УДК 681.321

УНИФИЦИРОВАННЫЕ СТРУКТУРЫ И ВАРИАНТЫ ПРОГРАММНО - АППАРАТНОЙ РЕАЛИЗАЦИИ ЖИВУЧИХ И БЕЗОПАСНЫХ СИСТЕМ

д.т.н., проф. В.С. Харченко, к.т.н. В.Г. Литвиненко

Предлагаются унифицированные структуры отказоустойчивых, живучих и безопасных систем. Сформулированы рекомендации по вариантам программно-аппаратной реализации средств, обеспечивающих их свойства.

Введение. Если требования по надежности являются традиционными практически для любых технических систем, то повышенные требования по живучести и безопасности функционирования специфичны для бортовой и наземной аппаратуры и оборудования летательных комплексов (ЛК), других комплексов критического применения [1-5]. Это объясняется, во-первых, тем, что системы ЛК функционируют в сложных условиях эксплуатации (при перегрузках, высокой температуре, повышенной радиации и т.д.), учет которых делает совершенно необходимым наличие специальных средств обеспечения живучести - средств адаптации к указанным условиям и сохранения хотя бы минимально возможного уровня работоспособности.

Во-вторых, отказы систем ЛК не только приводят к большим потерям, но и создают реальную опасность для людей и окружающей среды. Поэтому в таких системах должны быть реализованы специальные механизмы обеспечения безопасности (снижения потенциальной опасности) функционирования.

Цель статьи - разработка унифицированных структур живучих и безопасных систем, а также рекомендаций по аппаратно-программной реализации средств обеспечения этих свойств.

Унифицированная структура живучей системы. Для обеспечения живучести в информационно – вычислительной управляющей системе (ИВУС) должны быть предусмотрены следующие функции средства (рис.1):

а) **основные (а1) и резервные (а2) функциональные (избыточные) программно-аппаратные средства (модули)** ФПАСр - ОПАСр и РПАСр, обеспечивающие выполнение функций ИВУС при отсутствии отказов элементов и в случае их возникновения вследствие естественных причин (износ, старение - «естественные отказы» (ЕО)) и экстремальных внешних воздействий («экстремальные» отказы (ЭО));

б) **средства контроля** (СрК) технического состояния ОПАСр и РПАСр, которые осуществляют проверку их работоспособности. СрК могут быть разделены на:

б1) **средства непрерывного рабочего контроля** (СрРК), позволяющие оперативно обнаруживать свои отказы в ОПАСр и РПАСр, а также в других средствах ИВУС (включая СрК);

б2) **средства периодического тестового контроля** (СрТК), осуществляющие в установленные моменты времени (с заданной периодичностью) или в заданных режимах: после срабатывания СрК - для повышения достоверности проверки, в режимах естественного ожидания - для «фонового» тестирования, перед включением системы или выполнением наиболее важных функций - для предрабочего тестового контроля, в режиме самопроверки средств обеспечения живучести и др.;

в) **средства диагностирования и поиска дефектов** (СрД), обеспечивающие локализацию отказавших модулей (элементов, ТЭЗов) с требуемой глубиной. Включение этих средств осуществляется по сигналам от СрК (очевидно, что часть средств СрК и СрД могут быть общими);

г) **средства оценки технического состояния и определения уровня деградации** (СрОСД), которые по результатам контроля и диагностирования определяют способность системы выполнять набор заданных функций (ступень деградации, которая соответствует выявленному множеству отказавших элементов ОПАСр и РПАСр);

д) **средства коррекции (изменения) целей функционирования** (СрИЦФ), осуществляющие:

д1) отображение множества отказавших элементов на множество выполняемых функций - СрООФ;

д2) оценку программно-аппаратных ресурсов системы СрОР;

д3) определение набора функций, которые могут быть реализованы в сложившейся ситуации и определение целевой стратегии фукнкционирования СрОНФ;

е) **средства реконфигурации структуры (архитектуры)** (СрРС) ИВУС, обеспечивающие перекоммутацию связей между ее элементами с учетом результатов контроля, диагностирования и уточнения целей функционирования; эти средства, в свою очередь, могут подразделяться на:

е1) **средства задания последовательности конфигураций** (СрЗПК), которые осуществляют выбор алгоритма реконфигурации и перебор в соответствии с ним конфигураций для тестирования, оценки состояния и выбора наилучшего варианта структуры системы;

е2) **средства управления коммутацией связей** (СрУКС), непосредственно управляющих организацией соединительных магистралей между элементами системы;

ж) **средства фиксации и защиты от экстремальных воздействий** (СрФЗВ), представляющие собой совокупность:

ж1) датчиков, определяющих моменты (и, если возможно, уровень) их воздействия на систему - средств фиксации и момент завершения воздействия - **средств фиксации экстремальных воздействий** (СрФЭВ);

ж2) **средств включения защитных механизмов** (СрВЗМ). В простейшем случае это могут быть средства запоминания минимально необходимой информации о состоянии системы с использованием специальных стойких запоминающих устройств (СЗУ) и ее отключения;

ж3) **средств реанимации после воздействия** (СрРПВ), осуществляющих принудительное восстановление состояния системы путем считывания информации из СЗУ после проведения контроля, диагностирования, коррекции целей функционирования и реконфигурации;

