Лекция 5
Надёжность при проектировании систем автоматики

Темы: Основные определения понятий теории надёжности и надёжности, связанной с функциональной безопасностью. Среднее Время Между Отказами (MTBF). Интенсивность отказов. Вероятность безотказной работы. Коэффициенты надёжности компонентов PLC – систем. Анализ надёжности систем, связанных с безопасностью.

Предприятия химической, а также многие энергетические установки предъявляют особые требования к системам управления технологическими процессами. Аварийная остановка или некорректное завершение технологического процесса на подобных производствах могут привести к серьезным убыткам, а в некоторых случаях и к полному выходу установки из строя с последующим капитальным ремонтом. Именно поэтому ключевыми требованиями к системам управления этими объектами являются высокая надёжность аппаратной части и выполнения алгоритмов, а также возможность резервирования элементов системы управления.

Основные определения понятий теории надёжности

Надёжность — это свойство объекта сохранять во времени значения всех параметров и выполнять требуемые функции в заданных условиях применения.
Надежность — комплексное свойство, которое включает в себя безотказность, долговечность, ремонтопригодность и сохраняемость. В электроэнергетике и электромеханике к этим свойствам добавляют еще готовность, живучесть и безопасность.

 В промышленной автоматизации для количественной оценки надёжности чаще всего используется параметр «наработка на отказ» или параметр «интенсивность отказов», а в системах безопасности — «вероятность отказа при наличии запроса».

Пример
Если рассматривается система охраны нефтебазы, то нужно учитывать вероятность отказа системы во время попытки проникновения нарушителей на базу, а не в то время, когда их нет. С точки зрения надёжности охраны нужно рассматривать вероятность несрабатывания датчика охранной сигнализации в интервале времени, в течение которого может появиться нарушитель, и не нужно учитывать вероятность ложного срабатывания системы, поскольку она не влияет на выполнение функции охраны.

Безотказность — свойство объекта непрерывно сохранять работоспособное состояние в течение некоторого времени или некоторой наработки. Работоспособное состояние (работоспособность) — состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют требованиям нормативов. Наработка — продолжительность или объем работы объекта.

Долговечность — свойство объекта сохранять работоспособность до наступления предельного состояния при установленной системе технического обслуживания и ремонта. Предельным называется состояние, при котором дальнейшее применение объекта по назначению недопустимо или нецелесообразно либо восстановление его невозможно или невыгодно.

Ремонтопригодность — свойство объекта, связанное с приспособленностью к предупреждению и обнаружению причин появления отказов и повреждений, поддержанию и восстановлению работоспособности путем технического обслуживания и ремонтов.

Сохраняемость—свойство объекта сохранять значения показателей безотказности, долговечности и ремонтопригодности в течение и после хранения и (или) транспортировки.

Готовность — свойство объекта приступать к выполнению некоторых функций в любой момент времени по требованию, изменяя режим работы без нежелательных переходных процессов.
В это понятие включается и управляемость, и устойчивость, и относительная длительность (вероятность) нахождения в работоспособном состоянии.

Живучесть — свойство объекта противостоять внешним и внутренним возмущениям (нарушениям, воздействиям, отказам), не допуская их цепочечного развития и сокращения функционирования ниже жизненно необходимого уровня.

 В это понятие включается и неуязвимость объекта (в отношении утраты некоторых элементов), и стойкость объекта (в отношении к общим для всех элементов воздействиям).

Безопасность — свойство объекта не создавать опасности для людей и окружающей среды во всех возможных режимах работы и аварийных ситуациях. Учитывая безусловную важность этой составляющей, часто ее выделяют из понятия надежности, говоря о надежности и безопасности объектов.

 Основные определения понятий теории надёжности и надёжности, связанной с функциональной безопасностью, даны в IEC 61508.

Отказ

Отказом называется событие, заключающееся в нарушении работоспособности объекта. Факт отказа устанавливается на основании некоторых критериев отказа, то есть признаков, позволяющих судить о нарушении работоспособности.
Переход объекта с одного уровня работоспособности на другой, более низкий, называется отказом. Отказ, произошедший во время выполнения заданных функций, называется отказом в работе (отказом функционирования). Отказы бывают полные и частичные.

