы. Они предлагают широкий спектр свойств конструкции для различных применений. Надежность функций системы обеспечивают включение правил разработки и использование установленных процессов при применении системы. Компромиссный вариант конструкции может быть найден путем комбинации соответствующих технологий, отвечающих установленным требованиям конкретного применения. Экономический эффект для массового производства может быть получен при использовании модульного принципа компоновки и стандартизации. Система может включать автоматизированные функции самоконтроля и повышения результативности работы в виде встроенных тестов или других схем мониторинга. Вмешательство человека в функции системы может быть обусловлено только требованиями безопасности и охраны или социальными и экономическими причинами. В приложении D приведены контрольные перечни для аппаратного обеспечения, программного обеспечения и человеческого фактора.

6.2.5 Способы определения достижения надежности системы

Существует три общих подхода для определения того, что целевая надежность системы достигнута. Они служат разным целям и обладают различной точностью. На практике обычно используют комбинацию этих подходов:

a) демонстрация — работа системы в реальных условиях в течение времени, превышающего запланированное, что обеспечивает демонстрацию надежности работы системы. Типичные примеры включают:

- хронологию показателей надежности системы в условиях эксплуатации;
- документальную демонстрацию надежности;
- показатели готовности в течение гарантийного периода;

b) логический вывод состоит в применении статистических методов с использованием данных наблюдений соответствующих функций системы на основе установленных критериев и предположений, позволяющих перейти к числовым значениям, характеризующим свойства системы (показатели надежности, характеристики). Типичные примеры включают:

- прогнозирование состояния системы с заданной конфигурацией;
- применение моделирования;
- применение моделей зрелости;
- верификация испытаний системы;

c) прогрессивные свидетельства представляют собой объективные доказательства, полученные в контрольных точках разработки проекта на основе аргументов. Типичные примеры включают:

- безотказность и техническое обслуживание;
- программу повышения надежности.

6.2.6 Объективные свидетельства достижения надежности системы

Ниже приведены ключевые утверждения о характеристиках надежности системы для использования в качестве объективных свидетельств при приемке системы и продукции на этапах жизненного цикла системы. Для аудита и договорных целей объективные свидетельства необходимо документировать и заверять.

a) Утверждение о свойствах надежности и условиях эксплуатации системы, отражающее ожидания пользователей в коммерческой спецификации или предложении, основанном на информации об исследовании рынка. Это утверждение обеспечивает информацию для начала планирования проекта и разработки требований к надежности системы.

b) Заявление о характеристиках работы системы в спецификации надежности системы. Это заявление обеспечивает информацию для установления цели проектирования в области надежности и структуры системы.

c) Заявление о характеристиках безотказности и ремонтопригодности для каждой функции системы в требованиях функционального проектирования. Это заявление обеспечивает информацию для выбора технологии, принятия решений об изготовлении или приобретении комплектующих и установления требований к закупкам.

d) Заявление о характеристиках надежности и ремонтопригодности системы при эксплуатации и техническом обслуживании. Это заявление обеспечивает информацию для планирования и ло-

гистического обеспечения, контрактного технического обслуживания и специальных потребностей в обучении.

e) Заявление о соответствующих характеристиках и показателях надежности для приемки продукции, верификации соответствия и валидации результатов работы системы. Это заявление формирует основу для выполнения контрактных соглашений в соответствие с требованиями контракта на поставку продукции.

f) Все отчеты о надежности проекта, содержащие данные анализа надежности, статус испытаний и результаты демонстрации. Эти данные обеспечивают информацию для анализа проекта, изменений проекта, обновления процедур, корректирующих и предупреждающих действий для улучшения проекта.

6.3 Оценка надежности системы

6.3.1 Цель оценки надежности системы

Оценкой является оценка статуса или результатов конкретных действий или проблем в области надежности. Цель оценки состоит в определении способа решения проблемы. Результаты используют для объяснения и обоснования рекомендуемых действий. Процесс оценки облегчает выявление возможных альтернатив или вариантов решения проблемы. Это способствует выбору компромиссных проектных решений и предпочтительной закупаемой продукции. Оценка надежности системы должна соответствовать потребностям конкретного проекта и улучшению процесса.

6.3.2 Виды оценок

Оценка может быть объективной или субъективной. Объективная оценка представляет собой результаты непосредственных измерений объекта. Субъективная оценка присваивает значение свойству, особенности или качеству. Например, оценив качество функции программного обеспечения при применении системы, можно догадаться, как программное обеспечение разработано. Рассмотрение процесса проектирования формирует субъективное мнение об оценке. Цель — обеспечить уверенность пользователя программного обеспечения в его адекватности при применении. Не может быть уверенности в оценке, до тех пор, пока не будет запущено программное обеспечение для определения его качества в реальной работе. Это обеспечивает демонстрацию объективных свидетельств. В инженерной практике используют объективные и субъективные оценки, которые дополняют друг друга.

Ниже приведены основные цели проекта, связанные с оценкой надежности системы в основных точках принятия решения на стадиях жизненного цикла системы.

a) Идентификация рынка — определение потребностей рынка для обоснования инвестиций в разработку новой системы или модернизацию существующей системы для обеспечения конкурентности системы. Анализ рынка важен для обоснования основных инвестиций, включающих обязательства в отношении ресурсов. Действия по разработке системы включают идентификацию возможностей и ресурсов, оценку новой технологии для реального применения, анализ конкурентоспособности и ожиданий пользователя системы, определение степени обеспечения технического обслуживания, необходимого для поддержки и эксплуатации новой или усовершенствованной системы, а также определения ограничений по времени эксплуатации и стоимости при выходе системы на рынок, обеспечение соблюдения обязательных требований и определения экологических последствий внедрения системы. Первоначальную структуру и конфигурацию системы следует рассмотреть на соответствие сценариям эксплуатации системы. Стоимость жизненного цикла системы должна быть проверена на предмет возврата инвестиций. Ключевые оценки надежности для идентификации рынка включают в себя:

- прогнозирование надежности системы для удовлетворения ожидаемых потребностей рынка;
- оценку новых технологий, подходящих для применения в системе, влияющих на показатели надежности;
- идентификацию критических вопросов надежности, влияющих на удобство обслуживания и работоспособность системы;
- оценки надежности продукции потенциальных поставщиков и субподрядчиков;
- гарантию технического обслуживания, готовности и безопасности до тех пор, пока система не будет выведена из эксплуатации.

b) Проектирование и разработка системы — создание конструкции системы и оценка альтернативных вариантов. После выбора конструкции следует разработка системы. Это является одним из основных объектов инвестиций капитала и ресурсов. Действия по разработке системы включают анализ требований, конструирование конфигурации, проектирование и оценку технологии, субподрядные

работы и выбор поставщиков, изготовление и интеграцию системы, квалификационные испытания и верификацию, установку и транспортирование. Ключевыми оценками надежности на стадии проектирования и разработки являются:

- оценка функций системы, влияющих на показатели надежности;
- оценка структуры системы для оптимизации конфигурации системы с точки зрения безотказности;
- оценка доступности технического обслуживания;
- моделирование и оценка показателей готовности для определения критических неисправностей системы, уменьшения количества отказов и потребностей сопровождения при эксплуатации;
- верификация и анализ проблем безотказности для выбора корректирующих действий;
- оценка программ надежности поставщиков и субподрядчиков;
- оценка производства приобретаемой продукции, влияющей на повышение безотказности;
- оценки гарантийных стимулов и требований логистической поддержки при обеспечении безотказности.

c) Изготовление и производство системы. Целью является выполнение решений о приобретении и разработке элементов подсистем и выполнение обязательств по выделению ресурсов для изготовления и интеграции системы. Ключевыми оценками надежности на стадии изготовления и производства являются:

- оценка элементов системы и приобретаемой продукции на соответствие требованиям надежности для интеграции подсистем;
- оценка соответствия подсистем требованиям надежности;
- оценка процесса обеспечения качества;
- оценка результатов испытаний подсистем для интеграции системы;
- оценка результатов испытаний системы для подготовки к приемке системы.

d) Приемка системы в эксплуатацию. Целью является демонстрация потребителю готовности системы для приемки. Приемка системы означает передачу ответственности за эксплуатацию системы потребителю. С этого момента начинается гарантийный период (система отвечает ожиданиям конечных пользователей). Ключевыми оценками надежности на стадии приемки системы являются:

- оценка работы системы путем наблюдения за эксплуатацией системы и ведения записей об инцидентах;
- оценка потребностей в подготовке кадров и компетентности операторов и специалистов по техническому обслуживанию у потребителя;
- создание координационного центра для сбора данных и анализа данных об инцидентах для определения изменений показателей надежности и критичности неисправностей системы, требующих немедленных корректирующих действий;
- оценка технического обслуживания системы в эксплуатации и эффективности логистического обеспечения;
- выполнение процедур управления изменениями проекта и управления конфигурацией.

e) Улучшение системы. Целью является обоснование инвестиций для улучшения и модернизации существующей системы. Эти действия включают действия, аналогичные мероприятиям по проектированию и разработке новой системы и модернизации части системы. Для обеспечения функциональной совместимости и возможности улучшения работы системы следует рассмотреть вопросы преемственности существующей системы. Ключевыми оценками надежности системы на стадии улучшения системы являются:

- анализ стоимости и получаемых преимуществ для выполнения изменений;
- оценка влияния на показатели надежности изменений, связанных с добавлением новых свойств;
- реакция потребителей на предлагаемые изменения;
- оценка риска и значения улучшений.

f) Вывод системы из обращения или эксплуатации. Целью является изъятие системы из эксплуатации. Ключевыми оценками надежности на стадии вывода из эксплуатации являются:

- оценка стоимости вывода системы из эксплуатации;
- оценка выполнения обязательных и экологических требований при выводе системы из эксплуатации.

6.3.3 Методология оценки надежности системы

Методология оценки надежности связана с вопросами, касающимися процессов, подходов и стратегий.

Методология оценки надежности охватывает два важных процесса верификации и валидации:

a) верификация — процесс подтверждения результатов оценки. Верификацию следует проводить для поддержки решений в главных точках принятия решений на каждой стадии жизненного цикла системы;

b) валидация — процесс, обеспечивающий объективные свидетельства того, что система соответствует фактическим требованиям и ожиданиям пользователя.

Способы оценки часто являются уникальными с учетом различных ситуаций реализации проекта. Они включают в себя сочетание следующих подходов:

1) аналитического подхода включающего в себя такие действия, как анализ проектирования, моделирование системы, проверка соответствия стандартам и оценка соответствия спецификации;

2) экспериментального подхода включающего в себя такие действия, как испытания и техническая оценка функций системы, сборочных единиц приобретаемой продукции, интеграции подсистем, и приемка реальной системы;

3) консультативного подхода, включающего в себя такие действия, как анализ экспертов, использование наилучшей промышленной практики, консультации с поставщиками об информации о продукции, опрос потребителей и обратная связь с пользователями, участие в цепочке поставок, разработка инфраструктуры и улучшение;

4) договорного подхода, включающего в себя такие действия, как установление приемлемых границ риска для воздействия на окружающую среду при эксплуатации системы, для разработки продукции в конкретных регионах, переработки побочных продуктов и утилизации отходов, разработка экономических стимулов и социальных преимуществ в контрактных соглашениях и соблюдение изменений обязательных требований.

Стратегии требований оценки должны быть направлены на два основных аспекта проектирования надежности систем:

a) применение — аспект относится к соответствию специальным применениям проекта, отвечающим договорным требованиям. Необходимые действия направлены на оценку и анализ надежности системы в главных точках принятия решений жизненного цикла системы. Методы, разработанные для оценки, как правило, используют для валидации приобретаемой продукции и валидации системы или подсистем;

b) технология — аспект связан с оценкой технологий в стратегии проектирования и схемами сопровождения системы для облегчения обеспечения надежности работы системы. Основные оценки направлены на оценку технологических приемов, которые могут быть использованы при проектировании системы и определение жизнеспособности вспомогательных систем непрерывного сопровождения эксплуатации системы. Вопросы, касающиеся оценки и устаревания технологий, должны быть частью стратегии определения оценок.

