УДК 629.735.06

Воробьев В. М., д-р техн. наук,
Захарченко В. А., канд. техн. наук,
Енчев С. В.,
Березовский Б. Н.,
Кондратенко С. В.

ФОРМИРОВАНИЕ АЛГОРИТМА РЕАЛИЗАЦИИ ОТКАЗОУСТОЙЧИВОСТИ АВИОНИКИ ВЫСОКОЙ СТЕПЕНИ ЦЕЛОСТНОСТИ И ГОТОВНОСТИ

Аэрокосмический институт Национального авиационного универсистета

Рассматриваются вопросы формирования подходов к выработке алгоритма, обеспечивающего реализацию отказоустойчивой авионики перспективных воздушных судов. Сформированы требования со стороны обеспечения заданных уровней безопасности полетов, сочетающихся с поиском компромисса по экономическим критериям (стоимостью владения и минимумом эксплуатационных затрат). Раскрыты понятия отказоустойчивости авионики, функциональной целостности и пригодности функции; обсуждены вопросы их конструкции и техники реализации.

Отказоустойчивость как новое свойство авионики

Отказоустойчивость – продукт синергетического характера, ставший реальностью благодаря новым концепциям создания и внедрения в авионику интегральной модульной авиационной электроники IMA, начиная с 2000 года.

Отказоустойчивостью называется способность авионики (в общем случае оборудования) продолжать работать на каком-то уровне качества с установленными характеристиками после того, как произойдет один или более отказов в аппаратуре и/или программном обеспечении. Термин *«продолжающаяся работа»* охватывает целый диапазон определений от исправного технического состояния (полной работоспособности) всех самолетных функций до различных приемлемых (установленных, чаще называемых – работоспособных) уровней пониженной способности выполнять задание.

Отказ может представлять собой неисправность компонентов аппаратуры или дефект при реализации аппаратуры или программного обеспечения (ПО). Отказ формулируется как отвлеченное потенциальное свойство системы выполнять работу (функцию) и является фундаментальным понятием теории надежности.

Ввиду того, что концепция отказоустойчивости разрабатывалась для удовлетворения требований высокой надежности, то авиалинии – эксплуатанты стали настаивать на проведении технического обслуживания и ремонта (ТОиР) авионики на плановой основе. Философия отказоустойчивости и «продолжающейся работы» выглядит так: если в отказоустойчивой авионике отказывают модуль или функция, то система автоматически нейтрализует неисправность, реконфигурирует структуру и *продолжает работать* до планового ТО, когда неисправности будут устранены.

Алгоритм восстановления отказоустойчивости обеспечивается протеканием трех процессов:

– отказ должен быть идентифицирован (определен);

– отказавшие элементы (модуль или функция) должны быть определены и изолированы (локализованы);

– ресурсы перестраиваются и реконфигурируют, чтобы устранить остаточные явления на работу системы.

Для режима «продолжающейся работы» авионики необходимо иметь резер-

вирование ресурсов или иерархию задач, приносимых в жертву. Кроме того необходимо иметь ряд механизмов: контроля, переключения, восстановления, изоляции контроля и функции, предоставления путей реконфигурации. Так как реализация отказоустойчивости осуществляется с использованием современных технологий, т. е. процесс связан с усложнением структуры, то следует ожидать *уменьшение времени до первого отказа*.

Необходимо ответить на вопрос: способно ли новое свойство противостоять затратам на создание? Очевидно, что максимальный эффект от отказоустойчивости следует ожидать, если она закладывается на этапе проектирования.

Постановка задачи

Схемы применения отказоустойчивости авионики.

Существуют два подхода к реализации отказоустойчивых функций и определения их уровней.

1. Необходимо ответить на вопрос сертификации: как создать существенную *целостность работы*, чтобы по критичным для полета функциям обеспечить безопасность полета?

2. Как обеспечить достаточную пригодность авионики для получения экономических выгод от проведенных ТО в плановые сроки?

Эти задачи разные по целям и по реализации отказоустойчивости конструкции.

Совокупность требований к *функциям авионики* должна устанавливать, когда это необходимо, целесообразность и желательность отказоустойчивости и уровень, до которого она должна быть реализована. В этом случае необходимо установить *допустимые режимы деградирования характеристик*, которые ведут к неисправности функций, а также определить *временной интервал* гарантированной изоляции отказа *до достижения* неисправности функции.

Требования к функциям высокой целостности

Наиболее важными требованиями к функциям высокой целостности их характеристик являются следующие факторы.

1. Ни один единичный отказ не должен приводить к функциональной неисправности и создавать потенциальную опасность. Для аппаратуры системы это относится ко всему оборудованию: датчикам, источникам данных, вычислителям, исполнительным приводам, индикаторам.

