

## КОМПЬЮТЕРНАЯ ТЕХНОЛОГИЯ ПРОЕКТИРОВАНИЯ ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ УПРАВЛЕНИЯ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А. С. КУЛИК

**ВВЕДЕНИЕ.** Крупные аварии и катастрофы последних лет в ракетно-космической технике и в авиации выдвинули проблему безопасности и живучести летательных аппаратов в одну из актуальных проблем современности.

Для обеспечения безаварийного и надежного функционирования летательных аппаратов используется большой арсенал методов и средств построения систем управления, парирующих отказы. В большинстве случаев эффективность используемых способов оказывается на достаточной для предотвращения катастроф и ограничения их последствий на экономику, экологию и политику. В последние годы в ряде стран ведущие специалисты по автоматическому управлению активизировали исследования в направлении построения более эффективных отказоустойчивых систем управления. В результате проведенных исследований предложен ряд новых методов обеспечения активной отказоустойчивости систем управления. Вместе с тем до последнего времени отсутствовали работы систематизирующие и обобщающие полученные результаты для класса летательных аппаратов, а также работы по созданию конструктивной методологии построения систем управления с активной отказоустойчивостью.

**НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ОТКАЗУСТОЙЧИВОСТИ.** Известно два принципиальных пути в обеспечении отказоустойчивости систем управления (СУ). Первый - технологический, заключается в совершенствовании технологии производства элементов и СУ. Возможности этого пути ограничены известными пределами, описанными R. Lauber [1]. Второй путь - конструкторский, состоит в использовании методов построения "отказоустойчивых систем из надежных элементов". Для этого пути характерно использование следующих подходов: структурного, алгоритмического и системного.

Структурный подход связан с использованием резервных элементов и мажоритарного принципа обработки выходной информации. Это исторически первый подход, получивший широкое применение в авиационных и космических объектах.

Суть алгоритмического подхода состоит в использовании



алгоритмической избыточности для парирования отказов, как правило, путем сигнальных и параметрических подстроек на основе информации и рассогласования реального и эталонного поведения СУ. Первые работы этого направления связаны с разработкой адаптивного автопилота в Массачусетском технологическом институте и описаного Н. Whitaker [2]. Использование принципа самонастройки позволило в последующем создать целый класс беспилотных самонастраивающихся систем, обеспечивающих определенный уровень отказоустойчивости СУ.

Основное достоинство этих подходов заключается в конструктивности использования средств парирования отказов путем реконфигурации структуры и подстройки характеристик СУ.

Принципиальным недостатком структурного и алгоритмического подходов является неглубокое диагностирование причин аварийного функционирования СУ. Обычно, диагностирование заключается только в обнаружении отказов.

Для третьего, системного подхода характерно комплексное использование процедур диагностирование и парирование отказов, чем обеспечивается активная отказоустойчивость. Первая теоретическая работа этого направления была выполнена R. Beard [3]. В последующем это направление развивалось в работах А. Кулика [4,5], Y. Yang [6], R. Patton [7] и др. Проблематика системного обеспечения отказоустойчивости СУ представляется относительно новой и актуальной как в теоретическом, так и прикладном аспектах.

**НОВЫЙ ВКЛАД В ТЕОРИЮ СИСТЕМНОГО ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ СУ.** Проведенные под руководством автора теоретические и экспериментальные исследования позволили сформировать новое направление дальнейшего развития системного подхода. Это направление основывается на использовании трех принципов. Первый - трехуровневая иерархия обеспечения отказоустойчивости. Второй - глубокое диагностирование причин отказов. Третий - гибкое парирование последствий отказов.

Использование первого принципа приводит к формированию элементного, системного и надсистемного уровней обеспечения отказоустойчивости. С этой целью из всего множества вероятных видов отказов  $D = \{d_i\}_1^q$  выбираются виды отказов  $D_1$  с  $D$ ,



которые могут быть парированы на элементном уровне, исходя из имеющегося объема  $R_1$  элементной избыточности. Для системного уровня формируется подмножество  $D_2$  с  $D$  видов отказов, парируемых с помощью средств системной избыточности  $R_2$ . На третьем надсистемном уровне парируются виды отказов из подмножества  $D_3$  с  $D$  с помощью внешнесистемных средств избыточности  $R_3$ .

Реализация принципа глубокого диагностирования приводит на каждом уровне иерархии к декомпозиции задачи диагностирования на ряд взаимосвязанных следующих подзадач: построение диагностических моделей, обнаружение отказов, поиска места и установление классов отказов.

Диагностические модели строятся исходя из математического описания объекта диагностирования

$$\begin{aligned}\tilde{x}(k+1) &= f[\tilde{x}(k), u(k), \lambda, \xi(k)] \\ \tilde{y}(k) &= g[\tilde{x}(k), u(k), \lambda, \eta(k)],\end{aligned}\quad (1)$$

где  $\tilde{x}(k)$  - вектор состояния объекта диагностирования;  $u(k)$  - вектор входных воздействий;  $\lambda$  - вектор целевых параметров отказов;  $\tilde{y}(k)$  - вектор измеряемых переменных объекта;  $\xi(k)$  и  $\eta(k)$  - векторы помех;  $f[.]$  и  $g[.]$  - нелинейные функции;  $k = 0, 1, 2, \dots$ . Вектор целевых параметров  $\lambda$  формируется в результате параметризации видов отказов подмножеств  $D_i$ ,  $i = 1, 3$ .

