ТДА - лекция 9 - 01.11.2010.docx

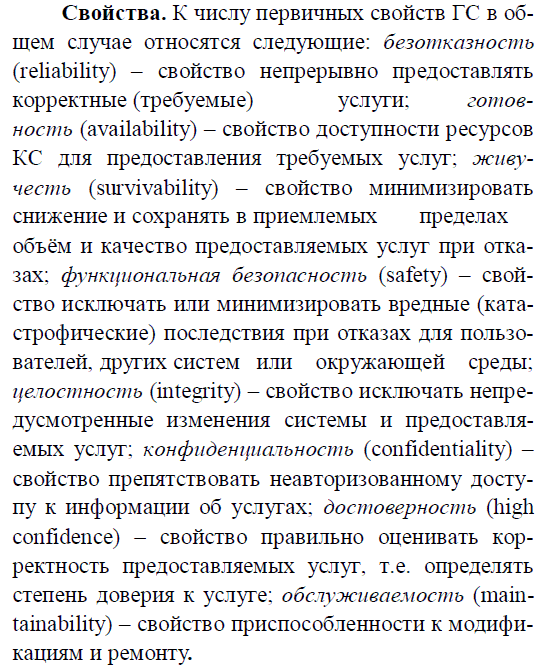
Тема: **Показатели избыточности и контролепригодности**

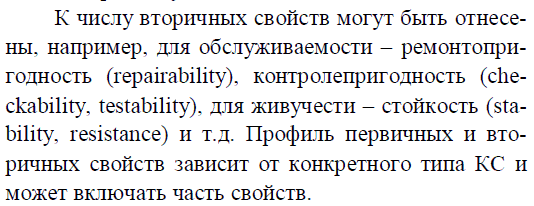
**Цифровых Модулей авионики**

**1. Отказоустойчивость и отказобезопасность авионики**

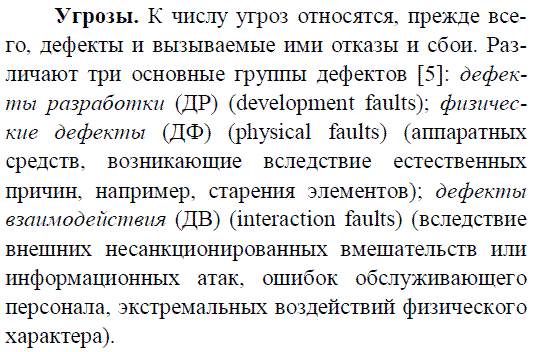
Сложившийся сегодня подход к проектированию авионики отражает общую тенденцию технического прогресса, связанную с интеграцией современной науки. К техническим проектам (и к авионике в первую очередь) предъявляется **требование высокой гарантоспособности**.

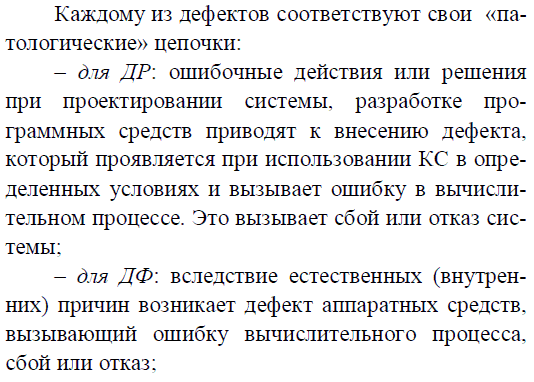
Сам термин “гарантоспособность” появился недавно, понимается как системная и функциональная надёжность и интегрирует в себе такие понятия (или такие первичные свойства) как

****

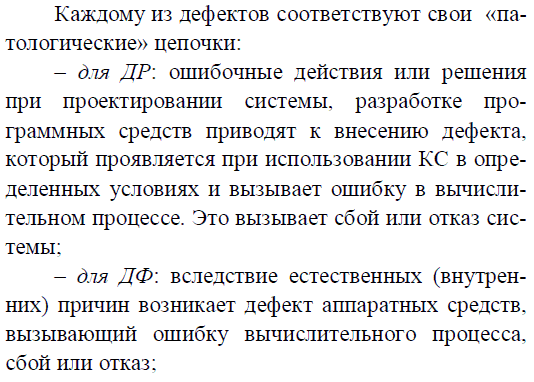
****

**КС – компьютерная сеть (БКС – бортовая КС)**

****

****

**Дефекты разработки**



С целью решению этой проблемы международными авиационными организациями разработаны и постоянно совершенствуются нормативные документы, устанавливающие определённый порядок проектирования, разработки, испытаний, сопровождения и документирования программного обеспечения авионики.