Для ПО это относится к потенциальным дефектам в программном обеспечении, которое реализует функции.

2. Контроль должен охватить все контуры, чтобы ни одна опасность не могла избежать обнаружения. Устройство контроля не может быть подвержено отказу. Несовместимость неисправности, ее обнаружения и реконфигурации надежности системы контроля.

3. Последовательность многочисленных отказов исследуется аналитически для установления того, что она (последовательность отказов) является событием маловероятным. Это исследование включает в себя: рассмотрение частоты отказов, зоны отказов, времени воздействия отказа (время считается с момента подтвержденного последнего работоспособного состояния).

4. Выполнение критичных функций для полета оговорено стандартом → вероятность полного функционального отказа представляет собой чрезвычайно маловероятное событие.

5. Ответственность за продолжение безопасной работы, т. е. то, что требуемая целостность достигнута, обеспечивается конкретной системой. Уверенность в этом осуществляется *верификационным тестированием* для установления соответствия требованиям в диапазоне ожидаемых рабочих условий и внешних воздействий.

Требования к пригодности функций

Для не столь критичных для безопасности полетов систем их структуры могут выполняться не по принципу *высокой степени целостности*, а *высокой степени готовности*, тогда главенствующим критерием является возможность получения *экономических выгод*. На реализующую конструкцию влияет набор факторов.

Высокая степень готовности закладывается в конструкцию, чтобы «выдержать» многочисленные неисправности и реализовать режим «продолжающейся работы». В этом случае допускается *один отказ*, делающий функцию неисправной или наличие нескольких (последовательность) необнаруженных отказов, что такие события чрезвычайно маловероятны.

Реализация осуществляется по *экономическому критерию* – компромиссу между стоимостью приобретения и экономией на ТО. Для реализации функции степени готовности устанавливаются:

– желаемая продолжительность службы;

– приемлемый уровень деградации характеристик (формулирование понятия отказа).

Обсуждение конструкции

Отказоустойчивость достигается множеством аппаратных и/или программных технических решений.

$$O = f(A, ПО, A \cap ПО),$$

$$O = \{A, ПО, A \cap ПО\},$$

где O – отказоустойчивость;

A – аппаратурная отказоустойчивость;

$ПО$ – отказоустойчивость программного обеспечения;

$A \cap ПО$ – отказоустойчивость аппаратуры и программного обеспечения.

Основной подход для обеспечения аппаратурной отказоустойчивости – контроль корректности входных и выходных сигналов и множество процессоров (одного и того же или разных уровней)

$$O_{АП} = f(КК_{вх|вых}, \{П_i\}),$$

где $O_{АП}$ – отказоустойчивость аппаратуры;

$КК_{вх|вых}$ – контроль корректности входных и выходных сигналов;

$\{П_i\}$ – множество процессоров одного или различных уровней (типов).

Для *программного обеспечения* отказоустойчивости возможно использование различных, одних и тех же функций, способов кодирования и сравнения / голосования выходной информации

$$O_{ПО} = f(\{КД\}, \{И_{вых}\});$$

$$O_{ПО} = \{КД, И_{вых}\},$$

где $O_{ПО}$ – отказоустойчивость ПО;

$КД$ – различные виды кодирования;

$И_{вых}$ – выходная информация сравнения / голосования.

Проектирование отказоустойчивых функций должно управляться набором технических требований, устанавливающих цели *целостности и готовности*, аналогично рабочим характеристикам.

Сертификация отказоустойчивости характеризуется рядом параметров, в зависимости от природы функций.

1. Приемлемая работа после отказа должна быть определена для любого режима. Фактически это означает, что деградировавшие характеристики (репрезентативные параметры) находятся на уровне (или лучше, т.е. выше) допуска системы по режимам

$$|x_i| \le |x_{доп}|,$$

где x_i – текущее фактическое значение параметра, для i-го режима.

$x_{доп}$ – значение параметра по стандарту.

В вероятностном плане техническое состояние системы $S_ф$ должно находиться в области множества состояний стандарта $S_{ст}$: $\{S_ф\} \subseteq \{S_{ст}\}$.

2. Функциональная неисправность требует определения и установки предельно-минимального уровня в отношении выполнения функции. Это означает формулирование отказа, как дискретного

случайного события на множестве состояний «продолжающейся работы» авионики. Успешная работа происходит при значениях

$$|x_{iф}| \le |x_{доп}|.$$

Для различных режимов работы функционирование авионики может осуществляться с потерей целостности («жертвенность функции»), т.е. могут существовать несколько пороговых значений параметров, характеризующих приемлемые уровни работы (или качество функционирования).