Отказы возникают вследствие применения ненадёжных схемотехнических решений на стадии проектирования контроллеров, электронных компонентов, изготовленных с нарушением техпроцесса, применения некачественных материалов, нарушения технологических режимов пайки, неточной установки компонентов на печатную плату, старения материалов, некачественного технологического оборудования, низкой культуры производства, отсутствия надёжных методов контроля, работы компонентов в предельных электрических режимах, нарушений условий эксплуатации и т.п.

Неисправностью называется состояние объекта, при котором он не соответствует хотя бы одному своему параметру, указанному в эксплуатационной документации.

Неработоспособностью называется состояние объекта, при котором он не способен выполнять хотя бы одну из своих функций, описанных в эксплуатационной документации

Пример.

Контроллер, у которого отказал один из каналов ввода, является работоспособным, но неисправным, если этот канал не может использоваться.

Наработкой называется продолжительность работы объекта, выражаемая в единицах времени или в количестве циклов (например, циклов срабатывания реле).

Различают наработку до отказа (от начала эксплуатации до первого отказа) и наработку между отказами (от начала работы после ремонта до очередного отказа). Используют также средние значения этих величин.

Среднюю наработку между отказами называют наработкой на отказ, в отличие от средней наработки до отказа.
Безотказность — свойство объекта непрерывно сохранять работоспособность в течение некоторого времени или наработки. Вероятность безотказной работы — вероятность того, что в пределах заданной наработки отказ не возникнет.

Коэффициент готовности — вероятность того, что объект окажется работоспособным в произвольный момент времени, кроме запланированных периодов, в течение которых его работа по назначению не предусматривается. Высокая готовность системы обеспечивается избыточностью, допустимостью сбоев, автоматическим контролем ошибок и диагностированием.

Сначала некоторые основные факты:
1. У каждой отдельной единицы оборудования, когда-либо сделанного, есть некоторая вероятность отказа.
2. У различных видов оборудования различной сложности есть различные вероятности отказа.

Пример

У короткой части медного провода есть очень низкая вероятность отказа. Производственный дефект, достаточно высокий электрический ток, чтобы расплавить медь, или физическое повреждение на провод - это события для повреждения провода.
Автоматический Регулятор Напряжения (AVR), с другой стороны, является очень сложным прибором. По упрощенному описанию функция AVR - измерить существующее напряжение, сравнить это с установленным напряжения и послать корректирующий сигнал, если фактическое измеренное напряжение и установленное напряжение не то же самое. Типично AVR делают вышеупомянутую функцию сотни раз в секунду. AVR также составлен из сотен отдельных частей, все из которых должны функционировать правильно иначе AVR откажет.
Из двух примеров видно, что вероятность отказа короткой части медного провода очень, намного меньше, чем вероятность отказа AVR.

Теперь предположим, что провод связан с AVR и что только эти два вида оборудования составляют типовую систему. Оба вида оборудования одинаково важны для системы, но у них есть весьма различные вероятности отказов. По аналогии, что "цепь только столь же сильна как своя самая слабая связь," вероятность отказа наших двух систем, провода и AVR, не может быть лучше, чем вероятность отказа самого слабого пункта. В нашей типовой системе это - AVR. Эта та же самая аналогия сохраняется для очень сложных систем с тысячами частей.

MTBF, MTTF

 Среднее время Между Отказом (MTBF - Mean Time Between Failures) и MTTF – (mean time to failure) использовалось больше 60 лет как основание для различных решений. За годы были развиты больше чем 20 методов и процедуры для предсказаний времени жизни (lifecycle).

MTBF - мера того, насколько надежный продукт. MTBF обычно дается в единицах часов; чем выше MTBF, тем более надежный продукт. Для электронных продуктов обычно предполагается, что во время полезного периода срока службы у частей есть постоянные нормы отказа. Нормы отказа части определяются показательным законом распределения.

