УДК 62-501.72:681.326.7 DOI: 10.18698/2308-6033-2021-7-2097

Проблемы организации вычислений в многомашинных вычислительных системах с программно-управляемой сбое- и отказоустойчивостью. Часть II

© И.В. Ашарина

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

Проведен анализ существующих подходов и методов организации сбое- и отказоустойчивых вычислений в распределенных многомашинных вычислительных системах (РМВС), определен и обоснован перечень задач, подлежащих решению. Рассмотрены области применения сбое- и отказоустойчивых систем управления сложными сетевыми и распределенными объектами. Вторая часть посвящена проблемам организации сбое- и отказоустойчивости в РМВС, исследовано системное, функциональное, тестовое диагностирование в качестве основы построения необслуживаемых сбое- и отказоустойчивых систем. Введено понятие самоуправляемой деградации (завершающейся выведением РМВС в состояние безопасного останова при критической степени деградации) как способа увеличения срока активного существования РМВС.

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

Введение. В первой части работы [1] рассмотрены формулировки понятия сбое- и отказоустойчивости систем управления сложными сетевыми и распределенными объектами управления, начиная с определения А. Авиженисa до сегодняшних дней. Определены недостатки приведенных формулировок, в том числе и фигурирующих в государственных стандартах. Предложена формулировка понятия сбое- и отказоустойчивости, не имеющая перечисленных недостатков.

Затронуты вопросы и задачи, решаемые посредством сетецентрического подхода к построению информационно-управляющих систем (ИУС), которые находят применение в различных областях человеческой деятельности и представляют собой актуальную проблему.

Проанализированы вопросы построения бортовых вычислительных систем (БВС) космических аппаратов (КА), живучесть которых обеспечивается свойством постепенной деградации с сохранением работоспособности по мере увеличения тяжести последствий отказов с учетом возникающих ограничений, в том числе и с неисправностями разных моделей как «враждебных» (византийских), так и не носящих враждебного характера.

Области применения сбое- и отказоустойчивых систем управления сложными сетевыми и распределенными объектами имеют широкий охват всех сфер человеческой деятельности:

– инфокоммуникационная система специального назначения (ИКС СН);

– методическое и модельно-алгоритмическое обеспечение решения задачи планирования операций информационного взаимодействия кластера малых космических аппаратов (МКА) дистанционного зондирования Земли (ДЗЗ);

– мультироботные системы.

Системное, функциональное, тестовое диагностирование как основа построения необслуживаемых сбое- и отказоустойчивых систем. В основе построения сбое- и отказоустойчивых систем ответственного применения лежат различные методы диагностирования, в том числе и самодиагностирования.

Особенность развиваемого в [2] подхода к такому наблюдению, как локальное самодиагностирование, заключается в решении задачи разметки диагностического графа. С этой целью вершинам и дугам диагностического графа присваиваются метки, которые позволяют разделить граф на подграфы по некоторому набору функциональных (диагностических) признаков и для каждой вершины указать ее принадлежность, место и поведение в том или ином подграфе. Такой подход, по мнению автора [2], соответствует построению живучих многопроцессорных систем. Функционирование системы описывается как процесс порождения и уничтожения подсистем, выделяемых для выполнения задач пользователя или задач, связанных с управлением системой, в том числе с определением ее технического состояния. Такая организация характерна для построения модульных систем. Взаимодействие между модулями такой системы основывается на использовании принципа близкодействия, характерного для клеточных автоматов [3], когда поведение каждого модуля определяется состоянием модулей, имеющих с ним физические связи. Эта тема была исследована в [4–6].

Самодиагностика без ремонта на системном уровне для многопроцессорных (модульных) вычислительных систем при множественных устойчивых неисправностях исследована в [5] и при использовании ненадежных тестов [7]. Выделена группа диагностирующих моделей, представляющих системы с полными ненадежными тестами, для которой приводится формальное обоснование отношения включения между моделями ненадежных тестов, дающего возможность объединять модели в группы с одинаковыми диагностическими свойствами.

Разработанная в [4–6] система состоит из модулей, каждый из которых, используя доступные ему средства функционального и тестового диагностирования, может проверить и оценить техническое состояние некоторых других модулей. Состояние системы определяется автоматически путем сопоставительного анализа полученных оценок, выполняемого модулями самой системы. Процесс определения состояния системы называют самодиагностированием, а сами системы —

самодиагностируемыми [7, 8]. Моделью самодиагностируемой системы служит орграф, вершины которого представляют модули системы, дуги — тестовые связи от тестирующих модулей к тестируемым. Дуги графа взвешены оценками (двоичными) состояния тестируемого модуля, которые дает ему тестирующий. В [7] предполагается использование полных, но ненадежных тестов. Это означает, что исходы тестирования, проводимого исправными модулями, достоверно определяют состояние тестируемых модулей. Результаты тестов, выполняемых неисправными модулями, ненадежны, поскольку заключение неисправного тестирующего модуля о состоянии тестируемого им модуля не зависит от фактического состояния последнего согласно модели Препарата — Метце — Чжена (ПМЧ-модели). В [9] описана модель Бранси — Грандони — Маэстрини (БГМ-модель), в которой неисправный тестирующий модуль не может выдать заключение, что неисправный тестируемый модуль исправен. В [9–11] представлены так называемые модели сравнения, в которых заключение о состоянии тестирующего и тестируемого модулей делается на основании сравнения результатов выполнения ими одной и той же (тестовой) задачи.

В [6] рассматривается теоретико-графовая модель самодиагностики на системном уровне при множественных устойчивых отказах. Анализируется группа моделей тестирования, основанного на применении полных ненадежных тестов. Для моделей этой группы получены необходимые и достаточные условия *t*-диагностируемости без ремонта. Изучается случай *t*-диагностирования без ремонта, когда по исходам однократного прохождения системой всех возможных тестов идентифицируются все неисправные модули, имеющиеся в системе, при условии, что их число не превышает указанного значения *t*.

