Надежность систем и устройств

Лекция 4. Методы повышения надежности, методы структурного резервирования

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

Из чего мы исходим?

- Требования к надежности системы, примеры
  - ВБР за период в 100 суток не менее 99%
  - средняя наработка до отказа не менее 1 года
  - среднее время восстановления не более 1 часа
  - средний срок службы не менее 5 лет
  - среднее число отказов за 5 лет не более 3
  - группа риска VII и выше

Примеры некорректных требований

- система должна работать безотказно не менее 100 суток
- время восстановления не должно превышать 1 час
- должна быть гарантирована безопасность

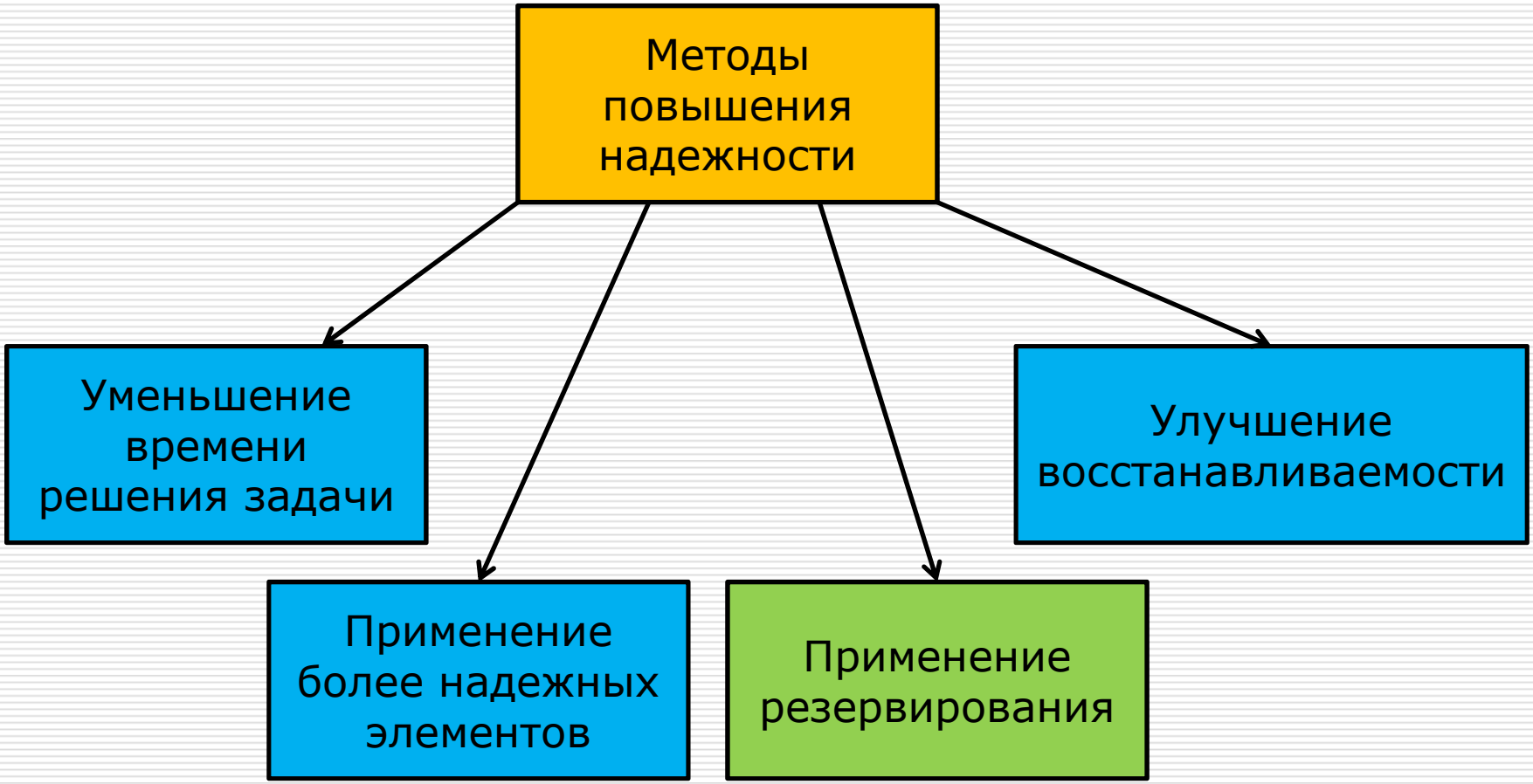
Источники требований

- стандарты (положено!)
- экономические соображения разного рода (сколько может стоить система и каковы потери от ее отказа)
- требования к системе более высокого уровня

