Инженерная логика обеспечения надёжности сложных систем

Виктор Каганов

This artcle discusses the possibility of the reliability of complex technical systems which are highly innovative, emerging in the analysis of possible failures of the system, if it is used by the developer of the generalized reliability model based on a functional diagram of the system.

Надёжность любого изделия как характеристика его эксплуатационных свойств выражается в виде полной вероятности выполнения изделием целевой задачи

$$P^* = H_i(\Delta\tau,\varsigma_i)\cdot E(\varsigma_i) \qquad (1)$$

где $H_i(\Delta\tau,\varsigma_i)$- вероятность нахождения изделия в работоспособном состоянии в течение интервала времени $\Delta\tau$, при условиях эксплуатации ς_i, и $E(\varsigma_i)$ - эффективность исправного изделия в условиях эксплуатации ς_i.

В дальнейшем, применительно к разрабатываемому объекту, мы будем пользоваться двумя терминами:

-- термином **изделие** (единица промышленной продукции, количество которой может исчисляться в штуках) во всех случаях, когда это необходимо, безотносительно его сложности;

-- термином **техническая система** (состоит из элементов объединённых связями и вступающих в определённые отношения между собой и внешней средой, чтобы осуществить процесс и выполнить целевую функцию) в тех случаях, когда рассматриваются вопросы, связанные с необходимостью декомпозиции изделия по функциональным признакам.

Говоря о факторах, в наибольшей степени влияющих на суть и логику решений, принимаемых разработчиком изделия, следует прежде всего назвать:

1. Техническое задание на разработку. Это документ, задающий в форме технических требований облик изделия, условия его эксплуатации, его параметры и выходной эффект, а также требования к его надёжности.

2. Новизна создаваемого изделия. При создании изделия, обладающего высокой новизной, разработчик сталкивается с существенным дефицитом знаний и опыта, необходимых для решения конкретных проектных и технологических проблем, а также с отсутствием или недостаточностью источников информации. Иными словами создание такого изделия происходит в условиях, когда у заказчика есть основания и желание считать, что создание необходимого ему изделия практически осуществимо, несмотря на то, что многих инженерных решений ещё не существует и их необходимо планировать в рамках развёртываемой разработки. В связи с этим реальный процесс создания такого изделия неизбежно сопровождается на каждом этапе совершением ряда более или менее существенных ошибок, которые вносятся в техническую документацию при её разработке и могут в дальнейшем явиться причиной отказов изделия или его неэффективной работы. Имеются в виду не злонамеренные ошибки, а нормальный процесс проектирования, когда разработчик вынужден принимать решения, опираясь лишь на те знания, которыми он располагает в момент принятия решения.

3. Применяемая разработчиком модель надёжности. О первых двух факторах можно говорить как о факторах, ставящих перед разработчиком задачи, требующие решения, в то время как применённая модель надёжности определяет реальную логику принятия решений, можно даже сказать технологию решения поставленных задач.

Наибольшие возможности при решении этих задач разработчику даёт обобщённая модель надёжности, рассматривающая в качестве единственного реального эквивалента

изделия его функциональную схему (модель), устанавливающую взаимосвязь между процессами, протекающими в системе от момента включения (первое действие) и до получения выходного эффекта (заключительное действие). Обобщённая модель надёжности устанавливает зависимость ресурсной характеристики изделия от конкретных физических процессов, протекающих как в распределении нагрузок между изделиями множества, так и в прочностной характеристике изделия.

Рассмотрим гипотетическое простейшее изделие - изделие, обладающее всего одним видом выходного эффекта и лишь одним видом возможного отказа. По отношению к такому изделию можно считать, что его эффективность $E = 1$ при нахождении изделия в работоспособном состоянии. В этом случае можно считать, что надёжность изделия равна вероятности его безотказной работы. Вероятность безотказной работы изделия (как доля изделий множества , сохранивших работоспособность в течение определённого периода времени) может быть вычислена в случае если нам известна функция плотности распределения времени безотказной работы $f(\tau)$ изделий множества, к которому принадлежит интересующее нас изделие.