В частности, ассоциацией **RTCA[[1]](#footnote-2)** разработаны (и поддерживаются) требования к процессу проектирования программного обеспечения авионики и тщательности его проверки в зависимости от его уровня критичности по безопасности, изложенные в стандарте **DO-178C** (последняя версия документа, 2005 г.) под названием **Software Consideration in Airborne Systems and Equipment Certification** (Требования к программному обеспечению бортовой аппаратуры при сертификации оборудования).

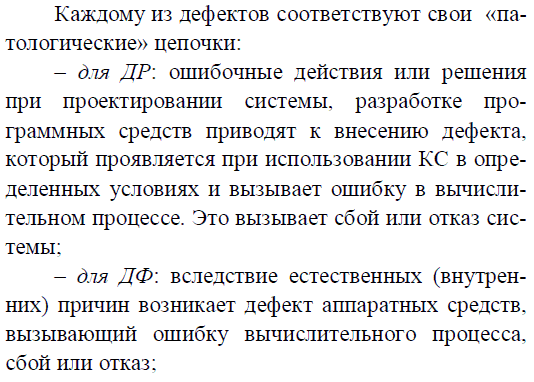
Проблемы обеспечения множества полетных функций, критичных для безопасности полета, стоят и перед разработчиками отказоустойчивого бортового оборудования. Эти проблемы возникают из-за того, что выполнение многих полётные функции все больше и больше подвергается неблагоприятному влиянию ***ошибок в конструкции аппаратуры***, которые достаточно трудно устранить из-за возрастающей сложности электронного оборудования.

Чтобы противостоять этой осознаваемой эскалации риска, стало необходимым более постоянным и контролируемым образом обеспечить возможность устранения конструктивных ошибок аппаратуры во время процессов конструирования и сертификации. Этой цели служит стандарт **DO-254** **- Design Assurance Guidance for Airborne Electronic Hardware** (Руководство гарантии проектирования бортовых электронных аппаратных средств).

Стандарт помогает уменьшить вероятность необнаруженных ошибок конструирования применением проверенных технологических методов, определенных в ходе предыдущих разработок, и аналогично DO-178С, устанавливает пять категорий гарантии безопасности разрабатываемой аппаратуры, соответствующие пяти уровня безопасности программного обеспечения.

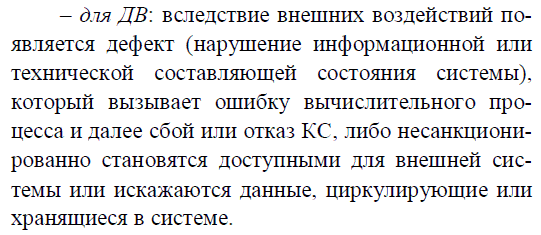
Руководящие положения стандартов **DO-178C** и **DO-254** представляют собой **консенсус авиационного сообщества** и являются **собранием наилучших практических промышленных данных** по гарантии разработки “безопасного” программного обеспечения и конструирования “безопасной” бортовой электронной аппаратуры, **используемых для реализации функций авионики высоких уровней безопасности.**

**Физические дефекты**

****

**Все возможные внутренние причины – деградационные процессы, приводящие к отказам и сбоям, изучены Вами на 3-ем курсе в дисциплине “Надёжность систем авионики”.**

**Внешние воздействия**

****

В разработанных МАК АП особо отмечена необходимость оценки безотказности БРЭО при воздействиях HIRF, так как к моменту введения в действие АП в американских и европейских правилах это требование уже существовало, а в ЕНЛГС его не было. Оценка безотказности аппаратуры при воздействиях HIRF связана с особой чувствительностью не­защищенных цифровых электронных схем, входящих в состав БРЭО, к этому типу внешних воздействий и возникающим вследствие этого отказам, влияющим на безопасность эксплуа­тации самолетов

Поэтому в современных условиях особенно актуальными являются задачи выбора функционально-структурного облика авионики и разработки эффективных средств, позво­ляющих оценить ее отказоустойчивость в условиях вероятного воздействия HIRF.

За последнее время в связи с быстрым разви­тием техники электромагнитная обстановка вокруг летящего самолета усложнилась [47] – увеличилось количество спутниковых систем, введены в действие наземные радиоэлектрон­ные станции широкого диапазона, быстро развиваются радиорелейные и тропосферные ли­нии связи системы Интернет и корпоративных информационных систем, сотовых и пейджерских систем связи, местных теле- и радиостанций. Повышенное высокочастотное электромагнитное излучение, создаваемое также и отказывающими коммерческими информаци­онными системами, теле- и радиостанциями, тоже может привести к функциональным отка­зам радиоэлектронного оборудования летательных аппаратов [48]. Отмечается [1], что на возникновение отказных состояний цифровой аппаратуры влияет не только мощность и частота микроволнового пакета, но и количество импульсов в этом пакете, так как современная цифровая аппаратура способна монотонно увеличивать остаток запасенной энергии до тех пор, пока он не превысит критическое значение и не возникнет отказ.