Для исследования диагностических свойств многопроцессорной системы, состоящей из N модулей, используется ее теоретико-графовая модель, включающая:

– множество процессорных модулей системы V, $|V| = N$;

– семейство $\mathcal{F}$ допустимых образов неисправностей;

– модель ненадежного тестирования $<A>$;

– спецификацию условий выполнения диагностики.

В [6] установлены необходимые и достаточные условия, которым должен удовлетворять диагностический граф системы, чтобы любой заданный образ неисправностей $F \in \mathcal{F}$ можно было отличить от всех остальных образов неисправностей из семейства $\mathcal{F}$.

Множество $\mathcal{F} = F(t)$ допустимых образов неисправностей многопроцессорной системы составляют все подмножества F модулей мощности не более кратности t допустимых неисправностей:

$$0 \le |F| \le t; \qquad 0 \le t \le N.$$

Случай $|F| = 0$ соответствует исправному состоянию системы, и она специфицируется как t-диагностируемая без ремонта.

Исчерпывающее перечисление моделей, различающихся соглашениями о свойствах надежности используемых тестов, приведено в [12].

Помимо некорректности определения отказоустойчивости, не позволяющего правильно решать задачи сбое- и отказоустойчивости [13], к другим недостаткам работ [4–6] можно отнести наличие таких неопределенных терминов, как тестирование и самотестирование. Не определено также, что понимается под диагностическим свойством, диагностическими возможностями, диагностической спецификацией.

В [14] рассмотрены два подхода к диагностированию процессов посылок информации в вычислительных системах при неизвестном исходном значении информации: внешнее диагностирование и самодиагностирование.

Показана многопутевая посылка информации в многоуровневых вычислительных системах сетевой структуры из одной или нескольких ЦВМ первого уровня в несколько ЦВМ последнего уровня, выполняемая с целью повышения достоверности передачи информации. Предлагаемый метод работает лишь при выполнении трех условий:

– известна структура системы, пути посылки информации и допустимое число неисправных ЦВМ на каждом уровне системы;

– среди путей посылки имеется хотя бы один, проходящий только по исправным ЦВМ;

– для анализа достоверных значений полученная информация доступна во всех ЦВМ последнего уровня.

При этом у получателя встают две задачи [14]: вычисление достоверного значения информации по определенному количеству ее копий; обнаружение и идентификация проявлений допустимых неисправностей, произошедших в процессе одной посылки или их последовательности.

Для современных необслуживаемых систем большой размерности и значительной сложности, с длительными сроками активного существования не подходит ставший традиционным метод маскирования неисправностей обнаружением и идентификацией узкого класса неисправностей в предположении возможности ремонта такой системы. Длительный срок активного существования может обеспечить только реализация управляемой деградации, использующей исправные компоненты системы до последней возможности. Поэтому разработка метода обнаружения и идентификации проявлений допустимых неисправностей самого широкого класса в коммутационной структуре, определения на его основе возможных значений посыла-

емых данных и формирования предложений для следующего этапа деградации этой среды, предложенные в [14], является важной и актуальной задачей.

В [14] введено понятие самоуправляемой деградации среды, под которой понимается способность системы самостоятельно и своевременно находить и идентифицировать обнаруженные проявления неисправностей ее компонентов и при возникновении допустимых отказов реконфигурировать свою структуру и переходить в следующее допустимое работоспособное состояние с возможным допустимым снижением собственных характеристик производительности и надежности. Если невозможен переход в следующее работоспособное состояние, система должна самостоятельно перейти в состояние безопасного останова. Одно из основных свойств таких систем — способность своевременно обнаруживать и идентифицировать случившиеся неисправности компонентов среды [14].

Следует отметить, что в [14] поставлена задача построить метод, при котором исправные цифровые вычислительные машины (ЦВМ) — получатели информации в процессе посылок — вычисляют всевозможные варианты значений посылаемой информации и для каждого из вариантов определяют допустимые совокупности «враждебных» неисправностей этих машин, причем при каждой из совокупностей возможно формирование результатов анализируемых посылок.

Результаты работы метода должны быть одинаковыми во всех исправных ЦВМ-получателях информации и соответствовать результатам, имеющим место в действительности. Подобная постановка задачи относится к области функционального самодиагиостироваиия вычислительных систем [15], позволяющего обнаруживать и идентифицировать проявления неисправностей, случившихся во время штатного функционирования системы.

Методы функционального диагностирования «враждебных» неисправностей, предлагавшиеся в [16, 17], были развиты и дополнены А.В. Лобановым, автором большого количества работ, посвященных сбое- и отказоустойчивости многомашинных вычислительных систем (МВС). В [18] рассмотрены МВС, в которых сбое- и отказоустойчивость достигаются одновременным решением одной и той же задачи на нескольких ЦВМ с взаимообменом результатами и выбором из них правильного. Предлагаемая реализация подхода динамической избыточности, состоящего в непрерывном функциональном диагностировании системы (обнаружении проявлений неисправностей и их идентификации по месту возникновения и типу (сбой, программный сбой или отказ) в процессе решения функциональных задач), обеспечивает восстановление вычислительного процесса при обычных сбоях и программных сбоях, реконфигурацию системы и восстановление при отказах. В системе допускается возникновение

«враждебной» неисправности одного элемента. При этом используется метод, обладающий достаточно высокой полнотой обнаружения неисправностей и возможностью гибкого задания критериев программного сбоя ЦВМ и ее отказа [19].