Проектирование системы

- Требования к надежности
- Структура системы, элементы системы, характеристики элементов
- Оценка надежности
- Надежность достаточна?
  - если нет, то какими методами надежность можно повысить наиболее дешево

Методы повышения надежности, классификация



Методы повышения надежности, классификация

- Уменьшение времени решения задачи – например, используем более быстрый алгоритм
  - поскольку интенсивность отказов от этого не меняется, вероятность безотказной работы увеличивается
  - даже для систем, работающих непрерывно, интенсивность отказов в режиме ожидания может быть меньше, чем в режиме активной работы
  - таким образом, средняя интенсивность отказов меньше

Методы повышения надежности, классификация

- Применение более надежных в данных условиях элементов – напрямую уменьшая интенсивность отказов
  - например, использование элементов промышленного или военного стандарта вместо элементов коммерческого стандарта
    - 0...70 C
    - -40...85 C
    - -55...125 C

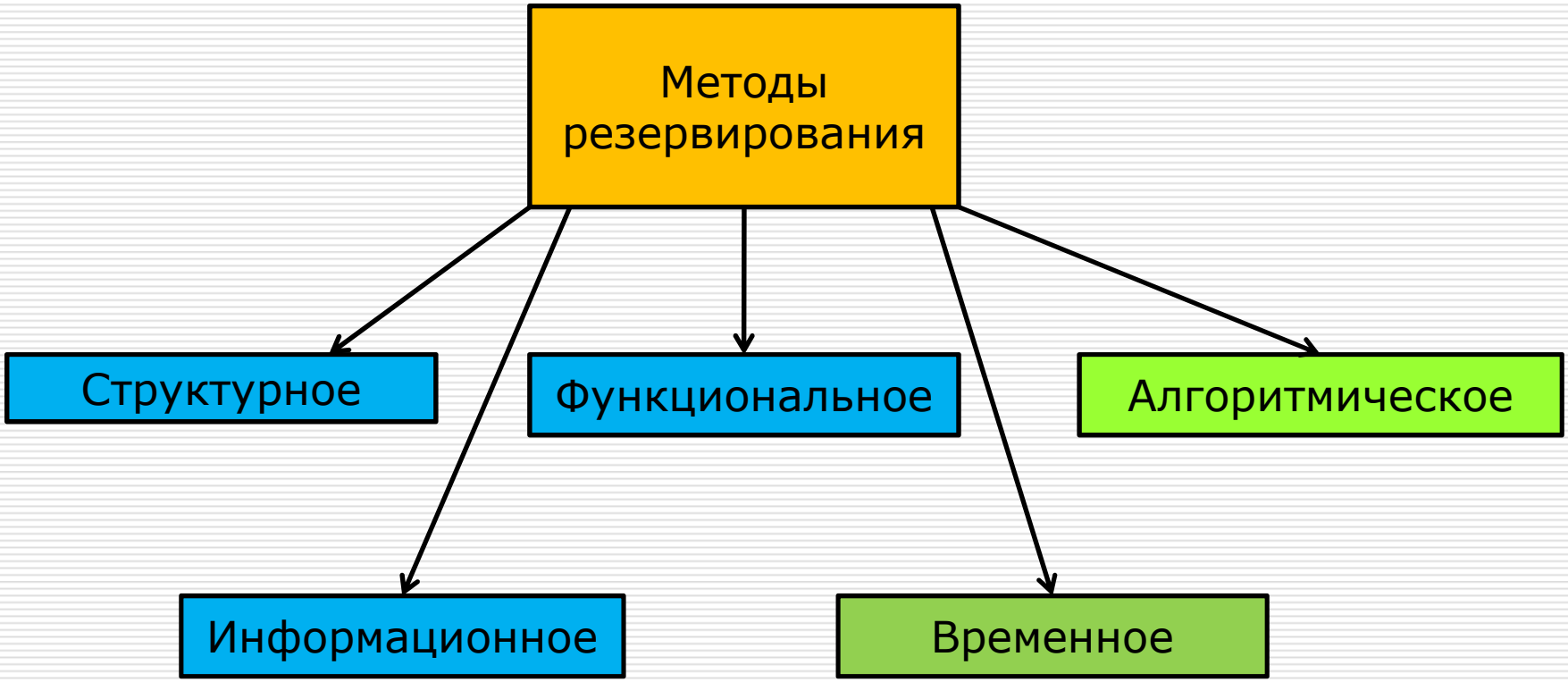
Методы повышения надежности, классификация