з) **средства восстановления информации после отказов и сбоев** (СрВИ), подразделяющиеся на:

з1) **средства запоминания состояния системы в момент прерывания по сигналам отказа** (СрЗС). Эти средства совпадают по функциям с СрВЗМ. Однако, для хранения информации могут использовать обычную оперативную память;

з2) **средства определения и управления последовательностью восстановления** (СрУПВ);

з3) **средства загрузки информации и осуществления рестарта** (СрЗИР). Средства СрУПВ и СрЗИР могут быть объединены с СрРПВ;

и) **средства оперативного парирования отказов и сбоев** (СрПОС), обеспечивающие нейтрализацию искажения информации, вызванного программно-аппаратными дефектами ОПАСр и РПАСр. В простейшем случае это могут быть внутриярусные, сетевые и узловые мажоритарные элементы (адаптивные и неадаптивные).

Варианты предпочтительной реализации (аппаратный – А, программный – П или программно - аппаратный – ПА) представлены в табл.1.

Унифицированная структура безопасной системы. Для обеспечения безопасного функционирования ИВУС должна содержать часть средств, используемых для обеспечения живучести и описанных выше. Это касается следующих средств: СрК, СрД, СрРС, СрПОС, СрВИ. Кроме того, в безопасных системах должны быть предусмотрены (рис.2):

а) **средства оценки последствий отказов** (СрОПО), которые обеспечивают выявление критических отказов;

б) **средства аварийного выключения системы** (СрАВ), которые, в свою очередь, состоят из:

б1) **средств минимизации последствий отказов** (СрМПО);

б2) **средств управления аварийным выключением** (СрУАВ).

Предпочтительные варианты реализации средств обеспечения безопасности приведены в табл. 2.

Таблица 1

Предпочтительные варианты реализации средств обеспечения живучести

№ п/п	Вид средств	Варианты предпочтительной реализации
а	ФПАСр	А, П, ПА
а1	ОПАСр	А, П, ПА
а2	РПАСр	А, П, ПА
б	СрК	А, ПА
б1	СрРК	А
б11	ПРВ, ПВР	А
б12	ФОР	А, ПА
б13	БСР	А, ПА
б2	СрТК	П, ПА
в	СрД	П, ПА
в1	ГТВ	П
в2	ПВР	А
в3	ФОР	А, П
в4	БСР	А, ПА
г	СрОСД	П
д	СрИЦФ	П
д1	СрООФ	П
д2	СрОР	П
д3	СрОНФ	П
е	СрРС	П, ПА
е1	СрЗПК	П, ПА
е2	СрУКС	ПА
ж	СрФЗВ	А, П, ПА
ж1	СрФЭВ	А
ж2	СрВЗМ	ПА, П
ж3	СрРПВ	ПА, П
з	СрВИ	П, ПА
з1	СрЗС	П
з2	СрУПВ	П, ПА
з3	СрЗИР	П, ПА
и	СрПОС	А

Таблица 2

Предпочтительные варианты реализации средств обеспечения безопасности

№ п/п	Вид средств	Варианты предпочтительной реализации
а	СрОПО	П, ПА
б	СрАВ	А, П, ПА
б1	СрМПО	П, ПА
б2	СрУАВ	А, ПА

В табл. 1 представлены средства контроля и диагностирования как живучих, так и безопасных систем. которые содержат [4] ПВР - преобразователь выходных реакций, ПРВ - преобразователь рабочих воздействий, ФОР – формирователь ожидаемых реакций, БСР – блок сравнения, ГТВ – генератор тестовых воздействий.

Заключение. Предложенные принципы структурной организации и варианты программной, аппаратной и программно-аппаратной реализации позволяют сделать вывод о возможности построения отказоустойчивых, живучих и безопасных ИВУС на единой системотехнической основе. Базовыми являются структурные элементы контроля, диагностирования, реконфигурации, восстановления процесса вычислений (управления), фиксации и защиты от экстремальных воздействий, коррекции целей функционирования, аварийного выключения. Описание таких элементов приводится в [4,6,7]. Конкретная архитектурная (программно-аппаратная) реализация зависит от требований к системе и выбирается с учетом затрат, надежностных и скоростных характеристик этих элементов.

ЛИТЕРАТУРА

1. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К.: Наукова думка, 1990. – 284 с.
2. Москатов Г.К. Безопасность автоматизированных комплексов. – М.: Машиностроение, 1989. – 232 с.
3. Волик Б.Г. О концепциях техногенной безопасности // Автоматика и телемеханика. – 1998. – №2. – С. 165 - 170.
4. Харченко В.С. Структурная организация отказоустойчивых и живучих систем летательных комплексов. – МОУ, 1992. – 240 с.
5. Росляков Д.Ч., Терехов И.А. Отказоустойчивая технология фирмы «Секвойя» // Электронное моделирование. – 1997. – №6. – С. 69 - 79.
6. Харченко В.С., Лысенко И.В., Мельников В.А. Оценка и обеспечение живучести информационных и управляющих систем технических комплексов критического использования // Зарубежная радиоэлектроника. – 1996. – №1. – С. 64 - 79.
7. Харченко В.С., Марков П.Е. Живучесть и безопасность систем управления летательных аппаратов и комплексов. – МОУ, 1994. – 91 с.

Поступила в редколлегию 13.11.2000