Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Гребенюк Виктор Михайлович
Московский государственный технический университет радиотехники, электроники и автоматики, МГТУ МИРЭА
Аспирант
Grebenyuk Viktor Mikhaylovich
Moscow State Technical University of Radioengineering, Electronics and Automation, MSTU MIREA
Post-graduate student
E-Mail: viktor.grebenyuk@gmail.com

Кузнецов Никита Викторович
Московский государственный технический университет радиотехники, электроники и автоматики, МГТУ МИРЭА
Соискатель
Kuznetsov Nikita Viktorovich
Moscow State Technical University of Radioengineering, Electronics and Automation, MSTU MIREA
E-Mail: nikita.v.kuznetsov@yandex.ru

Стандартизация и контроль качества продукции

Особенности тестирования надежности сложных информационных систем

Speciality of reliability testing of complex information systems

Аннотация: Обеспечение качества сложных информационных систем уже является трудоемкой задачей, ввиду особенностей таких систем. Однако к некоторым типам сложных информационных систем также предъявляются дополнительные требования для обеспечения высокой надежности, что требует ещё более тщательно разработанного подхода, ведь ценность результатов тестирования во многом определяется реалистичностью смоделированных сценариев использования и реалистичности конфигурации среды, в которой проводятся тесты.

Abstract: Quality assurance of complex information systems is a complicated task, because of the nature of such systems. Although, there are some complex information systems having additional reliability requirements which require even more considered quality assurance approach, because the value of the testing results strictly depends on a degree of realism of the selected use cases and environment setup used for testing.

Ключевые слова: Обеспечение качества, надежность систем, сложные информационные системы.

Key words: Quality assurance, system reliability, complex information systems.

***

1. Введение

В настоящее время почти все сложные информационные системы имеют как функциональные, так и нефункциональные требования и, как следствие, возникает необходимость в проведении тестирования на соответствие всему спектру предъявляемым требованиям. Традиционно, функциональному тестированию уделяется бóльшая часть внимания, и нефункциональное тестирование, зачастую, ограничивается только проверками

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

производительности, а остальные типы нефункционального тестирования, при этом, опускаются. В частности, должного внимания не уделяется тестированию на соблюдение требований «надежности», не смотря на то, что для большинства сложных систем помимо производительности, так же крайне важна их безотказность и работоспособность [5]. Одно из причин этого, является отсутствие универсальных методов и алгоритмов тестирования надёжности сложных информационных систем, а также критериев оценки надёжности и заданного уровня их значений [1].

Стандарт ГОСТ Р ИСО/МЭК 9126-93, описывают «надежность» (reliability), как одну из характеристик качества программного обеспечения, наряду с функциональными возможностями (functionality), практичностью (usability), эффективностью (efficiences), сопровождаемостью (maintainability) и мобильностью (portability) [2]. К подхарактеристикам надежности ПО относятся:

- безотказность – атрибут, который определяет функционирование системы без отказов (программы или оборудования);
- устойчивость к ошибкам – атрибут, который показывают на способность ПО выполнять функции при аномальных условиях (сбоях аппаратуры, ошибках в данных и интерфейсах, нарушениях в действиях оператора и др.);
- восстанавливаемость – атрибут, который показывают на способность программы к перезапуску для повторного выполнения и восстановления данных после отказов.

К некоторым типам систем (реального времени, радарных, систем безопасности, коммуникация и др.) предъявляются требования для обеспечения высокой надежности (недопустимость ошибок, точность, достоверность, удобство применения и др.) [1].

Данная статья описывает комплексный подход к тестированию надёжности системы с учётом особенностей сложных информационных систем, включая различные виды тестирования отказоустойчивости сложных информационных систем, параметры и метрики, подлежащие контролю при проведении такого тестирования, а также рекомендации для повышения корректности и эффективности проведенных тестов, ввиду особенностей тестирования надежности сложных информационных систем.