- Улучшение восстанавливаемости – увеличиваем интенсивность восстановления, а значит, и коэффициент готовности
  - быстрое время перезапуска системы во многих случаях решит проблему с надежностью (конечно, если короткие паузы в работе в принципе допустимы)

Методы повышения надежности, классификация

- Методы резервирования – используем для повышения надежности дополнительные ресурсы
  - как правило, самый СЛОЖНЫЙ и ДОРОГОЙ в применении способ
  - используется, если все остальные не подходят, нереализуемы, недостаточны

Методы резервирования, классификация



Методы резервирования, классификация (аппаратура)

- Информационное резервирование
  - используются дополнительные линии передачи информации или дополнительные разряды для хранения данных (например, 36 разрядов/линий вместо 32)
  - дешевый и эффективный способ при хранении и передаче данных
  - применяется на ВЫСОКОМ уровне системы (уровень устройств, передач между устройствами)
  - классический пример – CRC-код

Методы резервирования, классификация (аппаратура)

- Структурное резервирование
  - используются дополнительные элементы системы, дублирующие работу уже существующих (два процессора вместо одного)
  - способ дорогой, но в некоторых случаях – единственно возможный
  - примеры – холодный резерв, горячий резерв
- Функциональное резервирование
  - использование многофункциональных элементов, способных перераспределять нагрузку в процессе работы

Методы резервирования, классификация (ПО, АПК)

- Временное резервирование
  - увеличение времени, отведенного на решение задачи (это время может быть использовано, например, для перезапуска системы, или для многократного решения задачи)
- Алгоритмическое резервирование
  - решение задачи несколько раз, несколькими разными способами
- Оба метода эффективны для программного обеспечения или аппаратно-программных комплексов, часто используются в комбинации

Классификация методов структурного резервирования

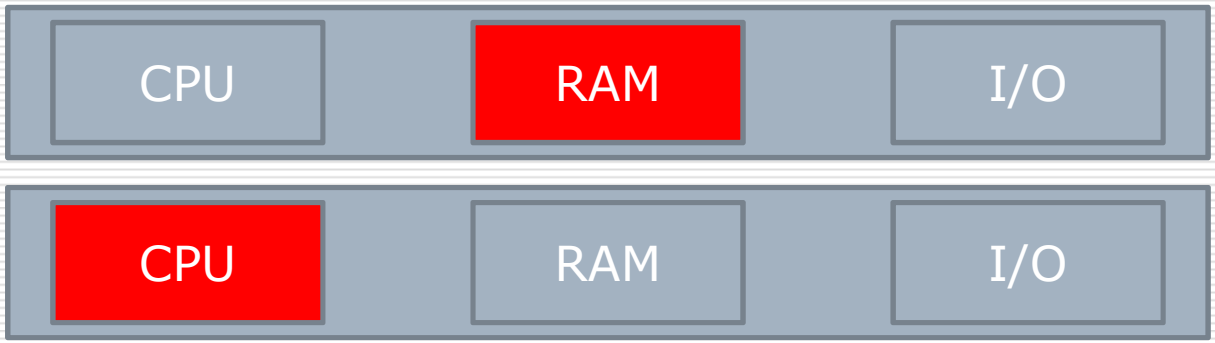
- Признаки классификации
  - Уровень резервирования
  - Кратность
  - Способ подключения резервных элементов