За период времени $O....\tau_i$ вероятность отказа любого из изделий множества определяется как $q = \int_0^{\tau_i} f(\tau) \cdot d(\tau)$, и вероятность его безотказной работы $P = 1 - q$. (2)

Помимо функции $f(\tau)$, которую мы можем считать ресурсной характеристикой изделия, нам также известно, что прочность изделий, образующих исследуемое множество, характеризуется функцией плотности распределения прочности $f(R)$, и на изделия действует повреждающая нагрузка, распределённая между изделиями множества случайным образом и имеющая функцию плотности распределения $f(Q)$ в любой момент времени.

На рис.1 приведена ресурсная характеристика гипотетического изделия, имеющая в своём составе типичные для многих видов изделий участки начальных (Н), случайных (С) и износовых (И) отказов.

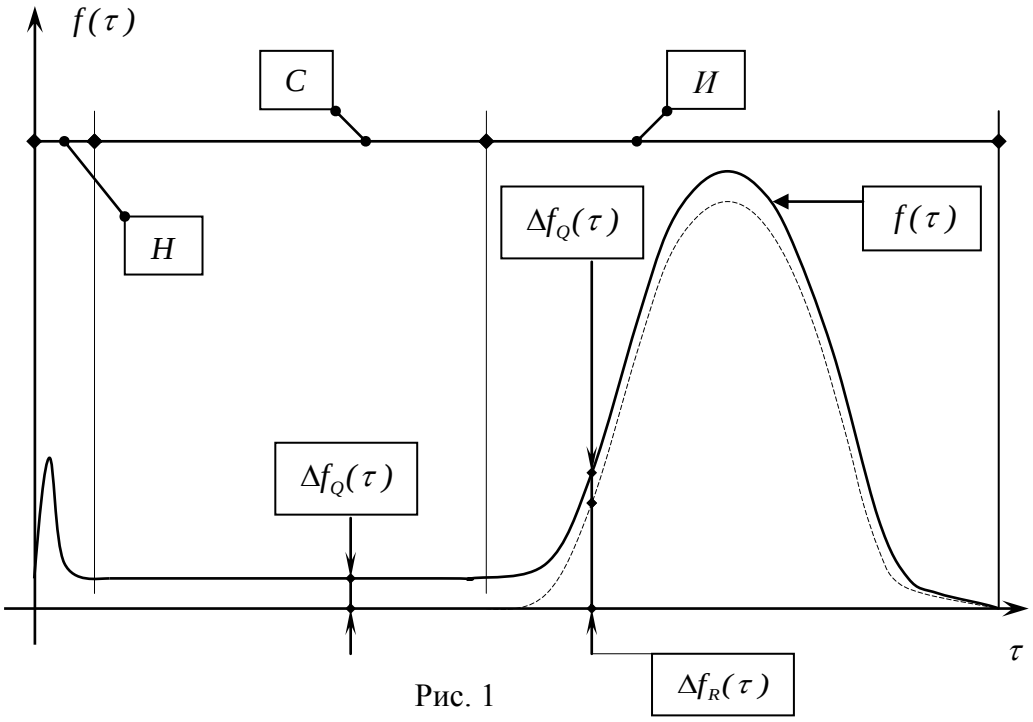


Рис. 1

Рассмотрим механизм формирования такой характеристики. Поскольку отказ любого j-того изделия, входящего в множество, происходит только в случае превышения действующей на него нагрузки над его прочностью $Q_j > R_j$, то очевидно, что эта ресурсная характеристика является статистическим отображением изменений, происходящих с течением времени в распределениях $f(Q)$ и $f(R)$, приводящих к многократному повторению ситуации $Q > R$ и к выходу из строя в конечном счёте всех изделий, образующих наше множество. В соответствии с этим ресурсная характеристика может быть представлена как $$f(\tau) = \Delta f_Q(\tau) + \Delta f_R(\tau) \qquad (3)$$