2. Анализ существующих практик проведения тестирования надежности программного и аппаратного обеспечения в целом

Вопросы обеспечения надёжности программного и аппаратного обеспечения широко представлены в литературе, что служит дополнительным индикатором актуальности данной темы. Бóльшая часть публикаций и учебных курсов посвящена методам повышения надёжности при разработке систем. Стоит отметить, что вопросы надёжности программного и аппаратного обеспечения часто рассматриваются отдельно, а не в совокупности [6,7].

Ещё одна часть публикаций, посвящена моделям оценки надёжности [5]. На данный момент времени разработано большое количество моделей надежности программных средств и их модификаций. Каждая из таких моделей определяет функцию надежности, которую можно вычислить при задании ей соответствующих данных, собранных во время функционирования систем или подобранных на основе дополнительных алгоритмов [8].

Другое направление публикаций представляет научно-прикладной материал, отражающий подходы и методы тестирования надёжности, а также применение таких подходов на практике [4,9]. Однако, как отмечено выше, зачастую, тестирование надёжности сводится к проведению отдельного вида тестов, например нагрузочного[4].

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Подводя итог анализа существующих практик проведения тестирования надежности программного и аппаратного обеспечения в целом, стоит отметить, что среди представленных публикаций отсутствуют примеры тестирования систем с учётом всестороннего анализа всех компонентов системы, включая как программные, так и аппаратные компоненты системы. Стоит также отметить, что ряд публикаций носит сугубо теоретический характер, что затрудняет корректное использование предложенных методов не практике.

3. Особенности обеспечения качества сложных информационных систем

Основной особенностью сложных информационных систем можно считать наличие нескольких подсистем, каждая из которых является отдельной системой, которые, в частности, обладают отдельной инфраструктурой, методологией разработки и жизненным циклом, технологиями разработки и обеспечения качества.

Исходя из перечисленных особенностей, можно выделить следующие особенности обеспечения качества сложных информационных систем:

1. Требуется комплексная координации активностей по обеспечению качества, в связи с большим количеством взаимодействующих частей;
2. Необходима четкая координация используемой инфраструктуры:
   - Контрольных данных,
   - Тестовых сред и стендов,
   - Версий программного обеспечения.
3. Необходима четкая координация активностей по созданию, верификации и исправлению документации для различных частей системы, гармонизированной в соответствии с жизненным циклом подсистем и их методологией разработки;
4. Необходима четкая координация активностей по управлению дефектами, найденными в отдельных подсистемах, но влияющих на функционирование всей системы;
5. Организационная структура системы обеспечения качества должна быть приспосабливаема к особенностям организационной структуры и штатного расписания различных подсистем.

Стоит отметить, что применение классических способов тестирования к распределённым информационно-управляющим системам (как частному случаю сложных информационных систем) либо не даёт должного эффекта, либо приводит к очень большим материальным затратам [3].

4. Способы построения механизмов отказоустойчивости

Как рассмотрено выше, понятие надежности системы сводится к обеспечению стабильности, устойчивости к ошибкам и восстанавливаемости системы, поэтому система проектируется с использованием специальных механизмов отказоустойчивости. В данном разделе проводится анализ механизмов отказоустойчивости: классификация этих механизмов с учетом достоинств и недостатков для каждого типа таких механизмов.

В большинстве случаев отказоустойчивость обеспечивается введением элементов избыточности (резервирования) в системе. Иными словами, для некоторых или всех компонентов (как для программных, так и для аппаратных) системы вводится аналогичный резервирующий компонент, идентичный основному по своей функциональности.

