ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.405— 2011

Надежность в технике

ОТБРАКОВОЧНЫЕ ИСПЫТАНИЯ НА РАННИЕ ОТКАЗЫ СЛОЖНЫХ СИСТЕМ, ИЗГОТАВЛИВАЕМЫХ В ЕДИНИЧНЫХ ЭКЗЕМПЛЯРАХ

IEC 62429:2007
Reliability growth — Stress testing for early failures in unique complex system (NEQ)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

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

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 14 декабря 2011 г. № 1493-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта МЭК 62429:2007 «Повышение безотказности. Отбраковочные испытания на ранние отказы сложных систем, изготавливаемых в единичных экземплярах» (IEC 62429:2007 «Reliability growth — Stress testing for early failures in unique complex system»)

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

ОТБРАКОВОЧНЫЕ ИСПЫТАНИЯ НА РАННИЕ ОТКАЗЫ СЛОЖНЫХ СИСТЕМ, ИЗГОТАВЛИВАЕМЫХ В ЕДИНИЧНЫХ ЭКЗЕМПЛЯРАХ

Dependability in technics.
Stress testing for early failures in unique complex system

Дата введения — 2012—09—01

1 Область распространения

Настоящий стандарт представляет собой руководство по повышению степени безотказности во время любых видов заключительных испытаний и приемо-сдаточных испытаний уникальных сложных систем. Он дает указания по проведению и выбору условий ускоренных испытаний и критериям их завершения. Слово «уникальный» означает отсутствие информации о подобных системах, а небольшое количество произведенных систем обусловливает ограниченность информации, извлекаемой из результатов испытаний для использования в будущем производстве похожих или аналогичных систем.

Настоящий стандарт затрагивает вопросы роста безотказности восстанавливаемых сложных систем, состоящих из аппаратных средств со встроенным программным обеспечением (ПО). Он может использоваться для описания процедуры приемо-сдаточных испытаний в процессе приработки с целью гарантировать, что безотказность поставляемой системы не находится под угрозой из-за программных ошибок, ошибок, вызванных недостаточной квалификацией специалистов, или производственных ошибок.

Настоящий стандарт охватывает только период ранних отказов жизненного цикла системы и не затрагивает период постоянства отказов и период отказов из-за изнашивания и старения. Он может также использоваться, когда организация хочет оптимизировать продолжительность испытаний в ходе производства опытных образцов единичных или нескольких экземпляров систем.

Стандарт применим главным образом к большим системам аппаратных средств/ПО, но не относится к большим сетям, например телекоммуникационным и энергетическим, так как испытуемые части таких систем обычно не могут быть изолированы во время испытаний.

Стандарт не распространяется на ПО, проверяемое отдельно, но изложенные в нем методы могут быть использованы во время испытаний больших вложенных программ в эксплуатационных аппаратных средствах, при моделировании эксплуатационных нагрузок.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий стандарт:
ГОСТ Р 27.002—2009 Надежность в технике. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию 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 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

Издание официальное

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, определения и обозначения

3.1 Термины и определения

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

3.1.1 **сокращение времени:** Сокращение времени испытания путем уплотнения времени использования по сравнению с типовым временем в эксплуатации.

Примечание — Например, круглосуточное испытание системы, эксплуатируемой в течение 8 ч в сутки.

3.1.2 **время выполнения:** Время, требуемое для выполнения заданного числа транзакций.

3.1.3 **ошибка в программе:** Неявная неисправность ПО.

3.1.4 **индикатор безотказности:** Нефункциональный параметр, который указывает на возможное наступление отказа в ближайшее время.

3.1.5 **испытание на коэффициент успеха:** Многократно повторяющиеся испытания, в которых не должно быть отказов.

3.1.6 **система:** Совокупность взаимосвязанных и взаимодействующих элементов.

3.1.7 **транзакция:** Набор входных параметров и нагрузок, выбранных из эксплуатационных нагрузок системы.

3.1.8 **анализ первопричин:** Действия по выявлению причин неисправности или отказа, с тем чтобы их можно было удалить из проекта.

3.2 Обозначения

C — общее число транзакций;
$D(t)$ — число неисправностей, обнаруженных за время t;
F_u — неприемлемое число неудачных транзакций из общего числа C транзакций;
i — число неисправностей;
M — вероятность того, что система с неприемлемой вероятностью безотказной работы проходит испытания без отказов;
N — число транзакций, выполненных без отказа;
p — неприемлемая вероятность отказа за одну транзакцию;
t — время испытаний;
t_{status} — предельное время испытаний;
$T_{D(t)}$ — время испытаний, в течение которого были обнаружены $D(t)$ неисправностей;
T_i — время испытаний, в течение которого была обнаружена i-я неисправность;
T_{min} — минимальное время испытаний, которое должно быть накоплено системой при 0 отказов;
z — значение мгновенного параметра потока отказов;
z_i — значение мгновенного параметра потока отказов для неисправности i;
θ_i — наработка на отказ для неисправности i;
δ — отсутствие отказа за время T_{min} при заданном значении мгновенного параметра потока отказов;
r_c — предполагаемое число оставшихся скрытых неисправностей системы.

4 Основные положения

Настоящий стандарт относится к большим программно-аппаратным системам, проверяемым с помощью моделирования эксплуатационной нагрузки. Поэтому в ходе испытаний неизвестно, вызван ли этот отказ оборудованием, ПО, эксплуатационной нагрузкой или их комбинацией. Отказ может быть вызван неисправностью аппаратных средств, например неисправностью оперативной памяти, изменением синхронизации, приводящим к конфликту данных, или электромагнитными помехами, приводящими к изменению передаваемых данных. Отказ может также быть вызван скрытой неисправностью ПО или несанкционированной информацией. В целях настоящего стандарта вопрос восстановления неисправности оборудования или изменения ПО рассматривается только с учетом степени влияния на результаты испытания, например в связи с использованием статистической модели.

Почти все современные системы содержат встроенное ПО. Программное обеспечение, как правило, проверяют на разрабатываемых аппаратных средствах с использованием транзакций, полученных

из спецификаций системы. Часто разработка ПО затягивается, что ограничивает время тестирования ПО. Как правило, недопустимо, чтобы потребитель первым использовал ПО на действующем оборудовании. Таким образом, стандарт для руководства испытанием и повышения безотказности оборудования со встроенным ПО является актуальным.

Что касается оборудования, предполагают, что ранние отказы вызваны его скрытыми неисправностями. В зависимости от типа и уровня нагрузки эти скрытые неисправности могут через некоторое время привести к постоянным или периодическим отказам. Пример — трещина в компоненте. В условиях работы в сухой атмосфере, без вибраций или ударов неисправность может оставаться скрытой. Но при эксплуатации во влажной атмосфере влага и загрязняющие вещества могут проникать через трещину и привести к коррозии, заканчивающейся необратимой неисправностью. Кроме того, вибрации или удары могут вызвать трещины, что через некоторое время приводит к необратимой неисправности.