при выполнении условия $$\int_0^\infty f(\tau) \cdot d\tau = 1 \qquad (4).$$

В выражении (3) $\Delta f_Q(\tau)$ - составляющая, характеризующая отказы,возникающие вследствие изменений, происходящих в распределении нагрузок, и $\Delta f_R(\tau)$ - составляющая, характеризующая отказы, возникающие вследствие изменений прочностной характеристики изделия. У нас есть все основания относиться к выражению (3) как к уравнению обобщённой модели надёжности.

Исследуем более детально физическую основу взаимосвязи ресурсной характеристики изделия с его прочностной характеристикой и действующей на изделие нагрузкой. Для этого воспользуемся понятием **риск отказа** $r = Bep\{Q > R\}$**.** Этот термин имеет смысл вероятности отказа изделия (доли вышедших из строя изделий), обладающего прочностной характеристикой $f(R)$, при реализации эксплуатационной нагрузки $f(Q)$ и действии её в течение какого-то времени, при этом имеется в виду, что изначально существует определённое наложение распределения нагрузки на прочностную характеристику изделия.

В качестве фактора, обуславливающего существование составляющей $\Delta f_Q(\tau)$, принимаем процесс **переадресации** нагрузки между изделиями, входящими в исследуемое множество. Термин **переадресация** нагрузки следует понимать буквально, так как именно переадресация нагрузки между изделиями множества в процессе их эксплуатации фиксируется исследователем как изменение нагрузки, действующей на какое-либо конкретное изделие, при неизменной во времени функции плотности распределения нагрузки $f(Q)$.

Используемое нами понятие "нагрузка" – это **воздействие любой физической природы, которое может приводить к отказу изделия или влиять на его выходной эффект.** Соответственно "прочность" – это **свойство (способность) изделия противостоять действующей на него нагрузке.**

Если при проектировании и изготовлении изделия не было допущено грубых ошибок, то старение и износ проявляются не сразу, и в ресурсной характеристике изделия образуется участок ,,случайных” отказов. Мы не считаем эти отказы случайными, так как условие возникновения отказа $Q>R$ справедливо во всех без исключения случаях. Случайный характер имеет процесс переадресации нагрузок, этот процесс может протекать с различной интенсивностью.

В качестве фактора, обуславливающего существование составляющей $\Delta f_R(\tau)$ принят **дрейф** прочностной характеристики изделия $f(R)$, связанный с существующими при хранении и эксплуатации изделия процессами старения и износа.

При разработке нового изделия разработчик неизбежно сталкивается с различными проблемами обеспечения надёжности, большая или меньшая острота этих проблем обуславливается степенью новизны изделия, а также требованиями заказчика, финансирующего разработку. В связи с этим необходимо отметить, что сегодня ни один

серьёзный заказчик не может безоговорочно согласиться с поставкой ему изделий, имеющих ресурсную характеристику аналогичную приведенной на рис.1 -- с ярко выраженными участками начальных и случайных отказов.

Для неремонтируемых изделий наличие таких участков в ресурсной характеристике недопустимо, так как оно означает, что часть изготовленных изделий попросту не пригодна для практического применения.

Для ремонтируемых изделий наличие в их ресурсной характеристике таких участков предполагает необходимость развёртывания переразмеренной сети ремонтных предприятий, что ведёт к необоснованным дополнительным затратам в период эксплуатации изделий и может отрицательно влиять на сбыт изготовленной продукции.

Таким образом, исходя из практических интересов заказчика, можно утверждать, что стратегическим направлением обеспечения надёжности вновь создаваемого изделия является получение ресурсной характеристики, не имеющей в своём составе участков начальных и случайных отказов.