MTBF и MTTF продукта могут быть вычислены как:

$$MTBF = \frac{t}{n}, \qquad (1)$$

$$MTTF = \frac{t}{N} \qquad (2)$$

Где t – время работы,
n – число отказавших элементов,
N – число испытываемых элементов
t - период времени
n – число отказавших элементов
Вероятность лежит в пределах:
$0.0 < p < 1.0$ или $0\% < p < 100\%$

Вероятность, что продукт будет работать в течение некоторого времени *t* без отказа:

P(*t*) = exp (-*t* /MTBF) (3)
тот показатель определяется отношение числа элементов продукта, безотказно проработавших до момента времени t к общему числу элементов продукта, работоспособных в начальный момент.

$$Q(t) = \frac{n}{N} \qquad (4)$$

Q(t) - вероятность отказа

$$P(t) = \frac{N_t}{N} = 1 - \frac{n}{N},$$ (5)

$$P(t) + Q(t) = 1$$ (6)

Вероятность безотказной работы P(t) представляет собой вероятность того, что в пределах указанного периода времени t, отказ продукта не возникнет.

Пример
Для продукта с MTBF 250 000 часов и интересующим временем работы 5 лет (43 800 часов):

P = exp (- 43800/250000) = 0.839289

Это значит, что есть вероятность на 83.9 %, что продукт будет работать в течение этих 5 лет без отказа, или что 83.9 % единиц будет все еще работать в течение этих 5 лет.

Интенсивность отказов λ(t)

Интенсивность отказов λ(t) - это число отказов n (t) элементов продукта в единицу времени, отнесенное к среднему числу элементов N_t продукта, работоспособных к моменту времени времени Δt:

$$\lambda(t) = \frac{n}{N_t \cdot \Delta t}$$ (7)

Где Δt - заданный отрезок времени.

Пример. 1000 элементов продукта работали 500 часов. За это время отказали 2 элемента. Отсюда,

$$\lambda(t) = \frac{n}{N_t \cdot \Delta t} = \frac{2}{1000 \cdot 500} = 4 \cdot 10^{-6} 1/t$$ (1/ч), т.е. за 1 час может отказать 4-е элемента из миллиона.

Если известно MTBF, то можно рассчитать интенсивность отказов λ как обратную величину MTBF:

$$P(t) = \exp\left[-\int_0^t \lambda(t) dt \right]$$

$$MTBF = \int_0^t P(t) dt = \int_0^t e^{-\lambda t} dt = \frac{1}{\lambda}.$$ (8)

Время безотказной работы равно обратной величине интенсивности отказов.

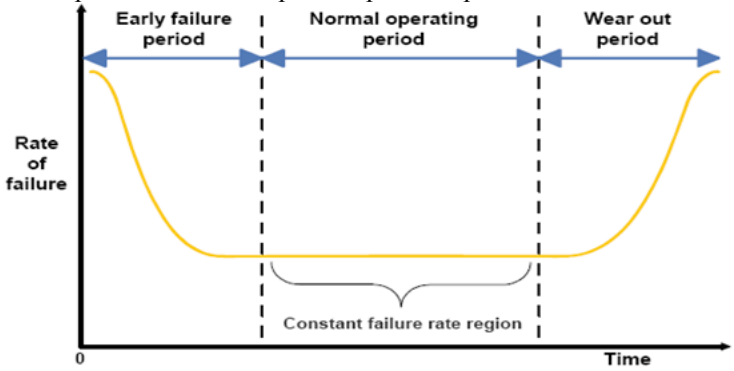

Рис. 1 Кривая интенсивности отказов во времени (*bathtub curve*)

Пример.