3. Должен быть определен допустимый риск функциональной неисправности из-за одного отказа.

$$\{S_{i\ од.отк}\} \subset \{S_{ст\ i}\}.$$

4. Должно быть определено время реакции системы на обнаружение отказа $t_{оо}$ (процесс идентификации), определение рабочей зоны и локализацию отказа $t_{ло}$ и перестройку структуры (реконфигурацию) $t_р$, таким образом

$$t_{\Sigma} = t_{оо} + t_{ло} + t_р; \qquad t_{\Sigma} \le t_{ст}.$$

5. Должен быть определен допустимый риск функциональной неисправности вследствие комбинации или последовательности отказов

$$t_{\Sigma\ сов} \le t_{ст}.$$

Вероятность возникновения совокупности отказов должна быть чрезвычайно малой.

$$P(t_{\Sigma\ сов}) \le P(t_{ст}).$$

6. Должно быть определено время, когда функция должна очиститься от отказа и подключена для выполнения функции

$$t_{вос} \le t_{вос.ст}.$$

Конструкция высокой степени целостности

В режиме функционирования авионики на ЖЦ ее ресурсы истощаются $(R_a \to 0)$, т .е. запас целостности убывает $(Ц_a \to 0)$. Конструирование ресурсов должно осуществляться таким образом, чтобы обеспечивался режим «продолжающейся работы» при наличии отказа. Это означает, что должны быть заложены в конструкцию авионики некоторые виды и формы функционального резерва. Необходимо выдержать любой единичный отказ и возможно все (или большинство) функциональных возможностей должны быть сохранены

$$ФВ \to 1; \quad Ц_a \to 1.$$

$$lim\, R_a \to 0$$

Отбрасывание жертвенных долей функции – это уже не функция высокой степени целостности, но оно возможно при реализации в силу экономической целесообразности (функция высокой степени готовности).

$$ФВ \to 1; \quad 0 < Ц_a < 1.$$

$$lim\, R_a \to 0$$

К конструкции высокой степени целостности предъявляется целый ряд специфических требований: изоляции ресурсов; охват периодическим контролем всех опасных неисправностей; реализация функций высокой степени целостности должна отвечать требованиям к рабочим характеристикам и спецификациям, что дефекты маловероятны; информирование экипажа о риске функциональной неисправности; проведение ТО на плановой основе до отказа функции по видимой информации для бригады ТО; объединение функций с различными уровнями целостности в одну систему с различным подходом при ТО, но процесс управления при разделении функций должен осуществляться ресурсами авионики самой высокой целостности.

Рассмотрим подробнее процесс обеспечения отказоустойчивости аппаратуры высокой степени целостности.

1. При наличии единичного отказа все (или большинство) функциональных возможностей должны быть сохранены, а авионика должна находиться в режиме «продолжающейся работы». Жертвенность ряда функций может быть рассмотрена и обоснована экономическими выгодами.

2. Различные компоненты резервирования, фактически представляющие ресурсы, должны быть изолированы и работать автономно. Контроль функции должен работать независимо от самой функции, чтобы любое событие (нормальное, ненормальное, ошибочное) не могли создать общий эффект в контроле или в самой функции.

3. Высокая эффективность контроля объясняется необходимостью помимо охвата рабочих характеристик и определения всех опасных последствий. Процесс периодического контролирования должен гарантировать ненормальные явления и обеспечить с уверенностью связь с механизмами реконфигурации.

4. Реализация функций высокой целостности должна отвечать требованиям рабочих характеристик и спецификациям конструкции (авионики) по критерию отказоустойчивости с гарантией, что дефекты конструкции маловероятны. Другими словами это означает, что конструкция (аппаратура) должна выполнять закрепленную функцию и быть свободной от любой незакрепленной функции. Это подтверждение называется *корректностью* и выполняется через комбинацию *тестов* и *анализ работы авионики* (обычно инженерный анализ путей успешного функционирования).

5. По мере расходования ресурсов $P_a \downarrow$ и целостности $Ц \downarrow$ авионики, критичной в обеспечении безопасности полетов, экипаж должен быть своевременно проинформирован о том, что при выполнении режима «продолжающейся работы» риск функциональной неисправности возрастает $П \uparrow$. Исходя из этого инициируются действия экипажа согласно нормативно-технической документации (РЛЭ, Регламента ТО и др.) или действий персонала ТОиР.

6. Какой объем информации должен быть видимым для экипажа и бригады ТОиР – это отдельный вопрос, имеющий конкретное приложение. В частности, длительное предупреждение о возможном переходе на другой режим работы (например, ручное управление) авионики теряет свою остроту, т. е. эффективность восприятия и реализации.