З

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Различные механизмы отказоустойчивости можно классифицировать с точки зрения резервирования компонент следующим образом:

1. Для компонент системы нет резервирования – при такой конфигурации в случае выхода компоненты из строя надо предпринимать действия по ее восстановлению;
2. Компоненты системы имеют «холодную замену» - то есть во время функционирования основной компоненты, замена остается в выключенном состоянии. В случае неполадок в основной компоненте, замена включается (вручную или автоматически), синхронизирует данные и начинает выполнять функции взамен основной компоненты.
3. Компоненты системы имеют «горячую замену» - то есть во время функционирования основной компоненты, замена включена, но не выполняет никаких функций, кроме синхронизации данных в некоторых случаях. В случае неполадок в основной компоненте, замена синхронизирует нужные данные и, не тратя времени на запуск, начинает выполнять функции взамен основной компоненты. В редких случаях для особо важных компонент «горячая замена» может выполнять абсолютно те же самые действия и вычисления, что и основная компонента, сравнивая выходной результат с вычислениями основной компоненты. Иными словами, одни и те же вычисления проводятся два раза (в замене и в основной компоненте) и результат сравнивается на выходе. Такие схемы вводят в случаях, когда вычисления или действия какой-то компоненты особо критичны.
4. Некоторые компоненты системы (особо критичные) имеют «горячую», а некоторые системы «холодную» замену. Такой подход позволяет сэкономить на ресурсах системы (подробнее об этом написано далее в разделе), обеспечив быстрое «переключение» для критичных компонентов в случае неполадок.
5. Для особо критичных систем вводятся несколько резервных копий компонентов, для того, что бы система продолжала работать даже в самых маловероятных ситуациях – когда отказ происходит и в основной компоненте, и в ее.
6. Иногда для увеличения пропускной способности системы (путем распараллеливания) для некоторых компонент вводятся, аналогичные им по функциональности компоненты, но обрабатывающие отличные друг от друга данные. В некоторых случаях эти компоненты могут служить друг для друга заменами – в случае отказа одной из компонент, все данные на обработку пойдут через другие компоненты.
7. Построение полной копии всей системы – для систем с особыми требованиями доступности, даже в случае глобальных катаклизмов (наводнение, война, пожар и пр.) выстраивается полная замена всей системы, как с программной, так и с аппаратной составляющей в другом дата центре, обычно сильно физически удаленном от дата центра основной системы.

Преимущества и недостатки каждого из перечисленных методов резервирования приведены в таблице 1.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Таблица 1

Преимущества и недостатки различных методов резервирования

Способ резервирования	**Преимущества метода**	**Недостатки метода**
1. Отсуствие резервирования	1. Экономия аппаратных ресурсов; 2. Экономия на проектировании и разработке сложных механизмов отказоустойчивости.	1. Значительное время на восстановление системы; 2. Система прекращает работу до момента полного восстановления; 3. Для восстановления системы необходимо человеческое вмешательство.
2. «Холодная» замена	1. Экономия аппаратных ресурсов (пока основная компонента работает, замене фактически не нужны аппаратные ресурсы); 2. Возможность разработки автоматических механизмов «переключения» на замену; 3. Система не будет функционировать только на время «переключения» на замену.	1. Для «переключения» на замену необходимо дополнительное время на включение и синхронизацию данных; 2. Необходимость разработки алгоритмов синхронизации основной компоненты и резервной копии.
3. «Горячая» замена	1. Наименьшее среди остальных вариантов время «переключения» на замену; 2. Возможность разработки автоматических механизмов «переключения» на замену; 3. Система не будет функционировать только на время «переключения» на замену.	1. Необходимы дополнительные аппаратные ресурсы для обеспечения работы резервной копии; 2. Необходимость разработки алгоритмов синхронизации основной компоненты и резервной копии.
4. Комбинация «горячих» и «холодных» замен	1. Относительная экономия аппаратных ресурсов; 2. Остальные положительные стороны «горячих» и «холодных замен», изложенные выше.	1. Недостатки режимов «горячей» и «холодной» замен, изложенные выше.
5. Несколько резервных копий на одну компоненту	1. Сверхнадежность.	1. Необходимость дополнительных ресурсов для замен; 2. Необходимость разработки дополнительных алгоритмов синхронизации данных между всеми заменами и основной компонентой.
6. Использование	1. Одним дополнительным	1. В случае выхода из строя одной

