Надежность систем и устройств

Лекция 1. Введение в теорию надежности

Глухих Михаил Игоревич, к.т.н., доц.
mailto: glukhikh@mail.ru

Курс по выбору

- Цифровая обработка сигналов (зачет + ?? экзамен ??)
  - ИЛИ
- Надежность систем и устройств (зачет + ?? экзамен ??)

Предмет курса

- Анализ надежности систем и устройств
  - И
- Способы повышения надежности систем и устройств

- Английское название – Reliability Engineering

Место курса

Дискретная математика

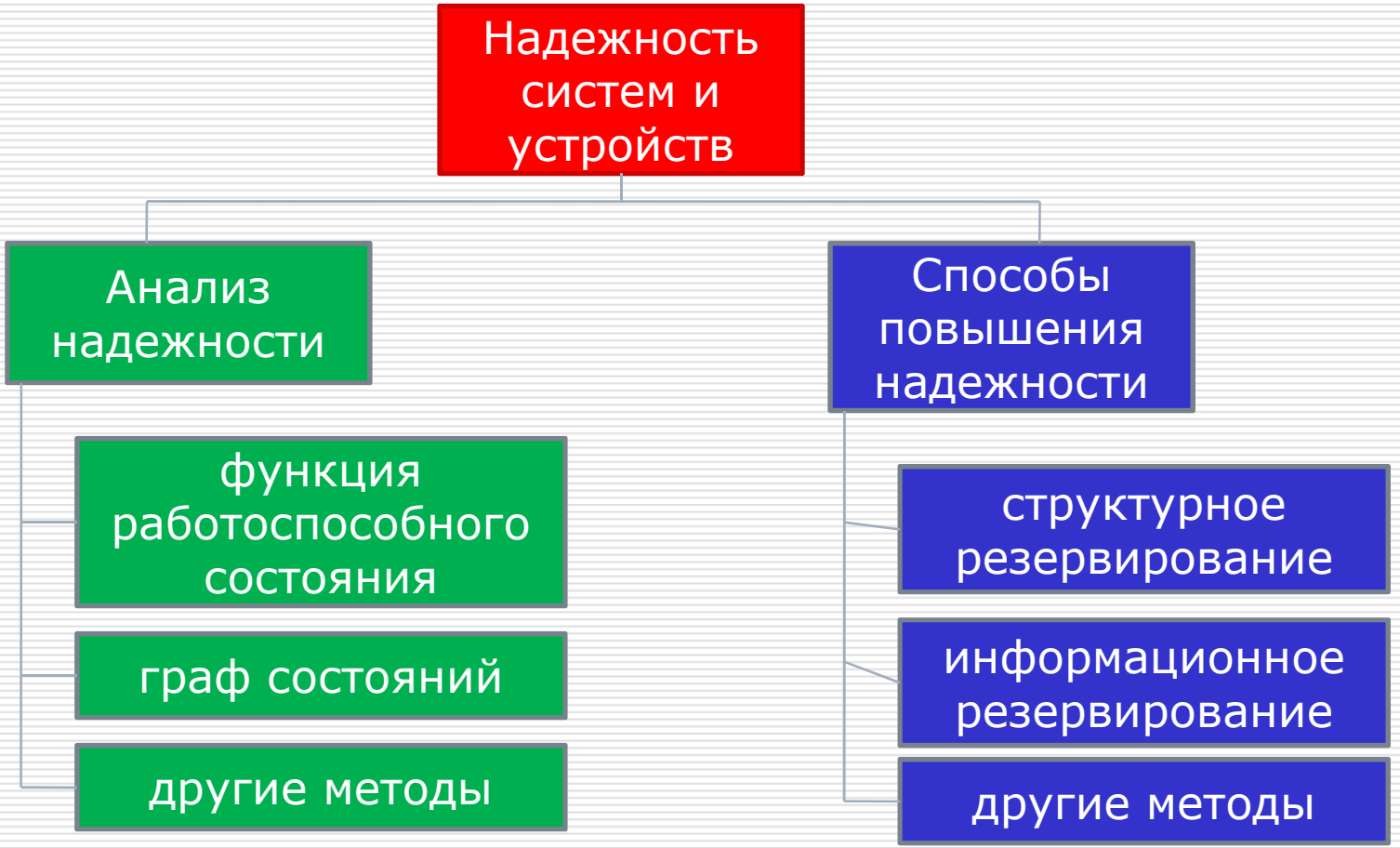
Системный анализ

АПДУ

Надежность систем и устройств

Методы обеспечения качества ПО

Разделы курса



Сайт курса

- Год 2011 – http://tiger.ftk.spbstu.ru/trac/edu-tn
- Год 2012 (в разработке) – http://kspt.ftk.spbstu.ru/course/depend
- Скорее всего, изменений в программе лекций и лабораторных работ будет немного

Программа лекций (1-5) – Глухих М.И.

1. Введение в теорию надежности
2. Анализ надежности на основе функции работоспособного состояния
3. Анализ надежности на основе графа состояний
4. Обзор методов структурного резервирования
5. Применение мажорирования

Программа лекций (6-10) – Моисеев М.Ю.

1. Информационное резервирование, линейные коды
2. Коды с произвольным кодовым расстоянием, характеристики кодов
3. Коды Рида-Соломона, сверточные коды
4. Другие классы кодов, теорема Шеннона
5. Временное, алгоритмическое и функциональное резервирование

Программа лабораторных работ (5)

1. Расчет показателей надежности с помощью логико-вероятностных методов
2. Расчет показателей надежности с помощью методов теории случайных процессов