Само по себе наличие этих участков в составе ресурсной характеристики изделия является следствием существенного наложения распределения повреждающей нагрузки на прочностную характеристику и интенсивная переадресация нагрузки. Исключение их из состава ресурсной характеристики возможно лишь при наличии верхнего ограничения повреждающей нагрузки на уровне более низком, чем нижнее ограничение прочностной характеристики. Реальным способом ограничения повреждающих нагрузок является преобразование или усечение их распределений путём введения в состав изделия тех или иных систем защиты, или введения ограничений по условиям эксплуатации и режимам работы изделия.

Нижнее ограничение прочности на нужном уровне может быть достигнуто применением высококачественных (высокопрочных) материалов и элементов конструкции, а также проведением контрольных диагностических испытаний, позволяющих отбраковать элементы конструкции изделия, имеющие прочность ниже уровня нормативной испытательной нагрузки.

Можно по-разному относиться к проблеме прогнозирования надёжности, но когда речь заходит о необходимости принятия конкретных и ответственных решений, приходится признать, что у разработчика есть лишь один путь к успеху – проведение анализа возможных отказов (АВО) разрабатываемого изделия. Хочет того разработчик или не хочет, но именно к этому в конечном счёте сводится по своей сути весь процесс проектирования даже в тех случаях, когда разработчик не проводит АВО как плановую и целенаправленную работу, а руководствуется своим опытом, технической интуицией и сложившимися техническими традициями.

Не вызывает сомнений то обстоятельство, что АВО, как механизм компенсации дефицита знаний, существующего при разработке изделий, обладающих высокой новизной, должен быть неотъемлемой частью процесса разработки нового изделия уже с самых первых проектных действий разработчика. По результатам АВО разработчик может принимать необходимые схемные и конструктивные решения, а также формирует конкретные задачи отработочных испытаний, основной целью которых является перевод представлений разработчика о возможных отказах и их последствиях из виртуальной области в область точных (или по крайней мере более или менее достоверных вероятностных) оценок. Необходимо также особо отметить возможность эффективного использования АВО для анализа последствий несанкционированных воздействий на систему – прежде всего неквалифицировнных действий обслуживающего персонала и даже диверсионных актов. Такой анализ может явиться основанием для создания подсистем, блокирующих несанкционированные действия и защищающих техническую систему от катастрофических отказов.

Состав изделия и характер его агрегатирования (деления на сборочные единицы и детали) регламентируется спецификацией или аналогичным конструкторским документом. Однако иерархическая структура изделия (комплект – комплекс – сборочная единица – деталь), установленная конструкторской документацией не раскрывает в полной мере существующих в системе функциональных связей вследствие чего практически не пригодна для проведения анализа возможных отказов.

По этой причине разработчик параллельно с созданием комплекта конструкторской документации вынужден проводить декомпозицию технической системы на подсистемы по функциональным признакам.

Мы сугубо формально говорим о декомпозиции технической системы, относя её к иерархической структуре, установленной спецификацией, в то время как фактически в процессе проектирования изначально происходит именно формирование функциональных схем системы и подсистем различного уровня, на их основе проводятся расчёты эффективности и работоспособности, принимаются необходимые конструктивно-компоновочные решения и формируется комплект конструкторской документации.

В конечном счёте разработчик приходит к тому, что создаваемая техническая система состоит из некоторого числа подсистем $A,B,....M$, соединённых и взаимодействующих между собой с определённой логикой при воздействии внешних и внутрисистемных эксплуатационных нагрузок $Q_1,Q_2,...Q_n$.