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

замен в качестве распараллеливания обработки	набором аппаратных ресурсов решается как проблема отказоустойчивости, так и проблема параллельной обработки данных.	компоненты, падает пропускная способность системы.
7. Построение полной копии системы	1. Работоспособность системы даже в случае глобальных катаклизмов.	1. Необходимость разработки сложных механизмов «переключения» между дата центрами (как с программной, так и с аппаратной точки зрения); 2. Двойные затраты на аппаратную составляющую системы; 3. Дополнительные затраты на аренду или построения дополнительного дата центра. 4. Разработка алгоритмов синхронизации данных между основной системой и ее заменой.

5. Виды тестирования отказоустойчивости

Принято делить факторы, влияющие на надежность программного обеспечения, на следующие 2 группы [7]:

1. Внутренние (ошибки проектирования при постановке задач; ошибки алгоритмизации задач; ошибки программирования; недостаточное качество средств защиты).
2. Внешние (ошибки персонала при эксплуатации; искажения информации в каналах связи; сбои и отказы аппаратуры ЭВМ).

Для того, чтобы обеспечить тестовое покрытие обоих типа факторов, предлагается разделить тесты на проверку отказоустойчивости на 3 основных типа, каждый из которых имеет свои подтипы: тестирование отказоустойчивости аппаратной составляющей системы, тестирование отказоустойчивости программной составляющей системы и тестирование восстановления системы после значительного сбоя (повлекшего сбой значительно части системы). В этом разделе мы рассмотрим каждый из этих типов подробно.

5.1. Тестирование программной составляющей

В тестировании программной составляющей можно выделить два основных подтипа тестирования в зависимости от механизмов резервирования: в случае, когда есть необходимость человеческих действий для преодоления последствий сбоев (в основном встречается в отсутствии резервирования) и в случае, когда механизмы отказоустойчивости автоматически переключают систему с поврежденной программной компоненты на ее замену.

5.2. Тестирование аппаратной составляющей

В зависимости от наличия механизмов отказоустойчивости в определенных аппаратных компонентах системы, можно проводить тестирование тех или иных компонент, наиболее часто встречающиеся: сервера, составляющие серверов, сервера баз данных, сетевая инфраструктура,

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

системы централизованного хранения данных (например, SAN – Storage Area Network).

Стоит заметить, что при тестировании аппаратной составляющей можно так же частично покрыть тестирование расположенной на ней программной составляющей. Так, например, отключение сервера повлечет за собой выход из строя расположенных на нем процессов.

5.3. Тестирование значительного сбоя

При наличии полной копии системы в отдельном дата центре проводится тестирование значительно сбоя – эмуляция глобального выхода из строя системы в основном дата центре и, как результат, перевод пользователей на запасной дата центр системы.

Стоит заметить, что тестирование значительного сбоя, или переход на запасной дата центр, в большинстве случаев является комплексной операцией, включающей в себя множество операций на инфраструктурном уровне, системном уровне и на уровне приложения.

6. Ключевые показатели для тестирования отказоустойчивости

Точно так же, как и в любом другом типе тестирования, при тестировании отказоустойчивости, должны быть определенные параметры и критерии (назовем их совокупно - метрики) по которым можно будет судить об успешности проведенного теста.

В данном разделе мы опишем часто используемые критерии оценки, применимые к тестированию надёжно сложных систем, и укажем наиболее подходящие метрики для конкретного вида тестирования отказоустойчивости.

Согласно общепринятому подходу, при анализе надежности ПО используются традиционные для технических систем критерии надежности [7]:

1. Вероятность безотказной работы.
2. Вероятность отказа.
3. Интенсивность отказов.
4. Средняя наработка на отказ.
5. Среднее время восстановления.
6. Коэффициент готовности.