В отличие от оборудования ПО детерминировано. Это означает, что скрытая неисправность ПО (обычно называемая ошибкой ПО) не приведет к отказу, пока не будет активирована часть кода, содержащая эту скрытую неисправность. Момент, когда это происходит, зависит от условий эксплуатации (например, от входных параметров и внутреннего состояния программы, контента памяти). Таким образом, существует определенное сходство между скрытыми неисправностями аппаратных средств и скрытыми неисправностями ПО. Активированная скрытая неисправность ПО может вызвать необратимые неисправности и зачастую — быть единственной причиной перемежающегося отказа.

Логические сбои носят систематический характер (т. е. они могут быть воспроизведены по желанию, если известна инициация неисправности, имеющей к ним отношение). Так как пусковой механизм каких-либо скрытых неисправностей определяется наугад в операционной среде системы, логические сбои наблюдаются как стохастический процесс. Таким образом, могут быть применены обычные меры безотказности (вероятное время следующего отказа, интенсивность отказов и т. п.). Как правило, степень надежности растет, когда скрытые неисправности удалены.

Таким образом, термин «скрытая неисправность» в настоящем стандарте используется для определения слабых мест аппаратных средств и ошибок ПО.

Отказ, вызванный сочетанием скрытых неисправностей аппаратных средств и ПО, может, например, быть обусловлен тем, что скрытая неисправность аппаратных средств привела к недостаточному охлаждению компонентов. Повышение температуры изменило время задержки в цепи, в результате произошел конфликт данных, приведший к сбою ПО. Другая возможная комбинация — ошибки проектирования аппаратных средств стали причиной недостаточного экранирования сигнальных проводников. Повышенный уровень электромагнитных помех исказил данные в проводниках сигнала, вызвав сбой в ПО в случае, когда ПО не имело средств исправления ошибок или когда уровень электромагнитных помех среды эксплуатации высокий.

Настоящий стандарт касается восстанавливаемых систем, которые производятся в очень небольшом числе, и результаты предыдущих испытаний подобных систем ограничены или вообще отсутствуют. Настоящий стандарт может быть использован, когда производитель хочет оптимизировать продолжительность внутреннего приемо-сдаточного испытания и отладки. В настоящем стандарте рассматривают методы проверки степени повышения надежности до или в момент поставки готовой системы. Поэтому испытание допускается проводить на предприятии-изготовителе или на предприятии конечного пользователя. Он может также быть использован, когда организация хочет оптимизировать продолжительность окончательной аттестации производства при изготовлении отдельных элементов, небольших серий или в ходе испытаний прототипа.

Настоящий стандарт может быть использован для одной или нескольких больших систем для улучшения характеристик только этих систем. Если пользователь системы повышает степень надежности за счет обновления аппаратного обеспечения и ПО улучшенными версиями, настоящий стандарт может быть использован для контроля степени повышения надежности.

Стандарт распространяется не только на ПО. Он может быть использован, когда встроенное ПО проверено в аппаратной системе с помощью тестовых стратегий, которые выявляют уменьшение числа отказов в зависимости от продолжительности испытания, например испытание ПО с имитацией эксплуатационной нагрузки. Описанные методы хорошо подходят для тестирования и повышения стойкости ПО к переходным процессам и нарушениям, вызванным эксплуатационной нагрузкой и аппаратной системой. Настоящий стандарт предназначен для больших аппаратных систем/ПО, но не пригоден для больших сетей, например, телекоммуникационных и электроснабжения, так как отдельные части таких сетей трудно выделить в ходе испытаний.

Проверка степени повышения безотказности — метод выявления и устранения скрытых неисправностей, но его недопустимо использовать в качестве основного средства достижения желаемого уровня надежности производимых систем. Большие системы часто производят в небольшом числе,

иногда только одну или несколько систем. Таким образом, оставшиеся скрытые неисправности, возникшие в ходе разработки и производства, должны быть определены путем проверки степени повышения надежности готовой системы. Тем не менее, для уменьшения числа скрытых неисправностей в создаваемой системе выполняют надлежащий контроль процесса и такие превентивные методы, как анализ видов и последствий отказов, анализ дерева неисправностей и экспертиза проекта. Кроме того, необходимо контролировать производственные и монтажные процессы, например с помощью статистического управления производственным процессом.

В некоторых случаях можно разделить большую систему на ряд аналогичных модулей. В этом случае аналогичные модули рассматривают как партию. Это позволяет обнаруживать скрытые неисправности модулей, но не отказы, вызванные взаимодействием модулей и между модулями, а также встроенным ПО.

Отказы, возникшие в результате взаимодействия между модулями, могут быть выявлены только путем проверки степени повышения безотказности готовой системы. В современных системах многие отказы обусловлены взаимодействием аппаратных средств и ПО. Эти отказы не могут быть найдены до момента готовности и функциональности всей системы

Настоящий стандарт распространяется только на начальный период отказов жизненного цикла системы. Он не охватывает период случайных отказов и период отказов вследствие износа.

При планировании процесса проверки повышения степени безотказности принимающие решения лица должны тщательно рассмотреть временные и финансовые затраты относительно производительности системы с учетом рисков и расходов, связанных с ранними отказами системы после ее поставки. Все отказы, выявленные в ходе испытаний, должны быть тщательно проанализированы для того, чтобы найти основную причину и гарантировать возможность применения опыта для предотвращения аналогичных проблем в других системах. Законченная система должна быть восстановлена или обновлена, повторно тестирована для нормальной эксплуатации, и документация на нее должна быть соответствующим образом обновлена. Если между настоящим стандартом и соответствующим договором или спецификацией возникают расхождения, применяются последние.

5 Планирование и проверка повышения степени безотказности

5.1 Шаг 1. Следует ли применять проверку степени повышения безотказности?

Проверка повышения безотказности имеет смысл в следующих случаях:

- экономия затрат за счет сокращения ранних отказов больше, чем расходы на проверку, с учетом необходимого мониторинга и контрольно-измерительной аппаратуры;
- отсутствуют результаты ранее проведенных испытаний всей системы, поскольку была произведена только одна или несколько систем или только одна система должна быть испытана;
- ожидаются ранние отказы из-за скрытых неисправностей, возникших в процессе сборки в компонентах или вследствие несоответствия допусков компонентов системы;
- серьезные ранние отказы модулей и компонентов должны быть исключены путем определения безотказности с учетом нагрузок до начала испытания системы;
- ожидаются ранние отказы в результате взаимодействия аппаратной системы и встроенного ПО;
- модель испытаний предполагает повышение безотказности, т. е. параметр потока отказов за время испытаний должен уменьшиться;
- при проведении испытаний с использованием моделируемых эксплуатационных нагрузок возможны нагрузки выше средних и добавление необычных релевантных нагрузок (искаженных, несанкционированных данных или условий перегрузки);
- возможные скрытые неисправности аппаратных средств преобразуются в постоянные или перемежающиеся за счет увеличения нагрузок окружающей среды, т. е. из-за увеличения температуры, колебаний температуры, вибрации, ударов и т. п.