Структурное резервирование, уровень применения

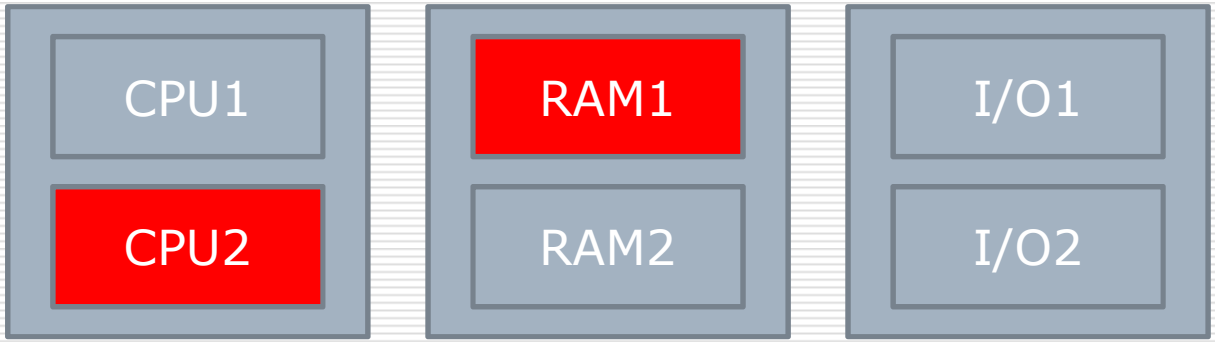
- Общее
  - применяется на уровне всей системы
- Групповое
  - применяется на уровне групп элементов
- Поэлементное
  - применяется на уровне отдельных элементов
- Какой из способов эффективнее?

Структурное резервирование, уровень применения

общее резервирование



поэлементное резервирование



Кратность структурного резервирования

- Отношение количества резервных элементов к числу основных элементов (к минимальному числу элементов, необходимому для работы системы)
- Может быть как целым, так и дробным числом
- Холодный резерв?

Структурное резервирование, подключение резервных элементов

- Включение замещением
  - постоянно в работе только основные элементы, в случае отказа они замещаются резервными (можно провести четкую границу – кто основной, а кто резервный)
- Постоянно включенный резерв
  - постоянно в работе все элементы, в этом случае резервные и основные элементы равноправны (четкую границу провести нельзя)

Включение замещением, варианты применения

- Ненагруженный или холодный резерв
  - до отказа основных элементов резервные элементы выключены (ЗИП), их интенсивность отказов близка к нулевой
  - при отказе основных элементов система останавливается, производится замена, система запускается заново
  - переключение обычно вручную
  - требования
    - понять, что основной элемент отказал (алгоритмы диагностики, время на диагностику)
    - время на остановку, замену и повторный запуск системы ($К_г$ < 100%)

Включение замещением, варианты применения

- Нагруженный или горячий резерв
  - до отказа основных элементов резервные элементы включены и дублируют действия основных элементов (но работают вхолостую)
  - при отказе основных элементов происходит переключение на резервные – вручную или автоматически
  - требования
    - понять, что основной элемент отказал (алгоритмы диагностики, время на диагностику)
    - время на переключение ($К_г < 100\%$)

Включение замещением, варианты применения

- Промежуточные варианты
  - нагружены частично – резервные элементы включены, но в состоянии ожидания
  - выигрывая во времени восстановления, проигрываем в интенсивности отказов, и наоборот

Способы диагностики отказа

- встроенные механизмы диагностики (например, CRC или дублирование)
- безопасный вариант (fail-silent) – система при отказе перестает выдавать данные
- опасный вариант – система выдает данные, но они неверны, и/или поступают с неправильной скоростью
- кто будет определять, что данные неверны?