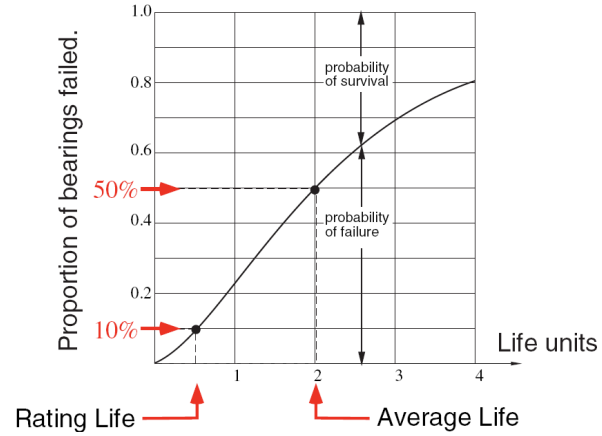

Рис. 2 Вероятность отказов шариковых подшипников
Источник: http://www.mech.eng.unimelb.edu.au/eng_design/learning/d300/R02_single.pdf

Показатели интенсивности отказов комплектующих элементов берутся на основании справочных данных.
Для примера в табл. 1 приведена интенсивность отказов λ(t) некоторых элементов и в таблице 2 - коэффициенты надежности .

Таблица 1

№	Наименование элемента	Интенсивность отказов, $*10^{-5}$, 1/ч
1	Резисторы	0,0001…1,5
2	Конденсаторы	0,001…16,4
3	Трансформаторы	0,002…6,4
4	Катушки индуктивности	0,002…4,4
5	Реле	0,05…101
6	Диоды	0,012…50
7	Транзисторы	0,01…90
8	Коммутационные устройства	0,0003…2,8
9	Разъемы	0,001…9,1
10	Соединения пайкой	0,01…1
11	Провода, кабели	0,01…1
12	Электродвигатели	100…600

Пример: Технология элементов обеспечивает среднюю интенсивность отказов $\lambda_i = 1*10^{-5}$ 1/ч. При использовании в системе $N=1*10^4$ элементарных деталей суммарная интенсивность отказов $\lambda_{system} = \sum_{i=1}^{n} \lambda_i$ $\lambda_{system} = N*\lambda_i = 10^{-1}$ 1/ч. Тогда среднее время безотказной работы

MTBF $= 1/\lambda_{system}$ =10 ч.

Если выполнить систему на основе 4-х больших интегральных схем (БИС), то среднее время безотказной работы увеличится в N/4=2500 раз и составит 25000 ч. или 34 месяца или около 3 лет.

Таблица 2

Наименование элемента	**Коэффициент надежности**
Резисторы	1,0
Конденсаторы	0,25…0,83
Трансформаторы	1,3…3,0
Катушки индуктивности	1…2
Реле	1…10
Диоды	1,3…30,0
Транзисторы	1,3…75,0
Электродвигатели	10…40

Надежность и Пригодность

MTBF воздействуют и на надежность, и на пригодность. Различие между надежностью и пригодностью является часто неизвестным или недооцененным. Высокая пригодность и высокая надежность часто идут взявшись за руки, но они не взаимозаменяемые сроки.

 Надежность - способность системы или компонента, выполнить его необходимые функции при установленных условиях в течение установленного периода времени.
Другими словами, это - вероятность, что система или компонент отработают в пределах его идентифицированного времени работы без отказов.

Пример.
Миссия самолета - прекрасный пример, чтобы иллюстрировать это понятие. Когда самолет взлетает, для него есть одна цель: закончить полет, как предназначено, благополучно (без катастрофических отказов).

Пригодность, с другой стороны, является степенью, для которой система или компонент являются эксплуатационными и доступными когда требующийся для использования.

 Пригодность (доступность) может быть рассмотрена как вероятность, что система или компонент находятся в состоянии, чтобы выполнить его необходимую функцию при данных условиях в данный момент времени. Доступность систем, программ, услуг и информации, когда необходимо, и без необоснованных задержек

Пригодность определена надежностью системы, так же как ее время восстановления, когда отказ действительно происходит. Когда система долго непрерывно работает, отказы неизбежны. Пригодность часто определяют так, что когда отказ действительно происходит, критическая переменная устанавливает, как быстро система может быть восстановлена.