DOT/FAA/AR-99/50 Управление авиации исследований

Вашингтон, DC 20591

Высокой интенсивности излучаемого поля (HIRF)

High intensity of a radiated field (HIRF)

**Анализ рисков от** **HIRF**

Поля высокой интенсивности излучения/ Поля излучения высокой

интенсивности

**Таким образом, одной из основных проблем построения комплексов авионики остается задача обеспечения их продолжительного функционирования.**

**Эта задача имеет три взаимосвязанные составляющих:**

* **надежность,**
* **готовность и**
* **обслуживаемость.**

Все эти три составляющие предполагают, в первую очередь, принятие мер по устранению неисправностей системы, порождаемых отказами и сбоями в ее работе.

Для решения задачи максимально используются все методы и средства, выработанные наукой и практикой для достижения высокого уровня надёжности, отказоустойчивости и живучести бортовых вычислительных систем в составе авионики.

**Так, повышение надежности** основано на принципе предотвращения неисправностей **путем снижения интенсивности отказов и сбоев** за счет

* **применения электронных схем и компонентов с высокой и сверхвысокой степенью интеграции,**
* снижения уровня помех,
* облегченных электрических, тепловых и механических режимов работы элементов, а также
* за счет совершенствования методов сборки аппаратуры.

**Устойчивость к отказам (Fault Tolerance).** Отказоустойчивые системы имеют в своем составе избыточную аппаратуру для всех функциональных блоков, включая процессоры, источники питания, подсистемы ввода/вывода и т.д. Если соответствующий функциональный блок неправильно функционирует, всегда имеется горячий резерв. В наиболее продвинутых отказоустойчивых системах избыточные аппаратные средства можно использовать для распараллеливания обычных работ. Время восстановления после обнаружения неисправности для переключения отказавших компонентов авионики на избыточные существенно ограничено.

**Модульный принцип построения вычислительной системы**, где каждый модуль охвачен полным аппаратным контролем, обеспечивающим высокую достоверность получаемых результатов. Отключение неисправного модуля в такой системе производится автоматически по срабатыванию встроенного апаратного контроля контроля.

Существуют два типа резервирования в структуре авионики: "горячее" и "холодное". При использовании "горячего" резервирования процесс переключения с основного устройства на резервное происходит мгновенно. При использовании "холодного" резервирования – с некоторой временной задержкой, во время которой резервному устройству передаются необходимые для продолжения работы данные.

**Специальное программное обеспечение является существенной частью систем высокой готовности.** При ***обнаружении неисправности системы*** оно обеспечивает управление конфигурацией аппаратных средств и программного обеспечения, а также в случае необходимости процедурами начальной установки, и перестраивает где надо структуры данных.

… О сложностях создания программ управления комплексом авионики можно понять не из аналитического анализа, а прочитать замечательные записки академика Е.А.Федосова, генерального директора одного из ведущих научных центров Российской Федерации, знаменитого ГосНИИАС (Государственный научно-исследо-вательский институт авиационных систем), который уже более полувека является головным в области создания комплексов авионики.

“… Нам пришлось создать на стенде достаточно большой объем программ, провести тысячи «полетов», и прежде чем Ту-160 был принят на вооружение, мы полностью отрабатывали двенадцать или четырнадцать версий программного обеспечения систем управления его оружием. При этом каждая редакция версии была доведена до логического конца, имела законченный вид, но поступали новые вводные, мы сталкивались с какими-то неизвестными доселе явлениями, и приходилось снова и снова менять алгоритмы. К тому же мы выгребали сотни и тысячи ошибок из каждой версии программы, пока не доводили ее до блеска…”.

“… Наряду с отладкой программ мы также отрабатывали методику оценки качества программного обеспечения, так называемую его верификацию. Это тоже очень сложная задача. Забегая вперед, скажу, что спустя десять лет, работая с фирмой «Рокуэлл Коллинз» над гражданским самолетом Ил-96М/Т, мы познакомились с американской системой верификации. Они проводят ее, как я определил это для себя, путем «долбления» зондирующими сигналами всех веточек программы в режиме «да» или «нет», и так узнают, работает эта веточка или не работает. Это очень громоздкий и «тупой» процесс, потому что число веточек очень велико... По завершении верификации программ Ил-96М/Т верификационные листы, когда их подшили, сложились в сорок толстенных томов. Если бы мы шли по этому пути, работая над Ту-160, то получили бы таких томов на порядки больше, поскольку программы в нем нацелены не только на решение навигационно-пилотажных задач, но прежде всего на выход в зоны боевого применения, выставку инерциальных платформ, пуск десятков ракет, имеющихся на борту... И если бы мы пошли по американскому пути верификации, то нам, наверное, всей жизни не хватило бы, чтобы ее провести.