Включение замещением, достоинства и недостатки

- Достоинства
  - Высокое соотношение стоимости и надежности (особенно для холодного резерва)
- Недостатки
  - Необходимость совершенных механизмов диагностики
  - Затраты времени на переключение элементов (особенно для холодного резерва)
  - Не годятся для систем однократного применения

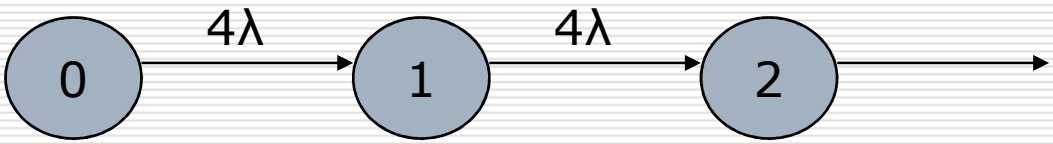
Включение замещением, область применения

- Непрерывное длительное применение (с возможностью ремонта)
- Имеются надежные алгоритмы диагностики, или время диагностики не критично
- Допускаются кратковременные остановки системы (готовность ниже 100%)

Включение замещением, пример

- Четырехпроцессорная вычислительная система. Процессоры идентичны. Все 4 процессора необходимы для работы. Интенсивность отказов любого из процессоров – $\lambda = 0.05$/год. Отказ обнаруживается всегда.
- Элемент замены – процессор, возможны кратковременные остановки системы на его замену.
- Требуется – вероятность безотказной работы в течение $t_0 = 2$ лет не ниже P=90%
- Сколько резервных процессоров?

Включение замещением, пример, решение

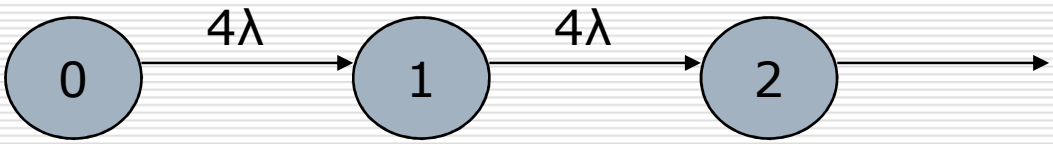


$$P_0'(t) = -4\lambda P_0(t)$$

$$P_1'(t) = 4\lambda P_0(t) - 4\lambda P_1(t)$$

$$P_0(t) = e^{-4\lambda t}, \qquad P_0(t_0)=67\%$$

Включение замещением, пример, решение



$$P_0'(t) = -4\lambda P_0(t)$$

$$P_1'(t) = 4\lambda P_0(t) - 4\lambda P_1(t)$$

$$P_0(t) = e^{-4\lambda t}, \qquad P_0(t_0)=67\%$$

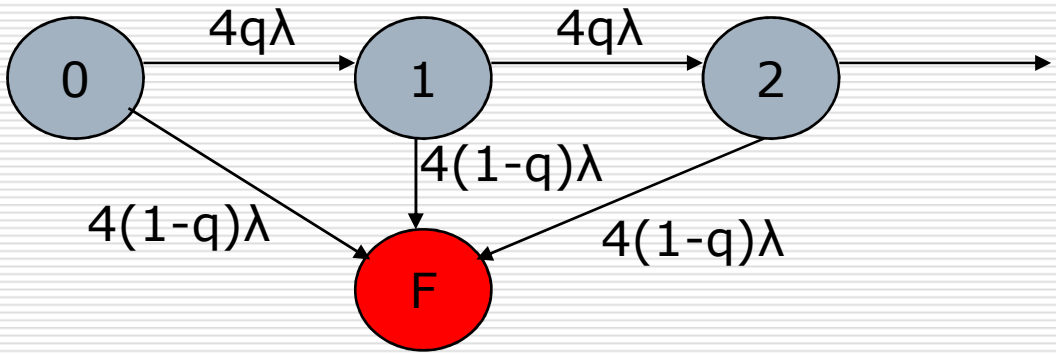
$$P_1(t) = 4\lambda t e^{-4\lambda t}, \; P_1(t_0)=27\%$$

какова кратность?

Включение замещением, пример, развитие задачи

- Как изменится ситуация, если вероятность обнаружения отказа процессора только q=80%?