На наш взгляд, можно отметить следующие показатели надёжности в тестировании отказоустойчивости сложных информационных систем:

1. Время предотвращение сбоя – суммарное время всех действий, необходимых для переключения компоненты на замену (или переключение всей системы на запасной дата центр).
2. Время возвращения в нормальное состояние – суммарное время всех действий, необходимых для переключения с резервной копии компоненты на основную компоненту (или переключение всей системы с запасного дата центра на основной).
3. Потери данных – наличие и количество потерянных данных во время сбоя.
4. Функциональные ошибки – наличие ошибок в функционировании системы во время обработки сбоя.
5. Утилизация аппаратных ресурсов – уровень использования аппаратных ресурсов

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

во время преодоления сбоев.

6. Влияние на метрики производительности – для систем с особыми требованиями к производительности, необходимо так же проверять влияние сбоя на производительность системы. Иными словами, стоит совмещать тестирование отказоустойчивости и производительности и обратить внимание на метрики производительности во время предотвращения сбоя.

Наиболее подходящие показатели для каждого из типов тестирования отказоустойчивости приведены в таблице 2.

Таблица 2

Примеры показателей надежности для различных типов тестирования отказоустойчивости

Тип тестирования	Наиболее подходящие показатели
Тестирование программной составляющей при мануальных действиях для предотвращения сбоев	1. Потери данных 2. Функциональные ошибки
Тестирование программной составляющей при автоматических действиях для предотвращения сбоев	1. Время предотвращение сбоя 2. Время возвращения в нормальное состояние 3. Потери данных 4. Функциональные ошибки 5. Утилизация аппаратных ресурсов 6. Влияние на метрики производительности
Тестирование аппаратной составляющей	1. Время предотвращение сбоя 2. Время возвращения в нормальное состояние
Тестирование значительного сбоя	1. Время предотвращение сбоя 2. Время возвращения в нормальное состояние 3. Потери данных 4. Функциональные ошибки 5. Утилизация аппаратных ресурсов

7. Корректность и эффективность проведения тестов отказоустойчивости

Существует множество факторов, которые надо учесть при проведении тестирования отказоустойчивости. В данном разделе мы рассмотрим наиболее значимые из них и проанализируем какие факторы наиболее критичны для каждого из видов тестирования отказоустойчивости.

На наш взгляд, от следующих факторов во многом зависит успешность и эффективность тестирования отказоустойчивости:

1. Тестирование одного одновременного сбоя – вероятность возникновения сбоев сразу в двух различных компонентах системы одновременно очень мала и, как следствие, для сокращения трудозатрат на тестирование стоит производить тестирование сбоя только в одном компоненте единовременно. Другими словами, при тестировании отказоустойчивости следует полностью восстановить систему от эмуляции текущего сбоя, прежде чем переходить к тестированию следующей

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

компоненты.

2. Проверка отказоустойчивости программной составляющей перед тестированием аппаратной составляющей – перед тем, как приступать к тестированию отказоустойчивости аппаратной составляющей, необходимо провести тестирование отказоустойчивости программной составляющей, расположенной на ней. Это необходимо для того, что бы при возникновении ошибок во время тестирования аппаратной составляющей можно было быть уверенным, что эти ошибки возникают не из-за некорректности механизмов отказоустойчивости аппаратной составляющей.
3. Необходимость понимания архитектуры системы для успешного создания сценариев тестирования отказоустойчивости – для успешного создания сценариев тестирования отказоустойчивости тестировщикам необходимо глубоко понимать архитектуру системы.
4. Необходимость вовлечения системных администраторов – так как, зачастую, тестировщики не обладают необходимыми правами доступа для эмуляции выхода из строя компонент, возникает необходимость вовлекать системных администраторов в тестирование отказоустойчивости для выполнения действий по эмуляции сбоев.
5. Необходимость функционирования компоненты во время проведения тестов на ее отказоустойчивость – необходимо создать такую ситуацию, что бы компонента функционировала (обрабатывала данные) во время эмуляции ее сбоя. Это необходимо для того, что бы реалистично провести тестирование, в особенности относительно проверок на потери данных.