3. Выбор оптимального варианта построения отказоустойчивой системы
4. Разработка интеллектуального устройства голосования для системы со структурным резервированием
5. Разработка кодера и декодера помехоустойчивого кода

Программные средства поддержки

- САПР Quartus II (работы 4,5)
- Digitek/GM Reliability Analyzer (работы 1-3)
- SciLab / MatLab (работа 2)

Литература

- Черкесов Г.Н. Надежность аппаратно-программных комплексов.
- Рябинин И.А. Надежность и безопасность структурно сложных систем.
- Курочкин Ю.А., Смирнов А.С., Степанов В.А. Надежность и диагностирование цифровых устройств и систем.

Литература

- ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения.
- ГОСТ 27.003-90. Надежность в технике. Состав и общие правила задания требований по надежности
- ГОСТ ЕН 1070-2003. Межгосударственный стандарт. Безопасность оборудования. Термины и определения.

Электронные источники (англ. язык)

- http://www.fault-tree.net – подборка статей и материалов по анализу надёжности

Причины возникновения сбоев и отказов в аппаратуре

- Аппаратура подвержена износу, но его скорость может меняться
- Климатические факторы
  - Повышенная температура
  - Прямые солнечные лучи
  - Влажность
  - Воздействие пыли
- Ударно-вибрационные воздействия
- Аномалии в аппаратуре

Причины недопустимости сбоев

- Серьезный финансовый ущерб, часто превосходящий стоимость системы (например, в промышленности при незапланированных остановках)
- Разрушение объекта управления (например, транспорт)
- Нанесение ущерба окружающей среде (например, атомная энергетика)