Полунатурное же моделирование, которое фактически дает возможность «жить» в реальном полете, позволило нам в кратчайшие сроки проверить в комплексе всю программу управления системами самолета и оружия. И только один раз, и то не на Ту-160, а на Ту-95МС, поймали режим, который в реальном полете привел к ложному срабатыванию одной из систем. Мы долго не могли понять, в чем дело, но когда на стенде запустили этот режим, то нашли ошибку в одной из веточек программы. Она как-то проскочила через «сито» режимов, которые мы моделировали...

В общем, как мы убедились на собственном опыте, глубина моделирования позволяла довольно тонко и детально тестировать все математическое обеспечение сложных авиационных систем. Хотя, может быть, западная методика верификации дает более полную ее картину, поскольку в принципе не допускает пропусков веточек, но зато очень трудоемка, занимает много времени, и я не убежден, что она правильно отображает динамическое взаимодействие элементов системы. Наше тестирование, помимо логического анализа цепочек программ и на соответствие с картами прошивок, позволяло еще и видеть, как система работает в динамике. Этот процесс, думаю, еще не осмыслен теоретически до конца, но он очень важен – взаимодействие «живой» программы и «живой» аппаратуры в реальном масштабе времени еще ждет своих исследований …”

Федосов Е.А. Полвека в авиации. Записки академика: Литературно-художественное произведение. – М: Дрофа, 2004. – 400 с., 48 л. цв. вкл.

Евгений Александрович

Полвека в авиации

Записки академика

Автор этой книги, академик Е. А. Федосов, – генеральный директор одного из ведущих научных центров страны, знаменитого ГосНИИАС (Государственный научно-исследовательский институт авиационных систем), который уже более полувека является головным в области создания комплексов авиационного вооружения. В воспоминаниях Евгения Александровича последовательно, десятилетие за десятилетием, отражены основные этапы послевоенного развития нашей боевой авиации и систем ее вооружения.

Эта книга – убедительное свидетельство того, что пресловутая «эпоха застоя» (конец 60-х – начало 70-х годов) на самом деле была наиболее бурным, драматичным и результативным периодом развития нашей авиации, плодами которого до сих пор живет и еще долго будет жить эта отрасль.

О роли авиации

«...Конечно, не заманчивость и новизна дела, не близкая возможность широкого осуществления заветной мечты человека летать по воздуху, не возможность нового и быстрого средства передвижения, а то, что правительства западноевропейских стран видят в воздушных кораблях будущее могучее средство обороны и нападения... Всеми невольно сознается, хотя еще точно и не формулируется, что готовится колоссальный переворот, последствия которого трудно еще предвидеть и учесть, и что те государства будут иметь все преимущества при столкновении с врагом, у которых будет в руках это новое орудие нападения и обороны. Было бы более чем ужасно, скажу даже преступно, если бы мы и в этом деле, как во многом другом, отстали от наших соседей...»

Из доклада князя Б. Голицына «Об общих директивах для правильной постановки дела воздухоплавания в России», прочитанного 13 декабря 1909 г. в Академии наук.

**Определение отказоустойчивости авионики** сформулируем следующим образом.

|  |
| --- |
| *Отказоустойчивость* – свойство архитектуры авионики,  обеспечивающее выполнение полётных функций  в течение заданного времени  при возникновении аппаратных и программных отказов. |

Для обеспечении отказоустойчивости авионики применяются два основных подхода:

1. Предотвращение отказов системы путем повышения технологического уровня изготовления компонентов авионики, минимизации ошибок разработчиков, программистов, операторов. Однако данный подход наталкивается на естественные ограничения технического и экономического характера.

2. Создание отказоустойчивых систем. При этом допускается возникновение отказов, но используются эффективные методы устранения их последствий. Обеспечение отказоустойчивости является одним из способов повышения надежности авионики.

По способу реализации отказоустойчивость подразделяется на пассивную и активную.

***Пассивная отказоустойчивость*** заключается в способности системы не потерять свои функциональные свойства в случае отказа отдельных элементов. В таких случаях говорят, что отказ маскируется системой. Пассивная отказоустойчивость связана с увеличением количества аппаратуры в несколько раз; она применяется обычно тогда, когда недопустимы даже кратковременные перерывы в работе систем, а также для обеспечения отказоустойчивости важнейших блоков или устройств системы.

Структура пассивно отказоустойчивых систем основана либо на мажоритарном принципе, либо на резервировании с контролем. Количество резервной и дополнительной аппаратуры в таких системах превышает количество основной аппаратуры.

***Активная отказоустойчивость*** реализуется в интегрированных многопроцессорных комплексах авионики с общей памятью, общей шиной, кольцевой, иерархической или другой структурой. Необходимым условием является наличие ресурсного обеспечения для осуществления реконфигурации структуры в случае отказов элементов.

