УДК 62-501.72:681.326.7

ПРИНЦИПЫ ПОСТРОЕНИЯ ОТКАЗОУСТОЙЧИВОЙ МНОГОЗАДАЧНОЙ РАСПРЕДЕЛЕННОЙ МНОГОМАШИННОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ СЕТЕВОЙ СТРУКТУРЫ

И.В. Ашарина
Акционерное общество «Научно-исследовательский институт «Субмикрон»
Россия, Москва, Зеленоград, Георгиевский проспект, дом 5, строение 2, этаж 4, помещение 1, комната 50
E-mail: asharinairina@mail.ru

А.В. Лобанов
Акционерное общество «Научно-исследовательский институт «Субмикрон»
Россия, Москва, Зеленоград, Георгиевский проспект, дом 5, строение 2, этаж 4, помещение 1, комната 50
E-mail: lav@se.zgrad.ru

В.Ю. Гришин
Акционерное общество «Научно-исследовательский институт «Субмикрон»
Россия, Москва, Зеленоград, Георгиевский проспект, дом 5, строение 2, этаж 4, помещение 1, комната 50
E-mail: grishin@se.zgrad.ru

В.Г. Сиренко
Акционерное общество «Научно-исследовательский институт «Субмикрон»
Россия, Москва, Зеленоград, Георгиевский проспект, дом 5, строение 2, этаж 4, помещение 1, комната 50
E-mail: submicron@se.zgrad.ru

Ключевые слова: сетецентрическое управление, многопроцессорные системы, репликация задачи, отказоустойчивость, взаимное информационное согласование, динамическая избыточность.

Аннотация. Рассматривается способ построения автоматической необслуживаемой многозадачной распределенной многомашинной вычислительной системы сетевой структуры, выполняющей набор целевых функций, необходимых внешним пользователям этой системы. Система характеризуется параллельным выполнением множества целевых задач, исполняемых на отдельных цифровых вычислительных машинах и в совокупности обеспечивающих выполнение задаваемых извне целевых функций. Предлагаются теоретически обоснованные решения, использующие репликацию задач. Рассматривается построение четырехуровневой архитектуры распределенных многомашинных вычислительных систем. Определяется суть предлагаемого интерфейса сбое- и отказоустойчивости системы, состоящего в парировании допустимых неисправностей и применения методов динамической избыточности. Используется наиболее общая модель враждебной (Византийской) неисправности.

1. Введение

Рассматриваются автоматические необслуживаемые многозадачные распределенные многомашинные вычислительные системы (РМВС) сетевой структуры, выполняющие набор целевых функций и характеризующиеся параллельным выполнением множества целевых задач на отдельных цифровых вычислительных машинах (ЦВМ), взаимодействующих между собой посредством взаимообмена сообщениями по каналам связи между ними. Создание таких РМВС из-за их сложности является бесполезным и весьма опасным без теоретически обоснованных решений в них вопросов

сбое- и отказоустойчивости (СОУ). Под СОУ понимается способность системы выполнять целевые задачи в условиях возникновения допустимых совокупностей неисправностей (сбоев и отказов) и их допустимых последовательностей. Качество СОУ в РМВС может достигаться двумя способами: 1) использованием аппаратурной избыточности входящих в нее ЦВМ (репликация аппаратуры), 2) решением одной и той же задачи на нескольких ЦВМ с последующим обменом результатами и выбором из них правильного (репликация задачи). В данной работе рассматривается второй способ достижения СОУ [1].

Игнорирование или недостаточное внимание проектировщиков РМВС к вопросам СОУ неизбежно приведет к появлению эффектов негативной эмерджентности, состоящих в трудно объяснимом, либо вообще необъяснимом ошибочном поведении РМВС или ее ошибочном результате. В данной работе предлагаются теоретически обоснованные решения, использующие репликацию задач: параллельное решение копий одной и той же задачи на нескольких ЦВМ, составляющих комплекс этой задачи, с взаимообменом результатами и выбором в каждой ЦВМ комплекса правильного результата, в предположении, что только меньшая часть этих результатов может быть ошибочной. Комплекс должен удовлетворять определенным структурным требованиям, при которых каждая исправная ЦВМ комплекса может определить вектор согласованных, возможно различающихся значений всех ЦВМ этого комплекса такой, что согласованное значение в векторе, соответствующее исправной ЦВМ, совпадает с его согласуемым значением [2-5].