7. При работе с накапливающимися неисправностями авионика деградирует и должно быть определено время процесса восстановления целостности, желательно при плановом ТОиР. В то же время эта информация должна быть невидимой экипажу и прозрачной для состава ТОиР. Таким образом, сохраняется история авионики и в конструкции предусмотрена возможность сделать запрос.

8. Так как вопрос требуемого уровня целостности авионики остается открытым, то очевидно функциональные системы будут иметь различную целостность $Ц_{ФС} = var$. При интеграции функций эти ресурсы объединяются, а обслуживание должно проводиться по принципу самого высокого уровня целостности. Этот эффект достигается за счет *разделения ресурсов и функций*, в соответствии с их уровнями

$$R_\Sigma = \sum_{i=1}^{n} R_i ;$$

$$Ц_\Sigma = \sum_{i=1}^{n} Ц_i ,$$

где $R_\Sigma, Ц_\Sigma$ – соответственно суммарные ресурсы и целостность; $R_i, Ц_i$ – соответственно ресурсы и целостность i-ой системы авионики.

Их разделение предполагает их независимость и изолированность, т .е. принцип автономности

$$R_1 \cup R_2 \cup ... \cup R_n = \bigcup_{i=1}^{n} R_i ;$$

$$Ц_1 \cup Ц_2 \cup ... \cup Ц_n = \bigcup_{i=1}^{n} Ц_i .$$

При разделении функций *управление* ими (как процесс) осуществляется ресурсами самой высокой целостности.

Конструкция аппаратуры высокой степени готовности

Достижение в реализации конструкции авионики высокой степени готовнос-

ти осуществляется, как и для конструкции высокой степени целостности, через уникальные факторы, которые выступают в виде ограничений на конструкцию ресурсов для выполнения рабочих функций. Так как аппаратура (авионика) высокой степени готовности не всегда значима в вопросах обеспечения безопасности полетов, то действенным способом повышения готовности является *резервирование*. Роль резервирования существенна, но если функция не используется в критичных случаях полета, то вполне возможна «жертвенность» функции или ее частей. Вполне возможно отбрасывание задачи. Например, система запуска авиадвигателя необходима на земле, а аварийный запуск в воздухе, обеспечивается функционально-минимальной структурой и использованием иных принципов раскрутки ротора (принцип авторотации). Подобные явления с системами управления механизацией крыла, когда при отказах посадка может осуществляться при неполно выпущенной механизации или даже при убранной конфигурации. С позиции безопасности полетов меняются риски благополучной посадки ВС, снижаются вероятностные оценки исхода полета.

Так как ресурсы теряются из-за неисправности, то функциональные возможности снижаются $ФВ\downarrow$, а остающиеся ресурсы сосредотачиваются на наиболее целесообразном направлении.

В случае, когда неисправность функции неопасна, то экстраординарные меры по изоляции резервных ресурсов не нужны, однако на практике контроль изолируется от контролируемой функции.

Хотя требование повышения эффективности контроля актуально для повышения готовности, однако наличие минимальных ошибок охвата контролем (с учетом новых возможностей от применения новой элементной базы IMA), а также неопределенные неисправности от недостаточной чувствительности компонент вносят свою «долю» в достигнутые результаты. Это в свою очередь объясняется тем, что отдельные компоненты авионики имеют на уровне функционально-минимальных структур недостаточную надежность. Применение структурного резервирования увеличивает сложность структур, существенно увеличивает стоимость оборудования, массу и габариты, т.к. первоочередной задачей является выполнение требований безопасности полетов.

Вследствие сказанного можно утверждать, что *улучшенная функциональная готовность является основной целью, а единственной стратегией реализации является максимизация значения времени между отказами*. При этом должно выдерживаться выполнение следующих соображений:

– реализация авионики высокой степени готовности должна осуществляться по принципу *выдерживания минимальной сложности* изделия при одновременном увеличении путей успешного функционирования;

– успешное решение первого условия позволит обеспечить компромисс между частотой появления неисправностей и уровнем резервирования;

– существенное повышения надежности отдельных функциональных систем, реализованных на базе недостаточно надежных элементов, может быть обеспечена только за счет резервирования (структурного, параметрического, режимного, информационного, функционального, эргатического и др.) [2].

Технические средства реализации отказоустойчивости авионики

Повышение отказоустойчивости и собственно реализация рабочих характеристик авионики обеспечиваются аппаратными и программными ресурсами, которые кроме того используются для дополнения друг друга: для обнаружения отказа, его идентификации, локализации и реконфигурации структуры. Рассмотрим технические возможности и средства реализации аппаратных и программных ресурсов.