Применение активной отказоустойчивости характеризуется более экономным расходом аппаратных средств, однако связано с некоторыми потерями времени при восстановлении работы системы после отказа (иногда возможны потери части данных). В общем случае процесс функционирования такой системы может быть представлен схемой, приведенной на рис. 2.5.1.

В то же время применение пассивной отказоустойчивости гарантирует практически бесперебойную работу системы и сохранение всей информации. Эти обстоятельства определяют области применения активной и пассивной отказоустойчивости.

**Дефекты:**

**-** разработки,

**-** физические,

**-** от внешних

воздействий

(HIRF)

Работоспособное состояние

Возникновение ошибки

Выявление ошибки

Локализация ошибки

Реконфигурация структуры

Анализ и принятие решения

Восстановление информации

Работоспособное состояние

Восстановление

вычислительного процесса

**Функции**

**системы**

**диагностики**

технического

состояния

**и**

**управления**

реконфигурацией

БЦВС

Рис. 2.5.1-1. Последовательность состояний процесса

функционирования отказоустойчивой системы

Контроль работоспособности отдельного сетевого компонента БЦВС может осуществляться следующими основными способами:

* непрерывный контроль;
* синхронный периодический контроль;
* асинхронный периодический контроль.

|  |
| --- |
| *Отказы обнаруживаются* средствами контроля,  *локализуются* при помощи средств диагностики  и *устраняются* автоматической реконфигурацией системы. |

|  |
| --- |
| *Реконфигурация* заключается  в перестройке структуры системы таким образом, чтобы ее  отказавшие компоненты были устранены от участия в работе;  при этом производительность БЦВС может уменьшается  (снижение функциональных способностей). |

**Кардинально проблема обеспечения надежного и отказоустойчивого функционирования вычислительных систем реального времени, требующих высокой достоверности результатов вычислений, может быть решена**

**только структурным способом на аппаратном уровне.**

С ростом сложности структуры бортовой вычислительной систем и повышением их быстродействия **резко растут**

**требования к достоверности результатов решения задач**,

поставленных перед вычислительной системой, а, следовательно,

**к системе контроля производимых вычислений**.

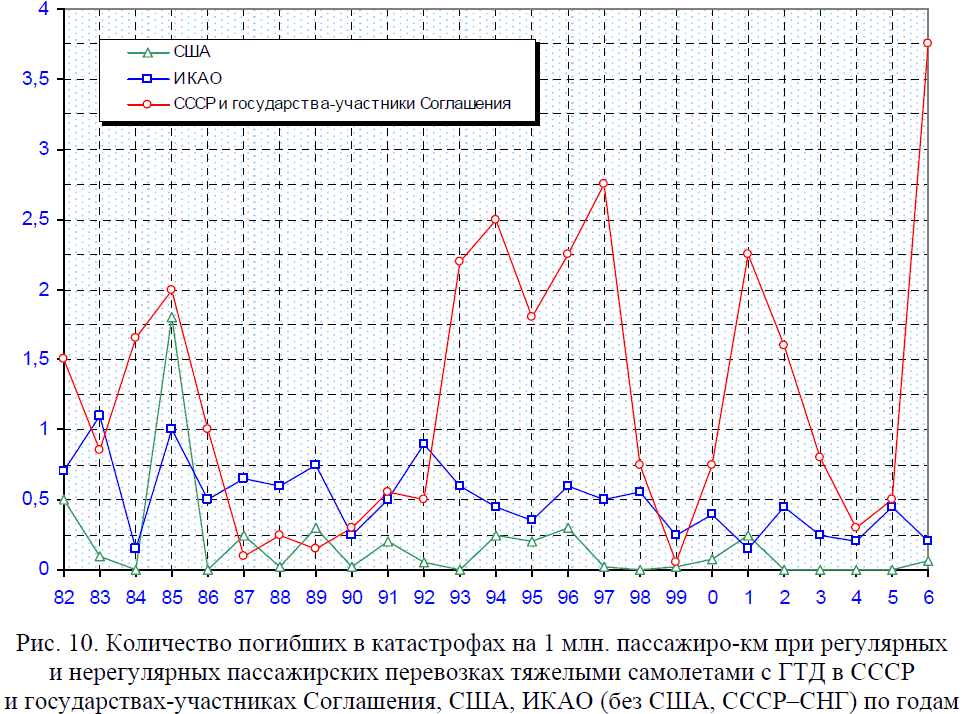
**Эффективность системы контроля становится одной из наиболее важных характеристик бортового вычислительного комплекса.**

**Отказобезопасность** - свойство технической системы при отказе некоторых частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей. Данное определение – общетехническое, относящееся в равной степени к авиации, космическим полётам, химическим и атомным производствам (заводы производства ТВЭЛ`ов, электростанции)

**Отказобезопасность** - свойство системы авионики при отказе некоторых компонент аппаратуры и/или программного обеспечения переходить в режим работы, обеспечивающий возможность безопасного продолжения полёта и выполнения посадки воздушного судна.