По принятой классификации сетей рассматриваемые РМВС относятся к однора́нговым, децентрализо́ванным или пи́ринговым сетям – оверлейным компьютерным сетям, основанным на равноправии участников. В таких сетях каждый узел (peer) может выполнять как функции клиента, так и функции сервера. Это позволяет обеспечивать длительный срок активного существования и продолжительную траекторию управляемой деградации. Математическая модель РМВС представляет собой смешанный граф, размеченный в соответствии с составом, структурой, функциями (и другими свойствами) РМВС. В такой графовой модели вершины представляют собой ЦВМ, коммутаторы, маршрутизаторы, устройства сопряжения с широковещательными каналами связи (УСШ). Ребра – дуплексные каналы связи, дуги – симплексные или псевдосимплексные каналы связи.

Особенности РМВС, обеспечивающие их живучесть, достоверность получаемых результатов, пропускную способность: 1) автономность ЦВМ, отсутствие общей памяти, межмашинное взаимодействие по двухточечным и шинным каналам связи; 2) многоуровневость системы и отсутствие централизованного управляющего органа; 3) параллельное решение многих взаимодействующих между собой задач; 4) необходимость автоматической самоорганизации системы для обеспечения масштабирования и защиты от несанкционированного доступа и воздействий неисправностей; 5) работа в режиме реального времени; 6) большой срок активного существования, обеспечиваемый применением динамической избыточности и управляемой деградацией системы при возникновении отказов ее элементов; 7) высокие требования по живучести системы и достоверности результатов ее работы.

2. Принципы построения многоуровневой РМВС

Предлагается четырехуровневая архитектура РМВС. На нижнем, первом уровне располагаются отдельные ЦВМ с их аппаратно-программным обеспечением, выполняющим реализацию всех вышележащих архитектурных уровней РМВС.

На втором уровне находится подсистема системного самодиагностирования, осуществляющая также организацию подсистемы ведения единого системного времени РМВС. Кроме того функцией подсистемы системного самодиагностирования является создание диспетчерского комплекса формируемой РМВС. При этом вся анализируемая исходная совокупность ЦВМ и каналов связи между ними, а также между ЦВМ и внешней средой, предназначенная для реализации требуемой РМВС, рассматривается как исходная система (ИС), обладающая необходимыми качествами для создания в ИС подсистемы единого системного времени и подсистемы системного самодиагностирования ИС, определения всех исправных и неисправных элементов (ЦВМ и каналов связи между ними, а также каналов связи между ЦВМ и внешней средой) и формирования начальной конфигурации РМВС. Подсистема системного диагностирования начинает действовать при начальном включении ИС и ее диагностирующие механизмы строят в каждой исправной ЦВМ из ИС при помощи механизмов взаимного информационного согласования одинаковые таблицы технического состояния исходной системы (ТСИС) с указанием всех исправных ее элементов. Затем все исправные ЦВМ из ИС на основе информации из ТСИС согласованно выбирают одну и ту же группу исправных ЦВМ, которая, исходя из заданного для нее уровня требуемой сбое- и отказоустойчивости, является достаточной по количеству ЦВМ и связям между ними, а также между этими ЦВМ и внешней средой. Эта группа согласованно в ИС образует диспетчерский комплекс (ДК) формируемой РМВС, имеющий

требуемый уровень своей сбое- и отказоустойчивости и являющийся четвертым, высшим архитектурным уровнем создаваемой РМВС. Затем созданному ДК передается управление действиями по дальнейшему формированию РМВС, а также по управлению этой РМВС в процессе ее целевой работы.