Функциональное диагностирование обнаруживает неисправности, искажающие результаты текущей функциональной работы. Однако в системе могут возникать неисправности, которые не влияют на текущие результаты и, следовательно, не обнаруживаются функциональным диагностированием. Эти так называемые латентные неисправности могут накапливаться в различных ЦВМ и при своем одновременном проявлении вызывать отказ системы даже при наличии в ней запасных исправных машин. Избежать накопления латентных неисправностей можно путем тестового диагностирования ЦВМ, выполняемого с помощью специально разработанной тестовой программы и обеспечивающего высокую полноту обнаружения неисправностей.

Особенности совместного использования функционального и тестового диагностирования. Метод организации одновременного функционального и тестового диагностирования в МВС, сопровождаемой непрерывным и сквозным функциональным диагностированием и параллельным поочередным тестовым диагностированием входящих в эту систему ЦВМ, обеспечивающий полный контроль над состоянием всех машин как в составе МВС, так и во всей вычислительной системе, исследован в [18]. Метод заключается в рассмотрении МВС, состоящей из n ЦВМ с номерами 1, ..., n (обозначенных $M_1, \ldots, M_n$) и соединенных n каналами межмашинной связи шинной архитектуры. Модели такой системы и аналогичной, представленной в [19], совпадают. Предполагается наличие одиночной неисправности, т. е. неисправной может быть либо одна ЦВМ — M_i, либо одно устройство сопряжения (передающее) — O_i, рассматриваемые как отдельные элементы системы.

Неисправность ЦВМ M_i проявляется как отсутствие необходимой передачи информации другим ЦВМ системы и/(или) как передача ошибочной информации. Неисправность O_i проявляется в воздействии на проходящее через него сообщение таким образом, что в p ЦВМ, где $n-1 > p \geq 0$ (n — общее число ЦВМ в МВС), сообщение может поступить без искажений, а в остальные ЦВМ — с произвольными, возможно неодинаковыми, искажениями.

Тестовое диагностирование состоит в подаче на проверяемый объект входных тестовых воздействий, считывании результатов теста и сравнении их с эталонными значениями. В процессе исполнения

тестовой программы ЦВМ формирует признак успешности проверки. «Враждебная» неисправность ЦВМ может привести, например, к формированию признака успешной проверки и при ее отрицательных результатах. Поэтому в случае возможности таких неисправностей тестовое диагностирование должно исключить либо свести к минимуму вероятность возникновения подобных ситуаций.

Согласно [18], одна часть МВС, выполняющая в данный момент функциональную сбое- и отказоустойчивую работу, называется рабочим комплексом, а другая часть системы, осуществляющая в тот же момент тестовое диагностирование, — тестирующим комплексом. При этом для корректного проведения тестового диагностирования ЦВМ в МВС должны выполняться два требования:

– ЦВМ из тестирующего комплекса не должна иметь возможности сформировать правильный результат тестовой программы иначе, как выполнив ее;

– оценка тестовой программы и, тем самым, оценка технического состояния тестируемой ЦВМ должна выполняться исправной частью МВС.

При тестовом диагностировании возможны два варианта подхода:

1) оценку результатов осуществляют сами тестируемые ЦВМ, и тогда для случая одиночной «враждебной» неисправности число одновременно тестируемых ЦВМ должно быть не менее четырех [20];

2) оценку результатов тестирования выполняют ЦВМ, принадлежащие рабочему комплексу [18].

Функциональная сбое- и отказоустойчивая работа рабочего комплекса в предлагаемом методе ведется с помощью алгоритма распределенного мажорирования АРМ-1 [19], выполняющего также непрерывное и сквозное функциональное диагностирование участвующих в нем ЦВМ. При обнаружении проявлений неисправностей алгоритм АРМ-1 строит логическое выражение подозреваемой области неисправности, задающее такие всевозможные допустимые совокупности сбоев, что при появлении сбоев любой из них возможно наблюдаемое поведение МВС. Идентификация проявившихся неисправностей осуществляется путем анализа выражения подозреваемой области неисправности на соответствие его заранее определенным критериям.

Все приведенное подразумевает согласованную работу всех исправных ЦВМ рабочего комплекса, которая основана на одинаковых данных, включающих информацию о техническом состоянии МВС, конфигурациях рабочего и тестируемого комплексов, едином системном времени и т. д. Предложенный метод позволяет существенно повысить надежностные характеристики МВС за счет удаления латентных неисправностей [21] в условиях возможности возникновения «враждебных» неисправностей элементов МВС.

Системное диагностирование [22] — традиционное направление исследований в области анализа технического состояния МВС. Технические системы (ТС), состоящие из взаимосвязанных модулей, которые могут проверять работоспособность друг друга, впервые были рассмотрены в [7]. В [23] вместе с достаточно полным обзором и анализом работ в этом направлении приведен перечень взаимосвязанных задач, образующих общую проблему системного диагностирования: построение диагностических моделей ТС, выбор способа диагностирования, определение класса неисправностей, подлежащих обнаружению и поиску, выбор тестов, анализ результатов тестирования.

Существуют различные модели неисправностей ЦВМ, часть из которых используется в системном диагностировании [23]. По степени общности эти модели можно разбить на два вида [17]:

1) «дружественные» неисправности;

2) «враждебные» неисправности.