Отказоустойчивые системы

Промышленность
Транспорт
Космос
Энергетика

Обширная функциональность

Сбои могут иметь серьезные последствия

Высокая сложность

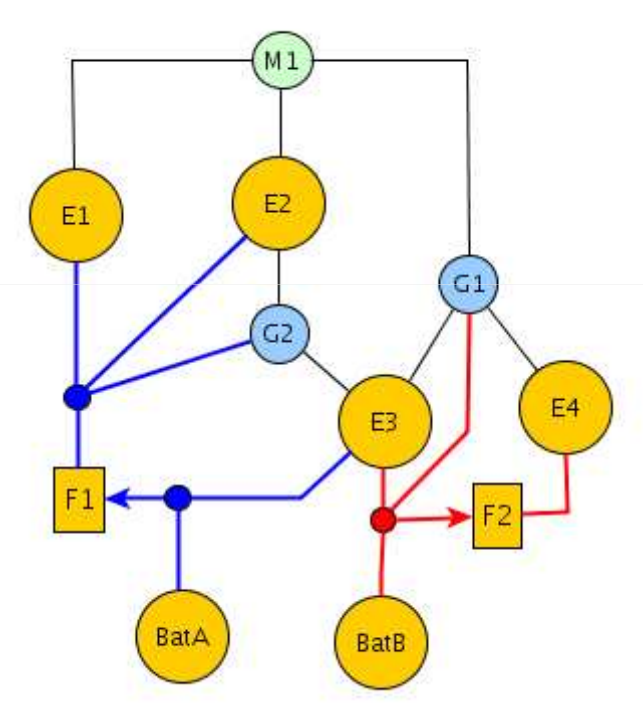
Большое количество сбоев

Недопустимость сбоев

Отказоустойчивые системы

Объекты классической теории надежности

- Элемент (структурный) – атомарный на данном этапе рассмотрения объект, входящий в состав системы
- Система – совокупность соединенных между собой структурных элементов

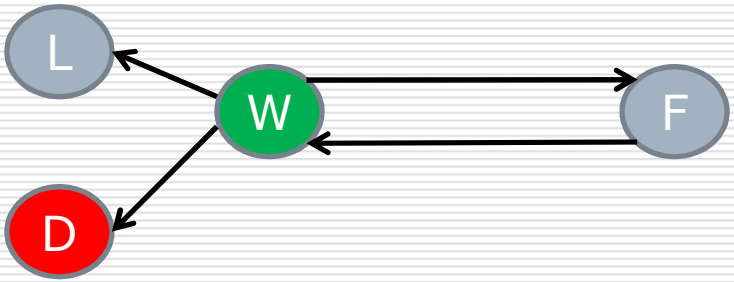


Состояния объектов анализа

- Работоспособен (operational state, work state) – все функции выполняются)
- Неработоспособен (fail state) – хоть одна функция не выполняется)
  - Предельное (limiting) состояние (ремонт невозможен или нецелесообразен)
- Частично работоспособен (в целом работает, но некоторые малозначащие функции не выполняются; отсутствует в классической теории)
- Опасное состояние (dangerous state) – возник ущерб большого масштаба

События в системе

- Отказ (fault) – нарушение работоспособного состояния
  - Сбой (interruption) – самоустраняется через несколько секунд
  - Частичный отказ – вызывает переход в частично работоспособное состояние
- Ресурсный (marginal) отказ – вызывает переход в предельное состояние
- Восстановление (restoration) – возврат в работоспособное состояние



Свойства

- Надежность (dependability) – свойство объекта выполнять все требуемые функции
  - Безотказность (reliability) – работоспособен непрерывно
  - Долговечность (durability) – максимально далеко предельное состояние
  - Ремонтопригодность (maintainability) – приспособленность к восстановлению
  - Сохраняемость (storability) – работоспособен при хранении и транспортировке

Свойства

- Безопасность (safety) – способность функционировать, не причиняя ущерба
- Отказобезопасность (fault safety) – способность не причинять ущерба при отказах
- Ущерб
  - Допустимого масштаба (вред) – остановка
  - Большого масштаба (коллапс) – авария

Свойства

- Отказоустойчивость (fault-tolerance) – способность объекта функционировать при наличии в его составе отказавших элементов
- Живучесть – способность функционировать в форсмажорных условиях

Показатели надежности

- Вероятностные
  - вероятность безотказной работы p(t)
  - вероятность восстановления r(t)
- Временные
  - средняя наработка до отказа MTTF, между отказами (на отказ) MTBF
  - средний срок службы, время восстановления, срок сохраняемости
- Частотные
  - частота отказов f(t) – среднее число отказов в единицу времени
  - интенсивность отказов λ(t) – среднее число отказов в единицу времени при условии, что элемент исправен
- Комплексные
  - коэффициент готовности (средняя вероятность работоспособного состояния)