Включение замещением, пример, развитие задачи, решение



$P_0'(t) = -4\lambda P_0(t)$

$P_1'(t) = 4q\lambda P_0(t) - 4\lambda P_1(t)$

$P_0(t) = e^{-4\lambda t}$, $P_0(t_0)=67\%$

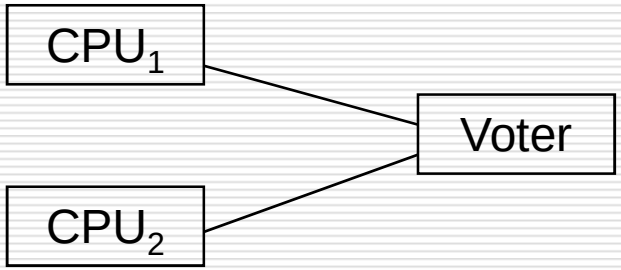
$P_1(t) = 4q\lambda t e^{-4\lambda t}$, $P_1(t_0)=21\%$

Постоянно включенный резерв, особенности применения

- Все элементы работают параллельно
- Для контроля правильности результатов обычно используется голосование
- При отсутствии других механизмов диагностики, для создания отказоустойчивой системы нужно как минимум три устройства
- Для создания системы, обнаруживающей свой отказ, достаточно двух

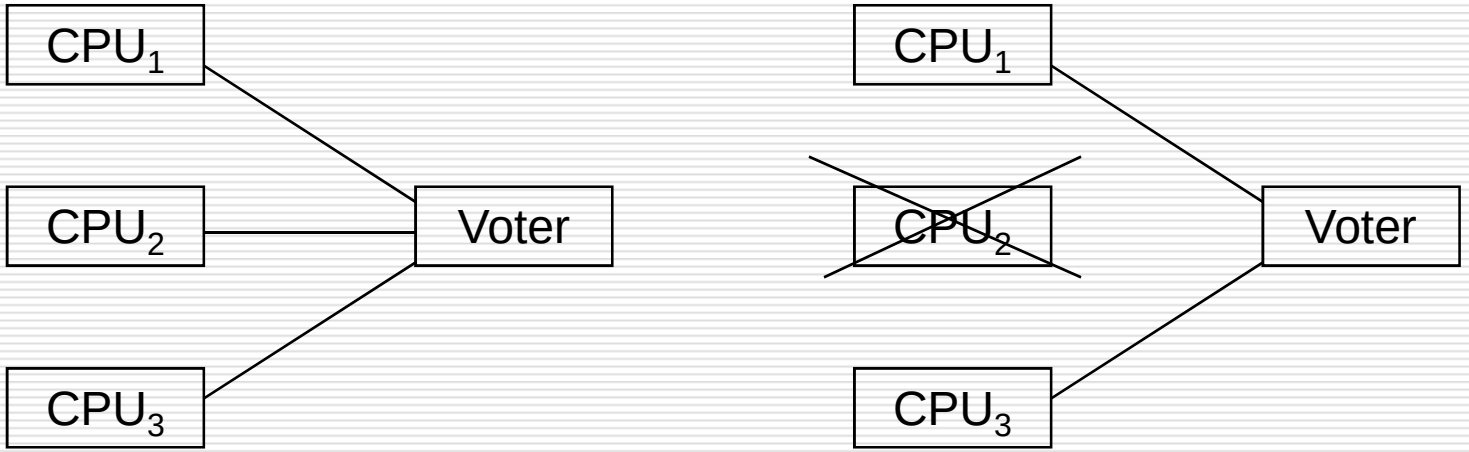
Система, обнаруживающая отказ (Fail-silent модуль)

- Если результаты различны – система включается
- Деградация невозможна



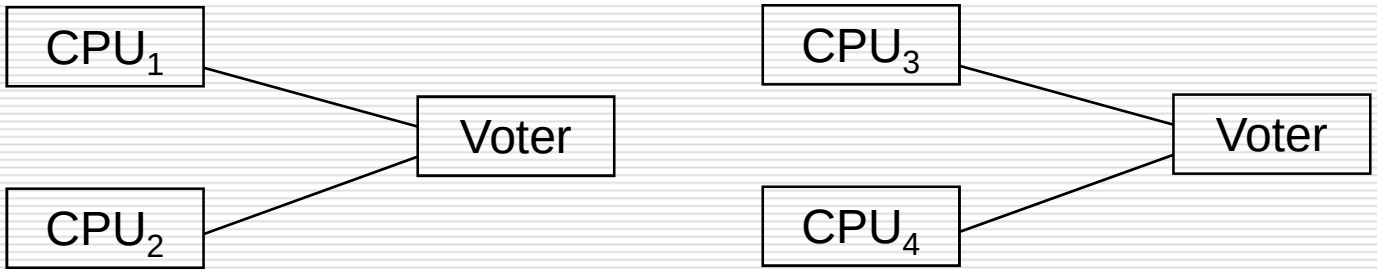
Классическая система с мажоритаром

- Результат, не совпадающий с двумя другими, маскируется
- Возможна деградация до 2 устройств (в fail-silent модуль)