При рассмотрении задачи определения класса неисправностей и анализа результатов тестирования [22] допускается возможность возникновения «враждебных» неисправностей, и тогда ставится задача распределенного, внутреннего диагностирования, т. е. системного самодиагностирования (ССД) МВС, при котором все исправные ЦВМ системы должны одновременно и одинаково обнаруживать и идентифицировать проявления неисправностей, появляющихся в процессе ССД, в условиях возможного возникновения «враждебных» неисправностей, а также рассматриваются организация процесса ССД и возникающие при этом проблемы. В [22] предложен метод ССД в МВС, учитывающий, во-первых, возможность влияния «враждебных» неисправностей на этапе обеспечения согласованности принимаемых решений и, во-вторых, модель неисправности ЦВМ в процессе взаимопроверок, совпадающую с ПМЧ-моделью [7]. Кроме того, приведен метод ССД, учитывающий возможность проявления «враждебных» неисправностей на всех этапах ССД и обеспечивающий ускорение идентификации имеющихся неисправностей по месту их возникновения и виду (сбой или отказ). При решении поставленных задач в [22] предполагается следующее:

– всем ЦВМ известны состав и формат локального синдрома проверок (ЛСП) каждой ЦВМ системы;

– работа всех исправных ЦВМ осуществляется с необходимой степенью синхронности, обеспечивающей правильность выполняемых межмашинных взаимодействий;

– ЦВМ-получатель межмашинного сообщения может определить его отправителя;

– для любой пары ЦВМ возможно только по одной их взаимопроверке;

– каждая из пар ЦВМ в системе имеет по два симплексных противоположно направленных канала связи, по которым осуществляется взаимообмен информацией между ЦВМ этой пары.

Задача анализа результатов тестирования условно делится на задачу выбора места дешифрации и на задачу построения алгоритма дешифрации.

Анализ полученного синдрома проверок может выполняться сосредоточенным методом дешифрации с использованием исправных средств, не входящих в анализируемую систему (внешнее обнаружение и диагностирование [24]), или распределенным методом с помощью самой же проверяемой системы (внутреннее обнаружение и диагностирование). Попытки распределенной дешифрации предпринимались в [24, 25].

Системное самодиагностирование можно представить в виде повторяющихся циклов, каждый из которых состоит из четырех фаз:

– выполнение проверяемыми ЦВМ предписанных им проверок, формирование результатов и их передача в проверяющие ЦВМ;

– анализ полученных результатов в проверяющих ЦВМ и формирование в каждой из них собственного ЛСП;

– взаимообмен собственными ЛСП между всеми ЦВМ системы и формирование во всех исправных ЦВМ глобальных синдромов проверки (ГСП) на основании полученных ЛСП;

– дешифрация ГСП в каждой исправной ЦВМ.

Согласованность результатов дешифрации во всех исправных ЦВМ системы может быть достигнута в результате того, что при любой допустимой неисправности системы, во-первых, любой ЛСП в ГСП всех исправных ЦВМ, относящийся к исправной ЦВМ, будет совпадать с собственным ЛСП этой ЦВМ, а любой ЛСП, относящийся к неисправной ЦВМ, будет одинаковым. Это гарантирует равенство ГСП во всех исправных ЦВМ. Во-вторых, к одинаковым ГСП во всех исправных ЦВМ будет применяться одинаковый алгоритм дешифрации. В этом случае задача формирования ГСП из отдельных ЛСП совпадает с задачей взаимного информационного согласования (ВИС) [20].

Требование полносвязности структуры РМВС как жесткое ограничение достижения сбое- и отказоустойчивости. Существуют различные алгоритмы ВИС, построенные для разных предположений о допустимых неисправностях и обладающие разной аппаратурной, временной и информационной избыточностью [26].

Цель системного диагностирования — восстановить работоспособное состояние системы. Для этого необходимы обнаружение и идентификация случившихся проявлений неисправностей как по месту возникновения неисправностей, так и по их виду. В связи

с этим в [22] предложены следующие уточнения видов проявлений неисправностей:

– сбой ЦВМ — событие, при котором предполагается, что искажению подверглась информация, не влияющая на ход и последующие результаты ее вычислительного процесса;

– программный сбой ЦВМ, внешним признаком которого считается проявление заранее оговоренной совокупности сбоев этой ЦВМ (критерий программного сбоя); в случае программного сбоя необходимо проведение специальных действий по восстановлению вычислительного процесса в сбившейся ЦВМ;

– отказ ЦВМ, объявляемый при проявлении заранее оговоренной совокупности программных сбоев этой ЦВМ (критерий отказа ЦВМ); при отказе необходимы изоляция неисправной ЦВМ, включение вместо нее запасной ЦВМ и восстановление вычислительного процесса во включенной ЦВМ.

Однако все приведенные в настоящей статье методы требуют соответствия одному очень жесткому условию: полносвязности МВС, т. е. в качестве модели такой МВС принят полный граф, вершины которого отображают ЦВМ, ребра — дуплексные каналы связи. Представленные методы позволяют полносвязной МВС обнаруживать и идентифицировать проявления «враждебных» неисправностей в процессе системного самодиагностирования при произвольных структуре графовой модели проверок и значении синдрома. Требование полносвязности — следствие использования в предлагаемых методах алгоритма ВИС из [20], предназначенного для получения во всех исправных ЦВМ одинакового значения ГСП. Применение алгоритма ВИС для неполносвязных структур МВС снимет это ограничение и в предлагаемых методах [22].

Использование алгоритма ВИС из [20] с требуемой им аппаратурной избыточностью $n > 3m$ (m — допустимое число неисправных ЦВМ в МВС) накладывает это ограничение и на необходимую аппаратурную избыточность всего метода ССД. Поэтому вместо оценки $n > 2m$ из [7] для случая внешнего диагностирования в предлагаемых методах ССД правильной оценкой будет $n > 3m$.

Недостатком предложенных методов является то, что из числа возможных проявлений неисправностей в процессе ВИС только малая часть их обнаруживается и учитывается при идентификации.

Полносвязные МВС исследуются также и в [27], сбое- и отказоустойчивость в них обеспечиваются путем решения одной и той же задачи несколькими ЦВМ с взаимообменом результатами и выбором из них правильного. Система состоит из p ЦВМ, каждая пара которых связана отдельным дуплексным каналом связи. Кроме того, каждая ЦВМ имеет отдельный канал связи с абонентами внешней среды, по которому она принимает входную и передает выходную информацию.