6.3.4 Значимость и последствия оценки

Оценка является предпосылкой и ключевым входом для принятия решений по проекту. Усилия по оценке должны быть рациональными и оправданными. Решения, принимаемые на основе оценок, должны быть выполнены в течение разумных сроков для достижения ожидаемого значения или преимуществ проекта. Это создаст необходимую уверенность в поддержке решений, принимаемых при проектировании. Следующие ключевые вопросы, которые показывают значение оценки, приведены для иллюстрации. Приведены типичные примеры, подчеркивающие их существенное влияние на выходы проекта:

a) время выполнения оценки важно для получения значимых результатов. Значимость оценки существенно снижается, если результаты оценки недоступны во время принятия главных решений. Например, прогнозирование безотказности, проведенное в процессе проектирования системы, может обеспечить важное понимание для отбора технологии, проектирования структуры, определения конфигурации и выбора элементов и компонентов системы для выполнения функций системы. Прогнозирование после завершения разработки проекта имеет ограниченное значение, если система скомпонована и готова к изготовлению;

b) обоснование стоимости оценки до начала ее определения целесообразно для планирования и результативного менеджмента проекта. Например, процесс PDCA в системах менеджмента качества, как правило, используют в качестве основы для планирования деятельности по определению оценок. Анализ инвестиций, связанный с оценкой, имеет решающее значение для обоснования крупных капитальных затрат и новых приобретений;

c) обеспечение поддержки инфраструктуры необходимо для выполнения методов оценки. Оно может включать изменение технических и организационных процедур для выполнения которых требуются время и усилия. Например, любая организация стремится к переходу от процесса модели зрелости программного обеспечения к процессу интеграции модели зрелости программного обеспечения. Для достижения признанного статуса и сертификации производства необходима корректировка технических ресурсов и методов управления;

d) планирование непредвиденных расходов помогает избежать неожиданных результатов проектирования или незапланированных задержек. Это может оказать влияние на распределение ресурсов, перераспределение работы, цепочки поставок, поставки продукции поставщиками и влияет на выполнение обязательств по вводу в эксплуатацию и приемке системы потребителем. Например, в основных точках принятия решений должны быть предусмотрены планы непредвиденных расходов, как часть процесса оценки, таких как проведение идентификации альтернативных поставщиков в случае нарушений, допущенных поставщиками, проведение технических проверок работ на критических проектах для удовлетворения целей поставок и изучение способов устойчивого финансирования капитальных вложений.

6.4 Измерение надежности системы

6.4.1 Цель

С инженерной точки зрения измерение надежности системы представляет собой процесс, при выполнении которого показателю надежности присваивают количественное значение. Количественное значение выводят на основе наблюдаемых данных о вре́менных показателях и количестве появлений инцидентов, что характеризует надежность системы. Процесс оценки включает в себя следующие действия:

a) определение типа и цели измерений в соответствии с контрактом, при эксплуатации или в конкретных условиях, таких как оценка продукции для количественного определения свойств надежности;

b) определение соответствующих данных и особенностей источников, данных для измерений;

c) использование эффективных вспомогательных систем, облегчающих процесс измерения, например, применение систем сбора данных, записей об отказах, результатах анализа и корректирующих действий, вопросников для обследования или других приемов;

d) интерпретация результатов измерений для установления тенденций изменения показателей работы, определение критических вопросов и рекомендуемых действий управления с объяснением и обоснованием;

e) документирование результатов измерений для хранения записей и объективных свидетельств аудита качества;

f) в [1] установлен процесс измерений, применимый к проектированию систем и программного обеспечения.

6.4.2 Классификации

Существует четыре общих класса измерений надежности для удовлетворения потребностей конкретного проекта.

a) Измерения присущих системе свойств надежности. Целью измерения является присвоение значения, характеризующего присущие системе свойства надежности. Этот класс измерений полезен для сопоставления свойств надежности проектов системы с различной структурой и конфигурацией. Процесс измерения выполняют на стадии концепции и определения системы для определения показателей надежности альтернативных вариантов. Цель направлена на обеспечение свидетельств возможности соответствия системы целям в области надежности для контрактных предложений или запросов. Количественные значения могут быть установлены в виде вероятности работоспособного состояния, среднего времени между отказами, ресурса или интенсивности отказов, которые количественно характеризуют готовность или безотказность системы. Измерения обычно выполняют методами прогнозирования в соответствии с *ГОСТ Р 27.301.*

b) Измерения надежности системы для оценки работы и эксплуатации. Целью измерений является присвоение количественного значения показателю надежности системы в эксплуатации. Этот класс измерений полезен для оценки надежности на стадии проектирования и разработки, когда приобретаемую продукцию и подсистемы испытывают для проверки адекватности работы. Эти измерения используют на стадии эксплуатации и технического обслуживания системы для определения соответствия установленным целям эксплуатации и обеспечения надежности. Процесс измерений проводят путем

испытаний приобретаемой продукции, подсистем и интегрированной системы для верификации и валидации работы системы и отслеживания ее состояния в эксплуатации. Данными измерений являются данные квалификационных испытаний продукции, результаты испытаний поставщиками подсистем, данные приемочных испытаний, записи и отчеты об эксплуатации и инцидентах. Числовые значения могут быть представлены в виде вероятности безотказной работы, вероятности отказа, продолжительности безотказной работы (наработки до первого отказа), ресурса, процента безотказной работы, частоты и продолжительности простоев.

c) Измерения надежности системы для улучшения ее работы. Целью является присвоение значений для количественного и качественного определения степени удовлетворенности потребителя или для определения значимости для потребителя улучшения системы. Это косвенные измерения, которые помогают определить влияние существенных свойств надежности на работу системы. Этот класс измерений направлен на поиск прямой и обратной связи с потребителем о работе системы или на определение значения обслуживания системы на этапе эксплуатации и технического обслуживания. Процесс измерений проводят посредством обследования пользователей, аудита, оценки рыночной цены, прямых контактов и диалога с потребителями и поставщиками. Обследования удовлетворенности потребителей направлены на выявление вопросов, волнующих потребителя. Разработку функций качества, как правило, используют для оценки работы системы, определения потребностей потребителей их преобразования в соответствующие технические требования и определения последующих действий в соответствии с этими требованиями. Значения могут быть установлены по шкале от 1 до 5 включительно для обозначения рейтингов от «плохо» до «превосходно».

d) Измерения надежности системы для определения экспозиции риска. Целью измерений является назначение количественного значения экспозиции риска, когда систему используют для охраны и безопасности. Это косвенное измерение для определения критичности свойств надежности, влияющих на работу функций системы. Этот класс измерений выполняют на стадии концепции и определение системы для выявления критических функций и элементов системы для конкретного применения системы или выполнения системой установленной задачи. Процесс оценки включает в себя определение вреда или угрозы, путем назначения их значимости и частоты возникновения. Классификация рисков может быть установлена качественно путем классификации событий, на катастрофические, критические, крупные, мелкие или незначительные. Значения вероятности присваивают для указания серьезности ситуации, например, один критический отказ за 10 лет. В *ГОСТ Р 51901.1* установлены методы оценки риска, влияющего на надежность работы системы. Подобный метод использован в стандартах серии *ГОСТ Р МЭК 61508* (см. также *ГОСТ IEC 61508-3*) по уровням безопасности для ранжирования функций безопасности (см. также *ГОСТ Р МЭК 61508-1*).

6.4.3 Источники измерений

Измерения показателей надежности системы могут быть выполнены путем испытания при моделировании условий эксплуатации, когда могут быть собраны соответствующие данные, или в реальной эксплуатации. Показатели надежности системы также можно оценивать с помощью прогнозирования на основе хронологических данных эксплуатации аналогичных систем или сведений из баз данных надежности при знании конфигурации системы и функций, составляющих систему элементов.

Данные измерений, связанные с надежностью, также могут быть получены из других источников, таких как программы испытаний поставщиков, данных технического обслуживания, сведений о гарантийных обязательствах и опросов потребителей. Важно, чтобы достоверность данных, используемых для оценки надежности, была проверена.

6.4.4 Вспомогательные системы

Достоверность данных для измерения надежности имеет важное значение для обеспечения точности, убедительности и непротиворечивости процесса получения и сбора данных. Это гарантирует, что соответствующие данные правильно использованы при анализе данных, что позволяет правильно интерпретировать результаты анализа. Проект системы сбора данных и ее форматы должны быть простыми и понятными для сбора соответствующей информации. Использование записей автоматизированных баз данных и доступ к интерактивной веб-информации повышает целесообразность применения системы сбора данных. Существуют различные, используемые в инженерной практике системы экономически эффективного сбора данных и облегчения измерений надежности. Эти системы являются неотъемлемой частью инфраструктуры системы менеджмента надежности. В зависимости от их конкретных функций эти системы могут быть классифицированы как вспомогательные системы для облегчения разработки надежности. Типичные вспомогательные системы, как правило, используют для сбора данных, записей об инцидентах, анализа проблем и корректирующих действий. Они включают в себя:

a) записи об отказах, информацию об анализе и корректирующих действиях, в том числе информацию о несоответствиях и отказах при испытаниях в процессе разработки, испытаний и интеграции системы;

b) данные об испытаниях приобретаемых систем для выявления аномалий при производстве для отслеживания темпов выхода продукции, выявления проблем и анализа причинно-следственных связей во время сборки продукции;

c) записи об инцидентах при эксплуатации системы, в том числе об инцидентах, влияющих на непрерывную работу системы, записи о действиях по техническому обслуживанию, критичности инцидента и отчет последующих запросов поддержки и времени, необходимого для устранения инцидента;

d) данные системы обеспечения запасными частями, в том числе данные о расходовании запасных частей и времени, необходимом для пополнения набора запасных частей, распределении запасных частей и о переустройстве запасов;

e) информацию системы обратной связи, в том числе жалобы пользователей, проблемы поставщиков и предложения сотрудников по улучшению инфраструктуры, стратегического планирования и решению проблем, которые повышают ценность проектов и менеджмента организаций.

6.4.5 Интерпретация

Правильная интерпретация результатов измерений имеет важное значение для оперативных корректирующих и предупреждающих действий и поддержки эффективной эксплуатации системы. В следующих примерах показано важное значение данных измерений или анализа после расшифровки и интерпретации для последующих действий:

a) приобретаемые и собранные данные должны соответствовать требованиям проекта. Для этого необходимо надлежащее планирование и разработка планов экспериментов. Для получения данных необходимы время и усилия. Если данные не могут быть использованы для решения текущих задач, то их не следует собирать. Цели процесса измерений должны быть четко определены. Например, сбор данных об эксплуатации старых систем, разработанных много лет назад, больше не изготавливаемых и не обслуживаемых, не слишком полезен для проектирования новой системы, использующей другие технологии;

b) преобразование измерений и интерпретация результатов должны содержать логические выводы для рекомендуемых действий. Данные измерений и собранная информация должны допускать проведение дальнейшего анализа, если это необходимо, для поддержки основополагающих обоснований или аргументов при принятии логических решений по обоснованию рекомендуемых действий. Следует отметить, что различная интерпретация измерений надежности может привести к различному пониманию при принятии решений. Например, коэффициент готовности 99,9997 % системы коммутации может быть подходящим для использования при вычислении вероятности функций системы, но было бы сложно разработать соответствующую схему демонстрации готовности системы;

c) при определении проблем надежности необходимо учитывать критичность, что способствует выявлению опасных ситуаций. Такие проблемы, обычно возникают в ситуациях, которые могут вызвать значительные угрозы безопасности без оперативного решения. Эти вопросы надежности могут включать аспекты, касающиеся ответственности и экспозиции риска, если они неправильно оценены в момент их возникновения. Эксплуатация система следует установленным процедурам. Инциденты системы фиксируют в соответствии с оценкой их критичности. Некоторые важнейшие вопросы должны быть решены немедленно или в течение ограниченного периода времени. Другие не критичные вопросы могут быть отложены на более позднее время или до модернизации системы. Например, модификация конструкции системы при ее эксплуатации для устранения вре́менной проблемы без надлежащего выполнения процедуры изменения конструкции может создать неизвестные долгосрочные опасности. Вре́менные мелкие изменения программного обеспечения для устранения локализованной проблемы без тщательного расследования могут привести к нарушению безопасности или работы системы в целом. Конструкция системы может включать средства, обеспечивающие отказоустойчивость. Если такие функции были отключены при введении вре́менных изменений без надлежащего разрешения, то система не защищена. Процесс интерпретации должен выявлять и предупреждать появление таких проблем, чтобы избежать повторения подобных инцидентов. Предупреждающие знаки и этикетки, размещенные в надлежащих местах, могут привлечь внимание.

Приложение А
(справочное)

Процессы жизненного цикла системы и их применение

А.1 Процессы жизненного цикла системы

А.1.1 Описание процессов жизненного цикла системы

На рисунке А.1 представлена логическая последовательность действий, применимых на каждой стадии жизненного цикла для обеспечения надежности системы при проектировании.