В примере, надежность самолета - самая критическая переменная, но когда отказ происходит, самое важное - это восстановить оборудование и запустить настолько быстро, насколько возможно, чтобы время простоя самолета свести к минимуму.

Расчёт показателей надёжности

Полная надежность системы основана на надежности каждого из ее компонентов. Вычисление составляющей надежности (R) начинается с величины среднего времени между отказами (MTBF) (данные изготовителем каждого компонента). Из этого можно определить ежегодную норму отказа, который используется, чтобы определить величину надежности. Статистическая величина MTBF представляет среднее время, которое требуется, чтобы произошёл отказ.

Пример.
MTBF 100 000 часов означает, что один отказ происходит каждые 100 000 часов в среднем.

Расчет надежности основывается на следующих допущениях:

1. Все элементы работают в нормальных технических условиях;
2. Отказы элементов являются событиями случайными и независимыми;
3. Все элементы работают одновременно;
4. Отказ любого элемента приводит к отказу всей системы;

При расчете надежности необходимо определить вероятность безотказной работы системы в произвольном интервале времени *t,* которая определяется выражением:

$$P(t) = e^{-\lambda t}$$

где $p(t)$ изменяется по экспоненциальному закону;

λ - интенсивность отказов системы (контура);

t **-** время, за которое определяется вероятность безотказной работы.

Тогда вероятность отказа системы можно определить, исходя из формулы:

$$P(t) + Q(t) = 1$$

Пример расчет надежности

Рассчитаем степень надежности одного контура управления, например, контура управления включением двигателя.
Интенсивность отказов λ, зависит от свойств деталей, режима их работы и условий эксплуатации. Значение λ для любого класса аппаратуры определяется статистическими методами в ходе эксплуатации.

Таблица 3 Значения интенсивности отказов устройств

Элемент системы	Интенсивность отказов, λ,
Преобразователь	0,025
Исполнительный механизм (двигатель)	0,03
Регулируемый орган (насос)	0,035
Источник питания	0,027

Интенсивность отказов для контура управления будет равна сумме показателей интенсивности отказов входящих в контур элементов.
Время *t,* за которое определяется вероятность безотказной работы, возьмем равным 1 году.

P(t) - вероятность безотказной работы
Q(t) - вероятность отказа
T - заданное время, в течение которого проверяются P(t) и Q(t) (1 год)
MTBF - среднее время наработки на отказ (время безотказной работы)
λ- интенсивность отказов

Дано:
t= 1
λ_1= 0,025 λ_2= 0,03 λ_3= 0,035 λ_4=0,027

Решение:
$\lambda = \lambda_1+\lambda_2+\lambda_3+\lambda_4$ λ=0,117
MTBF =1/λ MTBF = 8,54
$P(t) = (e)^{-t/MTBF}$

Q(t)= 1-P(t)
P(t)= 0.89
Q(t)= 0.11
Из проведённых расчётов видим что, вероятность безотказной работы составляет 0,89 или 89 %. То есть надёжность довольно высока.

Методы оценки надёжности

Существуют различные методы оценки надёжности: метод блок-схем (RBD – reliability block diagram), метод Markov, Monte Carlo - анализ.
Один способ определить надежность архитектуры системы - метод, названный анализом блок-схемы надежности - Reliability Block Diagrams (RBDs).

Блок-схемы надежности - это графическое представление компонентов системы и как они соединены между собой. Следует отметить, что это может отличаться от того, как компоненты физически связаны между собой. RBD упрощенной компьютерной системы с резервированием вентиляторов показана на рисунке.

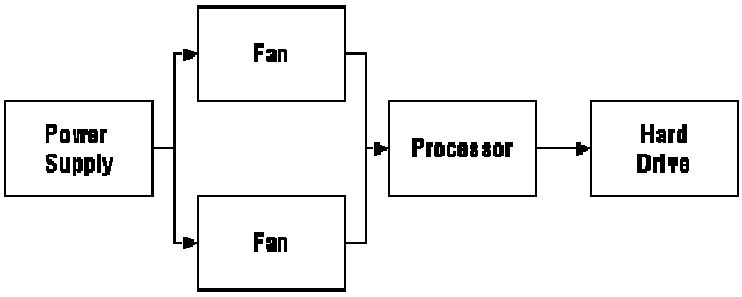

Рис. 3 Простейшая Блок-схема надежности.
Средствами повышения надежности системы является введение избыточности (см. лекцию 6)

Простейший метод расчёта надежности - распределить надежности равномерно между всеми компонентами.