А. Технические средства аппаратной реализации отказоустойчивости

Аппаратная отказоустойчивость обеспечивается различными средствами, а модульная интегральная конструкция IMA – определяет методы. Рассмотрим последовательно вопросы входного и выходного контроля, контролирования вычислительных характеристик, резервирования, неодинакового контролирования аппаратуры, реконфигурации и вырождения последовательности к отказам.

1. *Входной контроль*, если он вообще когда-либо используется в критических ситуациях полета для единственного источника информации, выполняет роль проверки на *приемлемость*, то есть сигнал направляется в канал вычисления после проверки попадания в предписанные ограничения:

$И \to В$, если $|x_c| \le |x_{доп}|$,

где $И$ – информация; $В$ – вычислитель.

При двух источниках информации сигналы сравниваются и при превышении отклонений от ограничений информация отвергается и используется ее предыдущее значение

$x_i - x_{i-1} = \Delta_i$, при $|\Delta_i| > \Delta_{доп} \Rightarrow$ отвергается и используется предыдущее значение x_{i-1}.

При трех и более источниках информация «голосуется» (принцип мажоритарности) и принимается значение большинства.

Если неисправная информация продолжает поступать, входной источник признается отказавшим и берется альтернативный.

2. *Контролирование вычислительных характеристик* осуществляется через сторожевые таймеры для контроля времени выполнения. Если значение времени превышает ограничение, то процессор снимается для диагностического тестирования (ДТ). При соответствии требованиям ДТ он вновь подключается к системе. Могут использоваться для вариантов ПО с пониженным временем исполнения (для сравнения). Алгоритм, таким образом, следующий:

$t_i - t_{ст} \le \Delta t \to$ система работоспособна;

$t_i - t_{ст} \ge \Delta t \to$ процессор (П) отключается и происходит ДТ, но при соответствии $\to$ авионике.

3. *Выходной контроль*, как и для единственного датчика входной информации, осуществляется для проверки на приемлемость. Для двух процессоров выходная информация не соответствует друг другу оба процессора отключаются $\to$ проходят ДТ для поиска отказавшего, исправный подключается вновь.

Для нескольких процессоров выходная информация «голосуется» и значение большинства пропускается к системе. Неисправные процессоры снимаются для проверки ДТ.

– $И_{вых1} \to П$, если $|x_c| \le |x_{доп}|$;

– $|x_{1вых} - x_{2вых}| = \Delta_{вых}$, при $\Delta_{вых} > \Delta_{доп} \Rightarrow$ $П_1$ и $П_2$ $\to$ ДТ: $ДТ_1/ДТ_2 \Rightarrow$ подключение к системе;

– $n_{ист.инф} \ge 3$; $x_{1вых}$, $x_{2вых}$, $x_{3вых}$, … $\Rightarrow$ $x_{1вых} = x_{2вых} = x_{3вых} \Rightarrow$ подключение к системе, также как и при двух любых.

4. *Выбор среднего значения* предполагает для трех и более датчиков информации ($n \ge 3$) отбрасывание максимального и минимального значений, а оставшийся сигнал проходит проверку на преемственность, т.е. значения датчика должно быть в поле допуска:

$n \ge 3$; $x_{max}, x_{min} \to$ отвергаются, $x_i \Rightarrow П = x_{доп}$.

5. *Разделение* функций используется для ограничения распространения отказа по системе и, следовательно, для снижения вероятности возникновения неисправности системы. Разделение минимизирует усилия по контролю и время для выполнения модификации аппаратуры и/или ПО.

6. *Голосование по множеству информации* используется для систем трижды и более раз резервированных $(n \geq 3)$, что позволяет допускать единичный отказ выходной информации. Если все резервированные выходы просуммированы и каждый имеет ограниченное влияние на общий эффект, то система всегда будет иметь правильное значение, независимо от отказа канала. Как и в технике среднего значения могут иметь место определенные классы двух отказов.

$$E(t) = \frac{E_1 + E_2 + \ldots + E_i + \ldots + E_n}{n} \leq E_{cm}(t).$$

7. *Резервирование*, в принципе, является единственным способом и методом повышения эффективности сложных систем. Различают много видов резервирования, когда создание потенциальной базы повышения надежности возможно через соответствующее введение избыточных ресурсов относительно функционально-минимальной структуры (ФМС) [2]. Аппаратура выходит из строя из-за неисправностей в ней в процессе функционирования, более широко – в процессе эксплуатации.