Первой задачей, решаемой ДК, является формирование всех необходимых комплексов целевых задач, которые составляют третий архитектурный уровень создаваемой РМВС. Это формирование, основанное на использовании необходимых структурно-диагностических, диагностических, алгоритмически-диагностических моделей, а также моделей процессов идентификации проявлений неисправностей, моделей процесса деградации РМВС и модели описания РМВС [6 - 8], включает, во-первых, выделение структур всех комплексов целевых задач, их внутрикомплексных и межкомплексных связей, соответствующих заданным уровням их сбое- и отказоустойчивости [3, 4], и отображаемых в таблице рабочей конфигурации системы (ТРКС), хранимой в каждой исправной ЦВМ создаваемой РМВС, во-вторых, сценариев и временных диаграмм внутрикомплексных и межкомплексных взаимодействий, в-третьих, определение всех необходимых алгоритмов внутрикомплексных и межкомплексных действий по реализации в создаваемой РМВС ее целевой работы, а также по созданию в РМВС интерфейса ее сбое- и отказоустойчивости и управлению работой этого интерфейса. При этом как необходимое условие успешной работы ДК предполагается, что ему известно: структура ИС; маршруты, кванты (неделимые временные промежутки, в течение которых происходит передача сообщения между смежными ЦВМ) [9] и форматы получаемых и передаваемых сообщений; форматы всех внутрикомплексных и межкомплексных обменов.

ДК строит индивидуальный алгоритм каждой ЦВМ прикладной системы и размещает его в памяти соответствующей ЦВМ в виде скомпилированной резидентной программы, а также обеспечивает передачу в каждую ЦВМ индивидуального алгоритма и синхронный их запуск (с точностью до кванта) в определенный момент времени работы РМВС [9].

Суть интерфейса сбое- и отказоустойчивости РМВС состоит в реализации метода парирования допустимых неисправностей (получение правильных значений выходной информации РМВС на основе репликации решаемых задач в комплексах задач), а также использования динамической избыточности, обеспечивающей обнаружение и идентификацию проявлений допустимых неисправностей и их допустимых последовательностей как по месту их возникновения, так и по типу (сбой, программный сбой, отказ). При идентификации допустимых сбоев (эти сбои парируются за счет избыточного количества копий результатов и целевая работа комплекса продолжается) они одинаково фиксируются в ТРКС всех исправных ЦВМ данного комплекса и проверяются на соответствие обнаруженных проявлений неисправностей заданным критериям программных сбоев или отказов идентифицированных элементов РМВС. Если обнаруженные проявления неисправностей некоторой ЦВМ соответствуют критерию ее программного сбоя, то исправные ЦВМ данного комплекса фиксируют в своих ТРКС программный сбой этой ЦВМ, осуществляют реализованную в системе возможность (аппаратную, программную или аппаратно-программную) ее изоляции и сообщают об этом в ДК. В свою очередь ДК определяет временной период, на который комплекс с неисправностью может быть исключен из целевой работы РМВС, например, приостанавливая целевую работу некоторой части РМВС, и передает комплексу указание на проведение им в этот период восстанавливающих действий, состоящих в восстановлении в памяти восстанавливаемой ЦВМ необходимой информации из памяти других исправных ЦВМ комплекса и затем втягивания этой ЦВМ в совместную с другими исправными ЦВМ комплекса целевую работу.

Комплекс, после завершения действий по восстановлению, сообщает результаты в ДК, который предпринимает необходимые действия по восстановлению целевой работы всей РМВС. В случае идентификации отказа ЦВМ в некотором комплексе диспетчерский комплекс предпринимает действия по реконфигурации этого комплекса или путем включения в него запасной ЦВМ или, при отсутствии таковой, по переводу этого комплекса на целевую работу со сниженным уровнем его сбое- и отказоустойчивости. Такое взаимодействие в процессе реализации интерфейса сбое- и отказоустойчивости РМВС верхнего архитектурного уровня ДК с нижележащим архитектурным уровнем целевых комплексов обеспечивает самоуправляемую деградацию РМВС вплоть до ее критического уровня с последующим переходом в режим безопасного останова РМВС и сообщения об этом ее внешнему пользователю.

Целевая работа РМВС и ее взаимодействие с реализуемым в этой РМВС интерфейсом сбое- и отказоустойчивости, должны основываться на теоретически доказанных методах и механизмах по системному самодиагностированию РМВС, парированию допустимых проявлений неисправностей с их идентификацией по месту возникновения и по типу, реконфигурации РМВС и восстановления целевой работы РМВС при сбоях и программных сбоях, самоуправляемой деградации РМВС при отказах, переходом в режим безопасного останова РМВС при исчерпании запасных ресурсов РМВС или возникновении недопустимых совокупностей неисправностей или недопустимых последовательностей таких совокупностей. Сложность этих методов и механизмов, а также их теоретического