5.2 Шаг 2. Определение отказа и сбор данных

Практический подход заключается в составлении перечня требований к системе и выявлении параметров, которые следует контролировать. Затем необходимо определить, как контролировать систему в ходе испытаний. Техническое задание на проведение испытаний должно определить релевантные и нерелевантные отказы.

Релевантные отказы представляют собой как внезапные отказы (функция отсутствует), так и постепенные отказы (деградация). Затем нужно определить отказы, связанные с ПО, т. е. отсутствие ответа, неправильный ответ, блокировка системы или чрезмерно большое время отклика. Отказы могут быть вызваны оборудованием, встроенным ПО или взаимодействием аппаратных средств и ПО, напри-

мер, изменением значения времени задержки, приводящим к конфликту данных, или электромагнитными помехами, вызывающими изменение данных.

Нерелевантные отказы представляют собой отказы, вызванные испытательным оборудованием, контрольно-измерительной аппаратурой или операторами испытаний. Если проверка повышения степени безотказности предусматривает испытание устойчивости системы к человеческим ошибкам (ошибкам, допущенным оператором), эти ошибки будут определены как релевантные отказы.

Следует постоянно контролировать функции и производительность системы, по возможности. Если это невозможно, функциональные испытания, включая проверку функций резервных элементов, проводят в определенные промежутки времени. Когда прилагают циклические нагрузки, работу системы проверяют после каждого цикла. Статус резервирования и автоматической реконфигурирации, а также другие релевантные внутренние параметры системы проверяют в ходе испытаний.

Изменения в системе, например замена модуля или переключение режимов работы, также должны быть зарегистрированы. На практике принято отображать в протоколе испытаний все события: запуск, останов, отказ, обновление, изменение конфигурации, т. е. режим работы и т. п. Рекомендуется приглашать команду испытателей и операторов пользователя, с тем чтобы они высказали свои замечания и предложения по работе системы.

При проведении испытаний по методам 1, 2, 4, 5 и 6 следует регистрировать наработки до отказа. При этом должно быть задано эталонное время. Это может быть, к примеру, время испытаний в часах или минутах, эксплуатационное время или время работы центрального процессора. Чтобы сократить время испытаний, можно уплотнять время или увеличивать нагрузку (ускоренные испытания). В ходе испытаний по методу 3 регистрируют число транзакций до отказа.

5.3 Шаг 3. Уровни нагрузок

5.3.1 Общие положения

До начала процесса проверки степени повышения безотказности следует выполнить всесторонний анализ процедуры испытаний. Этот план должен содержать метод(ы) испытаний, а также процедуры принятия решений и уровень достоверности. Должны быть заданы виды анализа отказов и процедуры отчетности. Процессы должны быть адаптированы к конкретной системе, а также к доступному оборудованию формирования нагрузок и возможным способам нагрузки системы.

Для того чтобы как можно быстрее выявлять отказы, проявляемые как скрытые неисправности, испытуемые системы следует нагружать так, чтобы возникали релевантные неисправности, без введения отказов, не связанных с эксплуатационными отказами, и без существенного сокращения срока службы системы, т. е. без износа паяных соединений или без компонентов с ограниченным сроком службы. Условия испытаний могут находиться вне заданных условий эксплуатации, но должны соответствовать возможностям проекта. Цель — предотвращение повреждения системы и возникновения неисправностей, которые невозможны при эксплуатации.

Размер самых больших частей крупногабаритных систем ограничивает нагрузки, которые можно применять. Поэтому, как правило, используются низкие коэффициенты ускорения испытаний. Поскольку испытания предназначены для выявления ранних отказов, это редко становится проблематичным. Уплотнение времени ускоряет только виды отказов, вызываемых повышенной нагрузкой(ами). В результате некоторые виды отказов, например коррозия, не ускоряются, а даже сокращаются. Однако в большинстве случаев это не столь серьезная проблема, так как испытания предназначены для выявления ранних отказов, а не отказов, вызванных износом и старением.

В этом испытании используют увеличенные нагрузки для выявления скрытых неисправностей, проявляемых в виде отказов быстрее, чем при эксплуатации. Для методов, непосредственно основанных на убывающем времени испытаний, например таких, как методы 1.2, 3, 6 и 7, не нужно оценивать коэффициент ускорения. Для методов 1.1, 4 и 5, если указана требуемая безотказность при эксплуатации, коэффициент ускорения должен быть задан.

5.3.2 Увеличенная эксплуатационная нагрузка

Нагрузка, которую легче всего увеличить, — это, как правило, эксплуатационная нагрузка. Основой для определения эксплуатационной нагрузки в ходе испытаний служат графики эксплуатации и применения. Весьма полезный метод — уплотнение времени, т. е. увеличение числа рабочих нагрузок за единицу времени. В этом случае коэффициент ускорения эксплуатационной нагрузки можно легко оценить как отношение операций при испытании к операциям при эксплуатации за тот же период времени.

Эксплуатационную нагрузку ПО часто можно увеличить с помощью реальных или смоделированных входных данных, вводимых чаще или большего объема, чем при штатном режиме эксплуатации. Следует решить, должны ли эксплуатационные нагрузки имитировать обычные эксплуатационные нагрузки или же включать необычные эксплуатационные условия, такие как несбалансированная

нагрузка, разброс нагрузки или экстремальные условия эксплуатации, несанкционированные, ошибочные или поврежденные данные.

Как правило, следует использовать высокие заданные эксплуатационные нагрузки. При заключении соглашения стороны могут договориться о том, что нагрузка может быть выше указанной максимальной нагрузки. В отсутствие соглашения нагрузка должна быть не выше указанной в технических условиях, если иное не утверждено организацией, уполномоченной принимать управленческие решения. Для резервных или защитных устройств, которые, как правило, не функционируют в системе, должны быть созданы условия активации этих устройств через регулярные промежутки времени.

5.3.3 Увеличение нагрузки окружающей среды

5.3.3.1 Общие положения

Для больших систем возможные типы нагрузок ограничены большим размером систем, например система может быть слишком велика, чтобы поместиться в климатической камере или в оборудовании для испытания на вибрацию. Некоторые части системы могут быть недоступны как при монтаже, так и при эксплуатации. Кроме того, присутствие обслуживающего персонала может сократить возможность повышения уровня нагрузки, например температуры окружающей среды.

В плане испытаний должны быть приведены типы нагрузок, их уровни и продолжительность.

5.3.3.2 Тепловая нагрузка

Рабочая температура системы часто может быть увеличена за счет повышения температуры в комнате или ограничения охлаждения (т. е. перекрытия вентиляционных входов и выходов или снижения скорости вентиляции). Также может быть уменьшена скорость потока охлаждающей жидкости. Кроме того, температура может быть циклической (термоциклирование). Термоциклирование должно включать в себя холодный старт, так как это часто приводит к максимальному тепловому градиенту в системе.