По мере добавления ресурсов к ФМС сложность возрастает, частота отказов также увеличивается:

– для функций высокой степени целостности (интеграции) это добавляет существенную часть стоимости предоставления сервиса;

– для функций высокой степени готовности конструкция обосновывается за счет поиска компромисса между возросшей стоимости резервированной системы $C_{р.п}$ и стоимости потерь из-за общих потерь при отказе функции $C_{н.р.п}$:

$$E = C_{р.п} - C_{н.р.п}.$$

Известны методы и модели оценки предсказания различных вариантов структур по выгодам с определенной надежностью при добавлении сложности [3,4]. В этом случае учитываются следующие соображения.

Использование резервирования в контурах энергетических каналов, а также в информационно-управляющих структурах должно сопровождаться *их изоляцией*. Выгоды от применения резервирования не могут быть реализованы, если ошибка или неисправность будет влиять существенно на общий эффект или другие контуры. Аппаратура или система будет вести непредсказуемо, если контроль не выявит такие события.

Для «замены» отказавшего датчика информации в отказоустойчивой авионике может применяться «*аналитическое резервирование*». В случае отказа датчика алгоритм использует сигналы оставшихся для определения сигнала отказавшего. Вычисленный сигнал обрабатывается как исправная информация в остальной части системы.

Аналогично для энергетических каналов авионики: оставшиеся исправные силовые исполнительные приводы и законы управления (САУ полетом, система управления механизацией крыла, электро- и гидроэнергетические станции) автоматически перестраиваются для компенсации неисправности.

8. *Применение аппаратуры различного (несхожего) типа* рассматривается как вариант реализации отказоустойчивых конструкций авионики и создания защиты от определенных видов дефектов. Однако такие конструкции имеют уникальные достоинства и недостатки.

Особенности реализаций несходной аппаратуры определяют следующие их свойства:

– несходная реализация может явиться *единственным способом* избежать общих отказов по режимам в общих контурах, когда как следствие усугубляются дефектами конструкции;

– отказы легко обнаружить, а потенциальную опасность удается снизить;

– дополнительной особенностью несходных реализаций является *увеличение стоимости разработки* и усилий *по созданию множества контуров и верификации*;

– каждый вариант должен продемонстрировать выполнение всех функций, а также подтвердить собственно *несходство*;

– если функция реализует защиту через наличие несходства, то это несходство должно быть доказано и показано, что не приводит к возникновению ошибок общих режимов.

9. *Контролирование аппаратуры* реализуется по одной из видов трех категорий:

– сравнением двух процессов;

– сравнением параметров относительно установленного порога;

– определением события.

При этом некоторые требования к контролю формируются из следующих соображений:

– каждый вид контроля должен быть согласован с уровнем целостности наблюдаемой функции;

– контроль должен быть защищен от ошибок или продублирован для гарантирования обнаружения неисправности;

– контроль аппаратуры предназначен для специальных контуров, за которыми он наблюдает;

– аппаратура контроля может одновременно наблюдать за характеристиками функции, реализованной программно;

– дополнительно к обнаружению события или превышению значения, контроль должен сообщать о ненормальном положении в конструкции авионики (прерыванием работы обрабатывающих средств; флагом, пассивно запрашиваемым другим процессором; переключением для реконфигурации или объявлением экипажу для принятия решения).

10. *Реконфигурация* структуры авионики представляет процесс или акт изменения ресурсов оборудования. Такими схемами реконфигурации аппаратуры являются: схемы «голосования», импульсы сбора, прерывания и переключатели управляющих данных. При реализации в аппаратуре эти схемы реконфигурации обычно предназначены для замены отдельных специальных параметров или путей прохождения данных. Таким образом, обеспечивается компромисс по критерию сложности контуров.

После реконфигурации аппаратура работает при пониженной надежности $R\downarrow$, целостности $Ц\downarrow$, ресурсах $P\downarrow$. Для систем с одним реконфигурируемым отказом система не может вторично выдержать такой отказ. Необходимо решить вопрос возвращения системы к исходному состоянию. При этом должен быть достигнут баланс между восстановлением от случайных отказов и восстановлением защиты от неисправностей, требующих специальных мер быть обнаруженными.

11. *Восстановление отказоустойчивости авионики к отказам* представляет собой событие, которое с некоторым доверительным уровнем доказывает, что компонент авионики (аппаратуры) не имеет отказа. Математическое предсказание вероятности представляет оценку с момента последнего восстановления отказоустойчивости. Если гарантирующего метода нет, что компонент не содержит отказа, то время пребывания в состоянии отказа растет до бесконечности $t_{отк.} \to \infty$ и вероятность появления неисправности приближается к единице $Q_{отк}(t) \to 1$ $(Q_{отк}(t) = 1 - P(t))$.