Совокупность уравнений работоспособности и эффективности локальных подсистем составляет алгоритм вычисления характерных для системы компонент выходного эффекта – их зависимость от параметров элементов системы $\pi_a,\pi_b,...\pi_l$ и действующих нагрузок $Q_1,Q_2,...Q_n$

$$E_{A..M} = ALG_E(\pi_a,\pi_b,....\pi_l,Q_1,Q_2,....Q_n).$$

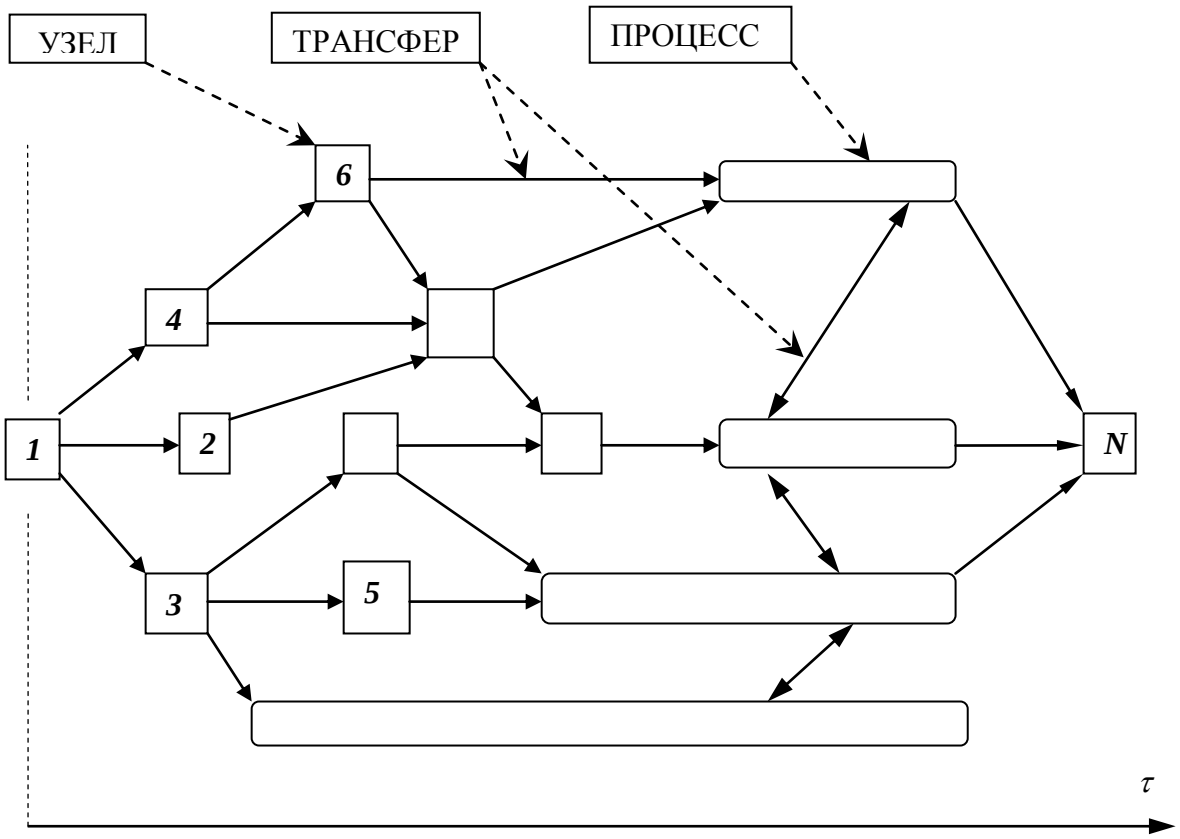
Следует отметить, что процесс разработки технической системы зачастую фактически отождествляется с процедурой разработки комплекта КД, когда многие технические решения принимаются на базе так называемой инженерной интуиции, а не на базе конкретных знаний. В этом случае функциональная схема не имеет реального статуса обязательного проектного документа, в лучшем случае ей отводится роль некоего творческого сопровождения процесса разработки КД. Есть все основания считать, что отсутствие такого документа самым негативным образом влияет на полноту (а следовательно и качество) расчётных оценок работоспособности и эффективности системы, а также делает невозможным проведение полноценного анализа возможных отказов и обоснованного планирования отработочных испытаний.