5.3.3.3 Уровень влажности

Испытание на стойкость к коррозии обычно проводят на уровне компонентов, а высокая относительная влажность воздуха может вызвать увеличение утечки токов.

Испытание на электростатический разряд проводят, как правило, отдельно, но низкая относительная влажность воздуха может быть изменена из-за присутствия обслуживающего персонала и работы движущихся частей. Таким образом, в некоторых случаях может быть соответствующее увеличение или уменьшение относительной влажности в системе или части системы в ходе испытания.

5.3.3.4 Механическое напряжение

Механические колебания могут быть введены с помощью вибрации оборудования или воздействия на шасси системы.

5.3.3.5 Напряжение и электрические импульсы

Напряжение питания может быть увеличено или уменьшено в нужную сторону. Переходные процессы могут быть введены в источники питания и сигнальные кабели.

5.4 Шаг 4. Анализ отказов и классификация отказов

5.4.1 Общие положения

Когда наблюдается отказ, в первую очередь следует зафиксировать время испытаний или число транзакций до отказа. После этого принимают решение, должна ли система быть остановлена из-за отказа или она может продолжать работать. Остановить работу системы может быть необходимо по следующим причинам:

- по соображениям безопасности;
- для того, чтобы отказ не привел к вторичному отказу, разрушению системы или ее части;
- в целях проведения анализа неисправности;
- для устранения неисправности, например ремонта составной части или замены элемента.

Как только классификация отказа установлена, должно быть принято решение: неисправный элемент должен быть восстановлен немедленно, или ремонт следует отложить. В некоторых случаях возможно продолжение испытаний при условии, что анализ указывает на вероятность того, что отказ не приведет к вторичным отказам и что все еще возможно проверить главную часть оставшейся системы. Это решение будет требовать инженерных знаний системы. В протоколе испытаний должно быть зарегистрировано, что часть системы не работает или не контролируется из-за неустраненной неисправности.

Если принято решение отложить ремонт, влияние на дальнейший ход испытаний должно быть рассмотрено и документировано, что часть этой системы не будет работать или избыточность может быть сокращена в ходе дальнейших испытаний. Оборудование с отказавшей составной частью обычно может быть отремонтировано путем замены модуля, компонента или перенастройкой. Замененные модули и компоненты будут сохранены для последующего анализа отказов. Как можно скорее должен быть сде-

лан тщательный анализ первопричин каждого отказа в целях реализации мер по исправлению положения в системе

Для связанных с ПО отказов вид отказа часто может быть устранен путем изменения кода. Обычно эти изменения вносят в качестве новой версии ПО, но часто может быть возможно продолжение испытаний следующим образом:

- регистрация отказа и времени испытаний до каждого отказа, но не прекращение испытаний в случае нового отказа;
- регистрация отказа и времени испытаний до каждого отказа и перезагрузка ПО в случае нового отказа;
- регистрация отказа и времени испытаний до каждого отказа и включение вставки в ПО, которая нейтрализует отказ, когда он происходит. Это может привести часть ПО в нерабочее состояние во время испытаний, что также должно быть указано в протоколе испытаний.

При продолжении испытаний должны быть учтены отказы, наблюдаемые в других частях системы. Должны быть рассмотрены реконфигурации и избыточность в системе. Это позволит продолжить испытания, но также это может означать, что наблюдаемые отказы могут быть вызваны неисправностью в другом модуле системы. Кроме того, должна быть проанализирована вероятность того, что местные неисправности из-за избыточности и автоматической реконфигурации не вызывают отказа системы. Таким образом, статус избыточности и автоматической реконфигурации, так же, как и другие соответствующие внутренние параметры системы, должны быть проверены в ходе испытаний.

Все отказы должны быть классифицированы как учитываемые или неучитываемые. Только учитываемые отказы используют в оценках безотказности и при принятии решений.

5.4.2 Учитываемые отказы

Учитываемые отказы вызваны слабыми компонентами, неадекватным дизайном, недостатками технологических процессов, скрытыми неисправностями ПО или взаимодействием между аппаратными средствами и ПО. Если устойчивость системы к ошибкам, допущенным оператором, включена в испытание, такие ошибки должны быть определены как учитываемые отказы.

5.4.3 Неучитываемые отказы

Неучитываемые отказы, как правило, вызваны ошибками человека, технического обслуживания или испытательным оборудованием. Их следует рассматривать как отказы, которых можно было бы избежать путем изменения процедур эксплуатации и обслуживания.

5.5 Шаг 5. Критерии остановки

5.5.1 Общие положения

Поскольку испытание основано на повышении безотказности, т. е. уменьшении числа отказов за один испытательный час, важно иметь критерии для прекращения испытаний. Такими критериями могут быть:

а) фиксированная программа испытания (5.5.2, методы 1,1 и 1,2);
б) графический анализ (5.5.3, метод 2);
в) испытание на коэффициент успеха (5.5.4, метод 3);
г) оценка безотказности (5.5.5, метод 4);
д) сравнение с приемочным мгновенным параметром потока отказов (5.5.6, метод 5);
е) оценка остаточных скрытых неисправностей (5.5.7, метод 6),
ж) проверка индикатора надежности испытания (5.5.8, метод 7).

При отсутствии отказа за некоторое установленное время и каждый раз, когда отказ был выявлен, должно быть принято решение об окончании или продолжении испытания. Все отказы должны быть зарегистрированы с указанием времени до отказа так, чтобы они были представлены и включены в обновленную оценку безотказности, особенно если изменения (ремонт) неэффективно удалили эту неисправность в ходе дальнейшего функционирования системы (см. 5.6).

Методы 1.1, 1.2, 2, 4, 5 и 7 эффективны для систем, где ожидается, что будут доминировать связанные с оборудованием отказы, а методы 3 и 6 рекомендуется использовать там, где будут преобладать, как ожидается, отказы, связанные с ПО.

Методы 1.2, 2, 3, 6 и 7 не зависят от коэффициента ускорения, используемого при испытании. Для методов 1.1, 4 и 5 оценка коэффициента ускорения необходима, если пользователи хотят базироваться на результатах испытания на безотказность в полевых условиях (см. 5.3.1).

Процедура принятия решений и доверительные уровни для различных методов рассмотрены в 5.5.2—5.5.8.

5.5.2 Метод 1. Фиксированные программы испытаний

5.5.2.1 Метод 1.1. Фиксированное число испытательных циклов

Согласно этому методу испытание прекращают по истечении определенного числа циклов испытания. Испытательные циклы разрабатывают по методике, соответствующей виду системы. Количество циклов может быть определено одним из следующих способов:

- на основании предыдущего опыта (например, по результатам испытаний или эксплуатации в полевых условиях), когда предполагают продолжительность периода ранних отказов в эксплуатационном времени, известно число эксплуатационных часов, эквивалентное одному циклу испытаний. Необходимое число циклов может быть найдено путем деления продолжительности раннего периода отказов в часах на число эквивалентных эксплуатационных часов за один цикл испытаний. Преимущество метода заключается в том, что он очень прост, но требует знания продолжительности периода ранних отказов у аналогичных предыдущих систем;

- на основании опубликованных известных кривых эффективности различных стресс-методов. Число циклов может быть определено с учетом уменьшения возвращений еще одного стресс-цикла. Преимущество данного метода в том, что никаких предварительных знаний о продолжительности начального периода отказа не требуется. Недостатком является то, что кривые имеют общий характер и могут быть в лучшем случае приблизительным руководством для конкретной системы в стресс-условиях.