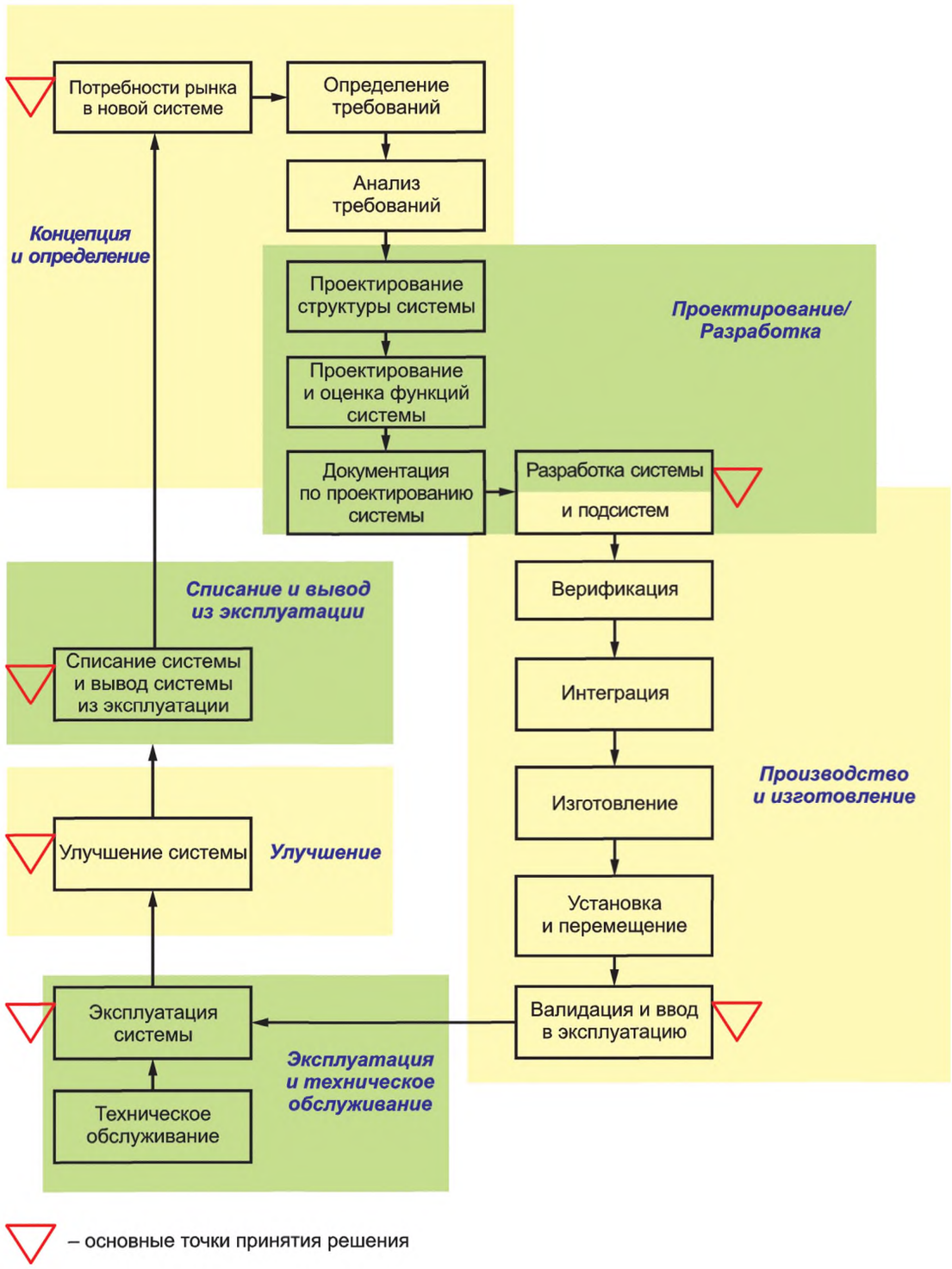

Рисунок А.1 — Процессы жизненного цикла системы

Первые три стадии жизненного цикла системы, т.е. концепция и определение, проектирование и разработка, производство и изготовление до перехода к стадии эксплуатации и технического обслуживания, накладываются друг на друга из-за повторения процессов. Это указывает на необходимость обеспечения непрерывности работы процесса в зависимости от потребностей проекта. Степень инженерных усилий при произвольно определенных границах смежных стадий зависит от сроков выполнения проекта и координации деятельности. На этих стадиях получают достаточно информации о системе для поддержки процесса принятия технических и бизнес-решений. Ниже приведено краткое описание каждой стадии жизненного цикла системы:

a) на стадии концепции и определения идентифицируют потребности рынка, определяют условия и срок эксплуатации системы, предварительные требования к системе и соответствие возможных проектных решений техническим требованиям производства (изготовления) системы. Выбор вариантов конструкции основан на анализе риска, оценке воздействий и практических инженерных подходах. Процесс деятельности включает определение требований, анализ требований, проектирование структуры и функций системы, оценку функций для обеспечения выполнения спецификаций системы в целом;

b) на стадии проектирования и разработки планируют и выполняют выбранные проектные решения для реализации функций системы. Это трансформируется в соответствующие действия по разработке системы, включая инженерное моделирование, создание опытного образца, оценку риска, идентификацию интерфейсов системы и элементов подсистем. Для верификации функциональной совместимости системы с внешними условиями проводят систематическую оценку функций системы, это позволяет выполнить валидацию конечной конфигурации системы. Планирование технического обслуживания, доступность технического обслуживания, процедуры эксплуатации и гарантии, а также поддержка процессов должны быть установлены до изготовления системы;

c) на стадии производства и изготовления принимают решения по приобретению и разработке элементов подсистем. В процессе производства выполняют такие действия, как применение технологий, изготовление, упаковка и поставка для обеспечения трансформации проекта системы в конкретную продукцию или элементы подсистемы. Изготовленная продукция или элементы могут представлять собой сочетание аппаратных и программных функций. Изготовление включает в себя такие действия, как интеграция функций системы, верификация подсистем и установка системы. Процедуры приемки системы должны быть разработаны вместе с потребителем, для испытаний системы в реальных условиях эксплуатации до ввода системы в эксплуатацию. Валидация должна быть частью испытаний для представления объективных свидетельств соответствия системы установленным требованиям. Следует отметить, что верификация и валидация являются действиями, которые выполняют на каждой стадии жизненного цикла и не только при интеграции системы, как показано на рисунке 2;

d) на стадии эксплуатации и технического обслуживания осуществляют доставку, введение системы в действие и обеспечение технического обслуживания при эксплуатации системы. Процесс включает в себя деятельность по эксплуатации и техническому обслуживанию системы в соответствии с требованиями к эксплуатации системы, подготовку операторов и персонала по техническому обслуживанию для обеспечения необходимых навыков компетентности, взаимодействие с потребителем, ведение записей о работе системы и записей об инцидентах и отказах для своевременного выполнения корректирующих и предупреждающих действий. Работу системы следует контролировать и проверять на регулярной основе, чтобы гарантировать, что безотказность и качество обслуживаемых объектов соответствуют требованиям;

e) стадия улучшения предусматривает улучшение работы системы с дополнением свойств, обеспечивающих повышение спроса пользователей на систему. Действия процесса включают улучшение программного обеспечения, дополнение оборудования, повышение навыков персонала, упрощение процедур для повышения эффективности эксплуатации системы, управление устареванием, изменение организационной структуры для повышения целесообразности и значимости системы для потребителя;

f) на стадии списания и вывода из эксплуатации система завершает существование. После прекращения работы системы для потребителя система может быть разобрана, перемещена для другого использования или утилизирована, если это возможно без ущерба для окружающей среды. Для сложных систем следует установить стратегию их вывода из эксплуатации, чтобы формализовать планирование и выполнение вывода из эксплуатации в соответствии с обязательными требованиями. Для потребительских товаров могут существовать обязательные правила относительно возврата и повторного использования или утилизации продукции.

А.1.2 Действия процесса на стадиях жизненного цикла системы

На рисунке 1 показана связь действий процесса на стадиях жизненного цикла системы. Основные точки принятия решений указывают начало и конец действий процесса на каждой стадии, где должны быть обеспечены ресурсы для продвижения технического процесса. Соответствующие данные о действиях процесса записывают. Записи обеспечивают необходимую информацию для анализа стоимости жизненного цикла, оценки риска и поддержки принятия технических и бизнес-решений.

Соответствующие данные включают в себя основные входы, необходимые для инициирования деятельности процесса на каждой стадии, основные действия в области надежности должны быть выполнены, соответствующие влияющие факторы рассмотрены и получены результаты. Когда это возможно, должны быть указаны приоритет и воздействие, имеющие отношение к действиям процесса. Это обеспечивает полезную информацию для оценки риска и стоимости жизненного цикла. При необходимости должны быть определены используемые технические подходы и инженерные методы.

А.2 Примеры инженерного применения процесса

А.2.1 Процесс на стадии концепции и определения системы

Входы:

- требования, потребности и пожелания потребителей;
- обязательные требования, относящиеся к здоровью, безопасности и экологии;
- политика компании при принятии решений;
- данные исследования рынка и конкуренции.

Таблица А.2.1 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Определение требований	
Определение потребителей системы, способов и продолжительности ее использования. Определение условий применения системы. Определение ограничений, связанных с возможными решениями системы. Определение вопросов наследия, связанных с совместимостью с существующими системами. Создание рабочего профиля системы. Документирование спецификации системы. Определение графиков и цели поставки. Получение откликов потребителей (запрос предложений), если применимо	Определение потребителей в области надежности, связанных с применением системы. Определение готовности системы и приемлемых для потребителей простоев. Определение технологических ограничений, связанных с областью применения системы и степенью достижения целей в области надежности. Получение хронологических знаний об эксплуатации существующих или аналогичных систем (если они доступны)
Анализ требований	
Определение границ системы, рабочих функций и характеристик по набору определенных требований системы. Оценка выявленных ограничений, влияющих на структуру проекта. Определение технических подходов и возможности изготовления системы. Определение технических и качественных мер, оценки вспомогательных систем. Определение возможности нести ответственность за работу системы. Определение потенциальных партнеров и требований к поставщикам	Определение сценариев эксплуатации для оценки надежности. Определение отказов системы и границ деградации. Определение ее работы экспозиции риска и критичности отказов системы. Определение количества персонала для технического обслуживания и существующего уровня их квалификации. Анализ структуры системы и распределения функций системы. Анализ готовности системы, обусловленной конфигурацией конструкции. Выполнение анализа дерева неисправностей для определения критических областей, требующих внимания при проектировании. Выполнение анализа видов, последствий и критичности отказов на уровне системы для поддержки и обоснования альтернативных вариантов проекта. Определение оценки готовности системы и стоимости компромиссов, влияющих на варианты проекта. Определение методов оценки надежности

Окончание таблицы А.2.1

Ключевые действия процесса	Действия, связанные с надежностью
Проектирование структуры	
Определение подходящих вариантов логической структуры проекта. Установление конфигурации системы. Распределение функций системы. Установление критериев проектирования и интерфейсов. Принятие решения об изготовлении или приобретении функций системы. Выбор технологий проектирования аппаратного и программного обеспечения для реализации функций. Принятие решения о соответствии системы установленным требованиям. Установление средств верификации и интеграции функций системы	Установление плана оценки надежности. Распределение готовности по функциям системы. Определение критериев отказа функций системы. Определение оценок безотказности каждой отдельной функции и при необходимости предложение альтернативных вариантов проекта. Определение критических функций, требующих внимания. Установление критерия технического обслуживания для проекта. Установление тестируемости функций системы для диагностики и рекомендации по действиям технического обслуживания
Проектирование и оценка функций	
Формализация процесса проектирования функций. Определение сочетания аппаратных и программных элементов для каждой функции проекта. Включение функций тестирования для проверки работоспособности. Установление критериев проектирования человеческого фактора. Установление экологических критериев проектирования. Установление эргономических критериев проектирования. Установление критериев проектирования электромагнитной совместимости. Установление критериев проектирования безопасности и надежности. Установление правил проектирования аппаратного обеспечения Установление схем зрелости программного обеспечения при проектировании. Моделирование работы системы на уровне функций для определения зоны действия отказа и стратегии восстановления системы. Верификация границ эксплуатации, функциональной совместимости проекта на соответствие требованиям к структуре проекта	Выполнение оценки безотказности. Выполнение оценки ремонтопригодности. Выполнение анализа видов, последствий и критичности отказов на функциональном уровне. Выполнение оценки взаимозаменяемости, отказоустойчивости и оценки риска на функциональном уровне. Разработка плана технического обслуживания и логистической поддержки. Установление процесса оценки поставщиков для обеспечения качества и соответствия требованиям безотказности. Установление процесса оценки и приемки приобретаемой готовой продукции
Документация по проектированию системы	
Документированная спецификация системы	Включение требований к надежности в спецификации системы

Рассматриваемые влияющие факторы:
- конкуренция;
- экономические вопросы;
- вопросы технологии;
- вопросы возможностей;

- экологические вопросы;
- правовые вопросы;
- вопросы распределения инвестиций во времени.

Аспекты, положительно влияющие на применение процесса:

- человеческие ресурсы;
- финансовые ресурсы;
- оборудование;
- интегральное проектирование и выполнение процессов;
- подтверждение надежности процесса.

Выходы:

- спецификации системы;
- знание проекта системы.

А.2.2 Процесс на стадии проектирования и разработки системы

Входы:

- спецификации системы;
- требования к структуре системы;
- план надежности.

Таблица А.2.2 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Проектирование системы	
Разработка плана проектирования и разработки системы. Установление требований к интерфейсу системы и подсистем. Установление связи с взаимодействующими системами. Установление требований к интерфейсу с человеком. Установление плана управления конфигурацией и процедуры изменения проекта. Установление физических размеров и стандартизованных посадочных мест для сборки. Установление норм излучений и восприимчивости для строительных объектов, кабелей и проводки внутри и снаружи зданий и оборудования	Установление программы надежности системы. Установление программы обеспечения качества. Формализация требований в области надежности для системы, подсистем и функций. Установление программы надежности для поставщиков. Установление критерия приемки по надежности и программы повышения надежности. Установление программы технического обслуживания и логистического обеспечения. Установление анализа записей, сбора данных об отказах и системы обратной связи с потребителем. Определение критерия безотказности человека. Определение условий гарантии
Разработка подсистем	
Начало собственной разработки подсистем. Начало разработки интерфейсов для обеспечения функциональной совместимости. Контроль и сотрудничество с поставщиками материалов и внешними разработчиками, действующими по контракту. Подготовка плана производства. Подготовка плана эксплуатации. Подготовка плана технического обслуживания и логистического обеспечения. Подготовка плана упаковки, обработки, хранения и транспортирования. Подготовка плана установки. Подготовка плана интеграции	Выполнение программы надежности для подсистем. Выполнение программы надежности для поставщиков. Разработка программы обеспечения запасными частями. Разработка программы испытаний программного обеспечения и диагностики

Рассматриваемые влияющие факторы:
- наличие и доступность соответствующих квалифицированных человеческих ресурсов;
- ориентация на цели при разработке графиков;
- риски проекта.