**Отказобезопасность** следует отличать от **отказоустойчивости,** хотя в реальных системах эти два требования могут выступать совместно. Понятие отказобезопасности шире и включает все факторы, влияющие на безопасность полёта. При анализе отказобезопасности рассматривается **эргатический интегрированный комплекс**

**“экипаж – воздушное судно – среда”**.



**2. Показатели избыточности и контролепригодности ЦМ**

Современная методология аналитической оценки параметров отказоустойчивости систем авионики находится в состоянии активного становления. Здесь по возможности кратко и в доступной форме представим некоторые подходы к оценке отказоустойчивости, доведенные до практической реализации. Для этого нам потребуются математические модели описания структур объектов авионики и процессов отказов/восстановлений в них.

Более того, на этапе проектирования следует закладывать такие структурные решения, которые позволили бы предотвратить отказы и предпринять упреждающие меры по их недопущению.

|  |
| --- |
| Построение отказоустойчивой авионики рассматривается  как задача формирования такой избыточной структуры,  в которой отказ элемента низкого иерархического уровня  не приводил бы к отказам на более высоком уровне. |

Одним из возможных подходов к **аналитической оценке параметров отказоустойчивости системы** в целом на основании известных характеристик отказоустойчивости элементов является математическое описание процессов отказов/восстановлений в структуре авионики. Сущность подхода состоит в следующем.

Представим визуальную модель системы в виде пространства технических состояний (каждое техническое состояние есть набор одинаковой кратности отказавших элементов и одинаковых последствий этих отказов) и графа переходов между этими состояниями (такая модель близка к моделям графа состояний и переходов Марковских процессов) [80].

Тогда резервирование увеличивает путь от полностью исправной системы (со всеми работоспособными элементами) до состояния неработоспособности системы, в котором кратность отказов соответствует отказам основных и резервных элементов. Под увеличением пути понимается количество промежуточных работоспособных состояний, в которых пребывает система при последовательном возникновении отказов, прежде чем окажется в состоянии неработоспособности.

Но увеличение пути, особенно при анализе и обеспечении безопасности, может быть достигнуто не только резервированием, но и реконфигурацией функциональной структуры системы. По существу при реконфигурации с целью сохранения приоритетных, например, для безопасности, функций или допустимых условий работоспособности, «жертвуют» при отказах другими функциями.

Отметим, что необходимыми условиями применения реконфигурации является наличие многих уровней работоспособности системы или её многофункциональность и наличие *встроенного контроля* (built-in-test - **ВІТ**).

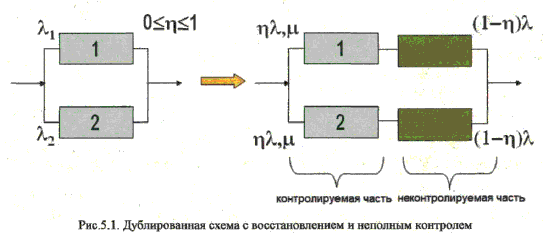
Наиболее рациональным способом обеспечения отказобезопасности является сочетание резервирования (небольшой кратности; например, дублирования, троирования) и реконфигурации. Надо сказать, что реконфигурация часто оказывается более эффективна, если могут возникать одновременно кратные отказы, обусловленные общей внешней причиной.

Оценка технического состояния системы обеспечивается наличием в системе функции и встроенных средств контроля (built-in-test equipment - BITE) технического состояния, которые определяют контролепригодность системы – ее приспособленность к обнаружению отказов и выявлению причин (места) их возникновения. Оперативный встроенный контроль технического состояния элементов и систем, контроль правильности выполнения функций (при его идеальной работе) позволяет:

* в полной мере реализовать возможности резервирования,
* своевременно принимать меры по реконфигурации систем и изменению режимов функционирования,

обеспечивая тем самым свойство отказобезопасности системы в целом. Однако контроль не является идеальным – во-первых, он сам отказывает, а во-вторых, не абсолютно все отказы и события им распознаются. Поэтому для обеспечения высоких показателей надежности и безопасности требуется проведение тщательного «надежностного» анализа систем объекта в целом с учетом многих факторов, одним из которых являются характеристики контроля [116,117]. Аппаратно-программные средства контроля в современных системах интегрированы в устройства управления. Такая интеграция усложняет процесс оценки показателей надежности и безопасности системы в целом и степени влияния средств и характеристик контроля на функционирование системы в частности.