В начальном состоянии системы q из p ЦВМ находятся в запасе (ненагруженный «холодный» резерв), а остальные $n = p - q$ ЦВМ составляют «горячий» резерв (технология резервирования электронного оборудования, в которой резерв подключен к системе и подменяет вышедшую из строя компоненту в автоматическом режиме) и представляют текущую рабочую конфигурацию МВС.

В [17, 26] исследованы полносвязные МВС, в которых допускается «враждебная» [17, 26] неисправность одной ЦВМ в текущей рабочей конфигурации.

Проблема функционального диагностирования [15] систем рассматриваемого класса, состоящая в обнаружении проявлений «враждебных» неисправностей в процессе функциональной работы и идентификации этих проявлений по месту возникновения в рабочей конфигурации, представлена в [16, 17]. Однако изложенные методы обладают малой обнаруживающей способностью и имеют другие ограничения, препятствующие их применению в реальных МВС. В [19] предложен метод функционального диагностирования «враждебных» неисправностей с существенно более высокими обнаруживающей способностью и точностью идентификации случившихся проявлений неисправностей. Однако этот метод предназначен для МВС с межмашинными каналами связи шинной архитектуры и широковещательным способом передачи межмашинных сообщений [19].

Обеспечение длительных сроков активного существования МВС предполагает не только многочисленные виды диагностирования, но и восстановление работоспособности МВС, являющееся не менее сложным и трудоемким, чем диагностирование. Например, в [27] предлагается метод организации работы МВС, сопровождающейся непрерывным функциональным диагностированием как при выполнении функциональных задач, так и в процессах восстановления. Управляемая деградация системы может быть осуществлена в случаях возникновения отказов, а при исчерпании резерва или недостаточной избыточности системы в момент идентификации программного сбоя ЦВМ предусмотрен безопасный останов системы, при котором все исправные ЦВМ этой системы должны согласованно перевести управляемые объекты в состояние, безопасное даже при отказе МВС. Предполагается, что в МВС имеется минимально необходимая аппаратурная поддержка действий системы при восстановлении ЦВМ, подвергшейся программному сбою, и при реконфигурации системы в случае отказов.

Исправную часть системы, осуществляющую восстановление сбившейся ЦВМ, называют восстанавливающим комплексом (ВК) [27], который представляет рабочую конфигурацию системы в процессе восстановления. Теоретическим обоснованием действий, связанных

с восстановлением работоспособности МВС, может служить метод функционального диагностирования и управляемой деградации в сбое- и отказоустойчивой МВС, работающий при следующих условиях:

– возможно появление в МВС более одной неисправной ЦВМ;

– последовательность возникновения неисправностей такова, что возможна организация работы системы при наличии в ее рабочей конфигурации не более одной неисправной ЦВМ;

– при обнаружении очередного отказа система должна анализировать имеющийся в рабочей конфигурации уровень избыточности и при его недостаточности выполнить безопасный останов системы.

Реализация данных условий возможна при обеспечении необходимого уровня избыточности рабочей конфигурации системы, высокой степени контролируемости действий при восстановлении, сбое- и отказоустойчивой работы ВК.

Уровень избыточности (число ЦВМ) в рабочей конфигурации определяется требованиями реализуемых в ЦВМ алгоритмов. Достоверность, одновременность и одинаковость принимаемых в системе решений при возможности возникновения «враждебных» неисправностей гарантируется только применением алгоритма ВИС [26], требующего в общем случае наличия в рабочей конфигурации $n \geq 3m+1$ ЦВМ (m — допустимое число неисправных ЦВМ). Поскольку такая рабочая конфигурация необходима и при восстановлении сбившейся ЦВМ, т. е. в составе ВК должно быть не менее четырех ЦВМ при $m = 1$, в полной (недеградированной) рабочей конфигурации системы, потенциально содержащей сбившуюся ЦВМ и ВК, в процессе функциональной работы должно быть не менее $n \geq 5$ ЦВМ.

Результатом идентификации проявлений неисправностей будет некоторая подозреваемая область неисправностей. Если в эту область входят только программные сбои или отказы некоторых ЦВМ, ее называют подозреваемой областью отказов [27].

Механизмы реализации процедур восстановления состоят из аппаратурной и программной частей. Аппаратурная часть кроме передачи восстанавливаемой информации обеспечивает выполнение блокировки сбившейся ЦВМ и ее последующий пуск со стороны ВК. Блокировка сбившейся ЦВМ должна вызывать ее принудительный безусловный переход в фиксированное начальное состояние восстановления и предотвращать возможность воздействия заблокированной ЦВМ на другие ЦВМ и внешние абоненты системы.

Конструкция механизмов восстановления информации в памяти сбившейся ЦВМ в значительной степени зависит от возможностей межмашинных каналов связи.

Широкое внедрение компьютерных сетей, распределенных МВС (РМВС) выдвигает на первый план проблемы обеспечения надежности их работы и достоверности выходных результатов [22, 28]. Их можно решить, применяя методы распределенного ССД для МВС с межмашинными каналами связи шинной архитектуры и широковещательным способом передачи межмашинных сообщений, что уменьшает число необходимых в каждой ЦВМ передающих и принимающих канальных устройств до величины n. Метод должен обеспечивать сбоеустойчивость ВИС, а также сквозное и непрерывное функциональное диагностирование как ВИС, так и всего процесса ССД.

В [22, 28] представлены распределенные методы системного диагностирования «враждебных» неисправностей ЦВМ, но в полносвязных системах. Область распределенных методов системного диагностирования «враждебных» неисправностей ЦВМ в неполносвязных системах как системах наиболее общего вида остается открытой, и к этой области относится метод, предлагаемый в [29]. Разработанный алгоритм распределенного системного диагностирования РСД-1, предназначенный для неполносвязных систем, имеющих определенные структурные свойства, снимает одно из наиболее жестких ограничений при построении сбое- и отказоустойчивых систем с длительными сроками активного существования.