Аспекты, положительно влияющие на применение процесса:
- наличие конкретных методов, необходимых для разработки;
- потребности в обучении.

Выходы:
- опытный образец;
- требования к поддержке работы системы и подсистем.

А.2.3 Процесс на стадии производства и изготовления

Входы:
- опытный образец.

Таблица А.2.3 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Изготовление	
Физическое производство подсистем. Изготовление аппаратных и программных элементов. Выполнение тестовой оценки функций. Проведение обучения операторов и специалистов по техничекому обслуживанию и ремонту. Обеспечение готовности испытательного оборудования и средств испытаний. Обеспечение готовности инструкции по упаковке, обработке, хранению и транспортированию	Выполнение программы надежности системы. Выполнение программы обеспечения качества. Выполнение программы надежности для поставщиков. Выполнение программы технического обслуживания и логистической поддержки системы. Выполнение записей, анализ, сбор данных об отказах и системы обратной связи
Интеграция	
Выполнение плана интеграции. Сборка и интеграция системы. Подготовка планов и процедур верификации и валидации. Подготовка плана приемки системы	Выполнение программы интеграции в части обеспечения надежности системы. Выполнение программы интеграции в части обеспечения качества
Верификация	
Выполнение плана верификации. Документирование результатов испытаний. Подготовка плана приемки системы. Проверка результатов верификации на соответствие с планом приемки системы	Выполнение оценки надежности подсистем. Документирование записей об отказах в процессе испытаний при верификации. Анализ записей об инцидентах и разработка рекомендуемых корректирующих и предупреждающих действий. Принятие решений по отклонениям, выявленным при верификации
Установка и перемещение	
Выполнение плана установки системы. Документирование записей и процедур об установке системы. Анализ стратегии перемещения для ее улучшения	Установление общих систем технического обслуживания и отчетности с потребителем для системы, установленной на территории заказчика. Мониторинг времени восстановления системы и пополнения комплекта запасных частей. Поддержка учета запасных частей на сайте потребителя

Окончание таблицы А.2.3

Ключевые действия процесса	Действия, связанные с надежностью
Валидация и ввод в эксплуатацию	
Выполнение плана валидации. Документирование результатов испытаний при валидации. Выполнение плана приемки системы. Внедрение схемы гарантий, если это применимо. Подписание потребителем документов о приемке системы для начала ее эксплуатации	Валидация того, что работа системы полностью соответствует требованиям надежности. Документирование записей в процессе испытаний при валидации. Анализ записей о несоответствиях для разработки рекомендуемых корректирующих и предупреждающих действий. Принятие решений по отклонениям, выявленным при валидации. Принятие решений по гарантийным случаям у потребителя

Рассматриваемые влияющие факторы::
- менеджмент трансформаций;
- ориентация на цели в графике поставок;
- гарантийные требования и стимулы.

Аспекты, положительно влияющие на применение процесса:
- менеджмент проекта;
- обучение потребителей.

Выходы:
- эксплуатация системы;
- поддержка пользователя.

А.2.4 Процесс на стадии эксплуатации и технического обслуживания системы

Входы:
- полноценная эксплуатация системы.

Таблица А.2.4 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Эксплуатация	
Выполнение стратегии эксплуатации системы. Мониторинг функционирования системы. Обеспечение ценности потребителя	Выполнение программы повышения безотказности. Выполнение системы сбора данных об эксплуатации системы. Проведение опроса об удовлетворенности потребителя
Техническое обслуживание	
Выполнение стратегии технического обслуживания и ремонта. Мониторинг технического обслуживания системы. Предоставление услуг потребителю. Выполнение действий технического обслуживания для внесения изменений	Анализ тенденций отказов. Анализ причин проблемных областей. Разработка рекомендаций по конструктивным или процедурным изменениям для постоянного улучшения. Определение качества обслуживания

Рассматриваемые влияющие факторы:
- возможности системы по выполнению своих функций;
- цепочка поставок для обеспечения запасными частями;
- критичные действия технического обслуживания.

Аспекты, положительно влияющие на применение процесса:
- менеджмент проекта;
- подготовка операторов и персонала по техническому обслуживанию и ремонту систем.

Выходы:
- показатели надежности системы;
- данные об удовлетворенности потребителя.

А.2.5 Процесс на стадии улучшения системы

Входы:

- новые требования потребителя;
- улучшенные свойства системы.

Таблица А.2.5 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Улучшение	
Определение новых требований. Разработка стратегии и плана улучшения. Оценка необходимости изменений и получаемых преимуществ. Выполнение улучшений. Выполнение действий по изменениям	Оценка влияния на надежность работы системы в результате изменений с добавлением новых функций. Исследование влияния стоимости жизненного цикла на принятие решения о выполнении изменений. Оценка риска и значения изменений. Проведение опроса об удовлетворенности потребителя результатами изменений

Рассматриваемые влияющие факторы:

- сроки изменений;
- возврат инвестиций.

Аспекты, положительно влияющие на применение процесса:

- управление изменениями;
- управление устареванием;
- одобрение или реакция потребителя на новые свойства системы.

Выходы:

- улучшенная работа системы;
- сопоставление удовлетворенности потребителя до и после улучшения.

А.2.6 Процесс на стадии вывода из эксплуатации, списание системы

Входы:

- возможности работы стареющей системы;
- конкурентоспособность и реализуемость существующей системы;
- увеличение затрат на техническое обслуживание и ремонт.

Таблица А.2.6 — Действия процесса

Ключевые действия процесса	Действия, связанные с надежностью
Вывод из эксплуатации	
Выполнение плана выхода из эксплуатации (изъятия из обращения). Выполнение стратегии повторного или другого использования. Обработка отходов для захоронения при утилизации. Уведомление пользователя о прекращении обслуживания. Предоставление информации об обеспечении новыми или альтернативными услугами	Оценка ограничений на деактивацию системы и влияния на изъятие системы из эксплуатации. Оценка воздействия утилизации системы на окружающую среду. Проведение опроса об удовлетворенности потребителя обслуживанием в связи с его прекращением

Рассматриваемые влияющие факторы:

- сроки вывода из эксплуатации;
- применение устаревших технологий;
- нормативно-правовые ограничения;
- социальные последствия прекращения эксплуатации системы.

Аспекты, положительно влияющие на применение процесса:

- менеджмент проекта.

Выходы:

- прекращение эксплуатации системы.

Приложение В
(справочное)

Методы разработки и обеспечения надежности системы

В.1 Общие положения

Методы являются полезными средствами решения общих технических проблем, включая проектирование надежности системы на различных стадиях жизненного цикла. Существует множество методов и поставщиков этих методов на рынке. Некоторые из них представляют собой стандартные формы и простые перечни; другие являются сложными интерактивными системами и часто требуют лицензионных соглашений для доступа к базе данных и технической поддержки. Методы обычно разрабатывают самостоятельно, основываясь на прошлом инженерном опыте, или они могут быть приобретены у поставщиков для облегчения подготовки персонала и различных применений проекта. Выбор соответствующих методов технического решения должен быть сделан инженерами или практиками, выполняющими задачи надежности. Поскольку к выбору метода привлекают инвестиции, инженеру или исполнителю следует рассмотреть вопрос о значимости класса технических проблем надежности, которые необходимо решить, определить частоту использования метода, обучение, необходимое для эффективного использования метода и доступность альтернативных методов использования более простых приемов решения этой проблемы с помощью набора простых методов, разработанных самостоятельно. Далее приведены типовые примеры общего применения аппаратного и программного обеспечения для конкретных ситуаций методов проектирования надежности систем.

В.2 Общее применение методов обеспечения надежности при проектировании

В.2.1 Безотказность и ремонтопригодность

Применительно к безотказности и ремонтопригодности метод использует приобретатель системы для обеспечения того, что требования покупателя к безотказности и ремонтопригодности определены и поняты как поставщиком, так и покупателем системы. Метод также обеспечивает средства достижения уверенности в том, что требования к безотказности и ремонтопригодности существуют или будут удовлетворены на протяжении срока службы.

Данный метод обеспечивает:

a) мотивированный аргумент аудита в поддержку утверждения о том, что определенная система удовлетворяет требованиям к безотказности и ремонтопригодности;

b) при наличии отчета о безотказности и ремонтопригодности — резюме о свидетельствах и аргументах о безотказности и ремонтопригодности для поддержки программы на промежуточных этапах;

c) уверенность в обеспечении безотказности и ремонтопригодности на основе их выполнения на промежуточных этапах.

Дополнительные сведения см. в [2].

В.2.2 Программа повышения надежности

Программу повышения надежности используют для улучшения безотказности системы на стадии проектирования и разработки системы. Повышение надежности направлено на реализацию целей в области безотказности системы путем поэтапного улучшения с использованием методов анализа проекта и испытаний на безотказность модулей или функций системы. Критичным является выявление и устранение недостатков проекта системы для постоянного улучшения ее безотказности. Обычно системами, которые получают преимущества от применения программ повышения надежности, являются системы, использующие новые методы проектирования структуры системы, новые и разрабатываемые компоненты системы и программного обеспечения. Концепция повышения надежности призвана сокращать вероятность возникновения отказов, вызванных недостатками конструкции через постоянное улучшение системы и ее функций на протяжении всего процесса проектирования и разработки. Программы повышения надежности должны быть интегрированы в процесс разработки и оценки системы для достижения экономически эффективных решений. Программа повышения надежности установлена в *ГОСТ Р 51901.6*. Модели повышения надежности и методы оценки безотказности на основе данных об отказах, включенных в программу повышения надежности, приведены в *ГОСТ Р 51901.16.*

В.2.3 Управления конфигурацией

Управление различными и последовательными конфигурациями системы является одной из главных задач надежности (например, техническое обслуживание и ремонт). Это обусловлено разнообразием интерфейсов, встречающихся в различных конфигурациях. Растущий спрос на взаимозаменяемость компонентов (аппаратного и программного обеспечения) и функциональную совместимость систем имеет непосредственное коммерческое значение и требует особого внимания к управлению конфигурацией. Это особенно верно для систем с продолжительным жизненным циклом, включающих компоненты с менее продолжительным ресурсом, которые часто заменяют на протяжении срока службы системы. Во время разработки системы управление конфигурацией системы значительно способствует обеспечению надежности. Управление конфигурацией имеет важное значение при изменении средств управления системы и значимых оценок надежности. Руководство по управлению конфигурацией приведено в *ГОСТ Р ИСО 10007*.

В.2.4 Байесовские сети

Байесовские сети (BBN) представляют собой мощную графическую формализацию для поддержки исследования неопределенности событий, с помощью различных форм доказательств. Они дают возможность моделирования неопределенности и комбинации различных типов доказательств, включая как субъективную информацию на основе заключений экспертов, так и объективные доказательства на основе измерений. Байесовские сети дают много или мало доказательств по усмотрению пользователя, т. к. они могут сделать прогноз при отсутствующих или неполных данных. Эта методология предлагает полезный подход для прогнозирования надежности системы на всех стадиях жизненного цикла, при наличии прямых и косвенных измерений надежности.

Существуют многочисленные доступные коммерческие программные продукты на основе байесовской сети, которые облегчают ввод данных и установку сети.

В.3 Методы проектирования надежности аппаратного обеспечения системы

В.3.1 Улучшение безотказности

Улучшение безотказности системы для элементов аппаратного обеспечения направлено на улучшение присущих свойств функций системы и факторов, влияющих на показатели безотказности системы. Основной акцент делается на технологии, используемые в конструкции системы, условия эксплуатации системы и применение функций системы для достижения целей работы системы. Существует много методов, применимых для оценки безотказности (см. *ГОСТ Р 27.301*). Улучшение безотказности может быть достигнуто за счет надлежащего включения рекомендованных результатов в практические решения, основанные на соответствующих входных данных для оценки безотказности. В большинстве случаев для определения наилучшего проектного решения необходимо компромиссное решение. Некоторые из этих методов могут быть использованы для проверки и контроля результатов анализа оценок, полученных для элементов того же самого аппаратного обеспечения.

Типовые примеры использования методов обеспечения безотказности включают:

- использование структурной схемы надежности (RBD) для определения потребностей в резервировании по сравнению с использованием одного элемента с более высокой надежностью и более высокой стоимостью;
- использование марковского анализа для системы со сложной структурой и сложными стратегиями технического обслуживания;
- использование анализа дерева неисправностей (FTA) для выявления критических отказов системы;
- использование анализа видов и последствий отказов (FMEA) для определения возможных видов отказов, последствий, причин и критичности соответствующих экспозиций риска;
- использование прогнозирования интенсивности отказов для оценки безотказности элементов аппаратного обеспечения.