Пример
Предположим, что система с пятью компонентами соединены последовательно. Надежность цепи 90% для данного времени работы.
Равномерное распределение цели всех компонентов потребует, чтобы надежность каждого компонента была бы 98% для указанного времени работы, так как $0{,}98^{5} = 0.9$

Анализ надёжности систем, связанных с безопасностью.

При анализе надёжности систем, связанных с безопасностью, вместо вероятности отказа используется понятие «вероятность отказа при наличии запроса», то есть вероятность отказа при наличии необходимости быть в состоянии готовности.
В системах, связанных с безопасностью, наработка до отказа рассматривается отдельно для опасных и безопасных отказов. Безопасным считается отказ, не вызывающий опасную ситуацию на объекте.

Классическая теория надёжности учитывает оба вида отказов.

Пример

В системе аварийного отключения исчезновение питания приводит к обесточиванию обмотки реле, и поэтому реле отключает нагрузку, переводя её тем самым в безопасное состояние. В такой системе отказ источника питания обмотки реле является безопасным отказом и поэтому не учитывается при расчёте вероятности отказа при наличии запроса.
Однако отказ такого же источника питания в системе автоматического пожаротушения, когда необходимо, наоборот, подать напряжение на насосы, рассматривается как опасный отказ.
Поэтому средняя вероятность отказа при наличии запроса в двух рассмотренных системах будет различной, несмотря на применение блока питания с одним и тем же значением наработки до отказа.

Учёт обычной наработки до отказа при проектировании систем безопасности может привести к неоправданно заниженным показателям надёжности и невозможности достижения требуемого уровня безопасности.

Большая доля отказов приходится на программное обеспечение (см. лекцию 8)

Производители компьютерных средств автоматизации уделяют вопросам надежности большое внимание: проводят жесткий отбор аппаратных средств, вводят дополнительные элементы (например, сторожевой таймер), дополнительные программы тестирования в процессе управления, контроль сохранности программы управления и данных, а также резервирование аппаратных средств и линий связи.

Результаты внутреннего тестирования и проверок компьютерных средств автоматизации фиксируются в служебной и архивной памяти. Эта информация берется из управляющей программы, поэтому при разработке программ необходимо учитывать влияние возможных отказов на качество управления. При создании системы управления необходимо учитывать ее устойчивость к отказам как при выборе технических средств, так и при проектировании схемы подключения и разработке управляющей программы. Отказ всегда возможен, поэтому

необходимо строить систему таким образом, чтобы можно было этот отказ своевременно обнаружить и минимизировать ущерб от его появления.

Правила дизайна для надежности систем с PLC

1. Понимание окружающей среды
2. Понимание того, как элементы отказывают
3. Применение активных мер по борьбе с элементами "высокого риска"
4. Прочная конструкция / отказоустойчивость
5. Простота проектирования
6. Интеграция отдельных компонентов системы
7. Надежность программных элементов и правильных алгоритмов задач
8. Обзор общей надежности инструментов и конструкции.

Литература

1.IEC 61508-7 (2000). Функциональная безопасность электрических/электронных/программируемых электронных систем, обеспечивающих безопасность. Часть 7. Обзор методов и средств измерения.
2. IEC 61508-3 (1998). Системы электрические/электронные/ программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению.
3. Смит Д.Д., Симпсон К.Д. Функциональная безопасность. — М.: Издательский дом «Технологии», 2004. — 208 с.
4. Александровская Л.Н., Афанасьев А.П., Лисов А.А. Современные методы обеспечения безотказности сложных технических систем. – М.: Логос, 2001. – 206с.