Заключение. Настоящая статья посвящена вопросам системного, функционального, тестового диагностирования, лежащим в основе построения необслуживаемых сбое- и отказоустойчивых систем, а также вопросам самодиагностирования, т. е. процессу определения состояния самодиагностируемой системы. Моделью самодиагностируемой системы служит орграф, вершины которого представляют модули системы, дуги — тестовые связи от тестирующих модулей к тестируемым. Дуги графа взвешены (двоичными) оценками состояния тестируемого модуля, которые дает ему тестирующий.

Рассмотрены вопросы полноты и надежности тестирования. Определено, что для современных необслуживаемых систем большой размерности и сложности, со значительными сроками активного существования не подходит ставший традиционным метод маскирования неисправностей или обнаружение и идентификации узкого класса неисправностей в предположении возможности ремонта. Длительный срок активного существования может обеспечить только реализация управляемой деградации, использующей исправные компоненты системы до последней возможности. Поэтому разработка метода обнаружения и идентификации проявлений допустимых неисправностей самого широкого класса в коммутационной структуре, определения на его основе возможных значений посылаемых данных и формирования предложений для следующего этапа деградации этой структуры — важная и актуальная задача.

Введено понятие самоуправляемой деградации среды, под которой понимается способность системы самостоятельно и своевременно обнаруживать и идентифицировать обнаруженные проявления неисправностей ее компонентов и при возникновении допустимых отказов реконфигурировать свою структуру и переходить в следующее допустимое работоспособное состояние с возможным допустимым снижением собственных характеристик производительности и надежности. При невозможности перехода в следующее работоспособное состояние система должна самостоятельно перейти в состояние безопасного останова. Одним из основных свойств таких систем является способность своевременно обнаруживать и идентифицировать случившиеся неисправности компонентов среды.

Обеспечение длительных сроков активного существования МВС предполагает не только многочисленные виды диагностирования, но восстановление ее работоспособности, являющиеся не менее сложными и трудоемкими, чем диагностирование.

Цель системного диагностирования заключается в восстановлении работоспособного состояния системы. Именно для этого необходимы обнаружение и идентификация случившихся проявлений неисправностей как по месту возникновения неисправности, так и по их виду. В связи с этим предлагается следующее уточнение видов проявлений неисправностей:

- сбой ЦВМ — событие, при котором предполагается, что искажению подверглась информация, не влияющая на ход и последующие результаты ее вычислительного процесса;
- программный сбой ЦВМ, внешним признаком которого считается проявление заранее оговоренной совокупности сбоев этой ЦВМ (критерий программного сбоя); в случае программного сбоя требуются специальные действия по восстановлению вычислительного процесса в сбившейся ЦВМ;
- отказ ЦВМ, объявляемый при проявлении заранее оговоренной совокупности программных сбоев этой ЦВМ (критерий отказа ЦВМ); при отказе необходимы изоляция неисправной ЦВМ, включение вместо нее запасной ЦВМ и восстановление вычислительного процесса во включенной ЦВМ.

ЛИТЕРАТУРА

[1] Ашарина И.В. Проблемы организации вычислений в многомашинных вычислительных системах с программно-управляемой сбое- и отказоустойчивостью. Часть I. *Инженерный журнал: наука и инновации*, 2021, вып. 6. http://dx.doi.org/10.18698/2308-6033-2021-6-2088

[2] Димитриев Ю.К. Локальное самодиагностирование в вычислительных системах с циркулянтной структурой. *Автоматика и телемеханика*, 2007, вып. 3, с. 187–198.

[3] Тоффоли Т., Марголус Н. *Машины клеточных автоматов.* Москва, Мир, 1991, 280 с.

[4] Димитриев Ю.К. Правила условного локального самоопределения и алгоритм диагностирования мультипроцессорной системы с циркулянтной диагностической структурой на их основе. *Автоматика и телемеханика*, 2012, вып. 5, с. 125–140.

[5] Димитриев Ю.К. О концептуальной основе сравнительного анализа и решения задач самодиагностики многопроцессорных систем для разных моделей ненадежного тестирования. *Автоматика и телемеханика*, 2015, вып. 7, с. 150–164.

[6] Димитриев Ю.К. Необходимые и достаточные условия t-диагностируемости многопроцессорных вычислительных систем для разных моделей ненадежного тестирования, полученные с помощью теоретико-графовой модели системы. *Автоматика и телемеханика*, 2016, вып. 6, с. 145–158.

[7] Preparata F.P., Metze G., Chien R.J. On connection assignement problem of diagnosable systems. *IEEE Trans. El. Comput.*, 1967, vol. EC-16, no. 12, pp. 848–854.

[8] Пархоменко П.П., Согомонян Е.С. *Основы технической диагностики. Оптимизация алгоритмов диагностирования, аппаратурные средства*. Москва, Энергия, 1981, 319 с.

[9] Barsi F., Grandoni F., Maestrini P. Theory of diagnosability of digital systems. *IEEE Trans. Comput.*, 1976, vol. C-25, no. 6, pp. 585–593.

[10] Chwa K.Y., Hakimi S.L. Schemes for fault tolerant computing — a comparison of modularly redundant and *t*-diagnosable systems. *Inf. Control*., 1981, vol. 49, no. 3, pp. 212–238.

[11] Malek M. A comparison connection assignement for diagnosis of multiprocessor system. *Proc. 7th Int. Symp. Comput. Archit*., *La Baule, USA, May 6–8, 1980*. New York, Association for Computing Machinery, 1980, pp. 31–35.