Этот недостаток может быть устранён путём документирования функциональной схемы – создания базового рабочего документа, обладающего хорошей наглядностью как в части маршрутов функциональных взаимодействий, так и в части их хронологии. Такой документ может быть разработан в виде ориентированного графа, формальным прототипом этого документа могут служить сетевые графики (СГ), широко используемые при планировании и управлении осуществлением научно-технических и иных проектов. В нашем случае речь идёт о создании *сетевой функциональной схемы-циклограммы (СФСЦ)* разрабатываемой технической системы.

Естественно, что СФСЦ и СГ могут обладать некоторым сходством, но по своей сути это два совершенно разных документа – так все элементы, формирующие СФСЦ, являются тем или иным действием, в то время как СГ образуют элементы двух типов – действие и событие. Это отличие связано с тем, что СФСЦ отображает массив взаимосвязанных физических процессов, прерывание любого из которых может означать выход системы из строя, а СГ отображает поэтапные действия людей (коллективов), участвующих в реализации какого-либо проекта. Событие в СГ имеет смысл завершения очеред-

ного действия и последующее действие может быть отсрочено или отменено административным решением.

Рассмотрим возможную графическую конфигурацию СФСЦ, раскрывающую логику происходящих в системе взаимодействий, но не их физическую суть поскольку речь не идёт о конкретной технической системе.



Приведенная выше СФСЦ образована несколькими графическими условными знаками, означающими различные по своему характеру действия, с привязкой этих действий к временной шкале τ.

1. Узел – кратковременное действие, в результате которого возникает выходной эффект (сигнал, воздействие, продукт и т.п.), который необходим для совершения последующих действий. Узлы имеют цифровую нумерацию (1,2,3,....N).

Для узлов от (1) до (N-1) имеется в виду промежуточный (локальный) выходной эффект и лишь для узла (N) выходной эффект системы.

2. Процесс – длительное действие (рабочее состояние системы или подсистемы), при котором осуществляется непрерывное взаимодействие между подсистемами, с окружающей средой или смежными системами, и создаётся выходной эффект, обеспечивающий решение целевой задачи или переход к последующим действиям (для систем, в которых предусмотрено накапливание выходного эффекта до определённого уровня). Процессы имеют общую с узлами цифровую нумерацию.

3. Трансфер – действие, в результате которого локальный выходной эффект, образовавшийся в узле или процессе, доставляется в подсистемы, где он участвует в создании нового выходного эффекта или инициирует его создание. Цифровая нумерация устанавливает маршрут трансфера (1-2,...4-7,...39-71,...и т.д).

4. Трансфер с обратной связью – взаимообмен выходными эффектами, служащий для регулирования режимов функционирования подсистем (как правило существует между двумя процессами).

Необходимо особо подчеркнуть, что каждое действие, входящее в состав СФСЦ, осуществляется соответствующей функциональной подсистемой, элементы которой могут входить в состав различных сборочных единиц разрабатываемого изделия, и именно это обстоятельство является ключевым для принятия конструктивно-компоновочных решений.

Используя эти условные знаки, разработчик формирует топографию ("скелет") функциональной схемы, привязанную к временной шкале. Однако для превращения "скелета" в полноценную функциональную схему необходимо дать расшифровку каждого действия – описание физической сути этих действий, характера взаимодействий и участвующих в них элементов конструкции или составных частей системы, а также образующийся выходной эффект. Необходимо также описать "сопутствующие" функциональные связи между подсистемами, не участвующие непосредственно в создании выходного эффекта, но влияющие на работоспособность элементов конструкции. К числу таких "сопутствующих" связей могут относиться взаимодействия с окружающей средой, а также различные помехи и нагрузки, возникающие при штатном взаимодействии элементов конструкции изделия.