Связь показателей надежности друг с другом

- f(t)= –dp(t)/dt
- λ(t)=f(t)/p(t)
- MTTF = $\int_0^{+\infty} tf(t)dt$

Режим применения объектов

- Непрерывное длительное применение – большое время требуемого функционирования, но возможен ремонт (приборы общего пользования)
- Показатели
  - средняя наработка между отказами
  - время восстановления
  - коэффициент готовности

Режим применения объектов

- Однократное применение – должен отработать безотказно определенный промежуток времени, а дальше неважно (ракета, автономный космический аппарат)
- Показатели
  - вероятность безотказной работы
  - время восстановления в режиме ожидания

Режим применения объектов

- Многократное циклическое применение – должен отработать безотказно все рабочие циклы (самолет)
- Показатели
  - коэффициент оперативной готовности (коэффициент готовности Х вероятность безотказной работы)
  - среднее время восстановления в режиме ожидания

Показатели безопасности

- Риск – вероятность попадания в опасное состояние
- Нормировка риска – на человека в час
- Группы риска (XII - IV), например, группа IV – $10^{-3} > r \geq 10^{-4}$

Типичные группы риска

- XII – естественная среда обитания
- VIII – общественный и железнодорожный транспорт
- VII – велосипед, бокс, гражданская авиация, автомобиль
- VI – мотоспорт, верхолазы
- V – летчики-испытатели
- IV – скачки, автогонки, альпинизм

Типичные риски

- водные гонки – 8×10^{-4}
- альпинизм – 7×10^{-4}
- горная разработка – 9×10^{-4}
- пожарное дело – 8×10^{-4}
- полиция – 2×10^{-4}
- ...

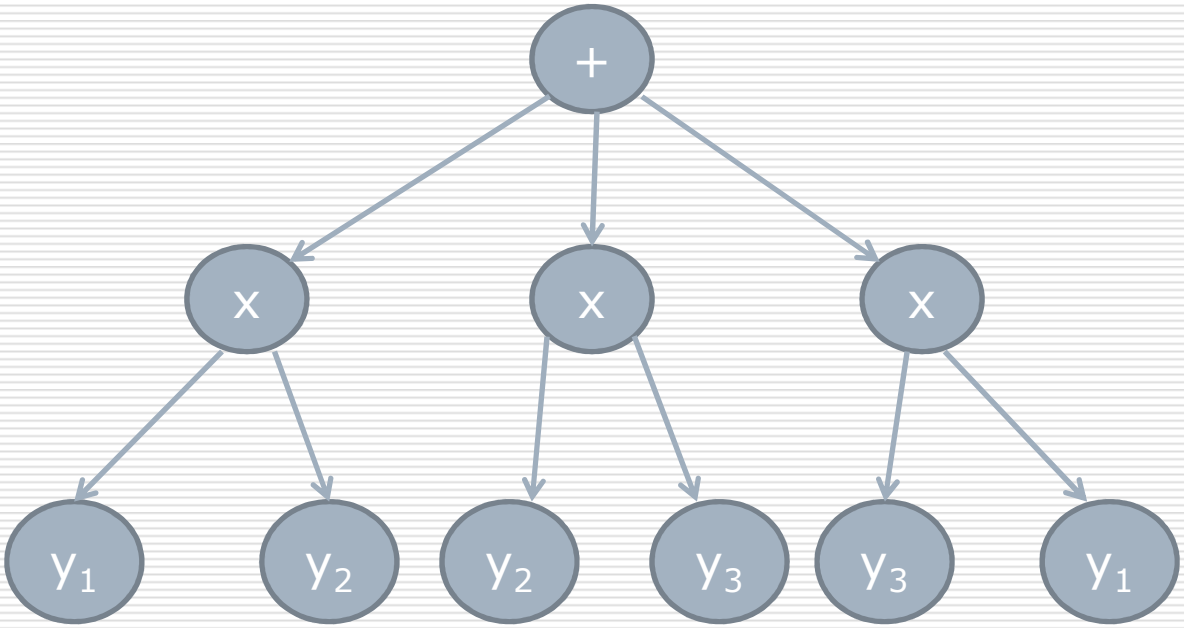
Обзор методов измерения/расчета показателей надежности

