Считаем, что в данной работе новыми являются следующие положения и результаты: методология, основанная на гипотетических моделях механизмов зрения в биологических системах и на ее основе многоуровневая технология обработки, анализа, содержательного описания, вербализации и поиска графической информации о технических объектах на основе новых моделей и методов, содержащая обратные связи между уровнями с целью автоматического возврата и уточнения информации в области изображения, указанной последующими уровнями.

Литература

1. *Кучуганов А.В.*, Биоинспирированные методы в задачах обработки, вербализации и поиска графической информации // Приволжский научный журнал. – Н.Новгород: ННГАСУ, 2013. № 1. С. 49-55.

2. *Л. Заде.* Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 165 с.

3. Дескрипционная логика: материал из Википедии. Date Views 16.04.2013 http://ru.wikipedia.org/

4. wiki/Дескрипционная_логика#cite_note-DLHandbook-4, последнее изменение этой страницы 13.03.2013.

5. *Дуд А. Р.* Распознавание образов и анализ сцен / пер. с англ. А. Р. Дуд, П. Харт. – М.: Мир, 1976. – 368 с.

6. *Васильева Н. А.* Методы поиска изображений по содержанию / под ред. Н. А. Васильева // Программирование. 2009. № 3. С. 1-30.

Methodology of graphics information analysis in decision support systems

Alexandr Valeryevich Kuchuganov, *PhD, «CAD Systems Department»*
Izhevsk State Technical University

This paper describes the results of the study to improve the automation degree of universality and effectiveness of the two-dimensional image processing and three-dimensional objects on the basis of famous and hypothetical models of mechanisms of biological systems.

Keywords: image analysis, bioinspired algorithms, images verbalization, description logics, linguistic variables, fuzzy attributed relational graph, pattern recognition.

УДК 62-501.72:681.326.7

ПРОБЛЕМА ОТКАЗОУСТОЙЧИВОСТИ В СЕТЕЦЕНТРИЧЕСКИХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМАХ

Анатолий Васильевич Лобанов*, д-р.техн. наук, ученый секретарь,*
Тел.: 8-499-731-15-03, e-mail: lav@se.zgrad.ru
Владимир Григорьевич Сиренко*, д-р.техн. наук, генеральный директор*
Тел.: 8-499-731-15-03, e-mail: lav@se.zgrad.ru
ОАО «НИИ «Субмикрон»
http://submicron.ru

Рассматриваются проблема организации сбое- и отказоустойчивых одноранговых, распределенных сетецентрических информационно-управляющих систем, динамически организуемых и выполняющих многозадачную целевую работу ответственного применения в распределенных оверлейных компьютерных сетях, наиболее важные их характеристики, принципы построения и особенности, философские сущности с точки зрения отказоустойчивости. Приводятся сведения об основных теоретических результатах в рассматриваемой области.

Ключевые слова: сетецентрическая система, распределенная система, комплекс ЦВМ, информационная безопасность, одноранговая сеть, враждебная неисправность, сбое- и отказоустойчивость, многозадачность

Предстоящее широкое внедрение сетецентрических информационно-управляющих систем ответственного и критического применения требует уделять особое внимание вопросам их информационной безопасности. Одним из составляющих этой безопасности является обеспечение заданной сбое- и отказоустойчивости.

Сетецентрическая информационно-управляющая система представляет собой распределенную систему в виде набора независимых компьютеров, соединенных каналами связи, рассматриваемую пользователями в виде единой объединенной системы [1]. Наиболее важные характеристики такой системы: a) от пользователей скрыты различия между компьютерами и способы связи между ними; b) пользователи и приложения единообразно работают в общем информационном пространстве распределенной системы, независимо от того, где и когда происходит их взаимодействие; c) система относительно легко поддается расширению или масштабированию; d) возможно, что в системе некоторые ее части могут временно выходить из строя, при этом пользователи и приложения не уведомляются о том, что эти части заменены или отремонтированы или что добавлены новые части для поддержки дополнительных пользователей или приложений. Принципы построения распределенной сетецентрической информационно-управляющей системы: 1) открытость (взаимодействие с внешней средой), 2) самоорганизация, 3) слабая иерархия в контуре принятия согласованных решений, 4) параллельное решение взаимосвязанных задач в режиме реального времени, 6) обеспечение информационной безопасности (заданной достоверности выдаваемой информации, заданной сбое- и отказоустойчивости для каждой из решаемых задач критического применения).

А.В. Лобанов

В.Г. Сиренко

Особенностями распределенной сетецентрической информационно-управляющей системы ответственного применения являются: а) автономность ЦВМ, б) отсутствие общей памяти, в) межмашинное взаимодействие по двухточечным и шинным каналам связи; г) многоуровневость системы и отсутствие централизованного управляющего органа; д) необходимость самосинхронизации и самоорганизации системы для обеспечения масштабирования, защиты от внешних воздействий, воздействий неисправностей и ошибок проектирования; е) работа в режиме реального времени; ж) большой срок активного существования; з) высокие требования по надежности работы и достоверности результатов.

Уязвимое место идеи сетецентрических информационно-управляющих систем – это вмешательство в процессы самосинхронизации и самоорганизации, разрушение циркулирующих в системах информационных потоков.

По существующей классификации сетей системы рассматриваемого класса относятся к однора́нговым, децентрализо́ванным или пи́ринговым сетям — это оверлейные компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные серверы и каждый узел может выполнять как функции клиента, так и функции сервера.

В отличие от архитектуры клиент-сервера, такая организация позволяет обеспечивать длительный срок активного существования и продолжительную траекторию управляемой деградации.

«Философской» сущностью рассматриваемых систем с точки зрения сбое- и отказоустойчивости являются: 1) сложность; 2) необходимость согласованной работы их элементов; 3) практическая невозможность точных выводов о техническом состоянии системы; 4) необходимость самостоятельного формирования этих выводов на основе

принимаемых заранее и, возможно, неточных критериев; 5) необходимость уточнения этих критериев со стороны самой системы в процессе ее целевой работы, возможность к самообучению и самоадаптация таких систем к условиям применения; 6) необходимость принимать и выполнять самостоятельные решения о реконфигурации и управляемой деградации системы; 7) необходимость проектирования таких систем «сверху-вниз» в условиях четких определений, понятий и моделей.

Процесс проектирования рассматриваемых систем «сверху-вниз» кратко можно представить в виде этапов: 1) определение неформальной цели проекта; 2) системный анализ условий применения проектируемого объекта, определение и анализ существующих ограничений, предположений, гипотез, теорий; 3) формулировка формализованной цели проекта в рамках принятых ограничений, предположений, гипотез, теорий, условий применения; 4) разработка обобщенных, обоснованных методов и алгоритмов реализации формализованной цели проекта, их моделирование и оценка; 5) декомпозиция обобщенных алгоритмов на аппаратурные части и программные части; 6) разработка технических заданий на аппаратурные и программные части; 7) реализация аппаратурных и программных частей; 8) стыковка аппаратурных и программных частей; 9) комплексные испытания проекта. Первые четыре этапа определяют архитектурную часть проекта.

В соответствии с традиционным подходом к проектированию сбое- и отказоустойчивых систем сперва разрабатывается архитектура целевой системы без учета вопросов обеспечения сбое- и отказоустойчивости. Затем формируются ТЗ на аппаратурные и программные части, в которых требование на сбое- и отказоустойчивость системы часто формулируется в виде требования к продолжению целевой работы при отказе одного электро-радио изделия (ЭРИ). Разработчики аппаратурных и программных средств, исходя из такого требования, вводят в разработанную архитектуру известные им автономные механизмы обеспечения сбое- и отказоустойчивости, которые при последующем анализе такого введения могут потребовать коррекцию архитектуры проектируемой системы. Такие итерации повторяются до тех пор, пока не будет найдено удовлетворительное решение при данных предположениях. Однако такой процесс проектирования из-за высокой сложности системы может приводить к появлению в них негативных эффектов эмерджентности, состоящих в появлении ошибочного поведения из-за возникновения непредусмотренных системных явлений, неадекватности реалиям принятых моделей, ограничений или теорий. Такие эффекты, при их возникновении, чрезвычайно трудно поддаются анализу и обычно необоснованно «списываются» на еще не исследованные или не отработанные элементы технологии или защиты от внешних воздействий (например, недостаточную радиационную стойкость ЭРИ). Поэтому весьма важно на начальных, архитектурных этапах проектирования ставить и решать архитектурные проблемы обеспечения сбое- и отказоустойчивости, применять адекватные модели, ограничения, предположения и теории. Эти открытые проблемы рассматриваются в настоящей работе.

При разработке крупных информационных и управляющих систем происходит концентрация сложности на начальных этапах (анализ условий применения и требований, проектирование спецификаций системы, разработка обоснованных методов и обобщенных алгоритмов), в то время как сложность и трудоемкость последующих этапов снижается. При этом, чем лучше прорабатываются начальные этапы, тем больше снижается трудоемкость последующих этапов, и чем раньше обнаруживается ошибка, совершенная на начальных этапах проектирования, тем дешевле обходится ее исправление. Для преодоления сложностей начальных этапов разработки предназначен структурный анализ, начинающийся с общего обзора системы, который затем все более детализуется, приобретая иерархическую структуру со все большим числом уровней.

Факторами сложности при проектировании сбое- и отказоустойчивых систем рассматриваемого класса являются: а) неприемлемость традиционных моделей неисправностей ЦВМ; б) необходимость распределенного, синхронизированного и согласован-

ного принятия решения; в) необходимость организации и управления динамической избыточностью системы (самореконфигурация и самоуправляемая деградация системы с переходом в безопасный останов при исчерпании ресурсов) при возникновении неисправностей или манипулировании соотношением «производительность- достоверность» для различных параллельно решаемых взаимодействующих задач.

Из всех используемых в настоящее время моделей неисправностей ЦВМ наиболее общей является модель *враждебной* (byzantine, rigorous, malicious) *неисправности*, при которой поведение неисправного процессора или ЦВМ допускается полностью произвольным, в том числе и подобным «злонамеренному», включая его неодинаковость по отношению к другим элементам системы. Эта модель покрывает все остальные модели, и методы организации сбое- и отказоустойчивых вычислений в условиях возникновения враждебных неисправностей будут обеспечивать защиту и от неисправностей всех других моделей. Модель враждебной неисправности отражает сложность нахождения причинно-следственной связи между видами проявлений неисправностей и имеющимися в действительности неисправностями таких сложных объектов как современная ЦВМ.

Использование модели враждебной неисправности определяет необходимость применения структурной графовой модели системы, в которой вершины отображают ЦВМ, а ребра и дуги – каналы связи между ними.

Повышение отказоустойчивости сетецентрической распределенной системы может достигаться за счет дорогостоящего обеспечения отказоустойчивости входящих в нее ЦВМ путем применения в них *n*-модульной избыточности (резервирования) и мажорирования выходных значений всех избыточных модулей. Другой подход, более учитывающий сетевую особенность рассматриваемых систем (замкнутость системы, наличие большого количества взаимосвязанных распределенных ЦВМ и возможность оперативного формирования из них требуемых вычислительных структур), состоит в репликации задач и введении в систему динамической избыточности, обеспечивающих: 1) парирование проявлений допустимых враждебных неисправностей за счет параллельного выполнения одной и той же задачи на нескольких ЦВМ с обменом полученными результатами и выбором из них правильного, 2) обнаружение и идентификацию по месту возникновения и типу (сбой, программный сбой, отказ) возникающих неисправностей, 3) восстановление целевой работы и исправления ошибочной информации после сбоев и программных сбоев, 4) реконфигурацию системы (с использованием запасных элементов) и восстановление целевой работы после отказов, 5) управляемую деградацию системы с возможным допустимым снижением характеристик вплоть до предельно заданной возможной конфигурации, 6) безопасный останов системы при невозможности построения такой конфигурации, 7) возможность перераспределения ресурсов системы для изменения соотношения производительность-достоверность между различными решаемыми задачами. Именно этот подход рассматривается в данной работе.

Группа всех ЦВМ, решающих копии одной и той же задачи, называется комплексом. В многокомплексной системе имеются несколько пронумерованных комплексов, которые решают разные задачи, обменивающиеся между собой информацией. Практическое применение рассматриваемого подхода должно основываться на принятом всеми участниками проектирования наборе понятий, терминов, определений и моделей. В работе [2] представлены самые общие подходы, модели, ключевые определения и понятия, необходимые при проектировании систем рассматриваемого вида, которые отражают вышеотмеченную «философскую» сущность таких систем. Модели разбиты на шесть групп: 1) структурно-диагностические модели, 2) диагностические модели 3) алгоритмически-диагностические модели, 4) модели процессов идентификации, 5) модель процесса деградации, 6) описание системы.

Аппаратно-программные механизмы обеспечения сбое- и отказоустойчивости рассматриваемых систем можно разделить на две группы: базовые и основные механизмы. Базовые механизмы гарантируют необходимую синхронность и согласован-

ность действий всех элементов системы в условиях возникновения допустимых враждебных неисправностей. Синхронность обеспечивается путем организации в системе и непрерывной работы подсистемы единого системного времени, включающей средства как начальной, так и промежуточной синхронизации.

Начальная синхронизация [3] осуществляется при начальном несинхронном включении различных ЦВМ системы и формирует путем взаимообмена сообщениями между включенными ЦВМ начальную конфигурацию системы в момент, когда эта конфигурация будет содержать достаточное количество исправных ЦВМ при условии, что среди ЦВМ конфигурации может иметься допустимое количество враждебно неисправных ЦВМ. Промежуточная синхронизация обеспечивает на основе межмашинного взаимообмена сообщениями требуемую синхронность внутренних часов автономных ЦВМ, расходящихся из-за индивидуальных значений дрейфов этих часов и возникновения допустимых враждебных неисправностей.

Согласованность действий и принимаемых решений в различных ЦВМ и подсистемах гарантируется применением алгоритмов взаимного информационного согласования (ВИС) [4]. Достижимость ВИС составляет концептуальную основу создания отказоустойчивых алгоритмов для решения основных задач организации распределенных вычислений. В настоящее время разработано значительное число алгоритмов, различающихся по постановкам задачи и критериям эффективности. Целью всех этих методов являлось только достижение ВИС, и специальная задача обнаружения и идентификации проявлений неисправностей в процессе ВИС не ставилась. Более того, в [4] утверждалось, что враждебный отказ в процессе ВИС диагностировать невозможно. Однако, исследуемая в настоящей работе задача организации сбое- и отказоустойчивых вычислений в сетецентрических как полносвязных, так и неполносвязных системах на основе динамической избыточности требует разработки алгоритмов ВИС, которые вместе с достижением ВИС обеспечивали бы также обнаружение и идентификацию проявившихся в процессе ВИС враждебных неисправностей, предотвращающих накопление латентных неисправностей, одновременное проявление которых может привести к отказу всей сетецентрической системы. Такие методы ВИС для однокомплексных полносвязных систем предложены в работах [5-7]. В [8; 9] представлены обоснованные методы ВИС для неполносвязных систем, а в [10] – метод ВИС для неполносвязных систем с обнаружением и идентификацией случившихся проявлений неисправностей. Задачи, связанные с обеспечением системного ВИС в многокомплексных системах, рассматриваются в [11-13].

Основные механизмы обеспечения сбое- и отказоустойчивости на основе динамической избыточности для рассматриваемых однокомплексных систем при возникновении допустимых враждебных неисправностей включают механизмы парирования допустимых враждебных неисправностей (гарантирования правильности выходной информации системы при возникновении допустимых неисправностей) [14-16; 18; 19], функционального диагностирования системы с обнаружением и идентификацией возникающих допустимых враждебных неисправностей в процессе целевой работы и тестового диагностирования однокомплексных системы [14-16, 18-23, 25] и двухкомплексных систем [17; 24], тестового диагностирования подсистем и системы в целом [20-24], восстановления целевой работы подсистем и системы в целом при возникновении программных сбоев и отказов, самоуправляемой реконфигурации и деградации комплексов и системы в целом, выполняемых также в условиях возникновения допустимых враждебных неисправностей [18].

Общий подход к созданию и организации целевой работы открытых сетецентрических систем в сети ЦВМ в условиях возникновения допустимых враждебных неисправностей, их парирования на основе репликации задач, обнаружения и идентификации, восстановления после сбоев и программных сбоев, самореконфигурации и самоуправляемой деградации до предельно допустимой конфигурации с переходом к безопасному останову системы при последующем возникновении неисправности рассматривается в [26].

Организация работы механизмов сбое- и отказоустойчивости многоуровневая: на нижнем уровне – базовые механизмы (синхронизация и ВИС). На следующем уровне – основные механизмы (парирования проявлений неисправностей, тестового и функционального диагностирования, восстановления, самореконфигурации и самоуправляемой деградации. Все остальные механизмы организации работы системы составляют более высокие уровни. Их основной задачей с точки зрения сбое- и отказоустойчивости является определение места и объема восстанавливаемой информации, а также периода выполнения восстановления при возникновении программных сбоев и отказов. Взаимодействие всех механизмов сбое- и отказоустойчивости составляет сущность интерфейса отказоустойчивости данной системы.

Приведенный список литературы показывает, что для ряда задач по обеспечению сбое- и отказоустойчивости рассматриваемых сетецентрических систем решение имеется. Однако значительно больше проблем и задач остаются открытыми. К ним относятся задачи снижения оценок сложности предлагаемых методов по объемам требуемых аппаратурной, временной и информационной избыточности, разработки приемлемых методов самоорганизации сбое- и отказоустойчивых параллельных взаимосвязанных вычислений на основе использования динамической избыточности, разработки и взаимной увязки всех необходимых архитектурных, аппаратурных и программных механизмов ее реализации, разработки методов моделирования и оценки эффективности таких систем, методов отладки и испытаний (включая инжекцию допустимых неисправностей и создание возможных нештатных ситуаций) как отдельных элементов и подсистем, так и системы в целом.

Литература

1. *Ефремов А. Ю., Максимов Д. Ю.* Сетецентрическая система управления – что вкладывается в это понятие? // Технические и программные средства систем управления, контроля и измерения: труды Третьей российской конференции УКИ-2012 с международным участием. М.: ИПУ РАН, 2012. С. 158-161.

2. *Лобанов А.В.* Модели замкнутых многомашинных вычислительных систем со сбое- и отказоустойчивостью на основе репликации задач в условиях возникновения враждебных неисправностей // Автомат. и телемех. 2009. № 2.

3. *Лобанов А.В.* Синхронизация и взаимное информационное согласование // Программирование. 1997. № 2.

4. *Генинсон Б.А., Панкова Л.А., Трантенгерц Э.А.* Отказоустойчивые методы обеспечения взаимной информационной согласованности в распределенных вычислительных системах // Автомат. и телемех. 1989. № 5.

5. *Лобанов А.В.* Взаимное информационное согласование с идентификацией неисправностей в распределенных вычислительных системах // Автомат. и телемех. 1992. № 4. С. 137-146.

6. *Лобанов А.В.* Взаимное информационное согласование с идентификацией неисправностей на основе глобального синдрома // Автомат. и телемех. 1996. № 5. С. 150-159.

7. *Лобанов А.В., Сиренко В.Г., Гришин В.Ю.* Взаимное информационное согласование в многомашинных вычислительных системах с обнаружением и идентификацией кратных враждебных неисправностей // Автомат. и телемех. 2003. № 4. С. 123-133.

8. *Лобанов А.В., Ашарина И.В., Мищенко И.Г.* Взаимное информационное согласование в неполносвязных многомашинных вычислительных системах // Автомат. и телемех. 2003. № 5. С. 190-198.

9. *Ашарина И.В., Лобанов А.В.* Взаимное информационное согласование в неполносвязных гетерогенных многомашинных вычислительных системах // Автомат. и телемех. 2010. № 5. С. 133-146.

10. *Лобанов А.В.* Взаимное информационное согласование с обнаружением и идентификацией враждебных неисправностей в неполносвязных многомашинных вычислительных системах // Автомат. и телемех. 2003. № 6.

11. *Лобанов А.В.* Алгебраический подход к задаче выделения комплексов при организации сбое- и отказоустойчивых параллельных вычислений в сетях ЦВМ // Открытое образование. 2011. № 2 (86). Ч. 2. С. 36-39.

12. *Ашарина И.В.* Алгебраический метод определения достаточной среды межкомплексной посылки при организации сбое- и отказоустойчивых параллельных вычислений в сетях ЦВМ // Открытое образование. 2011. № 2.

13. *Ашарина И.В.* Распределённый алгоритм системного взаимного информационного согласования в многокомплексных вычислительных системах // Образовательные ресурсы и технологии. 2014. № 2. С. 41-46.

14. *Лобанов А.В.* Протокол отказоустойчивого обмена // Приборы и системы управления. 1993. № 7. С. 8-11.

15. *Лобанов А.В., Нахаев С.А.* Обеспечение сбое- и отказоустойчивости в протоколе отказоустойчивого обмена // Приборы и системы управления. 1993. № 7. С. 12-13.

16. *Лобанов А.В.* Распределенное мажорирование информации с обнаружением и идентификацией неисправностей // Автомат. и телемех. 1997. № 1. С. 145-149.

17. *Лобанов А.В.* Организация сбое- и отказоустойчивой работы двухкомплексной многомашинной вычислительной системы. // Автомат. и телемех. 1998. № 2. С. 143-152.

18. *Лобанов А.В.* Организация сбое- и отказоустойчивых вычислений в полносвязных многомашинных вычислительных системах // Автомат. и телемех. 2000. № 12. С. 138-146.

19. *Лобанов А.В.* Обнаружение и идентификация неисправностей в распределенных управляющих вычислительных системах с программно-управляемой сбое- и отказоустойчивостью // Автоматика и телемеханика. 1998. № 1.

20. *Лобанов А.В.* Обнаружение и идентификация "враждебных" неисправностей путем одновременного сочетания функционального и тестового диагностирования в многомашинных вычислительных системах // Автомат. и телемех. 1999. №1. С. 159-165.

21. *Лобанов А.В., Сиренко В.Г., Гришин В.Ю.* Функциональное диагностирование в распределенном системном диагностировании многомашинных вычислительных систем // Автоматика и телемеханика. 2002. № 1. С. 152-158

22. *Сиренко В.Г.* Функциональное диагностирование процессов посылки информации в вычислительных системах при неизвестном исходном значении передаваемой информации. Автомат. и телемех. 2005. № 11.

23. *Сиренко В.Г.* Метод локализации «враждебных» неисправностей в многомашинных вычислительных системах // Известия вузов. Электроника. 2006. № 3. С. 38-43.

24. *Лобанов А.В., Сиренко В.Г.* Распределенные методы системного диагностирования // Автомат. и телемех. 2000. № 8. С. 165-172.

25. *Лобанов В.А., Гришин В.Ю., Сиренко В.Г.* Распределенное системное диагностирование враждебных неисправностей в неполносвязных многомашинных вычислительных системах // Автомат. и телемех. 2005. № 2.

26. *Лобанов А. В.* Стратегические и тактические проблемы и задачи в организации сбое- и отказоустойчивых вычислений на основе репликации задач в многокомплексных многомашинных вычислительных системах и сетях ЦВМ // Информационные технологии в науке, образовании, телекоммуникации и бизнесе: материалы XXXVI Международной конференции и дискуссионного научного клуба IT+SE'10. Майская сессия. Ялта-Гурзуф. – приложение к журналу «Открытое образование». 2010. С. 119-121.

The problem of tolerance in the net-centric information management systems

***Anatoliy Vasilyevich Lobanov**, Doctor of Engineering, Scientific Secretary*
***Vladidmir Grigoryevich Sirenko**, Doctor of Engineering, General Director*
Open Joint-Stock Company Scientific Research Institute «Submikron»

The authors discuss the problem of organization of failure and fault-tolerant torango-o, distributed, network-centric information management systems, dynamic-Cesky organized and performing multitasking target for critical applications in distributed overlay computer networks, the most important characteristics, principles and features, philosophical essence from the point of view of fault tolerance. The information about basic theoretical results in the area in question is provided.

Keywords: network-centric system, distributed system, multiprocessor complex, information security, peer-to-peer network, Byzantine fault, fault tolerance, multitasking.