Функционирование системы начинается с внешнего воздействия, инициирующего запуск системы (1), и заканчивается образованием выходного эффекта в узле (N). Для того, чтобы понять как формируется сеть промежуточных действий между действиями (1) и (N) рассмотрим логику принятия разработчиком необходимых для этого решений. Как это ни парадоксально, на первый взгляд, но при разработке системы, обладающей высокой новизной (с чистого листа), цепочка рассуждений разработчика и принимаемых им схемных и конструктивно-компоновочных решений выстраивается не от действия (1) в сторону действия (N), создающего выходной эффект системы, а в обратном направлении – от выходного эффекта к действию (N) и от действия (N) в сторону предшествующих действий. Это объясняется тем, что разработчик знает или в состоянии понять и принять решение о том, какое действие должно быть совершено для получения требуемого выходного эффекта и чем должно инициироваться и обеспечиваться это действие. Двигаясь именно таким образом (от выходного эффекта к действию создающему этот эффект), разработчик может постепенно сформировать всю СФСЦ и принять необходимые канструктивно-компоновочные решения. При разработке системы, обладающей ограниченной новизной, разработчик может заимствовать как фрагменты СФСЦ, так и части разработанных ранее систем.

Первоначальный вариант СФСЦ как правило носит укрупнённый характер, так как степень её детализации напрямую зависит от глубины конструктивной проработки составных частей и даже элементов конструкции технической системы. Совершенно естественно, что СФСЦ должна дополняться и детализироваться непрерывно в процессе разработки проектной и конструкторской документации, а также в процессе отработочных испытаний технической системы и её частей.

Разработку СФСЦ технической системы на определённом этапе проектирования можно считать завершённой, если разработчик приходит к выводу, что он сформировал алгоритм вычисления характерных для системы компонент выходного эффекта, соответствующий тому уровню знаний и понимания облика создаваемой системы, которыми он обладает на этом этапе, и для дальнейшей детализации и уточнения СФСЦ необходимо продолжение проектных иконструкторских разработок на базе уже принятых решений. При этом мы должны понимать, что на любом этапе разработки изделия СФСЦ существует как объединение понятных разработчику функциональных связей (действий), со-

здающих необходимый выходной эффект. Каждое из этих действий можно рассматривать как локальный фрагмент, который при необходимости может быть детализован и развёрнут в СФСЦ локальной подсистемы (по мере углубления знаний и расширения опыта разработчика).

Не требует особых пояснений то обстоятельство, что для получения выходного эффекта системы (выполнения ею целевой задачи) должны состояться все предусмотренные СФСЦ действия, или определённая часть этих действий. В связи с этим разработчик должен понимать необходимость достаточно глубокой детализации СФСЦ к моменту разработки подсистемы контроля и регистрации параметров процессов, протекающих в технической системе, так как эта подсистема (вспомогательная по своему назначению) должна обеспечить разработчика качественной информацией о работе функциональных элементов и подсистем в процессе отработочных испытаний и при эксплуатации серийных изделий.

Рассмотрим теперь какие технические возможности возникают в связи с существованием СФСЦ конкретной технической системы:

1. СФСЦ является своеобразной динамической моделью надёжности создаваемой системы. В рамках этой модели в качестве основного критерия, характеризующего надёжность технической системы, рассматривается вероятность несовершения какого-либо конкретного действия (вероятность неполучения необходимого выходного эффекта), в то время как основным критерием такого типа в математической модели является некая абстрактная вероятность отказа какого-либо структурного элемента. Эта особенность СФСЦ составляет принципиальное отличие обобщённой модели надёжности от математической модели – СФСЦ позволяет оценивать (прогнозировать) вероятность выхода из строя системы в любой момент времени, её значение соответствует вероятности несовершения действия, происходящего в системе в этот момент. Математическая же модель предусматривает оценку абстрактной вероятности отказа системы за какой-то промежуток времени, причём эта вероятность тем больше, чем дольше функционирует система, даже при отсутствии износовых процессов.