- Теория случайных процессов
  - Необходимо знать закон возникновения событий в системе
- Логико-вероятностные методы
  - Необходимо знать вероятности состояний элементов
  - Состояния элементов должны быть независимы
- Имитационное моделирование
  - Необходимо знать (приблизительно) закон возникновения событий в системе
  - Может применяться в ситуации, когда задача не решается аналитически
- Экспериментальные методы
  - Годятся всегда. Но требуют очень много времени. И наличия прототипа, который можно испытывать

Обзор методов расчета показателей надежности (Eng)

- Fault tree analysis (FTA) – аналог логико-вероятностных методов
- Event tree analysis (ETA) – анализ последствий определенных событий
- Failure mode and effects analysis (FMEA) – оценка, чем заниматься в первую очередь
- Markov analysis – графы состояний
- Probabilistic risk assessment (PRA) – аналог ETA, но для безопасности

Fault tree analysis, пример



Event tree analysis

- Пример см. 01_EventTree.pdf (взято с сайта http://www.fault-tree.net)

Показатели надежности современной элементной базы

- Чем надежнее элемент, тем сложнее его надежность определить
- От надежных к ненадежным:
  1. Микросхемы
  2. Платы и связи в составе платы
  3. Межплатные соединения и внешние контакты
  4. Механика

Показатели надежности современной элементной базы

- Измерение показателей безотказности:
  - Одновременное тестирование большой выборки (N) компонентов в течение большого (T) периода времени (однако, существенно меньшего срока службы)
  - Интенсивность отказов: $\lambda \approx n/NT$, где n - число отказавших элементов
  - Более точно: $\lambda < \chi^2(p, 2n+2)/NT$, где p - доверительная вероятность, χ^2 - квантиль распределения хи-квадрат. Чем больше n, тем точнее оценка и тем меньше $\chi^2(p, 2n+2)/n$
  - Пример: n=3, N=10000, T=10000 часов => $\chi^2=15.5$, $\lambda < 1.5 \times 10^{-7}$ 1/час

Показатели надежности современной элементной базы

- Измерение показателей долговечности:
  - испытания проводятся в экстремальных условиях (обычно при повышенной температуре)
  - результат умножается на коэффициент ускорения
  - например, для микросхем 1000 часов испытаний при 125 С эквивалентно 10 годам при 55 С
  - естественно, итог – приблизительный

Показатели надежности современной элементной базы

- MTTF для сравнительно ненадежных компонентов (1 год приблизительно 10000 часов):
  - блоки питания 30000-100000 часов
  - кулеры 50000-400000 часов
  - материнские платы 50000-300000 часов
  - приводы компакт-дисков 50000-100000 часов
  - винчестеры 0.5 млн - 1.5 млн часов
  - ПК в целом - 15000-25000 часов
- Все эти цифры не учитывают износ! Часто срок службы значительно ниже MTTF (например, для винчестеров 5-7 лет)

Показатели надежности современной элементной базы

- FR (failure rate), измеряется в FIT (failure in time, фит) – число отказов в час на 10^9 элементов
  - современные микросхемы: по данным Intel - 20-30 фит, другие производители – 10-100 фит;
  - 15 лет назад: порядка 100-1000 фит;
  - 30 лет назад: порядка 1000-10000 фит
- Период нормальной работы микросхем около 25-30 лет при нормальных условиях (оценка приблизительная!). Далее наступает период старения.
- Срок службы – порядка 50-1000 лет

Показатели надежности современной элементной базы

- Вероятность ошибочной передачи символа по каналу связи:
  - телефонная линия 10^{-2} - 10^{-3};
  - неэкранированная витая пара 10^{-5} - 10^{-6};
  - экранированная витая пара 10^{-7} - 10^{-9};
  - оптоволокно 10^{-11} - 10^{-15};
- Одна из главных проблем - контакты в разъемах

Далее

- Анализ функции работоспособного состояния