5.5.2.2 Метод 1.2. Фиксированное число безотказных циклов испытаний

Согласно этому методу испытания прекращаются по истечении заданного числа циклов испытаний, но последний цикл или определенное количество циклов должны быть без отказа.

В случае соответствующего отказа испытания продлеваются до необходимого числа безотказных циклов. Безотказной период может быть вычислен на основе прогнозов или знании о времени отказов слабых компонентов, известных из результатов предыдущих испытаний. Преимущество в том, что безотказной(ые) цикл обеспечивает(ют) повышенную уверенность в том, что ранние отказы системы были выявлены. Недостатком является то, что метод требует предварительного опыта работы с компонентами и модулями, используемыми в системе.

5.5.3 Метод 2. Графический анализ

В этом методе накопленное число учитываемых отказов представляют как функцию времени испытания для каждой отдельной системы. Как только обнаруживают учитываемый отказ, кривую корректируют. Трудность заключается в оценке того, как кривая может быть продолжена в будущем (см. рисунок 1).

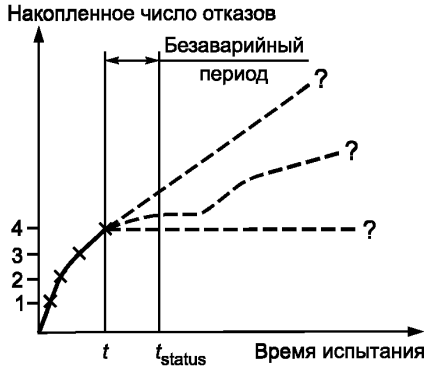


Рисунок 1 — Построение кривой отказов

Когда отказов не наблюдается за какое-то время или за фиксированное время t_{status}, построение кривой решений завершают. Эта кривая решений содержит один фиктивный отказ в конце времени испытаний (см. рисунок 2).

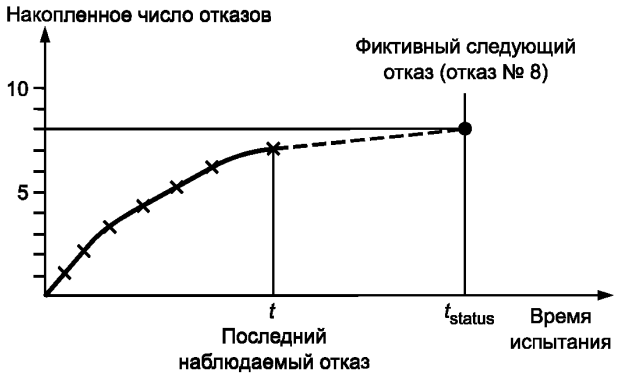


Рисунок 2 — Метод 2

Эта кривая решений может быть оценена. Критерий решения основывают на сравнении стоимости отказов, происходящих после поставки, с расходами на испытания.

Перед началом испытаний определяется минимальное число отказов в единицу времени испытания, которое обосновывает продолжение испытаний (например, один отказ за 24 ч испытаний). Это число может быть определено исходя из стоимости продолжения испытаний, расходов по устранению отказов во время испытаний или расходов по устранению отказов при эксплуатации системы, принимая в расчет эксплуатационные потери по причине отказов. Если наклон кривой решений в течение заданного времени (например, 24 ч времени испытаний) ниже согласованной стоимости, испытания останавливают.

5.5.4 Метод 3. Испытание на коэффициент успеха

5.5.4.1 Общие положения

Испытание на коэффициент успеха — это особый случай критерия, основанного на периоде, свободном от отказов. Целью испытания является подтверждение того, что вероятность отказа, скорее всего, будет ниже указанной верхней границы.

Проводят определенное количество испытаний системы со случайными эксплуатационными нагрузками. Если зафиксирован отказ, отказавшее изделие восстанавливают до начала продолжения испытаний. Продолжают испытание до тех пор, пока последовательные успешные транзакции не дадут достаточную уверенность в том, что вероятность выхода из строя находится на приемлемо низком уровне. Этот метод позволяет определить количество транзакций при условии, что определена максимально допустимая вероятность отказа. Метод предполагает, что каждая транзакция представляет собой независимый процесс из той же совокупности, имитирующей реальную эксплуатацию.

5.5.4.2 Количество необходимых транзакций

В этом методе моделируемые эксплуатационные нагрузки используют в качестве транзакций. Это гарантирует, что условия для тестируемой системы варьируются от транзакции к транзакции, например начальные условия, состояние буфера, регистры, меню пути и т. д. Поэтому скрытые неисправности, которые могут быть упущены при разработке программы испытаний, могут быть обнаружены этим методом.

В связи с тем, что только очень малая часть возможных комбинаций между входными параметрами, выходными параметрами и меню пути может быть реализована в ходе испытаний, нельзя быть уверенным, что вероятность отказа достаточно мала. Тем не менее можно вычислить вероятность того, что система с неприемлемой вероятностью безотказной работы прошла бы проведенные испытания. Транзакции считаются независимыми, если

$$M = (1 - p)^N, \quad (1)$$

где M — вероятность успешного прохождения системой N испытаний с неприемлемой вероятностью отказа p. Таблицы 1 и 2 приводят некоторые значения M для двух значений p и различных значений N.

Если C — общее количество транзакций в испытаниях и считается неприемлемым для F_u или более из них, которые привели к ошибке, то вероятность M того, что система с неприемлемой вероятностью отказа за транзакцию F_u/C прошла бы N испытаний успешно, может быть оценена так:

$$M = (1 - F_u/C)^N. \quad (2)$$

Таблица 1 — Вероятность того, что система с вероятностью отказа 0,001 пройдет N последовательных испытаний

$p = 0{,}001$	
N	$M = (1 - p)^N$
500	0,60638
600	0,54865
700	0,49641
800	0,44915
900	0,40639
1000	0,36770
1500	0,22296
2000	0,13520
2500	0,08198
3000	0,04971
3500	0,03014
4000	0,01828
4500	0,01108
4700	0,00907
5000	0,00672

Таблица 2 — Вероятность того, что система с вероятностью отказа 0,000001 пройдет N последовательных испытаний

$p = 0{,}000001$	
N	$M = (1 - p)^N$
1000000	0,36788
2000000	0,13534
3000000	0,04979
4000000	0,01832
5000000	0,00674
6000000	0,00248
7000000	0,00091
8000000	0,00034
9000000	0,00012
10000000	0,00005

5.5.5 Метод 4. Оценка безотказности

В этом методе используют статистические методы для оценки роста безотказности и сравнения оценки с безотказностью будущей системы.