[12] Kavianpour A., Friedman A. A different diagnostic model for multiprocessor systems. *Proc. Information processing 80 by IFIP Congress 80. Tokyo, Japan, October 6–9, 1980 and Melbourne, Australia, October 14–17, 1980*. North-Holland, IFIP, 1980, pp. 157–162.

[13] Димитриев Ю.К. Правила условного локального самоопределения и алгоритм диагностирования мультипроцессорной системы с циркулянтной диагностической структурой на их основе. *Автоматика и телемеханика*, 2012, вып. 5, с. 125–140.

[14] Сиренко В.Г. Функциональное диагностирование процессов посылок информации в вычислительных системах при неизвестном исходном значении информации. Часть I. Внешнее диагностирование. *Автоматика и телемеханика*, 2005, вып. 11, с. 135–154.

[15] Карибский В.В., Пархоменко П.П., Согомонян Е.С. *Основы технической диагностики. Модели объектов, методы и алгоритмы диагноза*. Москва, Энергия, 1976, 464 с.

[16] Lala J.H., Alger L.S., Gauthier R.J., Dzwonczyk M.J. A fault tolerant processor to meet rigorous failure requirements. *Proc. of the 7th AIAA/IEEE Digital Avionics Systems Conf., October 13–16, 1986, Fort Worth, TX, USA*. Fort Worth, IEEE, 1986, vol. 1, pp. 555–562.

[17] Мамедли Э.М., Самедов Р.Я., Соболев Н.А. Метод локализации «дружественных» и «враждебных» неисправностей. *Автоматика и телемеханика*, 1992, вып. 5, с. 126–138.

[18] Лобанов А.В. Обнаружение и идентификация «враждебных» неисправностей путем одновременного сочетания функционального и тестового диагностирования в многомашинных вычислительных системах. *Автоматика и телемеханика*, 1999, вып. 1, с. 159–165.

[19] Лобанов А.В. Обнаружение и идентификация неисправностей в распределенных управляющих вычислительных системах с программно-управляемой сбое- и отказоустойчивостью. *Автоматика и телемеханика*, 1998, вып. 1, с. 155–164.

[20] Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. *J. ACM.*, 1980, vol. 27, no. 2, pp. 228–234.

[21] Rennels D. Fault-tolerant computing-concepts and examples. *IEEE Tr. Comp.*, 1984, vol. C-32, no. 12, pp. 1116–1129.

[22] Лобанов А.В., Сиренко В.Г. Распределенные методы системного диагностирования многомашинных вычислительных систем. *Автоматика и телемеханика*, 2000, вып. 8, с. 165–172.

[23] Микеладзе М.А. Развитие основных моделей самодиагностирования сложных технических систем. *Автоматика и телемеханика*, 1995, вып. 5, с. 3–18.

[24] Kuhl J.G., Reddy S.M. Fault-diagnosis in fully distributed systems. *Proc. of the 11th Int. Symp. on Fault-Tolerant Computing. June 24–26 1981, Portland, Maine*. New York, IEEE, 1981, pp. 100–105.

[25] Liaw C.C., Maliya Y.K., Su S.Y.H. Self-diagnosis in nonhomogeneous distributed systems. *Proc. of the 12th Int. Symp. Fault-Tolerant Computing. June 15–18, 1982, Los Angeles, CA*. New York, IEEE, 1982, pp. 223–233.

[26] Генинсон Б.А., Панкова Л.А., Трахтенгерц Э.А. Отказоустойчивые методы взаимной информационной согласованности в распределенных вычислительных системах. *Автоматика и телемеханика*, 1989, вып. 5, с. 3–18.

[27] Лобанов А.В. Организация сбое- и отказоустойчивых вычислений в полносвязных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2000, вып. 12, с. 138–146.

[28] Гришин В.Ю., Лобанов А.В., Сиренко В.Г. Функциональное диагностирование в распределенном системном диагностировании многомашинных вычислительных систем. *Автоматика и телемеханика*, 2002, вып. 1, с. 154–160.

[29] Гришин В.Ю., Лобанов А.В., Сиренко В.Г. Распределенное системное диагностирование враждебных неисправностей в неполносвязных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2005, вып. 2, с. 148–157.

Статья поступила в редакцию 13.03.2021

Ссылку на эту статью просим оформлять следующим образом:

Ашарина И.В. Проблемы организации вычислений в многомашинных вычислительных системах с программно-управляемой сбое- и отказоустойчивостью. Часть II. *Инженерный журнал: наука и инновации*, 2021, вып. 7.

http://dx.doi.org/10.18698/2308-6033-2021-7-2097

Ашарина Ирина Владимировна — канд. техн. наук, доцент, старший научный сотрудник АО «НИИ «Субмикрон». e-mail: asharinairina@mail.ru

Issues of organizing computations in multicomputer systems with the software-controlled failure- and fault-tolerance. Part II

© I.V. Asharina

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

This three-part paper analyzes existing approaches and methods of organizing failure- and fault-tolerant computing in distributed multicomputer systems (DMCS), identifies and provides rationale for a list of issues to be solved. We review the application areas of failure- and fault- tolerant control systems for complex network and distributed objects. The second part further investigates the issues of organizing failure- and fault- tolerance in the DMCS. The systemic, functional, and test diagnostics are viewed as the basis for building unattended failure- and fault-tolerant systems. We introduce the concept of self-managed degradation (when the DMCS eventually proceeds to a safe shutdown at a critical level of degradation) as a means to increase the DMCS active life.

Keywords: *distributed multicomputer system, failure- and fault-tolerance, dynamic redundancy, malicious fault*

REFERENCES

[1] Asharina I.V. *Inzhenerny zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation*, 2021, iss. 6. DOI: 10.18698/2308-6033-2021-6-2088

[2] Dimitriev Yu.K. *Avtomatika i telemekhanika — Automation and Remote Control*, 2007, vol. 68, no. 3, pp. 545−556.