Следует отметить, что существуют ограничения на использование методов обеспечения надежности. Предположения, сделанные при формулировке задачи, имеют важное значение для обоснования и объяснения технического подхода. Инженерные решения, основанные на практическом опыте, необходимы для интерпретации результатов оценки безотказности, полученных до внедрения рекомендаций.

Вследствие того, что тепловой эффект и эффект электромагнитных помех влияют на работоспособность электронных компонент функций системы, целесообразно для анализа системы разработать средства составления термального бюджета и бюджета электромагнитной совместимости для ограничения экспозиции риска при катастрофических отказах системы. Такой подход представляет метод инженерного анализа для обеспечения безотказности системы. Устранение отказов и отказоустойчивость конструкции имеют решающее значение при проектировании критических систем.

В.3.2 Улучшение ремонтопригодности

Для улучшения ремонтопригодности важно рассмотреть простоту обслуживания восстанавливаемых элементов аппаратного обеспечения в виде сборочной единицы. Это означает, что неисправный или изношенный элемент может быть определен, изолирован, удален и заменен новым элементом. Критерии, устанавливающие ремонтопригодность при проектировании системы, связаны с разделением системы на блоки для облегчения доступа, конструкцией сменного блока, тестируемого сменного блока для обнаружения отказа, стоимостью и безотказностью сменного блока для обеспечения запасными частями. Также необходимо определить экономичность одноразового или заменяемого объекта (блока). Техническое обслуживание системы обычно связано с тремя основными уровнями ремонта:

a) уровень организации — восстановление системы выполняют на месте расположения системы, как правило, включающее в себя замену основных заменяемых объектов и представляет собой подключаемый модуль с относительно коротким временем изоляции и замены объекта;

b) средний уровень. Восстановление заменяемого объекта осуществляют в мастерской с оборудованием для дальнейших испытаний, диагностики, ремонта/доработки и восстановления объекта до его рабочего состояния. Это требует большой продолжительности выполнения работ и возвращения объекта в эксплуатацию;

c) уровень депо. Восстановление системы включает более обширный ремонт и доработку объекта для его восстановления до рабочего состояния. Это требует гораздо больше времени.

Если самый мелкий сменный блок является одноразовым, то техническое обслуживание системы является существенно более простым и включает только два уровня. Замена неисправного блока происходит только на уровне организации, а запасной блок поступает из депо, которое может быть изготовителем оригинального обо-

рудования. Никакой ремонтной мастерской не требуется. Задача здесь состоит в том, чтобы спроектировать одноразовый блок, который не наносит вред окружающей среде.

Тестируемость является важным параметром улучшения ремонтопригодности оборудования. Степень диагностики и тестового покрытия объекта часто диктуют время и трудоемкость, необходимые для определения неисправного элемента, которые истощают ресурсы технического обслуживания. Политика технического обслуживания и ремонта должна четко отслеживать такие блоки и определять, сколько раз неисправный блок прошел ремонт/доработку, прежде чем был утилизирован. Политика технического обслуживания и ремонта должна также анализировать и обеспечивать точность и результативность испытательного оборудования для четкого определения отказавшего элемента.

Ремонтопригодность конструкции должна рассматривать также человеческий фактор для облегчения взаимодействий при восстановлении и техническом обслуживании системы при эксплуатации. Вопросы охраны и безопасности следует учитывать при рассмотрении предупреждающего и корректирующего технического обслуживания. Руководство по обеспечению ремонтопригодности при проектировании приведено в [3].

В.3.3 Улучшение технического обслуживания и логистического обеспечения

Система технического обслуживания и логистического обеспечения направлена на поддержание работоспособности системы в соответствии с целями ее эксплуатации. Действия в основном проводят на стадии эксплуатации и технического обслуживания системы. Улучшения технического обслуживания и логистического обеспечения достигают за счет улучшения обслуживаемости системы в пределах ограничений, установленных конфигурацией системы и сценарием ее эксплуатации. Существуют значимые цели, которые должны быть достигнуты за счет улучшения, — внимательное обслуживание и упрощение процедур обслуживания. Улучшение также может быть достигнуто благодаря эффективной автоматизации отчетности по техническому обслуживанию и разработке системы анализа логистического обеспечения. Решение вопросов логистического обеспечения, касающихся централизованной или децентрализованной системы обеспечения депо, стратегического планирования и составления графика решения задач технического обслуживания, может привести к сокращению времени и трудоемкости технического обслуживания. В сегодняшней конкурентной среде, когда системы находятся в помещениях потребителя, основные работы по техническому обслуживанию могут быть выполнены сторонней организацией. Для аутсорсинга работ по техническому обслуживанию требуется дополнительная подготовка персонала с надлежащими навыками и компетенцией для выполнения необходимого обслуживания потребителей. Это обслуживающий персонал первой линии для рассмотрения жалоб потребителей. Сбор информации о проблемах потребителей в отношении выполненных сервисных работ и доверия потребителей стало главной проблемой координации процесса технического обслуживания системы. Для таких методов улучшения используют различные методы, включая техническое обслуживание, ориентированное на безотказность (RCM) (см. *ГОСТ Р 27.606*) и процесс интегрированного логистического обеспечения (LSI) (см. *ГОСТ Р 53392*).

В.4 Методы проектирования надежности программного обеспечения

В.4.1 Объектно-ориентированная методология

Это подход к моделированию системы как набора взаимодействующих объектов со связанными данными и свойствами. Подход основан на декомпозиции требований или конструкции системы в виде иерархического набора классов и объектов.

В.4.2 Методология структурирования

Метод, основанный на декомпозиции требований или конструкции системы в виде набора алгоритмических процессов, связанных определенным потоком данных. Процессы выполняют преобразование входных данных для генерации выходных данных. Декомпозиция может быть ориентирована на процедуры, данные или информацию. Методологии структурирования различаются по предназначенности для систем, работающих в режиме реального времени, или иных.

a) Метод, ориентированный на процедуры, — подход, который рассматривает алгоритмические процессы модели системы как ее фундаментальную характеристику. Определение данных следует из определенных процессов;

b) метод, ориентированный на данные, — подход, который рассматривает входные и выходные части модели системы как ее фундаментальную характеристику. Алгоритмические процессы выводят на основе структур данных;

c) метод, ориентированный на информацию, — подход, который использует логическую модель логических данных для интеграции информационных компонентов системы. В нем подчеркиваются основные требования к данным системы на уровне организации. Затем информационные компоненты системы создают на основе требований модели логических данных.

В.4.3 Функциональная декомпозиция проекта

Функциональная декомпозиция проекта представляет собой подход, направленный на определение модулей и интерфейсов, путем разделения заданных функций программного обеспечения системы. Процесс проектирования обычно выполняют после того, как разработаны требования к системе и выбрана концепция структуры системы. Итеративный процесс уточняет конструкцию методами «сверху вниз» или «снизу вверх». Это достигается путем деления системы на взаимодействующие функции или функциональные границы элементов системы. Иерархия проекта системы обычно включает три уровня: верхний, средний и низкий уровни. Работу каждого уровня иерархии

системы можно описать графически, представляя входы и выходы и процесс преобразования соответствующих функций. Каждый уровень блок-схемы можно представить, используя информацию, полученную из процесса декомпозиции функций. Эта диаграмма показывает, как элементы системы в структуре системы могут работать вместе, а функциональное описание каждого блока относится к его эксплуатации. Этот подход очень похож на метод структурной схемы надежности (RBD) с различными назначениями функций блока. Метод декомпозиции функций является мощным методом проектирования систем, который обеспечивает систематический подход к описанию иерархии системы и ее функций. Применение методов проектирования функций системы улучшает качество проекта и повышает надежность системы в эксплуатации. Примерами методов декомпозиции функций являются поэтапное улучшение проекта, проектирование структуры и проектирование в режиме реального времени.

В.4.4 Анализ ошибок

Анализ ошибок состоит:

- из процесса исследования наблюдаемой ошибки программного обеспечения с целью выявления ее источника;
- процесса исследования наблюдаемой ошибки программного обеспечения для идентификации такой информации, как причина ошибки, фаза процесса разработки, в ходе которой была введена ошибка, методология, с помощью которой ошибка может быть предотвращена или быстрее обнаружена, а также метод обнаружения ошибок;
- процесс исследования ошибок и отказов программного обеспечения для количественного определения интенсивностей и тенденций.

Анализ ошибок включает определение, являются ли причиной ошибок проблемы аппаратного или программного обеспечения.

В.4.5 Метод Дельфи

Это метод группового прогнозирования, обычно применяемый к будущим событиям, таким как разработка технологий, при которой используют оценки экспертов и сводки обратной связи об этих оценках для получения дополнительных оценок от этих экспертов до тех пор, пока не будет достигнут разумный консенсус. Метод используют при оценке затрат на программное обеспечение, включая оценку факторов, влияющих на эти затраты (детальное описание метода Дельфи приведено в литературе).

В.4.6 Метод автоматизированного проектирования и программного обеспечения для автоматизации процессов

Эти методы помогают автоматизировать один или несколько аспектов процесса проектирования программного обеспечения. Как правило, эти методы используют при проектировании, разработке и сопровождении программного обеспечения. Существует много подобных методов, созданных поставщиками программного обеспечения и используемых различными организациями для конкретных целей. Эти методы коммерчески доступны для облегчения применения программного обеспечения, такого как анализ структуры системы, управление требованиями, моделирование, разработка графического программного обеспечения, генерация кодов, реинжиниринг, отслеживание ошибок, разработка отчетов и помощь в авторизации. Упомянутые методы — это программные средства. Их применение должно соответствовать стандартным процедурам оценки для достижения поставленных целей. Руководство по классификации методов автоматизированного проектирования программного обеспечения установлено в [4] и [5].

В.4.7 Средства автоматизированного проектирования

Средства автоматизированного проектирования представляют собой набор программных услуг, частично или полностью автоматизированных с помощью программных средств, которые используют для поддержки деятельности человека в области разработки программного обеспечения. Действия средств автоматизированного проектирования, как правило, выполняют в среде разработки программного обеспечения и технического обслуживания проекта. Они охватывают такие направления, как спецификация, разработка, реинжиниринг или техническое обслуживание программных систем. Область средств автоматизированного проектирования охватывает несколько ситуаций; от управления несколькими методами в одной и той же операционной системе до полностью интегрированной среды, способной обрабатывать, контролировать все данные, процессы и действия жизненного цикла программного обеспечения. Средства автоматизированного проектирования оказывают поддержку деятельности человека посредством ряда услуг, которые включают возможности среды программирования. Программный процесс, поддерживаемый средствами автоматизированного проектирования, является вспомогательным или автоматизированным программным процессом. Средства автоматизированного проектирования можно рассматривать как вспомогательную систему. Более подробная информация о средствах автоматизированного проектирования приведена в [6].

В.4.8 Модель технологической зрелости

Организации используют эту модель для описания зрелости процесса программного обеспечения. Модель ранжирует организации по уровням от 1 до 5:

уровень 1: считается случайным или хаотичным;

уровень 2: повторяемые процессы;

уровень 3: определенные процессы (отраслевой минимальный стандарт на технические процессы);

уровень 4: измеряемые процессы;

уровень 5: оптимизированные процессы.

Модель технологической зрелости используют систематически, основываясь на наборе принципов для получения анкеты зрелости. Модель может возникнуть путем полной разработки структуры зрелости. Она предоставляет организации, использующей модель, эффективное руководство по установлению программ улучшения процессов.

Модель зрелости для программного обеспечения помогает организации повысить зрелость процесса разработки программного обеспечения, используя знания, полученные из оценки процесса программного обеспечения и обширной обратной связи с передовой промышленной практикой.

Модель зрелости направлена на процесс разработки. Участки процесса определяют блоки или объемы знаний на основе отраслевой практики. Уровень зрелости определяет зависимости и приоритеты для улучшения.

Уровень 1 является руководством для организации, направляющей ограниченные ресурсы по улучшению процесса на наиболее важные изменения. Установление приоритетов важно, поскольку организации с низкой технологической зрелостью программного обеспечения не имеют хронологических данных, но необходимо определить, действительно ли изменение является улучшением, то есть даст ли изменение статистически значимое улучшение в течение прогнозируемого периода времени, включая все расходы, связанные с внесением изменения, по сравнению с прежней ситуацией.

Уровень 2 направлен в основном на процессы управления для улучшения планирования, распределения времени и ресурсов, прослеживания и управления проектами.

Уровень 3 устанавливает определенные в организации повторяемые процессы разработки, которые становятся основой для будущих измеримых улучшений. Он также устанавливает методы сбора данных о процессе и продукции и методы определения, как выполнение и качество процесса влияют на бизнес-цели.

Уровень 4 направлен на варианты, которые не являются частью системы по общим причинам. Он признает, что процесс развития является системой и к нему могут быть применены статистические методы. Этот уровень используют для прогнозирования работы и качества процесса, на основе опыта и данных.