2. СФСЦ как документ является визуализированным перечнем возможных отказов технической системы – базовым документом для их анализа. Любое из формирующих СФСЦ действий может не состояться – и это будет отказом, возможные причины и последствия которого требуют детального анализа, так как локальный отказ подсистемы может привести к отказу системы в целом. Необходимо отметить, что СФСЦ позволяет при необходимости формировать перечни возможных отказов для любого момента функционирования системы.

Это свойство функциональной схемы и предопределяет все действия разработчика при проведении анализа любого из возможных отказов:

1.Формирование функциональной блок-схемы (конструктивного облика) локальной подсистемы, реализующей связи (взаимодействия) между функциональными и конструкционными элементами, участвующими в создании выходного эффекта подсистемы;

2. Формирование перечня особо опасных функциональных и конструктивных элементов выход из строя любого из которых (одного) приводит к отказу всей системы;

3. Формирование перечня сопутствующих взаимодействий между элементами подсистемы, создающих разного рода повреждающие нагрузки и помехи как для элементов исследуемой подсистемы, так и для элементов смежных подсистем;

4. Разработка алгоритмов расчёта прочности и устойчивости функциональных и конструкционных элементов по отношению к повреждающим нагрузкам и помехам;

5. Расчётное определение запасов работоспособности и эффективности подсистемы с учётом всех видов повреждающих нагрузок и помех, в том числе и при неблагоприятных их сочетаниях;

6. Планирование специальных отработочных испытаний с целью определения реальных запасов прочности и устойчивости, а также показателей эффективности локальных подсистем.

Испытания должны создать информационную обратную связь между объектами испытаний и разработчиком, что позволит ему на базе анализа результатов испытаний, включая в первую очередь анализ возникших отказов и неисправностей, оценить правильность принятых ранее решений.

Проведение АВО нельзя считать завершённым даже после окончания разработки комплекта технической документации на систему. Следует иметь в виду, что анализ *возможных* отказов неизбежно переходит в анализ отказов, *фактически возникающих* при испытаниях изделия и его составных частей. На основании анализа результатов отработочных испытаний принимаются (в случае необходимости) решения о схемных и конструктивных изменениях изделия, а также о завершённости его отработки или проведении дополнительных испытаний.

ЛИТЕРАТУРА

1. ***Базовский И.*** Надёжность. Теория и практика.: Пер. с англ.- М.: Мир, 1965,-375с.
2. ***Епифанов А.Д.*** Надёжность автоматических систем.- М.: Машиностроение, 1964,-336с.
3. ***Зажигаев Л.С., Кишьян А.А., Романиков Ю.И.*** Методы планирования и обработки результатов физического эксперимента.- М.: Атомиздат, 1978.-230с.
4. ***Каганов В.Л.*** К вопросу обеспечения надёжности изделий путём ограничения нагрузки.- В сб. Вибрационная прочность и надёжность двигателей и систем летательных аппаратов, вып. 9.- Куйбышев, КуАИ, 1982.- с.83-90.
5. ***Каганов В.Л., Капитонов В.А.*** Обобщённая модель надёжности и отработочные испытания.- В сб. Вибрационная прочность и надёжность двигателей и систем летательных аппаратов, вып. 10.- Куйбышев, КуАИ, 1984.-с.83-90.
6. ***Каганов В.Л., Капитонов В.А., Попов П.А., Прокудин С.Н.*** Планирование экспериментальной отработки с целью выявления запасов работоспособности.- В сб. Руководство по обеспечению надёжности изделий отрасли, книга XIX, ЦНИИМаш, 1986.
7. ***Хевиленд Р.*** Инженерная надёжность и расчёт на долговечность.- Пер. с англ.- М.-Л.: Энергия, 1966.-231с.