5.5.6 Метод 5. Сравнение с приемочным мгновенным параметром потока отказов

5.5.6.1 Предпосылки для метода

Этот метод включает в себя выполнение программы повышения безотказности системы, состоящей из аппаратного обеспечения и ПО. В ходе этого испытания постоянно применяют стресс-воздействия на систему в целях выявления слабых мест разработки и производства. Испытания связаны с применением как внешних, так и эксплуатационных нагрузок, в том числе экстремального потока данных

и создания условий для выявления скрытых неисправностей. По мере выявления и устранения скрытых неисправностей при разработке и производстве безотказность системы начинает расти. Этот рост моделируется с помощью модели роста безотказности, позволяющей группе разработчиков постоянно контролировать совершенствование безотказности. Наконец, математическое правило остановки определяет оптимальное время для выпуска системы.

Особенности программы испытаний включают в себя:

- процесс разработки, который полностью контролируется на предмет систематичности, предсказуемости, надежности и соответствия определенным методологиям и процедурам;
- все компоненты системы и материалы закупают у утвержденных поставщиков;
- все системные единицы произведены в условиях установившегося процесса;
- для системы выбран приемочный мгновенный параметр потока отказов в условиях испытаний. Он представляет собой определенный мгновенный параметр потока отказов, которого система должна достигнуть до прекращения испытаний. Предполагаемый фактор ускорения может быть использован для преобразования мгновенного параметра потока отказов от эксплуатационных условий к условиям испытаний (см. 5.3.1 и 5.5.1);
- этот приемочный мгновенный параметр потока отказов затем используют для определения минимального времени испытаний на основе вероятности не встретить какой-либо отказ в процессе испытания;
- стресс-испытание начинают, как только система доступна и продолжают до того, как система готова к поставке;
- испытание связано с применением внешних и эксплуатационных нагрузок, в том числе экстремальный трафик данных и условия для выявления слабых мест в новых проектах, а также испытание безотказности ПО при необходимости;
- по мере внесения изменений в конструкцию их включают в испытуемые системы;
- совокупность часов испытаний регистрируют для каждой системы, проходящей испытания;
- тест-мониторинг гарантирует, что все отказы системы, которые становятся явными на выходе, обнаружены.

По мере выявления и устранения в конструкции скрытых неисправностей компонентов и производственного процесса безотказность системы начинает расти.

5.5.6.2 Модель повышения безотказности

Модель повышения безотказности включает построение накопленной средней наработки на отказ на оси y и квадратного корня из суммарного времени испытания (T_i) на оси x. По мере появления отказов кривую роста безотказности обновляют. Улучшение безотказности будет наблюдаться как увеличение вертикальности наклона, в то время как ухудшение безотказности будет выражаться как уменьшение наклона. Эта модель роста безотказности позволяет команде разработчиков проводить мониторинг и отображать улучшение аспекта безотказности. При этом предполагается использовать модель роста безотказности не для определения количественных оценок или экстраполяции любых данных о безотказности или статистики, а в качестве графического инструмента для отображения хода испытаний для команды разработчиков. Следовательно, приемлемо объединять данные, полученные в ходе различных нагрузок и эксплуатационных испытаний. Пример модели повышения безотказности приведен в приложении Б.

5.5.6.3 Правило остановки

Правило остановки позволяет определить, когда система достигла предопределенного уровня безотказности, что позволяет завершить испытания. При каждом отказе время остановки пересчитывают, чтобы достичь предопределенного уровня безотказности. Все виды скрытых неисправностей могут обеспечиваться этим правилом остановки, оно также применимо и ко всей системе, так как объединяет аппаратные средства и ПО.

Каждая скрытая неисправность взаимосвязана с мгновенным параметром потока отказов. Скрытые неисправности с наиболее высоким параметром потока отказов должны проявляться первыми. В определенный момент все скрытые неисправности будут выявлены, либо останутся те скрытые неисправности, параметр потока отказов которых ниже, чем допустимый мгновенный параметр потока отказов z.

Правило остановки использует принцип скрытой неисправности мгновенного параметра потолка отказов, в силу чего у системы имеется неопределенное количество скрытых неисправностей, каждая из которых имеет свой мгновенный параметр потока отказов. У системы, которая в начальном состоянии содержала m скрытых неисправностей, будет наблюдаться уменьшение мгновенного параметра потока отказов, так же как число скрытых неисправностей из-за обнаружения и исправления будет уменьшаться по отношению к m. Если неисправности не корректируются или отказавший компонент заменяется ком-

понентом, содержащим такую же скрытую неисправность, тогда очевидно, что эта неисправность и связанный с ней мгновенный параметр потока отказов остаются внутри системы (см. 5.6). Далее скрытая неисправность мгновенного параметра потока отказов будет для краткости называться просто мгновенным параметром потока отказов.

Пример использования этого метода приведен в приложении Б.

Предположения для правила остановки могут представлять собой следующие варианты:

- в системе есть неопределенное количество скрытых неисправностей m;
- каждая скрытая неисправность i ($i = 1, \ldots, m$) независима, связана с мгновенным параметром потока отказов z_i и проявляется в виде пуассоновского случайного процесса;
- когда возникает отказ, его причину исследуют, а неисправность обнаруживают и устраняют. Во время исправления одной неисправности ни одна другая скрытая неисправность не возникает.

Правило остановки включает минимум времени T_{min}, чтобы избежать их завершения слишком рано:

$$T_{min} = -\frac{\ln \delta}{z}, \tag{3}$$

где z — допустимый мгновенный параметр потока отказов, а δ отражает вероятность, что не произойдет ни одного отказа за T_{min}. Предпочтительно иметь δ малой настолько, чтобы избежать ошибочного вывода о возможности закончить испытание, прежде чем встретятся отказы. Например, $\delta = 0{,}05$ означает, что вероятность достижения T_{min} без отказов составляет всего 5 %. Такое значение δ рекомендуется.

Когда же минимальное время испытания накоплено, правило остановки, указанное ниже, означает, что испытание должно завершиться за наименьшее время t, а именно:

$$\frac{1}{t - T_{D(t)}} + 3\sqrt{\sum_{i=1}^{D(t)} \frac{e^{-t/T_i}}{T_i^2 (1 - e^{-t/T_i})^2}} \le z. \tag{4}$$

Приемочный мгновенный параметр потока отказов z представляет установленный мгновенный параметр потока отказов, которого система должна достичь прежде, чем испытание будет завершено и система будет передана потребителю.

Выражение $1(t - N_{D(t)})$ в правиле остановки представляет точечную оценку мгновенного параметра потока отказов за период после последнего отказа.

Результаты испытания имеют смысл, только если требуемые параметры предназначенного применения соответствуют требуемым параметрам испытания.