В общем виде диагностические модели связывают отклонения сигнальных характеристик объекта  $\Delta x(k)$  и  $\Delta y(k)$  с отклонениями соответствующих целевых признаков  $\Delta \lambda_i$  с помощью таких соотношений

$$\begin{aligned}\Delta x(k+1) &= \psi[\tilde{x}(k), \Delta x(k), u(k), \Delta \lambda_i, \xi(k)], \\ \Delta y(k) &= \gamma[\tilde{x}(k), \Delta x(k), u(k), \Delta \lambda_i, \eta(k)],\end{aligned}\quad (2)$$

здесь  $\psi[.]$  и  $\gamma[.]$  - нелинейные функции, вид которых зависит от применяемого метода построения моделей.

Использование диагностических моделей позволяет формализовать процесс построения оптимальных по технико-экономическим критериям алгоритмов диагностирования с



заданной глубиной, оперативностью и достоверностью. В результате решения на каждом иерархическом уровне задач диагностирования получается соответствующая процедура диагностирования, представленная дихотомическим деревом, в узлах которого используются двузначные предикатные уравнения

$$\mu_j = S_2[\Delta y(k), V_\lambda(k), \delta_j], \quad (3)$$

где  $V_\lambda(k)$  - векторные функции чувствительности косвенного диагностического признака объекта  $\Delta y(k)$  по векторному целевому признаку  $\lambda$ ;  $\delta_j$  - пороговое значение выполнения соотношения под знаком предиката  $S_2[.]$ . Обработка массивов входных данных в каждом узле производится с применением соответствующего коэффициента доверия  $p$  и в результате полученное значение  $\mu_j$  определяет направление дальнейшего поиска целевых признаков отказов. Заканчивается дерево листьями соответствующими сформированным классам отказов  $K_i, i = \overline{1, n}$ .

Суть принципа гибкого парирования последствий отказов состоит в формировании для каждого класса отказов  $K_i$  адаптивной процедуры использования соответствующих элементов избыточности из подмножества  $R_i = \{r_1^i, r_2^i, \dots, r_l^i\}, i = \overline{1, 3}$ . Необходимость применения адаптивной схемы связана с неопределенным изменением технического состояния объекта, с динамическим характером происходящих процессов, с наличием избыточных средств парирования отказов. Формирование процедур парирования производится исходя из принципа действия объекта, его особенностей в аварийных режимах, а также с применением диагностических моделей (2).

Использование описанных трех принципов приводит к новой структуре СУ, укрупненная функциональная схема которой представлена на рис. 1. На первом, элементном уровне отказоустойчивая СУ состоит из объекта управления, измерителей (И), сервоприводов (СП) и регулятора (Р), включающих процедуру диагностирования (Д) и парирования (П) отказов. На втором, системном уровне производится процедура диагностирования всей СУ, а также парирования отказов с помощью системных средств. На подсистемном уровне осуществляется диагностирование качества работы



УРОВНИ  
ОБЕСПЕЧЕНИЯ  
ОТКАЗОУСТОЙЧИВОСТИ

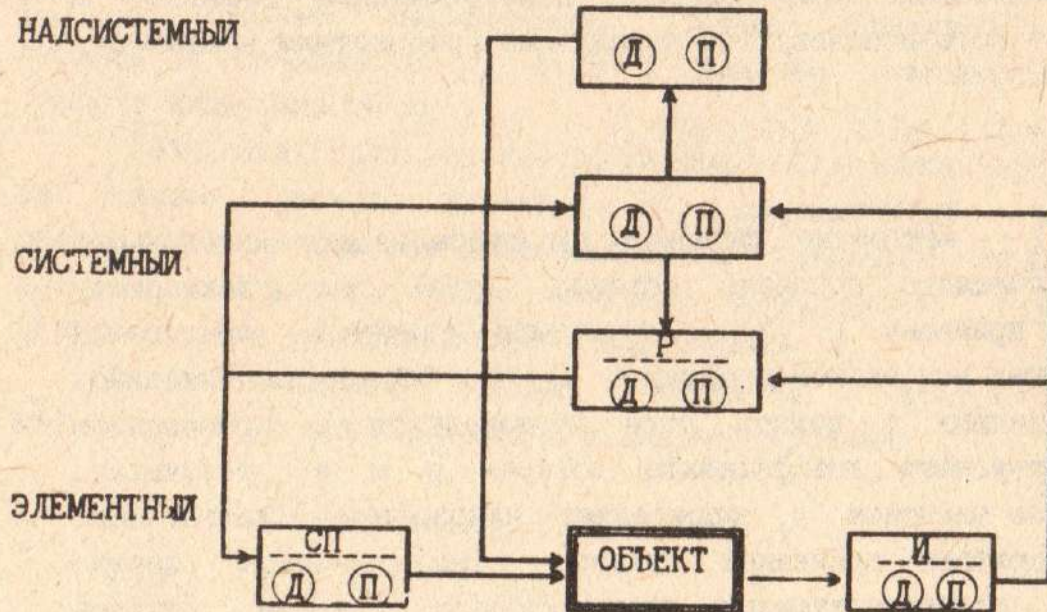


Рис. 1. Укрупненная функциональная схема отказоустойчивой СУ.