Дублирование fail-silent модулей (fail-operational)

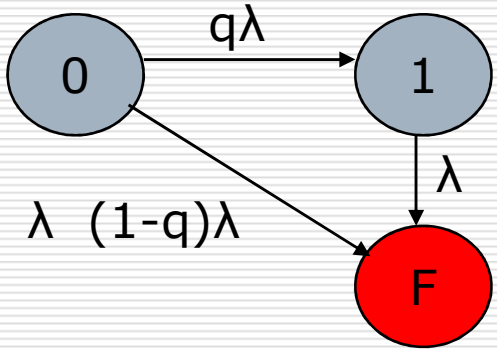
- Если один модуль выключается, вместо него начинает работать второй
- В реализации проще мажорированной схемы



Сравнение двух методов

- Пусть интенсивность отказов процессора $\lambda = 0.05$/год
- Сравнить вероятность безотказной работы за интервал в $t_0 = 5$ лет для системы с включением замещением (2 процессора) и системы с мажоритаром (3 процессора)
- Сопоставить результаты при вероятности успешного обнаружения отказа в системе с включением замещением q=100%, 80%, 50%

Сравнение двух методов, включение замещением



$P_0(t) = e^{-\lambda t}$

$P_1(t) = q\lambda t e^{-\lambda t}$

q	P_0+P_1
1	0.97
0.8	0.93
0.5	0.88

Сравнение двух методов, мажоритар

- $F(S)=e_1e_2+e_2e_3+e_3e_1=$
  $e_1(e_2+e_3)+e_1'e_2e_3=$
  $e_1(e_2'e_3')'+e_1'e_2e_3$
- $P(S)=p(1-(1-p)^2)+(1-p)p^2=$
  $3p^2-2p^3=3e^{-2\lambda t}-2e^{-3\lambda t}=0.875$

Итог сравнения

- Затраты системы с мажоритаром больше в полтора раза
- Ее надежность меньше даже при q=0.5
- Особенности
  - Начиная с p=0.5 ВБР системы меньше ВБР базового элемента
  - среднее время наработки до отказа ухудшается

Сравните с fail-operational вариантом

- Два варианта
  - второй fail-silent модуль в холодном резерве
  - второй fail-silent модуль в горячем резерве

Сравните с fail-operational вариантом

- Два варианта
  - второй fail-silent модуль в холодном резерве ($p=e^{-2\lambda t}+2\lambda t e^{-2\lambda t}$) 0.9
  - второй fail-silent модуль в горячем резерве ($p=2e^{-2\lambda t}-e^{-4\lambda t}$) 0.84

Система с мажоритаром, достоинства и недостатки

- Достоинства
  - Нет необходимости в средствах диагностики
  - Отказобезопасность – вероятность получить неправильный результат очень мала
- Недостатки
  - Большие затраты
  - Проблемы с синхронизацией
    - если у устройств один тактовый сигнал, то они расположены близко в пространстве и с высокой вероятностью откажут одновременно
    - если устройства расположены далеко в пространстве, то один тактовый сигнал сильно уменьшит частоту работы