Роль систем контроля должна оцениваться по влиянию их характеристик на вероятностные показатели надежности, безопасности. Проведем исследование надежности дублированной схемы с восстановлением по такому показателю безотказности как средняя наработка до отказа при следующих исходных данных. Встроенный контроль выявляет не все отказы рабочих элементов схемы. Долю отказов, выявляемых BIT, обозначим как η. Принято допущение об абсолютной надежности средств контроля. Элементы схемы равнонадежны с интенсивностью отказов и восстановления, равных соответственно λи μ. Восстановление работоспособности элементов происходит лишь при возникновении отказов, выявляемых BIT. Тогда дублированная схема может быть представлена как параллельное соединение двух каналов, каждый из которых состоит из контролируемой и восстанавливаемой и неконтролируемой и невосстанавливаемой частей (рис. 5.1).



**2. *Показатели и модель оценки характеристик контроля***

Для оценки степени влияния средств контроля на изменение работоспособности системы необходимо характеристики контроля определить на множестве возможных состояний системы, отражающих отказы элементов (модулей) системы.

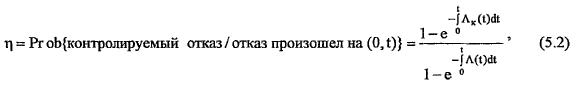
Интегральную оценку качества контроля будем проводить по показателю достоверность контроля. Но и отдельные составляющие, входящие в интегральную оценку, представляют интерес, как с точки зрения задания; обоснования требований, так и для понимания причин снижения интегральной характеристики, выявления степени влияния составляющих. Основными характеристиками контроля, регламентированными нормативной документацией, в том числе зарубежной, являются:

• **полнота контроля**;

• **глубина контроля**.

***Полнота контроля***характеризует долю отказов объекта контроля, обнаруживаемых при контроле работоспособности. В общем случае качество контроля определяется перечнем элементов (модулей), отказы которых выявляются контролем. Поэтому одной из характеристик полноты контроля может быть отношение числа контролируемых элементов к общему числу элементов рассматриваемого объекта контроля (например, в процентах). Однако для совместного моделирования «надежностного поведения» объекта и средств контроля желательно задавать полноту контроля как некоторый вероятностный показатель или как отношение показателей, характеристик надежности (отказа) контролируемых элементов ко всем элементам.

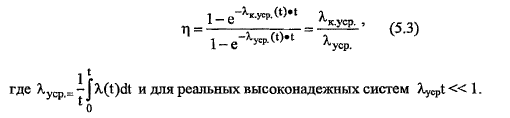
Целесообразность такого задания объясняется тем, что при моделировании «надежностного поведения» анализируемого объекта (например, системы), можно будет «разбить» общий поток отказов на две составляющие - выявляемые контролем отказы и «скрытые» отказы. Полноту контроля в этом случае можно определить как условную вероятностью контролируемого отказа, вычисленную при условии, что отказ произошел:



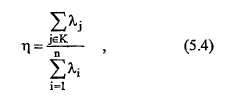
где Λ - суммарная интенсивность отказов объекта контроля (контролируемые + неконтролируемые);

Λк - суммарная интенсивность контролируемых отказов.

Проведя усреднение интенсивностей отказов на интервале (0,t), получаем:



Общие выражения (5.2, 5.3) для полноты контроля при экспоненциальных распределениях наработки до отказа элементов наиболее удобно задавать как отношение суммарной интенсивности отказов контролируемых элементов к суммарной интенсивности отказов всех элементов, т.е.



где η - полнота контроля;

*п* -количество элементов объекта контроля;

K - подмножество контролируемых элементов;

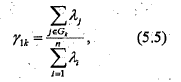
λ*i* - интенсивность отказа элемента.

В этом случае определяемая полнота является условной стационарной вероятностью контролируемого отказа, вычисленная при условии, что отказ произошел.

***Глубина контроля***характеризует «разрешающую» способность средств контроля. Понятие данной характеристики более разнообразное, чем полноты контроля. Например, можно понимать глубину контроля некоторой системы управления как глубину поиска неисправного компонента в иерархии компонент структуры системы: подсистема, ... , модуль, плата, элемент электро-радио изделия (ЭРИ). В данной работе глубина будет определяться через типовые элементы замены (в ряде зарубежных нормативных материалов такие элементы называются LRU - Line Replaceable Unit) следующим образом. Если, при возникновении контролируемого отказа, контроль указывает на некоторое подмножество элементов, которые возможно отказали, то эти элементы одновременно снимаются (в том числе и не отказавшие) и заменяются на работоспособные (это и является спецификой оперативного обслуживания).

По аналогии с полнотой глубину контроля также можно понимать как долю в общем количестве элементов анализируемого объекта контролируемых до одного LRU, двух LRU, трех LRU и.т.д. Таким образом, глубина контроля может быть представлена рядом распределения; Составляющие этого ряда - стационарные вероятности снятия одного, двух ..., *n* LRU (где *п* - число элементов объекта контроля), при условии возникновения одного отказа. Если эти вероятности выражены через отношения количества элементов соответствующих подмножеств LRU к общему количеству LRU (например, в процентах), то такая характеристика является качественной, в том смысле, что она не связана с вероятностной моделью комплекса «объект контроля – средства контроля».