нижних уровней и производится парирование отказов с помощью имеющихся средств. На рис. 1 не приведены связи уровней и поэтому не описана организация работы уровней.

**АППАРАТНО - ПРОГРАММНЫЕ СРЕДСТВА ПРОЕКТИРОВАНИЯ.** Разработанные теоретические основы построения отказоустойчивых СУ позволили сформировать принципы новой технологии и состав инструментальных средств проектирования. Технология проектирования базируется на использовании информационных возможностях ПЭВМ типа IBM PC AT, расширенных за счет аппаратного интерфейса с объектом. Создание новой компьютерной технологии связано с проведением многоэтапных исследовательских и конструкторских работ. Проведенные на первом этапе исследования позволили построить конкретную методику и разработать аппаратно-программные средства обеспечения отказоустойчивости на элементном уровне блока гироскопических датчиков. Так, создана автоматизированная система, включающая в себя стенд, микропроцессорный измерительный блок, ПЭВМ и комплекс программных средств. Стенд предназначен для имитации функционирования типового



блока гироскопических датчиков в номинальном и аварийном режимах. Микропроцессорный измерительный блок обеспечивает аналого-цифровое преобразование сигналов с датчиков, координатную их привязку, временное накопление, предварительную обработку информации и ее передачу в ПЭВМ. Комплекс программных средств предназначен для приема информации со стенда, ее обработки, хранения, визуализации и документирования.

Комплекс программных средств состоит из двух подсистем. Первая - предназначена для автоматизации проектирования диагностического обеспечения. Она включает программные средства анализа диагностируемости СУ по диагностическим моделям, минимизации логических моделей, использующие предикатные признаки, построения сбалансированных дихотомических деревьев, формирование машинных программ диагностирования СУ, а также создание программы парирования последствий отказов. Работа с первой подсистемой в диалоговом режиме позволяет создавать программы диагностирования и парирования отказов как элементов, так и СУ, представленных диагностическими моделями типа (2).

Вторая подсистема предназначена для автоматизации отладки программного обеспечения отказоустойчивости, включающего программы диагностирования, парирования и управления. Эта подсистема включает программные средства имитационного моделирования объектов исследования, визуализации процесса отладки, коррекции программного обеспечения отказоустойчивости и его документирования после отладки.

Разработанные программные средства использовались также при выполнении заказа НИИ ПЭМ по диагностированию блока датчиков, заказа Харьковского агрегатного конструкторского бюро - ХАКБ, по обеспечению отказоустойчивости рулевого привода АЭГРП и заказа КБ "Южное" по диагностированию системы электроснабжения изделия СМ-КИ.

**НАПРАВЛЕНИЯ ДАЛЬНЕЙШЕГО ИССЛЕДОВАНИЯ.** Для создания завершенной компьютерной технологии проектирования требуется создание стенда имитирующего функционирование типовых сервоприводов и разработка технологии и средств обеспечения его отказоустойчивости. Выполнение этих работ позволит перейти к разработке технологии и средств обеспечения



отказоустойчивости на системном и подсистемном уровнях.

Проведение этих исследовательских и опытно-конструкторских работ позволит создать современную технологию и аппаратно-программные средства производительного проектирования СУ с более высокими уровнями живучести, что позволит удовлетворить возрастающие требования к безопасности летательных аппаратов.

#### ЛИТЕРАТУРА

1. Lauber R.J. Aspects of Achieving Total Systems Availability IFAC/IMACS Symposium. SAFEPROCESS'91. Baden-Baden, Vol. 1, pp. 35-41.
2. Whitaker H.P. Adaptive control system. - In: Air, Space and Instruments. Draper Anniversary Volume. New York, MC. Graw Hill, pp. 207-234, 1963.
3. Beard R.V. Failure accomodation in linear system through self-reorganization. Ph. D. Thesis, MIT, Cambridge, 1971.
4. Kulik A.S. Synthesis of fault-tolerant dynamic control systems. Problems of Control and Information Theory, № 1, 1989, pp. 43-54.
5. Кулик А.С. Обеспечение отказоустойчивости систем управления. Харьков. ХАИ, 1991. - 90с.
6. Yang Y.Y. Sensor fault tolerant control and its application. IFAC/IMACS Symposium. SAFEPROCESS'91, Baden-Baden, Vol. 1, pp. 55-58.
7. Patton R.J. Robustness issues in fault-tolerant control. International Conference on Fault Diagnosis. TOOLDIAG'93, Toulouse, Vol. 3, pp. 812-836.