Процесс восстановления отказоустойчивости может быть включен в конструкцию авионики, чтобы иным способом определить *скрытые отказы*, при этом ограничивая время пребывания в состоянии отказа и, таким образом, снижая вероятность опасности:

$$\Delta t = t_{посл.восст.} - t_{тек.} \downarrow;\ Q_{отк}(t)\downarrow.$$

Восстановление отказоустойчивости может быть выполнено:

– самоконтролем конструкции авионики $(t_{сам})$;

– периодическим профилактическим ТО $(t_{ТО})$;

– контролем при ТО или первоначальном производственном контроле $(t_{ПК})$.

Каждое из этих решений налагает ограничение на время нахождения в состоянии отказа, при этом обычно: $t_{сам} << t_{ТО} < t_{ПК}$.

Все элементы аппаратуры должны иметь установленное время в состоянии отказа, чтобы вычислить вероятность опасности.

В. Технические решения, реализуемые программным обеспечением современной авионики

Так как ПО не изнашивается и не имеет зависимости частоты отказов от времени эксплуатации, то основные дефекты могут быть «заложены» при проектировании. Нарастающие сложности систем имеют тенденцию переносить (трансформировать) и на сложность ПО, что повышает потенциальную опасность остаточных дефектов проектирования даже после тщательного верификационного контроля. Это направление – применение методов обеспечения отказоустойчивости ПО и является попыткой нейтрализации дефектов проектирования. Рассматриваются типовые вопросы обеспечения отказоустойчивости ПО: N - вариантного программирования, блоков восстановления, согласованности, обработки особой ситуации, контроля реконфигурации и восстановления реконфигурации.

1. *N-вариантное проектирование* широко используется в технике обеспечения отказоустойчивости ПО. При использовании этого метода для организации отказоустойчивости ПО разрабатываются два или более независимых вариантов ПО для выполнения одной и той же задачи. Реализация вариантов может осуществляться последовательно одним процессором, но обычно в процессе участвует N-процессоров, работающих параллельно. Такая схема реализует дополнительный вариант повышения отказоустойчивости различных типов процессоров. Результаты «голосования» и наиболее вероятное значение передаются системе.

Достоинства и недостатки N-вариантного программирования ПО:

– параллельная обработка информации существенно быстрее;

– метод позволяет избежать общих ошибок через независимую разработку кодов, но степень независимости нужно доказать;

– для реализации высокой эффективности каждый вариант ПО должен быть верифицирован – иначе остаточные ошибки могут быть не редкими;

– стоимость аппаратуры повышается, поэтому N-вариантное программирование используется для функций с самыми высокими требованиями к целостности;

– при N-вариантном программировании, как и при неидентичном резервировании необходимо подтверждать различия программ.

2. *Блоки восстановления* – простейшая форма отказоустойчивого ПО. Результат кодирования подвергается приемлемой проверке. Если результат ошибочен, то осуществляется повтор до получения приемлемого результата. Кроме того могут использоваться другие варианты кодирования. Если результат не приемлем – ПО имеет ошибку. Недостатками блоков восстановления является дополнительное время выполнения и его повтор $\left(t_{\Sigma} = t_{код} + t_{код(повтор)}\right)$, а также снижение целостности приемлемой проверки и необходимость хранения информации для повторного вычисления с целью успешного восстановления.

3. *Согласованность* – представляет собой комбинацию блоков N-вариантного программирования и восстановления [1,2]. Это техническое решение работает по схеме: результат N-вариантного программирования «голосуется»:

– если два или более результата совпадают, то он выдается в систему $\left(P_1 = P_2 \Rightarrow \text{система}\right)$;

– если все результаты различные, то выход каждого варианта последовательно проверяется до получения приемлемого результата;

– если проверка не обеспечивает приемлемого результата, то ПО объявляется неисправным.

N -вариантное программирование широко используется для критичных ситуаций полета, но это не лучший вариант. Единственный вариант, как альтернативный путь был бы предпочтителен, если бы *ресурсы для разработки N – вариантного кода* были использованы к тщательному проектированию и полному подтверждению *одного варианта.*

4. *Обработчик особой ситуации* предназначен в процедуре создания отказоустойчивого ПО для ненормальных условий работы (деление на ноль, вычисление тангенса 90^0 и др.).

5. *Контролирование ПО*, также как функции контроля аппаратуры, приемлемы и в реализации ПО. При разработке программ особую сложность представляют вопросы определения граничных значений и сама целесообразность процедуры проверки.

Контроль ПО должен подтверждать, что программирование выполняется правильно с выдерживанием последовательности и с контролем хронометрирования. Кроме того, необходимы независимые средства, гарантирующие правильность работы центрального вычислительного блока для обеспечения высокой целостности. Реализация представляет комбинацию аппаратно и программно выполненных функций.