[3] Toffoli T., Margolus N. *Cellular Automata Machines*. MIT Press, 1987, 276 p. [In Russ.: Toffoli T., Margolus N. Mashiny kletochnykh avtomatov. Moscow, Mir Publ., 1991, 280 p.].

[4] Dimitriev Yu.K. *Avtomatika i telemekhanika — Automation and Remote Control*, 2012, vol. 73, no. 5, pp. 862−872.

[5] Dimitriev Yu.K. *Avtomatika i telemekhanika — Automation and Remote Control*, 2015, vol. 76, no. 7, pp. 1260−1270.

[6] Dimitriev Yu.K. *Avtomatika i telemekhanika — Automation and Remote Control*, 2016, vol. 77, no. 6, pp. 1060−1070.

[7] Preparata F.P., Metze G., Chien R.J. On Connection Assignment Problem of Diagnosable Systems. *IEEE Trans. El. Comput*., 1967, vol. EC-16, no. 12, pp. 848–854.

[8] Parkhomenko P.P., Sogomonian E.S. *Osnovy tekhnicheskoi diagnostiki Optimizatsiia algoritmov diagnostirovaniia, apparaturnye sredstva* [Fundamentals of technical diagnostics Optimization of diagnostic algorithms, hardware]. Moscow, Energiya Publ., 1981, 319 p.

[9] Barsi F., Grandoni F., Maestrini P. Theory of Diagnosability of Digital Systems. *IEEE Trans. Comput,* 1976, vol. C-25, no. 6, pp. 585–593.

[10] Chwa K.Y., Hakimi S.L. Schemes for Fault Tolerant Computing — A Comparison of Modularly Redundant and t-diagnosable Systems. *Inf. Control*., 1981, vol. 49, no. 3, pp. 212–238.

[11] Malek M. A Comparison Connection Assignment for Diagnosis of Multiprocessor System. *Proc. 7th Int. Symp. Comput. Archit., La Baule, USA, May 6–8, 1980.* New York, Association for Computing Machinery, 1980, pp. 31–35.

[12] Kavianpour A., Friedman A. A different diagnostic models for multiprocessor systems. *Proc. Information processing 80 by IFIP Congress 80. Tokyo, Japan, October 6–9, 1980 and Melbourne, Australia, October 14–17, 1980.* North-Holland, IFIP, 1980, pp. 157–162.
[13] Dimitriev Yu.K. *Avtomatika i telemekhanika — Automation and Remote Control*, 2012, vol. 73, no. 5, pp. 862−872.
[14] Sirenko V.G. *Avtomatika i telemekhanika — Automation and Remote Control*, 2005, vol. 66, no. 11, pp. 1824−1840.
[15] Karibskii V.V., Parkhomenko P.P., Sogomonian Ye.S. *Osnovy tekhnicheskoy diagnostiki. Modeli obyektov, metody i algoritmy diagnoza* [Fundamentals of technical diagnostics. Object models, methods and algorithms for diagnosis]. Moscow, Energiya Publ., 1976, 464 p.
[16] Lala J.H., Alger L.S., Gauthier R.J., Dzwonczyk M.J. A fault tolerant processor to meet rigorous failure requirements. *AIAA/IEEE Digital Avionics Systems Conf.*, *October 13–16, 1986, Fort Worth, TX, USA*. Fort Worth, IEEE, 1986, pp. 555–562.
[17] Mamedli E.M., Samedov R.Ya., Sobolev N.A. *Avtomatika i telemekhanika — Automation and Remote Control*, 1992, vol.53, no. 5, pp. 734−744.
[18] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 1999, vol. 60, no. 1, pp. 127−131.
[19] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 1998, vol. 59, no. 1, pp. 129−135.
[20] Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. *J. ACM.,* 1980, vol. 27, no. 2, pp. 228–234.
[21] Rennels D. Fault-tolerant computing-concepts and examples. *IEEE Tr. Comp.,* 1984, vol. C-32, no. 12, pp. 1116–1129.
[22] Lobanov A.V., Sirenko V.G. *Avtomatika i telemekhanika — Automation and Remote Control*, 2000, vol. 61, no. 8, pp. 1390−1396.
[23] Mikeladze M.A. *Avtomatika i telemekhanika — Automation and Remote Control*, 1995, vol. 56, no. 5, pp. 611−623.
[24] Kuhl J.G., Reddy S.M. Fault-Diagnosis in Fully Distributed Systems. *Proc. 11 th Int. Symp. Fault-Tolerant Computing, June 24–26 1981, Portland*, *Maine*. New York, IEEE, 1981, pp. 100−105.
[25] Liaw C.C., Maliya Y.K., Su S.Y.H. Self-Diagnosis in Nonhomogeneous Distributed Systems. *Proc. of the 12th Int. Symp. Fault-Tolerant Computing. June 15–18, 1982, Los Angeles, CA*. New York, IEEE, 1982, pp. 223–233.
[26] Geninson B.A., Pankova L.A., Trakhtengerts E.A. *Avtomatika i telemekhanika — Automation and Remote Control*, 1989, vol. 50, no. 5, pp. 579−590.
[27] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2000, vol. 61, no. 12, pp. 2059−2067.
[28] Grishin V.Yu., Lobanov A.V., Sirenko V.G. *Avtomatika i telemekhanika — Automation and Remote Control*, 2002, vol. 63, no. 1, pp. 139−144.
[29] Grishin V.Yu., Lobanov A.V., Sirenko V.G. *Avtomatika i telemekhanika — Automation and Remote Control*, 2005, vol. 66, no. 2, pp. 304−312.

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