обоснования напрямую зависит от принимаемой при этом модели неисправностей элементов РМВС. Из всех известных и используемых моделей неисправностей наиболее общей является модель враждебной неисправности, при которой поведение неисправной ЦВМ может быть полностью произвольным, неодинаковым по отношению к другим ЦВМ РМВС и даже подобным злонамеренному. При этом обоснованные методы и механизмы защиты от враждебных неисправностей будут гарантировано защищать и от неисправностей всех других моделей. Такие теоретически обоснованные методы построения механизмов сбое- и отказоустойчивых РМВС в условиях возможности возникновения враждебных неисправностей имеются и приводятся в работах прилагаемого списка литературы. Именно модель враждебной неисправности предлагается использовать при создании рассматриваемых РМВС.

Применение модели враждебной неисправности требует использования в создаваемой РМВС определенных аппаратурной, программной и временной избыточности, и снижение этой избыточности при сохранении теоретической обоснованности принимаемых архитектурно-алгоритмических, аппаратурных и программных решений является актуальным направлением дальнейших научных исследований.

3. Выводы

Обязательными требованиями к рассматриваемым сбое- и отказоустойчивым РМВС являются:

1) вычислительная целостность, определяющая возможность ошибки в вычислениях или недопустимой задержки;

2) покрытие неисправностей, определяющее меру хорошей работы используемых механизмов отказоустойчивости и означающее условную вероятность правильного восстановления системы при возникновении неисправности.

Уязвимым местом РМВС является разрушение процессов самосинхронизации и самоорганизации, циркулирующих в системах информационных потоков.

В АО «НИИ «Субмикрон» имеется достаточно большой научно-теоретический задел в рассматриваемой области, а также определенный опыт в построении однокомплексных сбое- и отказоустойчивых многомашинных информационно-управляющих систем, а в настоящее время проводятся интенсивные теоретические разработки методов построения сбое- и отказоустойчивых многозадачных, многокомплексных РМВС. Эра таких систем уже наступила и отставшие сейчас в будущем отстанут безнадежно!

Список литературы

1. Лобанов А.В., Ашарина И.В, Гришин В.Ю., Сиренко В.Г. Макетный образец высокоадаптивной распределенной сетецентрической многокомплексной сбое- и отказоустойчивой управляющей системы – актуальная проблема // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10, № 1. С. 48-55.
2. Ашарина И.В., Лобанов А.В. Построение алгоритмов системного взаимного информационного согласования в системах управления группировками КА ДЗЗ и сокращение их временной избыточности // Специальный выпуск журнала «Вопросы электромеханики. Труды ВНИИЭМ», М: АО «Корпорация «ВНИИЭМ», 2017. С. 45-54.
3. Ашарина И.В., Лобанов А.В. Выделение комплексов, обеспечивающих достаточные структурные условия системного взаимного информационного согласования в многокомплексных системах // Автоматика и телемеханика. 2014. № 6. С. 115-131.
4. Ашарина И.В., Лобанов А.В. Выделение структурной среды системного взаимного информационного согласования в многокомплексных системах // Автоматика и телемеханика. 2014. № 8. С. 146-156.
5. Ашарина И.В., Лобанов А.В. Взаимное информационное согласование в неполносвязных гетерогенных многомашинных вычислительных системах // Автоматика и телемеханика. 2010. № 5. С. 133-146.
6. Лобанов А.В. Модели замкнутых многомашинных вычислительных систем со сбое- и отказоустойчивостью на основе репликации задач в условиях возникновения враждебных неисправностей // Автоматика и телемеханика. 2009. № 2. С. 171-189.
7. Лобанов В.А., Гришин В.Ю., Сиренко В.Г. Распределенное системное диагностирование враждебных неисправностей в неполносвязных многомашинных вычислительных системах // Автоматика и телемеханика. 2005. № 2. С. 148-157.
8. Лобанов А.В. Взаимное информационное согласование с обнаружением и идентификацией враждебных неисправностей в неполносвязных многомашинных вычислительных системах // Автоматика и телемеханика. 2003. № 6. С. 175-186.
9. Лобанов А.В., Ашарина И.В., Мищенко И.Г. Взаимное информационное согласование в неполносвязных многомашинных вычислительных системах // Автоматика и телемеханика. 2003. № 5. С. 190-198.