Контроль ПО может быть использован для подтверждения правильной работы аппаратных функций. Техника разнообразна:

– возвращение выходной информации на вход и получение сигналов для определения неисправностей по пути передачи данных;

– выполнение периодической диагностики позволяет обеспечить высокие уровни охвата контролем.

6. *Реконфигурация ПО* имеет дело с реконфигурацией функций, т.е. более сложную структуру, чем с использованием аппаратуры. Алгоритм выбора сигнала может использоваться применительно к большому числу параметров, используя для этого *среднее значение* или *весовое голосование для выбора приемлемого значения*. Выравнивание между источниками информации может обеспечить согласование по сдвигу времени или допускам систем.

При управлении сигналами процесс может быть инициирован или приостановлен, программы обработки исключений обеспечивают уникальное программирование или выполняются на специальные события. Возможен повторный запрос данных для очередной попытки выполнения.

7. *Возобновление нечувствительности к отказам* не предполагается, так как ПО не изнашивается и ПО продолжает предоставлять закрепленные функции неограниченно. Однако у ПО имеется тенденция деградировать в процессе модификации или коррекции. Это проявляется в появлении ошибок после модернизации в зонах программы, которые не предполагалось изменять.

Существенное внимание уделяется *верификации* каждого варианта экстраполяции существующего ПО.

8. *Роль контрольно-измерительных устройств и индикаторов* высока, так как отказоустойчивые системы требуют обнаружения и идентификацию очень высокого процента возможных отказов.

Эти требования предусматривают тщательное проектирование встроенных систем контроля (ВСК), в международной транскрипции – BITE и операций, которые выполняются. Создание BITE базируется на результатах анализа «дерева отказов» и/или анализа неисправных режимов и их влияния (FMEA). Рекомендации ARINC 624 «бортовая система технического обслуживания» должны обсуждаться.

Выводы

Концепция внедрения с 2000 года отказоустойчивой авионики на поколениях перспективных ВС ставит целью повышение уровня безопасности полетов с учетом достигнутых новаций:

– применение новой элементной базы авиационной электроники IMA и использования синергетических ее качеств (отказоустойчивость, интеграция и разделение ресурсов, стандартизация и унификация, гибкий кабинный интерфейс и др.);

– спутниковая навигация и радиосвязь и др.

Конструкция авионики должна обеспечивать максимальное использование распределенных ресурсов для уменьшения резервирования до минимума. Такая интеграция снижает стоимость владения через снижение стоимости приобретения, потребности в резервах, массе и объеме авиационного и радиоэлектронного оборудования. Резервирование ресурсов, требуемое для увеличения сроков проведения ТО, зависит от продолжительности увеличенного интервала ТО и статистической вероятности успешно выдержать интервал до полного отказа оборудования. Для комплекта полностью отказоустойчивой авионики интервал времени предупреждения о необходимости ТО для отдельных функций авиационной электроники составляют 15000 часов, все функции авионики продолжают функционировать в течение 200 часов после первого отказа с 99% вероятностью успеха.

Авиалинии желают иметь стоимостную эффективность при внедрении новых технологий, включающую в себя *полную стоимость жизненного цикла* и *выгоды альтернативных технологий*. При этом авиалинии пришли к следующим выводам:

– полная отказоустойчивость авионики, более достижимая на базе IMA, чем в традиционном исполнении, может оказаться экономически невыгодной;

– частичное внедрение отказоустойчивости может быть достигнуто, если она закладывается на этапе проектирования.

Список литературы

1. *ARINC 651*. Руководство по проектированию интегральной модульной авиационной электроники: Пер. с англ. США. – Мериланд, 1991. – 278 с.

2. *ДСТУ 3589-97*. Системи та комплекси авіаційного обладнання. Надійність та експлуатація. Терміни та визначення. – К.: Держстандарт України, 1998. –28 с.

3. *Буловский П. И. Зайденберг М. Г.* Надежность приборов систем управления. Справочное пособие. – Л.: Машиностроение, 1975 . – 328 с.

4. *Воробьев В. М., Захарченко В. А., Вашку Ж. О., Воробьев А. В.* Системная эффективность комплекса «экипаж – ВС – среда» // Кибернетика и вычислительная техника: Сб. науч. трудов. – К.: ИК им. В.М. Глушкова НАНУ, 2000. – Вып.126. – С.48-76.

5. *Воробйов В. М., Захарченко В. П., Кічігін А. А.* Обґрунтування методу моделювання процесу функціонування електроенергетичного комплексу повітряного літака. – К.: Автошляховик України, 2004. – №7. – С.65-69.