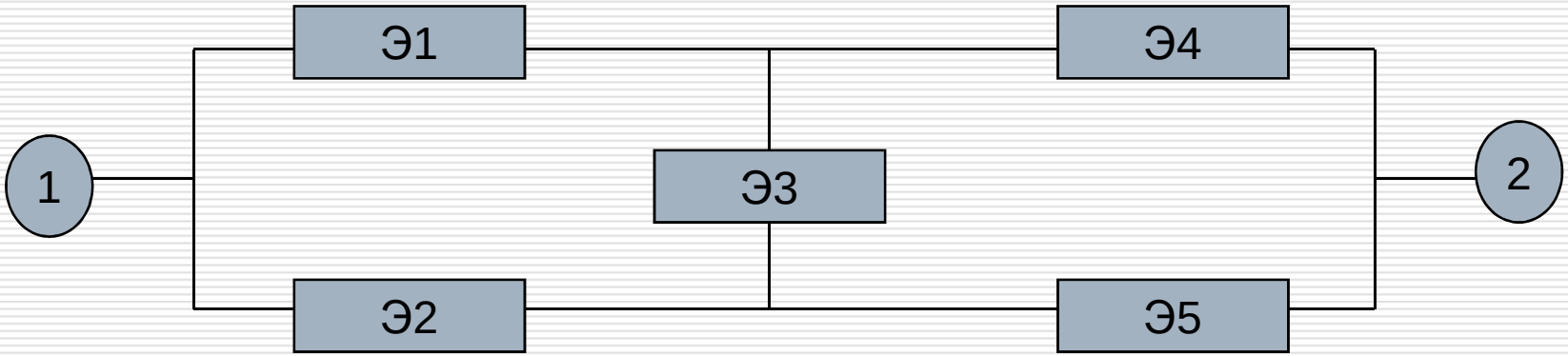
Система с мажоритаром, область применения

- Системы однократного применения
- Любая, где неприменимы более эффективные методы
- На практике – области, где диагностика отказов затруднена, а безопасность и надежность очень важны

Слабые места в структуре системы

- Предположим, у нас имеется некоторая структура, надежность которой недостаточна
- Проблема – с чего начать ее улучшение?
- Ответ – найти элементы, являющиеся слабыми местами, и в первую очередь повысить их надежность, или резервировать их

Способы поиска слабых мест



- $F=E_1E_4+E_1'E_2E_5+E_1E_4'E_2E_5+E_4'E_2'E_1E_3E_5+ E_1'E_5'E_2E_3E_4$
- $P=P_1P_4+(1-P_1)P_2P_5+P_1P_2(1-P_4)P_5+(1-P_4)(1-P_2)P_1P_3P_5+(1-P_1)(1-P_5)P_2P_3P_4$
- Пусть $P_1=92\%$, $P_2=94\%$, $P_3=80\%$, $P_4=86\%$, $P_5=97\%$

Вклад элемента в надежность

- Принять надежность элемента за 100%
- Вклад W = полученное увеличение надежности

Вклад элемента в надежность

- Принять надежность элемента за 100%
- Вклад W = полученное увеличение надежности
- W_1=0.50%, W_2=0.63%, W_3=0.19%, W_4=0.56%, W_5=0.45%
- По аналогии – ущерб
  - принять надежность за 0%
  - ущерб = полученное уменьшение надежности
- Возможно нормирование по стоимости

Структурная важность

- Удобно получать из ОДНФ
  - $F=E_1E_4+E_1'E_2E_5+E_1E_4'E_2E_5+$ $+E_4'E_2'E_1E_3E_5+E_1'E_5'E_2E_3E_4$
- Структурная важность E_i –
  - сумма $2^{-(r-1)}$ для термов с E_i
  - минус сумма $2^{-(r-1)}$ для термов с E_i'
  - здесь r – ранг конъюнкции – число элементов в конъюнкции

Структурная важность

- Удобно получать из СДНФ
  - $F=E_1E_4+E_1'E_2E_5+E_1E_4'E_2E_5+$ $+E_4'E_2'E_1E_3E_5+E_1'E_5'E_2E_3E_4$
- Структурная важность $G(E_i)$ –
  - сумма $2^{-(r-1)}$ для термов с E_i
  - минус сумма $2^{-(r-1)}$ для термов с E_i'
  - здесь r – ранг конъюнкции – число элементов в конъюнкции
- $G_1=G_2=G_4=G_5=0.375$, $G_3=0.125$

Выбор способа поиска слабых мест

- Используем вклад, если нам нужно определить, какой из элементов требует замены
- Используем структурную важность, если нам нужно распределить элементы между местами структуры