5.5.7 Метод 6. Вычисление оставшихся скрытых неисправностей

Этим методом вычисляют параметры статистической модели отказов аппаратных средств и ПО системы как функции времени проведения испытания.

Соответствующие статистические модели основаны на наблюдаемом числе отказов в зависимости от времени испытания.

Статистическая модель должна быть оценена в соответствии с конкретными условиями испытания (например, уровень стресс-воздействий) и конкретной системой. Она имеет то преимущество, что вероятность определенного числа оставшихся скрытых неисправностей (например, менее одной скрытой неисправности) может быть оценена. Недостатком является более сложная процедура, которая включает в себя формирование статистической модели. В некоторых случаях статистическая модель не описывает данные достаточно адекватно. Ни одна модель не будет соответствовать данным точно, так что часто необходимо проверять модель по критерию согласия.

Использование этого метода включает в себя следующие шаги:

- регистрируют время испытания до каждого отказа;
- выбирают соответствующую статистическую модель отказа, позволяющую оценить количество оставшихся скрытых неисправностей;
- оценивают параметры модели, выбранные в шаге, на основе наблюдаемых отказов;
- определяют критерий остановки как вероятность того, что остальные скрытые неисправности в системе будут меньше, чем r_c выявленных скрытых неисправностей в системе (r_c может быть равно 1);
- вычисляют вероятность того, что остальные скрытые неисправности в системе будут меньше, чем r_c;
- продолжают испытания, пока вероятность не станет ниже требуемого указанного r_c.

5.5.8 Метод 7. Испытания по индикатору безотказности

Индикатор безотказности может быть использован для выявления скрытых неисправностей, прежде чем они проявят себя в виде отказов. Индикатор безотказности — это параметр, который не явля-

ется одним из функциональных параметров системы, но который может быть наблюдаемым в ходе испытаний. Примерами таких индикаторов являются, например, электрически контролируемый уровень шума или повышение температуры, контролируемое инфракрасной камерой. Кроме того, могут быть задействованы механические шумы и потребление мощности. Для ПО допустимо использовать время отклика.

В современных микропроцессорных системах могут быть встроены и апробированы ряд самопроверяемых или сканирующих границы функций, с тем чтобы проверить состояние системы.

Использование таких индикаторов безотказности должно быть согласовано в договоре и указано в протоколе плана испытания. Все данные по индикаторам безотказности должны быть тщательно проверены, и если скрытая неисправность будет найдена, должен быть сделан анализ причин ее возникновения. При отсутствии скрытых неисправностей работу системы, если это возможно, следует продолжить в течение достаточного времени для того, чтобы увидеть, если отказ выявится позже, что он был отмечен отклоняющимся значением индикатора.

Преимуществом метода тестирования индикатора является то, что он может обнаружить скрытые неисправности, прежде чем они разовьются в отказы. Кроме того, может быть легче контролировать второстепенные параметры, чем первичные (функциональные) параметры. Недостатком является то, что индикатор может обнаружить только определенные виды отказов, и нужно будет использовать большое количество индикаторов, либо система будет проверяться на наличие одного или нескольких крупных отказов и повреждений. Необходимы дополнительные исследования по индикаторам безотказности, прежде чем они будут широко использоваться в промышленности. Тем не менее они являются весьма перспективными в части тестирования и профилактики.

Все правильные, как и неправильные, решения должны быть зарегистрированы, и должна быть создана матрица, чтобы обобщить правильные индикации, а также все типы ошибок для каждого индикатора безотказности (см. таблицу 3). Процент наблюдений в каждой ячейке таблицы 3 должен быть зарегистрирован.

Для обеспечения эффективности каждый индикатор безотказности должен указывать на область или какой-либо конкретный компонент, где обнаружены потенциальные проблемы. Выбор индикаторов безотказности, следовательно, требует инженерных знаний о системе, а также хорошего знания отказов, их развития и первых признаков их появления.

Таблица 3 — Правильные и неправильные решения на основе индикаторов безотказности

Наличие скрытой неисправности	Индикатор безотказности результатов испытаний	
	Индикатор безотказности указывает на существование скрытой неисправности	Индикатор безотказности не указывает на существование скрытой неисправности
Скрытая неисправность существует	Правильное решение	Индикатор недостаточно чувствителен
Скрытая неисправность не обнаружена	Индикатор слишком чувствителен	Правильное решение

5.6 Шаг 6. Верификация ремонта и повышение безотказности

Когда после возникновения отказа вносят изменения в систему, чтобы удалить скрытые неисправности и улучшить систему, результат этих изменений должен быть оценен в последующих (или расширенных) испытаниях в отношении их эффективности, и необходимо убедиться, что это не еще один отказ, не проявлявшийся ранее. Дополнительное время испытаний будет зависеть от характера этих изменений. Изменения могут также быть проверены путем моделирования или отдельным, специально подготовленным испытанием, например ускоренным испытанием. Такая проверка часто будет не в состоянии обнаружить возможные взаимодействия измененной части системы с другой частью этой системы. Таким образом, испытание на системном уровне часто приходится продлевать, особенно если ремонт отложен и ряд изменений вносятся в систему в одно и то же время, например новая версия устройства или новые версии ПО.

По итогам проверки эффективности изменений должен быть уточнен ожидаемый рост безотказности. Любые наблюдаемые виды отказов, которые не были исключены системными изменениями, количество их повторений в испытании, а также любые дополнительные отказы, связанные с изменениями, должны быть включены в эту оценку.

5.7 Шаг 7. Отчетность и обратная связь

Окончательный отчет должен содержать следующую информацию:

- описание системы, включая пересмотр аппаратного обеспечения и ПО;
- адаптация к конкретным контрактам и системным требованиям (например, реорганизация и сокращение штатов);
- контроль параметров и определение отказов (см. 5.2);
- краткие справки по эксплуатации и использованию — действующие нагрузки в ходе испытания (см. 5.3);
- проверка условий и оборудования (см. 5.3), виды и уровни стресс-воздействий, нагрузки и продолжительности циклов;
- сокращение срока службы недолговечных деталей;
- время отказов и их классификация (см. 5.4);
- процедура анализа отказов для поиска их причин (см. 5.4);
- критерии остановки и уровень достоверности (см. 5.5);
- прекращение испытаний (см. 5.5);
- ремонт и изменения, внесенные в ходе испытания;
- циклический рост испытаний в соответствующих случаях;
- изменения, внесенные в ходе испытания (новая версия аппаратного обеспечения и ПО), и то, как система была восстановлена, или обновление и повторное тестирование для нормального функционирования;
- изменения, сделанные после испытания, — системную документацию обновляют по мере необходимости;
- выводы по результатам испытания — достигнутая безотказность, если возможно, и уровень доверия.