Уровень 5 направлен на общие причины изменчивости, анализ причин дефектов, оценку возможных изменений для сокращения или предотвращения дефектов и определение, действительно ли эти изменения являются улучшениями. Это процесс оптимизации или непрерывного совершенствования.

Модель зрелости обеспечивает эталон для сравнения возможностей процесса разработки организации и используется как предсказатель качества продукции.

По мере расширения использования и опыта работы с моделью зрелости, были разработаны модели для различных дисциплин и технических применений. Одна такая модель является моделью зрелости проектирования систем (SE-CMM). Зрелость программного обеспечения характеризует способность программного обеспечения организации успешно работать с точки зрения затрат, графика работ, функциональности и качества продукции. Зрелость имеет несколько аспектов, в том числе:

1) квалификация, опыт, навыки и мотивация персонала, выполняющего работу и управляющего работой;
2) воспроизводимость процесса;
3) технологии, которые доступны и применимы.

Отдельные модели зрелости для разработки программного обеспечения (SW-CMM) и проектирования систем (SE-CMM), используемые организациями, создали путаницу в индустрии программного обеспечения. Они становятся лишними и часто контрпродуктивными на практике. Различия между моделями SW и SE затрудняют использование организацией одновременно обеих моделей.

Преодоление этой путаницы состоит в борьбе с несоответствием путем создания интегрированной модели зрелости (CMM). Эта модель устраняет несоответствия в архитектуре, подходе, терминологии и других проблемах совместимости между SW CMM, SE-CMM и связанными с ними моделями. Результат создания представляет собой набор моделей и вспомогательной инфраструктуры, именуемых далее CMMi[1)].

[1)] См. также www.sel/cmu.edu

Приложение С
(справочное)

Руководство по условиям применения систем

С.1 Понимание условий применения систем

Руководство по условиям применения систем представляет собой анализ условий эксплуатации конечной продукции при интегрировании ее в систему. Это обеспечивает предоставление информации об условиях эксплуатации системы для проектирования с использованием приобретаемой продукции и выбора материалов, подходящих для применения системы. Соответствующие критерии для разработки или выбора приобретаемых аппаратных средств обеспечивает рассмотрение функционального проекта. Примеры, приведенные ниже, относятся к общим системам, установленным на земле.

Значение представления всеобъемлющего набора критериев проекта обусловлено следующими соображениями:

a) опыт показывает, что проекты конкретной продукции или приобретаемых объектов часто не отражают взаимосвязь интерфейса с человеком, электромагнитных, климатических и механических условий и других факторов работы системы, рассматриваемых с точки зрения перспектив применения конечной продукции. Представленный ниже подход облегчит проектирование структуры системы и интеграцию закупаемой продукции в соответствии с требованиями рынка;

b) сбор данных, ссылки на стандарты и требования пользователя могут потребовать значительных усилий. Настоящее руководство предоставляет ссылки и входы для проектирования спецификаций;

c) существующая тенденция разработки продукции — это переход от проектирования к удовлетворению требований пользователя, поскольку время выхода на рынок новой продукции ограничено. Настоящее руководство представляет широкий спектр сегментов применения, где условия использования и требования к продукции могут быть преобразованы в данные для разработки и приобретения экономически эффективной продукции и упрощения интеграции системы;

d) средства контроля условий работы и характеристики работы продукции применяют на уровнях системы, подсистемы и продукции как экономически эффективные меры достижения оптимальных проектных решений и удовлетворения меняющихся требований глобального рынка. Это отражает тенденцию к международному сотрудничеству и гармонизации стандартов для облегчения разработки системы и продукции.

С.2 Процесс определения требований к окружающей среде

На рисунке С.1 представлен общий вид процесса определения требований.

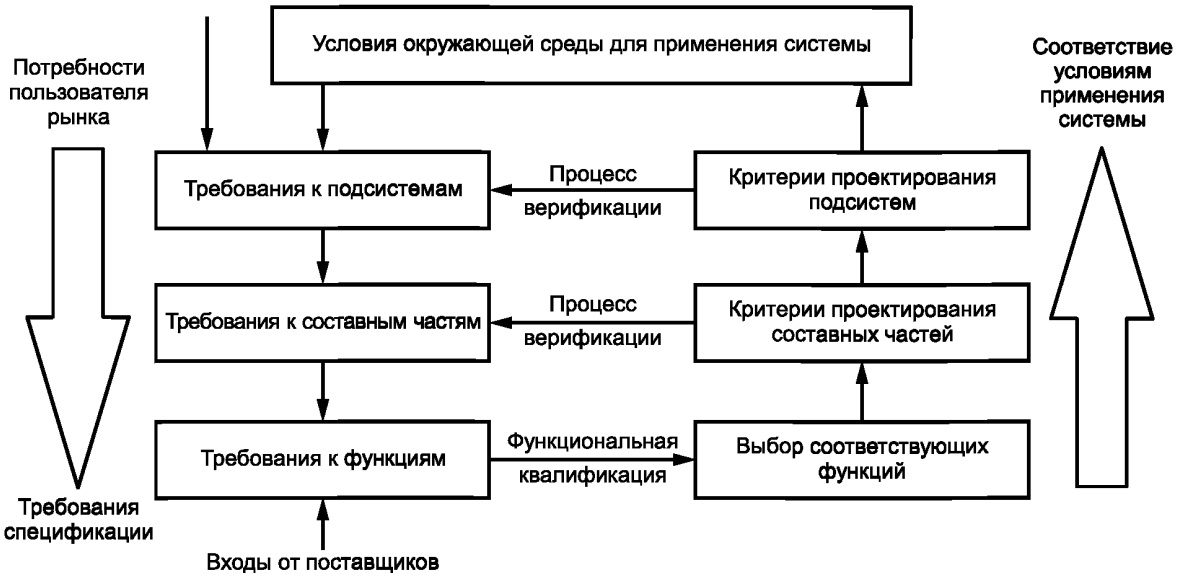

Рисунок С.1 — Процесс определения требований среды

Определение требований представляет собой процесс «сверху вниз», который включает определение условий эксплуатации системы с учетом ее интеграции из подсистем, комплектующих и функционального применения. Условия эксплуатации системы преобразуют в требования к составным частям и функциям. Потребности рынка и затраты, как правило, используют для разработки требований спецификации.

В дополнение к процессу определения требований используют процесс верификации параллельного проекта. Это восходящий процесс, обеспечивающий выполнение требований на каждом этапе предполагаемого проектирования, от выбора функционального применения до интеграции системы. Цель состоит в том, чтобы соответствовать или превышать требования конечного пользователя к работе системы.

Условия среды системы для ее конечного использования приведены в разделе С.3. Требования, относящиеся к условиям применения комплектующих системы, идентифицируют в виде конкретных характеристик их работы. Они допускают классификацию условий работы комплектующих и идентификацию экспозиции воздействия применимых условий окружающей среды.

С.3 Условия окружающей среды системы

С.3.1 Классификация условий окружающей среды системы

На рисунке С.2 показаны условия применения системы и соответствующие воздействия. Отмеченные электромагнитные, климатические и механические условия, воздействующие на систему при предназначенном применении, обеспечивают направления классификации условий работы составных частей системы при проектировании.

Следует отметить взаимосвязь между воздействиями среды и эксплуатационными характеристиками, обусловленную особенностями конструкции составных частей (см. *ГОСТ Р 53613, ГОСТ Р 53614, ГОСТ Р 53615*).

Вид воздействия	Помещение с управляемыми условиями среды	Помещение для клиентов			На открытом воздухе	Передвижное помещение	Транспортирование	Хранение
		Промышленное помещение	Торговое помещение	Жилое помещение				
Электромагнитное	E1	E3	E3	E3	E2	E4		
Климатическое	C1	C3	C2	C2	C4 C5	C4		C6
Механическое	M1 M2 M5	M1	M1 M2	M1 M2	M1	M3	M4	

Рисунок С.2 — Матрица условий применения системы и соответствующих воздействий

С.3.2 Электромагнитные условия

Электромагнитные условия в зависимости от расположения системы охватывают следующие варианты:

E1 — система находится в помещении с управляемой средой (например, в лаборатории, пустой комнате);

E2 — система расположена на открытом воздухе;

E3 — система находится в помещении потребителя;

E4 — система находится в портативной камере или передвижном помещении.

С.3.3 Климатические условия

Климатические условия в зависимости от расположения системы охватывают следующие варианты:

C1 — система находится в помещении с управляемой средой (например, в лаборатории, пустой комнате);

C2 — система находится в помещении с управляемой температурой;

C3 — система находится в помещении с неуправляемой температурой (например, в неотапливаемом гараже);

C4 — система находится на открытом воздухе, но имеется защита (например укрытие);

C5 — система находится на открытом воздухе без укрытия (например, поле);

C6 — хранение.

С.3.4 Механические условия

Механические условия охватывают следующие варианты:

M1 — система расположена стационарно;

M2 — система расположена в портативной камере;

M3 — система расположена в передвижном помещении;

M4 — система находится в условиях транспортирования;

M5 — система находится в условиях землетрясения.

С.4 Конструктивные характеристики, подверженные влиянию условий применения

На конструктивные характеристики влияют условия применения системы. Эти характеристики отражают функционирование системы. Они зависят от структуры системы, технологий, используемых в функциях системы, и стратегии сборки для достижения оптимальной работы в эксплуатации. Корреляция и взаимосвязь характеристик проекта с окончательными условиями применения системы необходимы для разработки условий применения системы. Процесс определения взаимосвязи заключается в выявлении общих характеристик и ограничения худшего случая для проектов составных частей при использовании системы. Цель состоит в обеспечении целостности и надежности составных частей системы при ее применении в различных условиях. Составление матрицы воздействий обеспечивает технический подход к анализу вариантов конструкции объекта и выбору альтернативных технологий.

Таблица С.4 — Характеристики проекта, подверженные влиянию условий применения системы

Особенности функционирования системы	Характеристики проекта, подверженные влиянию условий применения системы
Электромагнитная совместимость (ЭМС)	Структура системы. Ограничения ЭМС по бюджету и излучению. Частоты. Требования к экранированию и фильтрации
Температура окружающей среды	Потребление и распределение мощности. Тепловой бюджет и ограничения по температуре. Методы охлаждения. Механизмы передачи тепла
Качество	Качество процесса. Критерии приемлемости. Мониторинг и ликвидация несоответствий. Квалификация поставщиков
Надежность	Готовность и допустимые продолжительность и частота простоев. Среднее время между отказами. Среднее время восстановления. Стратегии технического обслуживания и обеспечения. Ресурс и периоды безотказной работы
Совместимость с окружающей средой	Условия окружающей среды процесса жизненного цикла. Проектирование сокращения влияния на экологию, повторного использования и переработки. Воздействия окружающей среды. Экспозиции рисков

С.5 Особенности системы для рассмотрения проекта

С.5.1 Введение

Информация о корреляции и составление матрицы взаимосвязей (см. рисунки С.2 и С.3) может облегчить разработку конкретной функции системы или составной части для использования в заданных условиях применения системы. Следующие описания конкретных свойств функционирования системы предоставляют полезную информацию обратной связи, необходимую для рассмотрения проекта.

С.5.2 Вопросы проектирования электромагнитной совместимости

Электромагнитная совместимость — это способность объекта функционировать под воздействием электромагнитного шума или без его излучения. Излучение — это электромагнитная энергия или нежелательный шум, исходящие от источника. Источниками излучения могут быть высокочастотная, встроенная в электронную схему или модуль синхронизация. Устойчивость по отношению к воздействию электромагнитных полей — это способность объекта противостоять электромагнитному шуму. Это происходит при эксплуатации радио- и телевизионных передатчиков или по отношению к электростатическим разрядам. Многие страны регулируют уровни излучения для предотвращения помех. Проекты электронных объектов должны соответствовать ограничениям на излучение для успешного применения и продажи продукта. Разделение — метод, используемый при разработке объекта для обеспечения соответствия требованиям электромагнитной совместимости. Для перевода требований электромагнитной совместимости с уровня системы на уровень составных частей и уровень модулей требуется составление

бюджета электромагнитной совместимости. Для этого необходим детальный анализ устройств, используемых в модулях, стратегии экранирования, размещения компонентов, маршрутизации кабелей и печатного монтажа. Вклады всех источников излучения внутри модуля используют для определения границ излучения конструкции. Это предел допуска для конструкции модуля, который может повлиять на работу модуля в составной части при интеграции в систему, подверженную воздействию электромагнитных полей.

С.5.3 Вопросы проектирования температурных условий

Требования к температуре сильно зависят от функций системы и воздействия окружающей среды на составные части или модули при работе системы. Основная проблема заключается в генерации тепла при работе системы и его отведении для обеспечения устойчивой работы системы. На генерацию тепла влияет работа устройств, потребляющих энергию и излучение тепла всеми компонентами внутри корпуса модуля. Стратегия удаления тепла может быть основана на теплопроводности, конвекции и излучении. Типичными ситуациями охлаждения системы являются принудительная вентиляция или естественная конвекция. Работа модуля с высокой плотностью компоновки деталей чувствительна к источникам тепла внутри модуля. Температура окружающей среды также влияет на работу модуля. Аномальное повышение температуры, вызванное внутренними источниками тепла или в результате внешней теплопередачи, влияет на безотказность модуля. Тепловой баланс рассеиваемой мощности потенциальных источников, выделяющих тепло, является основой для идентификации, сокращения и удаления нежелательного тепла, генерируемого в модуле. При проектировании термальных условий необходимо выполнить анализ рассеивания энергии, повышения температуры, скорости охлаждения и термальных условий устройства. Расчет температурного баланса необходимо выполнять на всех уровнях иерархии системы.