Ключевые факторы для различных видов тестирования отказоустойчивости приведены в таблице 3.

Таблица 3

Ключевые факторы для различных видов тестирования отказоустойчивости

Тип тестирования	**Наиболее важные факторы**
Тестирование программной составляющей при мануальных действиях для предотвращения сбоев	1. Тестирование одного одновременного сбоя; 2. Необходимость детального знания архитектуры системы; 3. Необходимость вовлечения системных администраторов; 4. Необходимость функционирования компоненты.
Тестирование программной составляющей при автоматических действиях для предотвращения сбоев	1. Тестирование одного одновременного сбоя; 2. Необходимость детального знания архитектуры системы; 3. Необходимость функционирования компоненты.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://publ.naukovedenie.ru

Тестирование аппаратной составляющей	1. Тестирование одного одновременного сбоя; 2. Необходимость детального знания архитектуры системы; 3. Необходимость вовлечения системных администраторов; 4. Проверка отказоустойчивости программной составляющей перед тестированием аппаратной составляющей.
Тестирование значительного сбоя	1. Необходимость детального знания архитектуры системы; 2. Необходимость вовлечения системных администраторов.

8. Заключение

В статье был проведен анализ существующих практик проведения тестирования надежности программного и аппаратного обеспечения в целом, выделены особенности тестирования надежности сложных информационных систем, а также предложены различные виды тестирования отказоустойчивости сложных информационных систем, как и параметры, подлежащие контролю при проведении такого тестирования. Кроме того, были выработаны рекомендации для повышения корректности и эффективности проведенных тестов, ввиду особенностей тестирования надежности сложных информационных систем.

ЛИТЕРАТУРА

1. Волков В.Г., Автоматизированная система контроля и обеспечения надежности программных средств // http://www.unn.ru/pages/issues/vestnik/99999999_West_2009_5/27.pdf
2. ГОСТ Р ИСО/МЭК 9126-93 “Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению”
3. Ключёв А.О., Маковецкая Н.А., Проблемы тестирования системного информационного обеспечения распределённых информационно-управляющих систем // http://www.ict.edu.ru/ft/001795/vestnik10_7.pdf
4. Котов С.Л., Нагрузочное тестирование как элемент формирования безопасных систем // http://www.ooogic.ru/downloads/loading%20test%20as%20an%20element.pdf
5. Лаврищева Е.М. , Петрухин В.А., Методы и средства инженерии программного обеспечения // http://window.edu.ru/resource/699/41699/files/lavrishcheva_petrukhin.pdf
6. Липаев В.В., Проектирование и производство сложных заказных программных продуктов // http://www.computer-museum.ru/books/lipaev/lip_proektirovanie_slognoe.pdf
7. Павловская О.О., Статические методы оценки надежности программного обеспечения // http://dspace.susu.ac.ru/bitstream/handle/0001.74/778/7.pdf?sequence=1
8. Темичев А.А., Андреев Е.И., Кычкин А.В., Автоматический контроль надёжности системы распределённого мониторинга энергопоказателей // http://www.ssc.smr.ru/media/ipuss_conf/14/4_07.pdf
9. Jie M., Honlin Zh., Wenbo X., Jin L., Reliability Testing Methods for Critical Information System based on State Random // http://www.ipcsit.com/vol16/6-ICICM2011M009.pdf

Рецензент: Сидорин Виктор Викторович, заведующий кафедрой конструирования и производства радиоэлектронных средств факультета радиотехнических и телекоммуникационных систем МГТУ МИРЭА, доктор технических наук, профессор.