Результат роста безотказности можно установить следующими способами:

- метод 1.1: фиксированная программа испытаний была принята без отказов или со следующими отказами (приводят перечень отказов);
- метод 1.2: последний цикл фиксированной программы испытаний прошел без отказов;
- метод 2: отказы не наблюдались во время испытания с момента A до момента B (в отчете должны быть даны числа A и B — см. рисунок 2);
- метод 3: N транзакций были выполнены без отказов. Вероятность того, что система имеет параметр потока отказов F_u/C, равна M или ниже (см. 5.5.4.2);
- метод 4: наработка на отказ системы после испытаний роста безотказности составляет (число, которое указывают в отчете);
- метод 5: мгновенный параметр потока отказов после повышения безотказности оценивается с помощью $\leq z$ [(см. уравнение (4)];
- метод 6: оцениваемое число оставшихся отказов < C;
- метод 7: во время испытаний не наблюдалось аномальных величин показаний индикаторов безотказности (в отчете должен быть перечень используемых индикаторов отказов).

Приложение А
(справочное)

Практический пример метода 3. Испытания на коэффициент успеха

Требуется испытать многократно применяемое встроенное ПО системы. Опыт показывает, что время испытаний будет зависеть от времени, необходимого для определения соответствующих скрытых неисправностей, заложенных в программу.

Для испытаний были записаны 25000 транзакций от реальной эксплуатационной нагрузки прежней системы. Они считаются покрывающими типичные эксплуатационные случаи испытуемой системы.

Решено, что система может быть переведена из режима испытаний в режим нормальной эксплуатации, если вероятность более 5 таких транзакций вызывает отказ меньше или равный 10 % (то есть $F_u = 5$).

Число необходимых транзакций в ходе испытания определяют по формуле

$$M = (1 - F_u/C)^N \qquad (A.1)$$

или

$$0{,}10 = (1 - 5/25000)^N = (0{,}9998)^N,$$

где $N = 11500$ транзакций.

Поэтому 11500 из 25000 транзакций необходимо выбрать случайным образом.

Если неисправности не обнаружены, испытание пройдено и может быть остановлено.

Приложение Б
(справочное)

Практический пример метода 5. Сравнение с приемочным мгновенным параметром потока отказов

Б.1 Участок роста безотказности

Пример метода показан с использованием данных, содержащихся в таблице Б.1. Накопленное время испытаний до отказа для каждой неисправности представлено в графе 2. После каждого наблюдаемого отказа эта информация затем преобразуется в графах 4 и 5 и используется для построения осей Y и X соответственно участку роста безотказности, а также для определения момента остановки (графа 5). Полученный участок роста безотказности показан на рисунке Б.1. Можно заметить из таблицы Б.1 и из рисунка Б.1, что устойчивый рост безотказности происходит примерно через 42000 накопленных минут испытаний (20-го отказа).

Примечание — При испытаниях ПО время испытания часто измеряют в минутах.

Таблица Б.1 — Пример роста безотказности и моментов остановки

№ отказа i	Накопленное время до отказа T_i, мин	Накопленная наработка на отказ $\theta_i = \frac{T_i}{i}$, мин	$\sqrt{T_i}$, мин^{0,5}	Момент остановки t, мин
1	2	3	4	5
1	1	1	1	10010
2	60	30	8	10070
3	8230	2743	91	31130
4	8300	2075	91	35030
5	8350	1670	91	37570
6	12568	2095	112	42510
7	15556	2222	125	47260
8	19876	2485	141	52590
9	19900	2211	141	56150
10	19910	1991	141	59220
11	27200	2473	165	64570
12	27210	2268	165	67770
13	27700	2131	166	79850
14	28660	2047	169	73840
15	34450	2297	186	78080
16	37400	2338	193	81660
17	37410	2201	193	84350
18	41250	2292	203	87920
19	42000	2211	205	90660
20	42100	2105	205	93130
21	44020	2096	210	95940
22	48600	2209	220	99360
23	51600	2243	227	102430
24	55100	2296	235	105600
25	82100	3284	287	117120
26	108300	4165	329	133740



Рисунок Б.1 — График роста безотказности по данным таблицы Б.1

Б.2 Правило остановки

Приемочный мгновенный параметр потока отказов принят $z = 1 \times 10^{-4}$ отказов на минуту испытаний, и δ выбрана равной 0,05. Минимальное время испытания T_{min} рассчитывают следующим образом:

$$T_{min} = -\frac{\ln \delta}{z} = -\frac{\ln(0{,}05)}{1 \times 10^{-4}} = 30000.$$

Испытание не следует прекращать до 30000 мин, даже если отказов не возникало. Как только происходит каждый отказ, время остановки пересчитывают.

Графа 5 таблицы Б.1 показывает предположительное время остановки. Если первый отказ появляется хотя бы после 1 мин, $T_{D(X)}$ в этом случае равно 1 и расчет времени остановки после отказа № 1 приведен ниже:

$$\frac{1}{t - T_{D(t)}} + 3 \times \sqrt{\sum_{i=1}^{D(t)} \frac{e^{-t/T_i}}{T_i^2 (1 - e^{-t/T_i})^2}} = \frac{1}{t-1} + 3 \times \sqrt{\frac{e^{-t/1}}{1^2 (1 - e^{-t/1})^2}} \le z = 1 \times 10^{-4}.$$

Наименьшее значение t (до ближайших 10 мин), которое удовлетворяет этому уравнению, составляет 10010 мин.

Примечание — Эта величина меньше, чем минимальное время испытания.

Предполагаемое время остановки для отказа № 3 составляет 31130 накопленных минут испытания. Расчеты приведены ниже:

$$\frac{1}{t - T_{D(t)}} + 3 \times \sqrt{\sum_{i=1}^{D(t)} \frac{e^{-t/T_i}}{T_i^2 (1 - e^{-t/T_i})^2}} = \frac{1}{t - 8200} + 3 \times$$

$$\times \sqrt{\frac{e^{-t/1}}{1^2 (1 - e^{-t/1})^2} + \frac{e^{-t/60}}{60^2 (1 - e^{-t/60})^2} + \frac{e^{-t/8230}}{8230^2 (1 - e^{-t/8230})^2}} \le z = 1 \times 10^{-4}.$$

Наименьшее значение t, удовлетворяющее этому уравнению, составляет 31130 мин.

Этот результат показывает, что испытание продолжается до 31130 накопленных минут. Тем не менее, следует отметить, что до того, как этот период времени будет достигнут, был обнаружен другой дефект, продливший время остановки до 35030 мин. Испытание прекращается, если этот момент остановки был достигнут без каких-либо дальнейших отказов.

В этом примере испытание было остановлено после 133740 мин (около 3 мес испытаний), поскольку ни один отказ не наблюдался между 108300 и 133740 мин.

УДК 62-192:658.562:006.354 ОКС 21.020 Т59

Ключевые слова: надежность, сложные системы, единичные экземпляры, испытания на ранние отказы

Редактор *П.М. Смирнов*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 29.07.2014. Подписано в печать 12.08.2014. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,20. Тираж 113 экз. Зак. 3101.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru