УДК 62-501.72:681.326.7 DOI: 10.18698/2308-6033-2019-7-1902

Восстановление целевой работы в автоматической сбое- и отказоустойчивой многозадачной распределенной информационно-управляющей системе

© А.В. Лобанов, И.В. Ашарина

АО «НИИ «Субмикрон», Москва, Зеленоград, 124460, Россия

Рассмотрена организация процессов восстановления целевой работы после допустимых сбоев и отказов в автоматической сбое- и отказоустойчивой многозадачной информационно-управляющей распределенной многомашинной системе сетевой структуры, выполняющей набор целевых функций, задаваемых внешними пользователями. Система характеризуется параллельным выполнением множества взаимодействующих целевых задач, исполняемых на отдельных вычислителях, представляющих собой организованные совокупности цифровых вычислительных машин (ЦВМ). Заданный уровень сбое- и отказоустойчивости задачи обеспечивается путем ее репликации — параллельного выполнения копий этой задачи на нескольких ЦВМ, составляющих вычислитель (комплекс), с обменом результатами и выбором из них правильного. Представлены характеристики, принципы построения, особенности таких систем и их «философская» сущность с точки зрения сбое- и отказоустойчивости. Определены факторы сложности при проектировании сбое- и отказоустойчивых систем рассматриваемого класса. Принята самая общая модель враждебной неисправности ЦВМ, при которой ее поведение может быть произвольным, неодинаковым по отношению к другим взаимодействующим с ней ЦВМ, в том числе подобным злонамеренному. Рассмотрена часть проблемы организации динамической избыточности в разрабатываемой системе, возникающая после того, как в этой системе в некотором комплексе (или некотором множестве F комплексов) со стороны исправных ЦВМ каждого такого комплекса была обнаружена допустимая совокупность неисправностей и каждая такая неисправность была также синхронно и согласованно идентифицирована по месту возникновения и по типу как программный сбой определенной ЦВМ этого комплекса. Эта часть проблемы решается посредством восстановления в идентифицированной в состоянии программного сбоя ЦВМ некоторого комплекса всей необходимой информации, передаваемой в нее из исправных ЦВМ данного комплекса. Определен состав команд, необходимых для такого восстановления, а также действия комплекса в процессе восстановления.

Ключевые слова: *распределенная многомашинная вычислительная система, сбое- и отказоустойчивость, мультиагентная система, динамическая избыточность, враждебная неисправность*

Введение. Широкое внедрение автоматических распределенных многомашинных информационно-управляющих систем сетевой структуры для автоматизации процессов управления сложными организационно-техническими комплексами ответственного применения делает чрезвычайно актуальной проблему обеспечения сбое- и отказоустойчивости таких систем, а также удлинения срока их активного автономного

существования. Возникающие при этом научно-технические вопросы, имеющиеся обоснованные их решения и открытые области научного поиска, представлены в работе [1].

При проектировании распределенных многомашинных информационно-управляющих систем сетевой структуры необходимо решение различных задач технической диагностики: диагностирование, верификация, идентификация неисправности по месту и типу (сбой, программный сбой, отказ) [2].

Вопросы надежности и отказоустойчивости, диагностического обеспечения вычислительных систем разной структуры рассматриваются в работах [3, 4].

Большой интерес вызывают работы таких известных ученых в данной области, как М.Ф. Каравай [5], А.С. Степанянц, В.С. Викторова [6], В.А. Ведешенков [7].

В [8] рассмотрен теоретический подход (модель, метод оценивания и способ обеспечения живучести), применение которого способствует обеспечению и оцениванию и живучести распределенных сетей связи в условиях внешних деструктивных воздействий.

Целью работы [9] является рассмотрение вопросов синтеза диагностической модели распределенной вычислительной системы (РВС), которую можно отнести к классу дискретно-событийных, когда работа системы представляется на языке последовательностей некоторых событий. В данном случае такими событиями являются события информационного обмена (приема и выдачи информации) между программными модулями системы.

Целью настоящей статьи является исследование проблемы организации в автоматической необслуживаемой информационно-управляющей распределенной многомашинной вычислительной системе (РМВС) сбое- и отказоустойчивого параллельного выполнения множества $Z = \{Z_1, Z_2, \ldots, Z_t\}$ взаимодействующих между собой t ($t > 0$) целевых задач, каждая из которых должна выполняться на отдельном вычислителе, и взаимодействие между задачами должно осуществляться посредством обмена сообщениями между соответствующими вычислителями по каналам связи между ними.

Сбое- и отказоустойчивость и увеличение срока активного существования РМВС должны обеспечиваться, во-первых, посредством репликации в вычислителе каждой i-й целевой задачи Z_i ($1 \le i \le t$) в соответствии с заданным для нее уровнем μ_i сбое- и отказоустойчивости, определяющим допустимое количество неисправностей принятой модели в этом вычислителе, при котором проявления допустимых неисправностей могут быть парированы за счет обеспечения возможности гарантированного вычисления правильной выходной информации данной задачи из копий выходной информации, формируемых на выходах этого вычислителя, например, применением ма-

жорирования или кворумирования. Репликация целевой задачи Z_i в исполняющем ее вычислителе состоит в параллельном выполнении ее копий на нескольких неизбыточных ЦВМ, составляющих задачный комплекс K_i этой целевой задачи (данного вычислителя), с обменом между всеми ЦВМ задачного комплекса результатами выполнения целевой задачи и выбором из них в каждой из исправных ЦВМ правильного результата, в предположении, что не более чем μ_i из этих копий результатов могут быть ошибочными. При этом в каждой исправной ЦВМ задачного комплекса будет сформирована правильная выходная информация. Во-вторых, использованием в системе механизмов динамической избыточности, обеспечивающих обнаружение проявлений допустимых неисправностей, их идентификацию по месту возникновения и по типу (сбой, программный сбой, отказ), необходимую реконфигурацию системы и восстановление целевого вычислительного процесса при сбоях и программных сбоях, осуществление самоуправляемой реконфигурации или деградации РМВС при отказах (изоляция отказавших элементов, требуемая реконфигурация РМВС с использованием запасных элементов и восстановление целевого вычислительного процесса). При отказах и отсутствии запасных элементов должен выполняться переход к целевой работе со сниженными уровнями сбое- и отказоустойчивости и/или должна осуществляться предусмотренная функциональная деградация РМВС посредством исключения из исполняющихся целевых задач наименее приоритетных, с расформированием их задачных комплексов и переводом составляющих их ЦВМ в запас. При достижении критического уровня сбое- и отказоустойчивости и возникновении следующей неисправности, а также при возникновении недопустимых неисправностей система должна переходить в режим безопасного останова и ожидания предусмотренных при проектировании РМВС указаний из внешней среды с последующим выполнением этих указаний. В системе также должна быть предусмотрена возможность перераспределения имеющихся ресурсов с целью варьирования соотношением производительность — достоверность для различных параллельно решаемых взаимодействующих целевых задач, когда в определенные периоды времени для более приоритетных задач выделяется больше избыточности за счет ее уменьшения для менее приоритетных задач.

Особенности и факторы сложности проектирования распределенной многомашинной вычислительной системы. Особенностями рассматриваемых РМВС ответственного применения являются:

а) автономность ЦВМ;

б) отсутствие в РМВС 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 необходимой адаптации, 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.

Уязвимым местом таких РМВС является сложность механизмов самосинхронизации и самоорганизации, разрушение их и циркулирующих в системах информационных потоков.

С точки зрения сбое- и отказоустойчивости «философской» сущностью рассматриваемых систем являются:

а) сложность;

б) необходимость синхронизированной и согласованной работы их элементов;

в) практическая невозможность точных выводов о техническом состоянии системы;

г) необходимость самостоятельного формирования этих выводов на основе принимаемых заранее и, возможно, неточных критериев;

д) необходимость уточнения этих критериев со стороны самой системы в процессе ее целевой работы, возможность к самообучению и самоадаптация таких систем к условиям применения;

е) необходимость принимать и выполнять самостоятельные решения о реконфигурации и управляемой деградации системы;

ж) необходимость проектирования таких систем «сверху-вниз» в условиях четких определений, понятий и моделей при тесном взаимодействии разработчиков целевых задач и разработчиков проблем обеспечения сбое- и отказоустойчивости.

Факторами сложности при проектировании сбое- и отказоустойчивых систем рассматриваемого класса являются:

а) неприемлемость традиционных (константных, логических, обрывов и коротких замыканий проводников и др.) моделей неисправностей ЦВМ;

б) необходимость распределенного, синхронизированного и согласованного принятия решения в различных ЦВМ системы;

в) необходимость организации и управления динамической избыточностью системы.

В качестве модели неисправности принимается самая общая модель враждебной неисправности отдельной ЦВМ, при которой ее поведение может быть произвольным, неодинаковым по отношению к другим взаимодействующим с ней ЦВМ и даже подобным злонаме-

ренному. Модель враждебной неисправности отражает сложность нахождения причинно-следственной связи между видами проявлений неисправностей (ошибками) и имеющимися в действительности неисправностями таких сложных объектов, как современная ЦВМ и их взаимодействующие совокупности. Защита от враждебных неисправностей будет гарантировать защиту от неисправностей любой другой известной модели.

С точки зрения вычислительной мощности и потоков обрабатываемой информации предлагаемые в работе принципы построения РМВС полностью удовлетворяют всему спектру возможных космических объектов (космических аппаратов, КА), представленных ниже:

а) микро-КА с отдельным вычислителем и малыми потоками обрабатываемой информации; мини-КА, содержащие более одного вычислителя;

б) малофункциональные КА с вычислителем, предназначенным для обработки потока информации средней и высокой мощности;

в) многофункциональный КА (в том числе пилотируемый) для решения параллельных взаимодействующих целевых задач;

г) группировка из микро- и мини-КА, взаимодействующих между собой для решения общих синергетических задач путем взаимообмена информацией между всеми КА;

д) группировка из КА всех вышеперечисленных типов и наземных средств, а также группировка группировок, обеспечивающая решение критических проблем.

В настоящей статье рассматривается проблема восстановления целевой работы в РМВС, возникающая после обнаружения в некотором комплексе (или некотором множестве F комплексов) допустимой совокупности (допустимых совокупностей) неисправностей, каждая из которых была также синхронно и согласованно идентифицирована всеми исправными ЦВМ соответствующего комплекса по месту возникновения и по типу как программный сбой или отказ определенной ЦВМ этого комплекса. Синхронность и согласованность означает, что все исправные ЦВМ комплекса одновременно (в одном и том же временном отрезке, с приемлемой точностью начинающемся и заканчивающемся во всех исправных ЦВМ комплекса), одинаково и правильно, в соответствии с принятыми критериями сбоя, программного сбоя и отказа, идентифицировали обнаруженные проявления неисправностей как по месту их возникновения (с точностью до принятых моделей неделимых объектов неисправностей), так и по типу (сбой, программный сбой, отказ) [10].

В настоящей статье предполагается, что всей работой РМВС управляет системный диспетчерский комплекс (СДК), представляющий собой сбое- и отказоустойчивую подсистему РМВС, согласованно управляющую всеми процессами интерфейса сбое- и отказоустойчи-

вости, реализованного в рассматриваемой РМВС и обеспечивающего, во-первых, парирование допустимых совокупностей неисправностей, и, во-вторых, все необходимые действия по реализации отмеченных выше требований динамической избыточности. Объектом, исполняющим функции СДК, может быть:

а) отдельный комплекс с принятым достаточным уровнем сбое- и отказоустойчивости;

б) подсистема РМВС или вся РМВС в целом, которая объединяется в отведенные временные отрезки в отдельный специальный комплекс, выполняющий функции СДК. При идентификации программного сбоя ЦВМ в некотором задачном комплексе (далее — восстанавливаемый, подлежащий самовосстановлению задачный комплекс) информацию об этом событии данный задачный комплекс передает в СДК, который анализирует все выполняемые в задачных комплексах целевые процессы и взаимодействия между ними, определяет период времени восстановления, на который восстанавливаемый задачный комплекс может быть выведен из процесса решения предписанной ему целевой задачи, и сообщает об этом данному комплексу, а также всем другим комплексам, взаимодействующим с ним. Кроме того, СДК сообщает всем этим взаимодействующим между собой комплексам алгоритмы их работы, во-первых, во время этого периода, и, во-вторых, по его окончании в случаях как успешного, так и неуспешного восстановления. При наступлении периода восстановления все взаимодействующие между собой задачные комплексы выполняют предписанные им из СДК целевые и восстанавливающие действия и по окончании периода восстановления сообщают в СДК об успешных или неуспешных его результатах. В свою очередь, СДК, получив эти сообщения, принимает решения по дальнейшей организации целевого вычислительного процесса.

Процесс восстановления в восстанавливаемом комплексе состоит в следующем. Все исправные ЦВМ этого комплекса согласованно образуют восстанавливающий подкомплекс (ВПК) восстанавливаемого комплекса и переходят к процессу восстановления, состоящему в следующем. Во-первых, предусмотренными аппаратно-программными средствами восстанавливающие ЦВМ из ВПК согласованно и безусловно переводят восстанавливаемые ЦВМ этого комплекса в режим восстановления и блокируют их каналы межмашинной связи по возможности вмешиваться в работу любой ЦВМ из ВПК. Такая блокировка может быть осуществлена также программным способом посредством игнорирования в исправных ЦВМ восстанавливаемого задачного комплекса, подсистемы РМВС или всей РМВС в целом непредусмотренных действий восстанавливаемых ЦВМ. В режиме восстановления восстанавливаемая ЦВМ ожидает от ВПК поступле-

ния последовательности команд собственного восстановления, в состав которых должны входить:

1) команда записи в заданную область памяти этой ЦВМ данных, поступивших в составе этой команды;

2) команда чтения данных из заданной области памяти восстанавливаемой ЦВМ и передача этих данных каждой ЦВМ из ВПК;

3) команда перехода восстанавливаемой ЦВМ к выполнению программы в ее памяти с задаваемого в команде адреса либо к выполнению программы, передаваемой в составе данной команды.

В составе программ каждой ЦВМ из целевого комплекса должна быть программа восстановления восстанавливаемой ЦВМ из этого комплекса, которая должна завершаться последней из указанных команд, переводящей восстанавливающие и восстанавливаемую ЦВМ восстанавливаемого комплекса к выполнению его целевой задачи. Также в программе восстановления может быть предусмотрено предварительное тестовое диагностирование восстанавливаемой ЦВМ. Проявления программных сбоев восстанавливаемой ЦВМ, соответствующие принятому критерию отказа ЦВМ, например две подряд неудачные попытки восстановления, должны восприниматься со стороны РМВС как отказ этой ЦВМ, вызывающий необходимость ее исключения из восстанавливаемого комплекса и из рабочей конфигурации РМВС, подключения запасной ЦВМ, если она имеется, и аналогичного восстановления в ней целевой работы восстанавливаемого комплекса. В случае отсутствия запасной ЦВМ данный комплекс должен быть переведен по команде из СДК в режим целевой работы с пониженным уровнем сбое- и отказоустойчивости. При достижении принятого критического уровня сбое- и отказоустойчивости в самом СДК и возникновении в нем следующей неисправности РМВС должна перейти в режим безопасного останова, индивидуального для РМВС и зависящего от условий ее применения. В этом режиме РМВС должна сообщить о своем переходе в режим безопасного останова внешнему пользователю и перейти в режим ожидания от этого пользователя специальных команд управления РМВС. Содержание этого режима и состав команд, исполняемых в нем, в настоящей статье не рассматриваются.

Все описанные действия по восстановлению в РМВС целевой работы в случаях идентификации допустимых совокупностей программных сбоев и отказов должны быть в достаточной степени синхронизированными и согласованными для всех исправных ЦВМ из РМВС. Поэтому в РМВС должны быть реализованы базовые механизмы синхронизации и взаимного информационного согласования как в отдельных задачных комплексах и подсистемах РМВС, включающих несколько комплексов, так и во всей РМВС в целом.

Синхронность обеспечивается также путем организации в системе непрерывной работы подсистемы единого системного времени, включающей средства как начальной, так и промежуточной синхронизации автономных часов в отдельных элементах системы.

Начальная синхронизация должна осуществляться при начальном несинхронном включении различных ЦВМ системы и должна формировать 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 автономных часов различных ЦВМ, расходящихся из-за индивидуальных значений дрейфов этих часов и возникновения допустимых враждебных неисправностей.

Согласованность действий и принимаемых решений в различных ЦВМ и подсистемах РМВС гарантируется применением алгоритмов взаимного информационного согласования (ВИС) [11]. Достижимость ВИС составляет концептуальную основу создания отказоустойчивых алгоритмов для решения основных задач организации распределенных вычислений. В настоящее время разработано значительное количество 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 [11] утверждалось, что враждебный отказ в процессе ВИС диагностировать невозможно. Однако исследуемая в настоящей статье задача организации сбое- и отказоустойчивых вычислений в РМВС, как полносвязных, так и неполносвязных, 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 РМВС. Такие методы ВИС для однокомплексных полносвязных систем предложены в работах [12–14]. В работах [15, 16] представлены обоснованные методы ВИС для неполносвязных систем, а в статье [17] — метод ВИС для неполносвязных систем с обнаружением и идентификацией случившихся в процессе ВИС проявлений враждебных неисправностей. Задачи и их решения, связанные с обеспечением системного ВИС в многокомплексных системах, рассматриваются в работах [18–22].

Организация работы предлагаемых механизмов сбое- и отказоустойчивости должна быть многоуровневой:

на нижнем уровне — базовые механизмы (синхронизация и ВИС);

на следующем уровне — основные механизмы:

- парирование проявлений неисправностей;
- тестовое и функциональное диагностирование;
- восстановление;
- самореконфигурация;
- самоуправляемая деградация.

Все остальные механизмы организации работы системы должны составлять 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.

Заключение. Рассматриваемая в настоящей статье проблема удлинения срока активного автономного существования, а также сбое- и отказоустойчивости автоматических РМВС сетевой структуры, предназначенных для автоматизации процессов управления сложными организационно-техническими комплексами ответственного применения, включает целый ряд еще не решенных научно-технических проблем и задач. Это 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 преднамеренное создание возможных нештатных ситуаций) как отдельных элементов и подсистем, так и системы в целом. Особо следует отметить необходимость математического моделирования, практического макетирования и апробации предлагаемых алгоритмических и аппаратно-программных решений с целью их отработки и получения оценочных характеристик по используемым ресурсам.

НИИ «Субмикрон» имеет давний успешный опыт разработки и практического внедрения в космической отрасли Российской Федерации рассматриваемых однокомплексных распределенных систем [23, 24]. К сожалению, имеется также и последующий весьма дорого-

стоящий отрицательный опыт, когда отступление от предлагаемых принципов и методологии построения рассматриваемых сбое- и отказоустойчивых РМВС привело к появлению эффектов отрицательной эмерджентности (необъяснимое ошибочное поведение) в их целевой работе в штатных условиях применения, и устранение этих эффектов, по мнению авторов настоящей статьи, возможно только при перепроектировании механизмов сбое- и отказоустойчивости РМВС на основе предлагаемых принципов и методологии. Наиболее эффективное развитие и теоретических результатов, и практического опыта в области построения рассматриваемых сбое- и отказоустойчивых РМВС может быть достигнуто в приемлемые сроки и приемлемой стоимостью только в НИИ «Субмикрон» путем адекватного моделирования такой системы (что потребует предварительного создания соответствующей системы моделирования), а также построения макетного образца РМВС, его исследования и оценки.

ЛИТЕРАТУРА

[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. DOI: 10.24411/2409-5419-2018-10019

[2] Пархоменко П.П., ред. *Основы технической диагностики. Кн. 1. Модели объектов, методы и алгоритмы диагноза*. Москва, Энергия, 1976, 464 с.

[3] Сильянов Н.В., Ломакина Л.С. Диагностическое обеспечение многофункциональной бортовой вычислительной системы. *Материалы XIII Всероссийского совещания по проблемам управления (ВСПУ–2019). Москва, 17–20 июня 2019 г*. Москва, ИПУ РАН, с. 2874–2878.

[4] Клейман Л.А., Фрейман В.И. Повышение надежности устройств беспроводных систем управления на основе метода анализа тепловых карт. *Материалы XIII Всероссийского совещания по проблемам управления (ВСПУ–2019)*, *Москва, 17–20 июня 2019 г*. Москва, ИПУ РАН, с. 2866–2873.

[5] Каравай М.Ф. Минимизированное вложение произвольных гамильтоновых графов в отказоустойчивый граф и реконфигурация при отказах. I. Одноотказоустойчивые структуры. *Автоматика и телемеханика*, 2004, № 12, с. 159–177.

[6] Викторова В.С., Лубков В.Н., Степанянц А.С. Надежностные модели и анализ систем с защитой. *Автоматика и телемеханика*, 2018, № 7, с. 117–137.

[7] Ведешенков В.А. О путевом методе системного диагностирования цифровых систем со структурой симметричного двудольного графа. *Автоматика и телемеханика*, 2014, № 9, с. 133–143.

[8] Белов А.С., Скубьев А.В. Теоретический подход по оцениванию и обеспечению живучести распределенных сетей связи в условиях информационного противоборства. *Наукоемкие технологии в космических исследованиях Земли*, 2018, т. 10, № 2, с. 22–31. DOI: 10.24411/2409-5419-2018-10038

[9] Грузликов А.М., Колесов Н.В. Дискретно-событийная диагностическая модель для распределенной вычислительной системы. Слияние цепей. *Автоматика и телемеханика*, 2017, № 4, с. 126–134.

[10] 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.

[11] Генинсон Б.А., Панкова Л.А., Трантенгерц Э.А. Отказоустойчивые методы обеспечения взаимной информационной согласованности в распределенных вычислительных системах. *Автоматика и телемеханика*, 1989, № 5, с. 3–18.

[12] Лобанов А.В. Взаимное информационное согласование с идентификацией неисправностей в распределенных вычислительных системах. *Автоматика и телемеханика*, 1992, № 4, с. 137–146.

[13] Лобанов А.В. Взаимное информационное согласование с идентификацией неисправностей на основе глобального синдрома. *Автоматика и телемеханика*, 1996, № 5, с. 150–159.

[14] Гришин В.Ю., Лобанов А.В., Сиренко В.Г. Взаимное информационное согласование в многомашинных вычислительных системах с обнаружением и идентификацией кратных враждебных неисправностей. *Автоматика и телемеханика*, 2003, № 4, с. 123–133.

[15] Ашарина И.В., Лобанов А.В., Мищенко И.Г. Взаимное информационное согласование в неполносвязных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2003, № 5, с. 190–198.

[16] Ашарина И.В., Лобанов А.В. Взаимное информационное согласование в неполносвязных гетерогенных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2010, № 5, с. 133–146.

[17] Лобанов А.В. Взаимное информационное согласование с обнаружением и идентификацией враждебных неисправностей в неполносвязных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2003, № 6, с. 175–185.

[18] 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.

[19] Ашарина И.В. Алгебраический метод определения достаточной среды межкомплексной посылки при организации сбое- и отказоустойчивых параллельных вычислений в сетях ЦВМ. *Открытое образование*, 2011, № 2 (86), ч. 2, с. 29–32.

[20] Ашарина И.В. Распределенный алгоритм системного взаимного информационного согласования в многокомплексных вычислительных системах. *Образовательные ресурсы и технологии*, 2014, № 2 (5), с. 45–50.

[21] 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.

[22] Ашарина И.В., Лобанов А.В. Выделение структурной среды системного взаимного информационного согласования в многокомплексных системах. *Автоматика и телемеханика*, 2014, № 8, с. 146–156.

[23] Лобанов А.В. Протокол отказоустойчивого обмена. *Приборы и системы управления*, 1993, № 7, с. 8–11.

[24] Лобанов А.В., Нахаев С.А. Обеспечение сбое- и отказоустойчивости в протоколе отказоустойчивого обмена. *Приборы и системы управления*, 1993, № 7, с. 12–13.

Статья поступила в редакцию 02.07.2019

Ссылку на эту статью просим оформлять следующим образом:

Лобанов А.В., Ашарина И.В. Восстановление целевой работы в автоматической сбое- и отказоустойчивой многозадачной распределенной информационно-управляющей системе. *Инженерный журнал: наука и инновации*, 2019, вып. 7.

http://dx.doi.org/10.18698/2308-6033-2019-7-1902

Лобанов Анатолий Васильевич — д-р техн. наук, старший научный сотрудник, ученый секретарь Акционерного общества «Научно-исследовательский институт «Субмикрон». e-mail: lav@se.zgrad.ru

Ашарина Ирина Владимировна — канд. техн. наук, доцент, старший научный сотрудник Акционерного общества «Научно-исследовательский институт «Субмикрон». e-mail: asharinairina@mail.ru

Restoration of target work in automatic failure- and fault-tolerant multitasking distributed information-control system

© A.V. Lobanov, I.V. Asharina

JSC "Scientific Research Institute Submicron", Moscow, 124460, Russia

The paper deals with the organization of target work recovery processes after admissible failures and faults in an automatic failure and fault tolerant multitask distributed multi-machine system of the network structure performing a set of the target functions set by external users. The system is characterized by parallel execution of a set of interacting target tasks performed on separate computer subsystems, which are organized sets of digital computers. The specified level of failure- and fault-tolerance of the task is provided by its replication, i.e. parallel execution of copies of this task on several computers that make up the system, with the exchange of results and the choice of the correct one.

The study introduces the characteristics, principles of construction, features of the considered systems and their "philosophical" essence from the point of view of failure- and fault-tolerance. Within the research, we determined the factors of complexity in the design of failure- and fault-tolerant systems of this class. The most general model of malicious computer failure is adopted, in which the computer behavior can be arbitrary, different in relation to other computers interacting with it, and even as malicious. We focus on the part of the problem of organizing dynamic redundancy in the developed system. The problem arises after an acceptable set of faults is detected in this system in some complex (or some set of F complexes) by each of the fault-free digital computers of each such complex and each such fault is also synchronously and consistently identified by place of origin and by type as a software failure of a certain digital computer of this complex. This part of the problem is solved by restoring all necessary information identified in a state of software malfunction of a certain complex. The information is transmitted to this digital computer from fault-free digital computers of this complex. The list of instructions required for such a recovery, as well as the actions of the complex in the recovery process, is determined.

Keywords: *distributed multi-machine system, failure- and fault-tolerance, multiagent system, dynamic redundancy, malicious failure*

REFERENCES

[1] Lobanov A.V., Asharina I.V., Grishin V.Yu., Sirenko V.G. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli — High Tech in Earth Space Research*, 2018, vol. 10, no. 1, pp. 48–55.

[2] Parhomenko P.P., ed. *Osnovy tekhnicheskoj diagnostiki. Kn. 1. Modeli obektov, metody i algoritmy diagnoza* [Fundamentals of technical diagnostics. Book 1. Object models, methods and diagnosis algorithms]. Moscow, Energiya Publ., 1976, 464 p.

[3] Silyanov N.V., Lomakina L.S. *Materialy XIII Vserossijskogo soveshchaniya po problemam upravleniya (VSPU–2019)* [Proceedings of the XIII VSPU], Moscow, June 17–20. Moscow, Institute of Control Sciences RAS Publ., 2019, pp. 2874–2878.

[4] Klejman L.A., Frejman V.I. *Materialy XIII Vserossijskogo soveshchaniya po problemam upravleniya (VSPU–2019)* [Proceedings of the XIII VSPU], Moscow, June 17–20. Moscow, Institute of Control Sciences RAS Publ., 2019, pp. 2866–2873.

[5] Karavay M.F. *Avtomatika i telemekhanika — Automation and Remote Control*, 2004, no. 12, pp. 159–177.
[6] Viktorova V.S., Lubkov V.N., Stepanyanc A.S. *Avtomatika i telemekhanika — Automation and Remote Control*, 2018, no. 7, pp. 117–137.
[7] Vedeshenkov V.A. *Avtomatika i telemekhanika — Automation and Remote Control*, 2014, no. 9, pp. 133–143.
[8] Belov A.S., Skubev A.V. *Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli — High-Tech in Earth Space Research (H&ES Research)*, 2018, vol. 10, no. 2, pp. 22–31.
[9] Gruzlikov A.M., Kolesov N.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2017, no. 4, pp. 126–134.
[10] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2009, no. 2, pp. 171–189.
[11] Geninson B.A., Pankova L.A., Trantengerts E.A. *Avtomatika i telemekhanika — Automation and Remote Control*, 1989, no. 5, pp. 3–18.
[12] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 1992, no. 4, pp. 137–146.
[13] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 1996, no. 5, pp. 150–159.
[14] Lobanov A.V., Sirenko V.G., Grishin V.Yu. *Avtomatika i telemekhanika — Automation and Remote Control*, 2003, no. 4, pp. 123–133.
[15] Lobanov A.V., Asharina I.V., Mishchenko I.G. *Avtomatika i telemekhanika — Automation and Remote Control*, 2003, no. 5, pp. 190–198.
[16] Asharina I.V., Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2010, no. 5, pp. 133–146.
[17] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2003, no. 6, pp. 175–185.
[18] Lobanov A.V. *Otkrytoe obrazovanie — Open Education*, 2011, no. 2 (86), part 2, pp. 36–39.
[19] Asharina I.V. *Otkrytoe obrazovanie — Open Education*, 2011, no. 2, pp. 29–32.
[20] Asharina I.V. *Obrazovatelnye resursy i tekhnologii* (*Educational resources and technology*), 2014, no. 2, pp. 41–46.
[21] Asharina I.V., Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2014, no. 6, pp. 115–131.
[22] Asharina I.V., Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2014, no. 8, pp. 146–156.
[23] Lobanov A.V. *Pribory i sistemy upravleniya* (*Instruments and control systems*), 1993, no. 7, pp. 8–11.
[24] Lobanov A.V., Nakhaev S.A. *Pribory i sistemy upravleniya* (*Instruments and control systems*), 1993, no. 7, pp. 12–13.

Lobanov A.V., Dr. Sc. (Eng.), Senior Researcher, Scientific Secretary, JSC "Scientific Research Institute Submicron". e-mail: lav@se.zgrad.ru

Asharina I.V., Cand. Sc. (Eng.), Assoc. Professor, Senior Researcher, JSC "Scientific Research Institute Submicron". e-mail: asharinairina@mail.ru