С.5.4 Вопросы обеспечения качества

Анализ качества охватывает все неотъемлемые свойства объекта (системы, составной части, модуля или компонента), которые создают способность системы соответствовать установленным и подразумеваемым требованиям. Качество означает соответствие требованиям; поэтому для соответствия требованиям устанавливают критерии приемлемости и процедуры контроля. Это обеспечивает постоянное соответствие установленным стандартам с использованием соответствующих механизмов, встроенных в систему или процесс, что способствует постоянному улучшению. Процессы обеспечения качества и контроля качества хорошо известны, т. к. методы обеспечения качества при проектировании описаны в соответствующей документации, а в настоящем стандарте подробно не рассмотрены.

С.5.5 Вопросы обеспечения надежности

Надежность — свойство присущее системе, которое обеспечивает готовность системы оказывать предусмотренные услуги по запросу (см. также *3.1.5 ГОСТ 27.002—2015*). Готовность — одно из свойств надежности, на готовность влияют безотказность, ремонтопригодность, а также такая характеристика системы, как обеспечение технического обслуживания и ремонта. Вопросы надежности рассмотрены также в других стандартах.

С.5.6 Вопросы обеспечения совместимости с окружающей средой

Совместимость с условиями окружающей среды важна на современном рынке. Воздействия на окружающую среду объекта и модуля при распоряжении (замене или утилизации) представляет собой сложную ситуацию для разработчиков и изготовителей продукции. Типичные требования пользователей или потребителей имеют форму договора о возврате, в соответствии с которым поставщик продукции заменяет ее до постановки ее на обслуживание. Договоры о возврате также распространены в сегодняшнем бизнесе, где поставляемое количество запасных частей, которые были сохранены или куплены пользователем, но не использованы до конца согласованного периода времени, поставщик должен выкупить. При проектировании и изготовлении составных частей и модулей следует учитывать их повторное использование и утилизацию. Переработка побочных продуктов в процессе производства для минимизации отходов утилизации является еще одним фактором, который следует учитывать при исследовании воздействия на окружающую среду. Следует также исследовать сокращение излучений и отходов процесса жизненного цикла объекта.

Приложение D
(справочное)

Контрольные перечни для обеспечения надежности систем

D.1 Контрольные перечни для управления обеспечением надежности систем при проектировании

D.1.1 Общие положения

Контрольные перечни по надежности систем применимы к жизненному циклу системы в основных точках принятия решений для облегчения анализа управления проектом. Эти контрольные перечни выявляют критические проблемы, которые необходимо решить для валидации завершения ключевых действий в области надежности системы на каждой стадии выполнения проекта. Рекомендуется регулярно проводить анализ основных точек принятия решений для последовательного выполнения задач обеспечения надежности. Это гарантирует, что все критические проблемы рассмотрены и решены. Записи, связанные с таким анализом, могут быть использованы в качестве объективных свидетельств обеспечения надежности проекта. Контрольные перечни отражают процессы передачи ответственности и смены владельца в течение всего жизненного цикла системы. Эти контрольные перечни могут быть использованы поставщиком и потребителем при отработке проекта для обеспечения соответствия установленным требованиям применения системы.

D.1.2 Контрольный перечень идентификации рынка

a) Определен показатель надежности системы и его применение, определено намерение заменить существующую систему и повысить ее эффективность;

b) установлено время внедрения новой системы с заданными свойствами надежности;

c) определены условия эксплуатации системы, конкретные факторы, влияющие на надежность, и связанные с этим обязательные требования;

d) определены технические возможности для обеспечения надежности при разработке системы;

e) определены и оценены ресурсы, необходимые для поддержки проектирования надежности;

f) определены капитальные вложения и приобретение конкретных методов надежности и вспомогательных механизмов разработки системы;

g) выявлены потенциальные потребители, вероятные конкуренты, заинтересованные в разработке системы с упором на обеспечение надежности;

h) определены ожидаемые требования к работе и особенности системы, включая идентификацию уникальных проблем надежности и ожиданий потребителей, например, устойчивость к ошибкам программного обеспечения;

i) определены сценарии изменения надежности системы в эксплуатации, функциональная совместимость с другими системами, предпочтения технологического проектирования и связанные с этим проблемы;

j) определены требования к техническому обслуживанию системы и ее логистической поддержке для обеспечения надежности системы в эксплуатации;

k) установлены маркетинговая стратегия и план действий для обеспечения надежности системы в эксплуатации;

l) создана проектная группа для подготовки и выполнения технической работы, обладающая знаниями в области надежности;

m) решение о разработке или отказе от разработки системы должно быть обосновано с учетом стратегии обеспечения надежности.

D.1.3 Контрольный перечень для разработки системы

a) Для выполнения задач надежности установлен план разработки проекта;

b) проанализированы требования к системе и оценке показателей надежности;

c) определены стратегия проектирования, выбор технологий и действия по обеспечению надежности при разработке системы;

d) установлены и выполнены план качества и процесс обеспечения надежности;

e) выполнены процесс стандартизации и правила обеспечения надежности при проектировании;

f) в соответствии с требованиями к системе определены структура и физическая конфигурация системы;

g) установлен план интеграции системы и подсистем;

h) в соответствии с требованиями к работе системы определены проекты деления аппаратного обеспечения, интерфейсы программного обеспечения и участие человека;

i) установлены требования к надежности системы и условиям ее эксплуатации;

j) завершена разработка стратегии испытаний, тестового покрытия и функциональной оценки системы;

k) функции системы проверены на соответствие требованиям надежности;

l) выполнена валидация проектов системы и надежности функций системы;

m) работы по проекту, передаваемые третьей стороне, партнерам по разработке, привилегированным поставщикам скоординированы и выполнены;

n) для обеспечения альтернативных требований проекта идентифицированы и скоординированы вторичные источники;

p) для обеспечения надежности системы разработаны приемлемые вспомогательные системы и стратегии поддержки;

q) завершена разработка документации по проекту, инструкций по подготовке персонала и процедурам испытаний;

r) определены техническое обслуживание для изготовления составных частей и связанные вопросы надежности;

s) для системы установлен план эксплуатации и ее поддержки;

t) установлен план логистического обеспечения;

u) установлены политика технического обслуживания и уровни ремонта компонентов нижнего уровня сборки системы;

v) принятие или отклонение решения о реализации продукции должны быть обоснованы.

D.1.4 Контрольный перечень для реализации продукции

a) Установлен план реализации продукции;

b) выполнены задачи обеспечения качества надежности продукции;

c) выполнены координация и контроль оценки надежности продукции поставщиков;

d) определена приобретаемая готовая продукция, необходимая для включения в систему;

e) выполнена оценка продукции и подсистем для верификации надежности;

f) выполнены испытания и оценка системы и подсистем;

g) достигнута интеграция подсистем и системы;

h) установлен план управления конфигурацией и остановки проекта;

i) выполнена валидация требований к работе системы;

j) установлена стратегия приемки системы;

k) установлены и внедрены анализ записей об отказах и система корректирующих действий;

l) принятие или отклонение решений о передаче системы и принятии ее пользователем должно быть обосновано.

D.1.5 Контрольный перечень для приемки системы

a) План приемки системы установлен на основе консультаций с потребителем;

b) план демонстрации надежности системы и применимый гарантийный период установлены и приняты потребителем;

c) система записей об инцидентах выполнена, и установлены критерии для записей;

d) выполнен план эксплуатации и поддержки системы для обеспечения ее надежности;

e) проведено обучение операторов системы и персонала по техническому обслуживанию системы и сертификация, где это применимо;

f) идентифицирована, скоординирована и одобрена поддержка системы сторонними поставщиками таких услуг как калибровка и поверка;

g) установлены процедуры передачи системы потребителю для эксплуатации;

h) выполнена юридическая передача прав собственности на систему потребителю (в соответствии с контрактом);

i) принятие и отклонение решения о введении системы в эксплуатацию должны быть обоснованы.

D.1.6 Контрольный перечень для эксплуатации

a) Выполняется план эксплуатации и поддержки системы;

b) выполняются процедуры контроля и мониторинга работы системы;

c) система записей об инцидентах выполняется для отслеживания надежности, бесперебойной работы, действий по техническому обслуживанию, а также корректирующих и предупреждающих действий;

d) действия по техническому обслуживанию отслеживаются;

e) активированы процедуры изменения проекта и план управления конфигурацией;

f) реализуется план материально-технического обеспечения;

g) выполняется анализ эксплуатации системы;

h) выявляются аномалии эксплуатации и области для улучшения;

i) установлена тенденция изменения надежности системы;

j) проводятся обследования по удовлетворенности конечного пользователя;

k) принятие или отклонение решения для сохранения в эксплуатации существующей системы должно быть обосновано.

D.1.7 Контрольный перечень для улучшения

a) Установлены потребности рынка по улучшению системы;

b) проведена оценки риска и значения изменений для обоснования усилий по улучшению;

c) проведена верификация влияния на показатели надежности в результате изменений, связанных с улучшениями;

d) исследовано и валидировано влияние на окружающую среду и другие аспекты, включая обязательные требования и безопасность изменений, связанных с улучшениями;

e) установлены графики затрат и сроков выполнения работ по улучшению;

f) определены ресурсы, необходимые для улучшения;

g) принятие или отклонение решения об улучшении системы должно быть обосновано.

D.1.8 Контрольный перечень для вывода из эксплуатации

a) Установлены необходимость и сроки вывода системы из эксплуатации;

b) определены причины вывода системы из эксплуатации, такие как моральный износ, экономические и нормативные ограничения;

c) определена заменяющая система для обеспечения непрерывного оказания услуг;

d) проведена оценка социальных последствий, связанных с прекращением работы системы;

e) принятие или отклонение решения о выводе системы из эксплуатации должно быть обосновано;

f) установлен и обеспечен план плавного перехода от старой системы к новой.

D.2 Контрольный перечень для применения аппаратного и программного обеспечения и человеческого фактора при проектировании

D.2.1 Общие положения

Контрольные перечни для применения аппаратного обеспечения, программного обеспечения и человеческого фактора могут быть использованы при проектировании системы. Они облегчают процесс проектирования и разработки системы. Выбор элементов, представляющих собой комбинацию аппаратного и программного обеспечения при проектировании функций системы, часто является компромиссом, облегчающим взаимодействие с человеком. Человеческий фактор играет важную роль в максимизации надежности системы. Для оптимального проектирования следует рассматривать контрольные перечни дополнительно.

D.2.2 Контрольный перечень для проектирования аппаратного обеспечения

a) Установлены требования к аппаратному обеспечению системы;

b) определены элементы аппаратного обеспечения, выделенные для проектирования функций системы;

c) известны и оценены технология и хронология безотказности аппаратного обеспечения;

d) определена конфигурация аппаратного обеспечения системы;

e) установлены спецификации для проектирования;

f) определены концепция упаковки и схема компоновки аппаратного обеспечения;

g) выполнен анализ теплового баланса в эксплуатации для определения областей нагрева и схем охлаждения в отношении условий окружающей среды модуля и условий эксплуатации системы;

h) установлен бюджет электромагнитных воздействий в профиле эксплуатации для определения требований к экранированию, фильтрации, распределению и размещению;

i) установлены интерфейс и возможности подключения функционального модуля;

j) определены план подачи энергии и поставок, а также стандарт электрического напряжения для системы;

k) проведено моделирование надежности системы для рассмотрения вариантов резервирования и проектирования;

l) выполнены функциональный анализ и распределение показателей безотказности с определением значений для каждой функции системы;

m) разработан план интеграции системы и подсистем;

n) проведен анализ ремонтопригодности и тестируемости системы, а также определено тестовое покрытие системы;

p) по возможности требования к наличию встроенного тестирования включены в проект для облегчения идентификации неисправностей и изоляции отказов;

q) свойства отказоустойчивости включены в критические функции системы;

r) установлены концепция и уровни технического обслуживания;

s) определен комплект обеспечения запасными частями сборок самого низкого уровня сборки;

t) определено время оборота запасных частей;

u) проведено моделирование системы (где это необходимо) для демонстрации готовности;

v) верифицированы результаты испытаний системы для обнаружения изоляции и ремонта отказов, а также время восстановления;

w) приобретаемое аппаратное обеспечение исследовано для включения в функции системы;

x) разработаны планы и процедуры испытаний системы, подсистем и функциональных модулей;

y) выполнена проектная документация для изготовления и сборки аппаратного обеспечения.