С точки зрения «надежностного» анализа глубина контроля влияет на показатели ремонтопригодности, в частности, на среднее время восстановления работоспособности, на число ЗИП. Для формирования моделей потоков восстановления глубина контроля может определяться аналогично полноте через отношения суммарных интенсивностей отказов для каждого члена, указанного ряда распределения по количеству снимаемыx LRU:



где γ1к - характеристика 1 глубины контроля для *k* снимаемых элементов (модулей LRU);

*Gk* - подмножество контролируемых элементов, при отказе любого из которых снимается *k* элементов.

Другой вероятностной характеристикой глубины контроля может быть отношение математического ожидания числа отказов в системе к математическому ожиданию числа съемов за заданное время:



**3. Влияние характеристик контроля модуля**

**на достоверность диагностирования**

Обозначим:

- состояние работоспособности (неработоспособности) объекта контроля;

- состояние объекта признаётся работоспособным (неработоспособным) средствами контроля.

Тогда формально можно определить следующие результаты взаимодействия объекта и средств контроля:

* работоспособное состояние объекта признается контролем как работоспособное, что записывается АВ;
* работоспособное состояние объекта признается контролем как неработоспособное, что записывается А;

• неработоспособное состояние объекта признается контролем как работоспособное, что записывается В;

• неработоспособное состояние объекта признается контролем как неработоспособное, что записывается .

Правильная оценка состояния объекта контроля происходит, когда результат взаимодействия объекта и средств контроля имеет вид АВ или .

Определим достоверность контроля как

D = P(АВ) + P() , (5.8)

а недостоверность как

= 1 – D = Р(А) + Р(В) . (5.9)

Составляющие недостоверности контроля можно записать

(5.10)

где Р(А), Р() – вероятности работоспособного состояния и отказа объекта контроля;

– условные вероятности признания контролем отказа объекта, при условии его работоспособности, и работоспособности объекта, при условии его отказа, соответственно.

Для вычисления условных вероятностей воспользуемся аппаратом деревьев событий, введя в качестве учитываемых факторов полноту контроля и состояния контроля (работоспособность, и два вида отказа). Деревья событий, в принципе, являясь переборным методом, удобны для вычисления условных вероятностей тем, что позволяют декомпозировать всю задачу, помещая условие в корень дерева и рассматривая его как исходное событие. Причем условие может состоять не из одного события, а из любой их логической комбинации. Агрегирование показателей, вычисленных для выделенных при декомпозиции частей, в данном случае, проводится по формулам условной вероятности (в частности, (5.10)). Обозначим η *–* полнота контроля, *K*, *K*лс, *K*нс – события работоспособности и отказов типа ложного срабатывания и несрабатывания контроля. На рис 5.7 и 5.8 представлены соответствующие деревья событий.

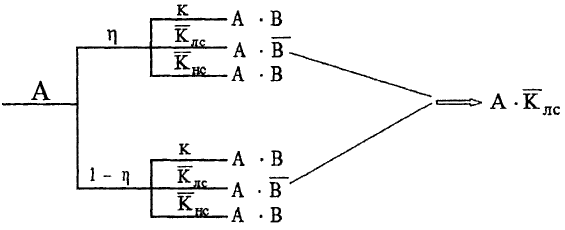


Рис. 5.7. Дерево событий для вычисления условной вероятности

признания контролем отказа объекта, при условии его работоспособности

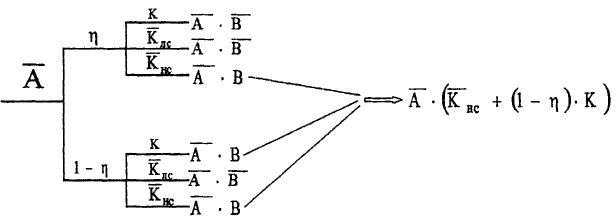


Рис. 5.8. Дерево событий для вычисления условной вероятности

признания контролем работоспособности объекта, при условии его отказа

После вычисления по ним искомых условных вероятностей, в соответствии с (5.9) получим



Здесь возникает еще один вопрос, как относиться (с точки зрения достоверности) к указаниям контроля на два или более LRU, при отказе одного из них (т.е. как ввести в недостоверность глубину контроля). Предлагается отнести такую ситуацию также к недостоверности контроля, так как идентификация хотя бы одного работоспособного LRU как отказавшего, приводит к необходимости изъятия его (их) из системы, а значит это несовершенство контроля. Такая ситуация возникает, когда событие АП^ПК происходит с условной вероятностью (1 – γ11). Таким образом, окончательно получаем



Исмпа

1. **RTCA** (Radio Technical Commission for Aeronautics –Радиотехническая комиссия по аэронавтике) – международная ассоциация, которая разрабатывает стандарты авиации. [↑](#footnote-ref-2)