D.2.3 Контрольный перечень для программного обеспечения системы

a) Установлены требования к программному обеспечению;

b) определена структура системы;

c) стандарты на проектирование и разработку программного обеспечения выполнены;

d) программные средства и услуги для поддержки разработки программного обеспечения приобретены;

e) установлено разделение и распределение функций программного обеспечения;

f) установлен интерфейс и протокол функций программного обеспечения;

g) установлены требования к программному обеспечению;

h) установлены график поставок и планы предварительного и детального проектирования программного обеспечения;

i) функции программного модуля протестированы и верифицированы на соответствие требованиям проекта;

j) приобретаемое программное обеспечение исследовано для включения в функции системы;

k) установлены критерии приемки программного обеспечения;

l) проведены приемочные испытания для определения соответствия программного обеспечения критериям приемки;

m) проведены испытания, оценка квалификации программного обеспечения системы на соответствие требованиям к функционированию системы;

n) определено программное обеспечение для эксплуатации и технического обслуживания системы;

p) подготовлена документация (для копирования) программного обеспечения.

D.2.4 Контрольные перечни для проектирования действий человека

a) Определена цель разработки действий человека;

b) установлен план использования человеческого фактора при применении проекта;

c) установлены концепции проектирования использования человеческого фактора для обеспечения удобства использования, оперативной пригодности, распределения функций и уровня автоматизации, признания возможностей и ограничений человека при эксплуатации и техническом обслуживании системы;

d) интерфейсы системы с человеком оценены с точки зрения простоты идентичных функций для согласованности в работе, совместимости с другими существующими системами такого типа и осведомленности пользователей об информационных дисплеях и коммуникациях;

e) интерфейсы «человек—компьютер» проанализированы с точки зрения оформления экрана для обеспечения пользователю дружественного взаимодействия, элементов управления вводом и механизмов управления, простоты ввода и редактирования данных, графической информации и ее отображения, средств обновления и прерывания, функций управления файлами, окна сообщений и справочных услуг. Важно, чтобы сообщения системы были правильными, полными и понятными, а не вводящими в заблуждение;

f) в конструкции системы предусмотрены отказоустойчивость, устойчивость к ошибкам и простота управления в критических и аварийных ситуациях, простота включения и отключения автоматических функций, простота диагностических процедур для управления в случае отказов и удобство навигации в условиях деградированного режима работы системы для выполнения корректирующих действий;

g) в конструкции системы предусмотрены легкость доступа при замене съемных элементов на самом низком уровне монтажа, надлежащая маркировка для предупреждения об опасности и эксплуатации и доступ к техническим руководствам и документам по техническому обслуживанию, монтажу и ремонту;

h) определены уровень автоматизации, квалификация и навыки, необходимые операторам и специалистам по техническому обслуживанию системы;

i) подготовлена проектная документация для разработки руководств по эксплуатации и техническому обслуживанию системы.

D.2.5 Контрольный перечень для окружающей среды

a) Определена цель проектирования в отношении окружающей среды;

b) установлены требования к окружающей среде при применении проекта;

c) экологические стандарты и положения проанализированы и включены в концепцию проектирования, и выполнен план, направленный на сокращение количества сборок и деталей аппаратных средств и их повторное использование или переработку;

d) количество деталей, используемых при сборке, сведено к минимуму для сокращения времени сборки и демонтажа для повышения эффективности процесса переработки;

e) рассмотрена возможность применения модулей конструкции для сменных элементов на нижнем уровне замены с одной функцией, допускающей варианты обслуживания, функциональное обновление и рециркуляцию деталей;

f) рассмотрено объединение не перерабатываемых частей в одном месте для облегчения разборки и быстрого удаления для утилизации;

g) рассмотрена возможность размещения высокоценных частей в местах легкого доступа для обеспечения частичной разборки, оптимального возвращения и утилизации;

h) рассмотрены части конструкции для обеспечения удобства разборки вручную;

i) рассмотрено исключение литых металлических вставок и арматуры в пластмассовых деталях при сборке для улучшения разделения и переработки пластмассовых деталей.

j) рассмотрено выполнение заметных точек доступа и разъема в логической последовательности для улучшения подготовки персонала по разборке и техническому обслуживанию системы;

k) по возможности необходимо отключать электропитание или режим ожидания для экономии энергии и уменьшения загрязнения;

l) минимизировано количество крепежных элементов для сокращения времени сборки и разборки;

m) рассмотрена стандартизация использования инструментов при сборке и разборке для экономии средств и времени;

n) рассмотрена легкость доступа к точкам крепления для улучшения технического обслуживания;

p) рассмотрение возможности использования оснастки для улучшения разборки и снятия деталей;

q) рассмотрено использование крепежных материалов совместимых с соединяемыми деталями для улучшения рециркуляции деталей;

r) рассмотрена легкость разделения несочетаемых деталей для улучшения их разделения при рециркуляции;

s) использование клеев, как правило, не рекомендуется из-за трудностей при разборке деталей, особенно если два соединенных материала должны быть разделены при утилизации. Кроме того, даже для совместимых материалов клей может загрязнить материалы, затрудняя переработку;

t) количество и длина соединительных проводов и кабелей должны быть минимизированы для уменьшения времени сборки и разборки и устранения возможных электромагнитных помех;

u) для улучшения разборки рассмотрена возможность создания хрупких соединений для незаменяемых частей.

D.3 Контрольные перечни для использования приобретаемой продукции

D.3.1 Введение

Приобретаемую готовую продукцию (COTS) широко используют при применении системы для экономики и критичности времени выхода системы на рынок при ее разработке. Такая продукция, как правило, ориентирована на рынок, и ее пригодность для использования продемонстрирована широким спектром использования. Может быть приобретена продукция в виде аппаратного или программного обеспечения или их комбинации. Типичными примерами такой продукции (список может быть расширен) являются источники питания, программное обеспечение для бизнес-приложений и программируемое электронное контрольное оборудование. Покупатель продукции не влияет на характеристики продукции, ее свойства и требования к ее эксплуатации. Правильный выбор приобретаемой продукции для включения в систему имеет первостепенное значение для обеспечения надежности системы. Существуют определенные риски, связанные с выбором приобретаемой продукции и валидацией ее пригодности для конкретного применения системы независимо от требований к продукции и продемонстрированного ею соответствия этим требованиям. Это связано с отсутствием влияния покупателя на свойства продукции и ее эксплуатационные характеристики. Использование приобретаемой продукции для критического применения системы требует дополнительных усилий по ее оценке.

D.3.2 Контрольный перечень для идентификации требований

a) Приобретаемая продукция должна быть коммерчески доступна с уникальной идентификацией и достаточной информацией о продукции, функциональное описание позволяет оценить пригодность продукции для предполагаемого применения;

b) на рынке существует несколько поставщиков аналогичной продукции;

c) на этикетке продукции должны быть указаны наименование, модель, серийный номер или дата изготовления;

d) описание продукции должно содержать требования к продукции, инструкции по установке и эксплуатации, процедуры подключения, требования к интерфейсу, необходимость и степень технического обслуживания и поддержки;

e) должны быть обеспечены предупреждающие этикетки и процедуры для обеспечения безопасности при эксплуатации;

f) должна быть представлена информация о гарантии на продукцию;

g) должна быть доступна для проверки информация о показателях безотказности и ремонтопригодности, истории применения продукции, данных об испытаниях;

h) должно быть представлено заявление об аттестации качества продукции.

D.3.3 Контрольный перечень для оценки записей

a) Записи о функционировании продукции, содержащие соответствующие документы, подтверждающие ее соответствие требованиям, должны быть доступны для проверки;

b) соответствующие документы, включая план, процедуры и условия испытаний, а также записи об испытаниях следует использовать для демонстрации соответствия продукции установленным требованиям;

c) предусмотренные испытания, предназначенные для оценки условий отказоустойчивости, если это применимо к заявкам на продукцию, должны быть доступны для проверки.

D.3.4 Контрольный перечень для гарантии на продукцию

a) Информация и записи о качестве продукции доступны для проверки;

b) данные об оценке соответствия продукции доступны для проверки;

c) данные эксплуатации продукции доступны для подтверждения заявления о надежности работы продукции;

d) частота возврата продукции и тенденции отказов доступны для проверки;

e) записи о техническом обслуживании продукции доступны для проверки;

f) оценка риска, свойств продукции и свойств соответствующего процесса завершены для критического применения системы. Конкретная оценка включает (но не ограничиваясь) выявление отказов, необходимость резервирования и установление уровня целостности приобретаемой продукции, подходящей для критической работы системы. Уровень целостности — это обозначение диапазона свойств продукции, необходимого для поддержания рисков системы в допустимых пределах. Методика определения уровней целостности установлена в *ГОСТ Р ИСО/МЭК 15026*.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ 27.002—2015	NEQ	IEC 60050-191:1990 «Международный электротехнический словарь. Часть 191. Надежность и качество услуг»
ГОСТ IEC 61508-3—2018	IDT	IEC 61508-3:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
ГОСТ Р 27.014—2019 (МЭК 62347:2006)	MOD	IEC 62347:2006 «Руководство по установлению требований к надежности систем»
ГОСТ Р 27.301—2011	NEQ	IEC 60300-3-1:2003 «Управление надежностью. Часть 3-1. Руководство по применению. Методы анализа для определения общей надежности. Руководство по методологии»
ГОСТ Р 27.606—2013	NEQ	IEC 60300-3-11:2009 «Управление надежностью. Часть 3-11. Руководство по применению. Техническое обслуживание, направленное на обеспечение надежности»
ГОСТ Р 51901.1—2002	IDT	IEC 60300-3-9:1995 «Менеджмент надежности. Часть 3. Руководство по применению. Раздел 9. Анализ риска технологических систем»
ГОСТ Р 51901.3—2007 (МЭК 60300-2:2004)	MOD	IEC 60300-2:2004 «Менеджмент надежности. Часть 2. Руководство по менеджменту надежности»
ГОСТ Р 51901.6—2005 (МЭК 61014:2003)	MOD	IEC 61014:2003 «Программа повышения надежности»
ГОСТ Р 51901.16—2017 (МЭК 61164:2004)	MOD	IEC 61164:2004 «Повышение надежности. Статистические критерии и методы оценки»
ГОСТ Р 53613—2009 (МЭК 60721-2-2:1988)	MOD	IEC 60721-2-2:1988 «Классификация внешних условий. Часть 2-2. Природные внешние условия. Осадки и ветер»
ГОСТ Р 53614—2009 (МЭК 60721-2-3:1987)	MOD	IEC 60721-2-3:1987 «Классификация внешних условий. Часть 2-3. Природные внешние условия. Давление воздуха»
ГОСТ Р 53615—2009 (МЭК 60721-2-4:1987)	MOD	IEC 60721-2-4:1987 «Классификация внешних условий. Часть 2-4. Природные внешние условия. Солнечное излучение и температура»
ГОСТ Р 57193—2016 (ИСО/МЭК 15288:2015)	NEQ	ISO/IEC 15288:2015 «Системная и программная инженерия. Процессы жизненного цикла систем»
ГОСТ Р ИСО 10007—2007	IDT	ISO 10007:2003 «Системы менеджмента качества. Руководящие указания по управлению конфигурацией»

Окончание таблицы ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО/МЭК 12207—2010	IDT	ISO/IEC 12207:2010 «Системная и программная инженерия. Процессы жизненного цикла программных средств»
ГОСТ Р ИСО/МЭК 15026—2002	IDT	ISO/IEC 15026:1998 «Информационная технология. Уровни целостности систем и программных средств»
ГОСТ Р МЭК 60300-1—2017	IDT	IEC 60300-1:2014 «Менеджмент надежности. Часть 1. Руководство по управлению и применению»
ГОСТ Р МЭК 61508-1—2007	IDT	IEC 61508-1:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
ГОСТ Р МЭК 61508-2—2012	IDT	IEC 61508-2:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
ГОСТ Р МЭК 61508-4—2012	IDT	IEC 61508-4:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
ГОСТ Р МЭК 61508-5—2012	IDT	IEC 61508-5:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
ГОСТ Р МЭК 61508-6—2012	IDT	IEC 61508-6:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению IEC 61508-2 и IEC 61508-3»
ГОСТ Р МЭК 61508-7—2012	IDT	IEC 61508-7:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
ГОСТ Р ИСО/МЭК ТО 15271—2002	IDT	ISO/IEC TR 15271:1998 «Информационная технология. Руководство по применению ISO/IEC 12207» (Процессы жизненного цикла программных средств)

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты;
- NEQ — неэквивалентные стандарты.

Библиография

[1]	ISO/IEC 15939	Systems and software engineering — Measurement process
[2]	DEF STAN 00-42	Part 3: Reliability and Maintainability Assurance Guide — Reliability and Maintainability Case
[3]	IEC 60300-3-10	Dependability management — Part 3-10: Application guide — Maintainability
[4]	IEEE Std 1175.1	IEEE guide for CASE tool interconnections — Classification and description
[5]	ISO/IEC 14102	Information technology — Guideline for the evaluation and selection of CASE tools
[6]	ISO/IEC 15940	Information technology — Software Engineering Environment Services

УДК 62-192:658.51.011:658.562:623:006.354 ОКС 03.120.01

Ключевые слова: надежность в технике, жизненный цикл, управление программой

БЗ 1—2020

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 03.12.2019. Подписано в печать 23.12.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 5,02. Тираж 40 экз. Зак. 552.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru