

# **Надежность систем и устройств**

---

## **Лекция 5. Методы структурного резервирования (мажорирование)**

**Глухих Михаил Игоревич, к.т.н., доц.**  
**[mailto: glukhikh@mail.ru](mailto:glukhikh@mail.ru)**

# Лабораторная работа №3

---

1. Произвести анализ структурной важности для передающей цепи.
2. Произвести анализ сложной системы управления.
3. Произвести повышение надежности системы управления.
4. Оформить отчет по проделанной работе.

# Лабораторная работа №3

---

- Пример анализа структурной важности передающей цепи (lab1sample)
- Пример анализа структурной важности сложной системы управления (lab3sample и две модификации)

# Рассмотрено на прошлой лекции

---

- Уровни и кратность резервирования
  - Включение замещением (холодный и горячий резерв)
    - требуется надежная диагностика
    - возможны остановки системы
  - Постоянно включенный резерв (схемы с голосованием)
    - большие затраты, низкая надежность
    - требуется надежная синхронизация
-

# Проблема отказобезопасности

---

- Вариант 1 – обнаружили, что в системе что-то не так
  - разные результаты при голосовании
  - отсутствуют выходные данные
- Вариант 2 – отказ не обнаружен
  - неверные данные на выходе системы
- Оба варианта – отказы, но последствия их могут быть различны!

# Возможность отказобезопасности

---

- Управление космическим аппаратом
  - постоянно в полете – постоянно нужны данные
  - даже если отказ обнаружен, сделать, скорее всего, ничего не удастся
- Семафор на железной дороге
  - если обнаружен отказ, можно семафор закрыть, ничего особенно плохого от этого не будет

# Требования к отказобезопасности

---

- Пусть авария системы (из-за получения неверных результатов) представляет собой опасность для жизни оператора. Пусть мы хотим свести риск к VIII группе ( $10^{-7}$  -  $10^{-8}$  1/час), при этом интенсивность отказов системы составляет 0.05/год. Какой должна быть вероятность успешного обнаружения отказа?

# Требования к отказобезопасности

---

## □ Решение

- 0.05 отказов/год  $\sim 5 \cdot 10^{-6}$  отказов/час
- вероятность обнаружения  $p$
- имеем риск  $5 \cdot 10^{-6} \cdot (1-p) < 10^{-7}$
- отсюда  $1-p < 0.02$ , или  $p > 0.98$



# Обнаружение отказа

---

- Системы с резервом
  - если сработала внутренняя диагностика
- Системы с мажоритаром
  - если сам мажоритар в рабочем состоянии, и не произошло случайного совпадения неправильных данных

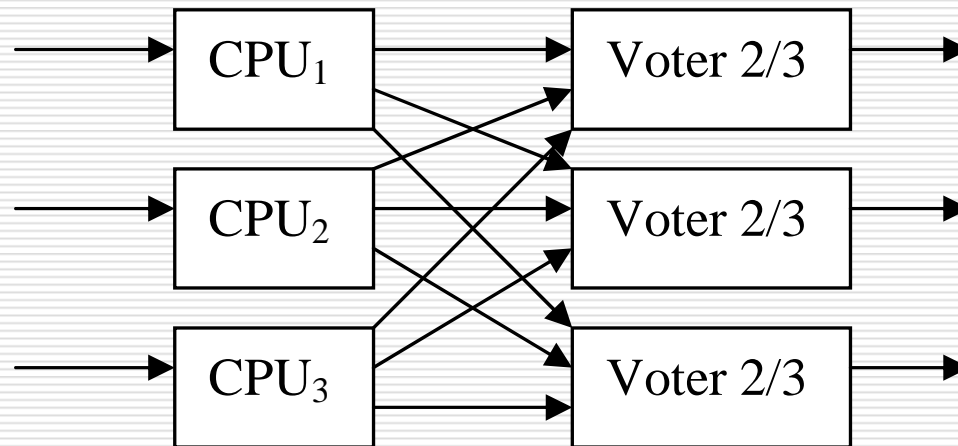
# Схемы с высокой отказобезопасностью

---

- Основные проблемы:
  - схемы внутренней диагностики элементов системы могут давать неверный результат
  - мажоритары также подвержены отказам
- Одно из решений
  - резервирование мажоритаров

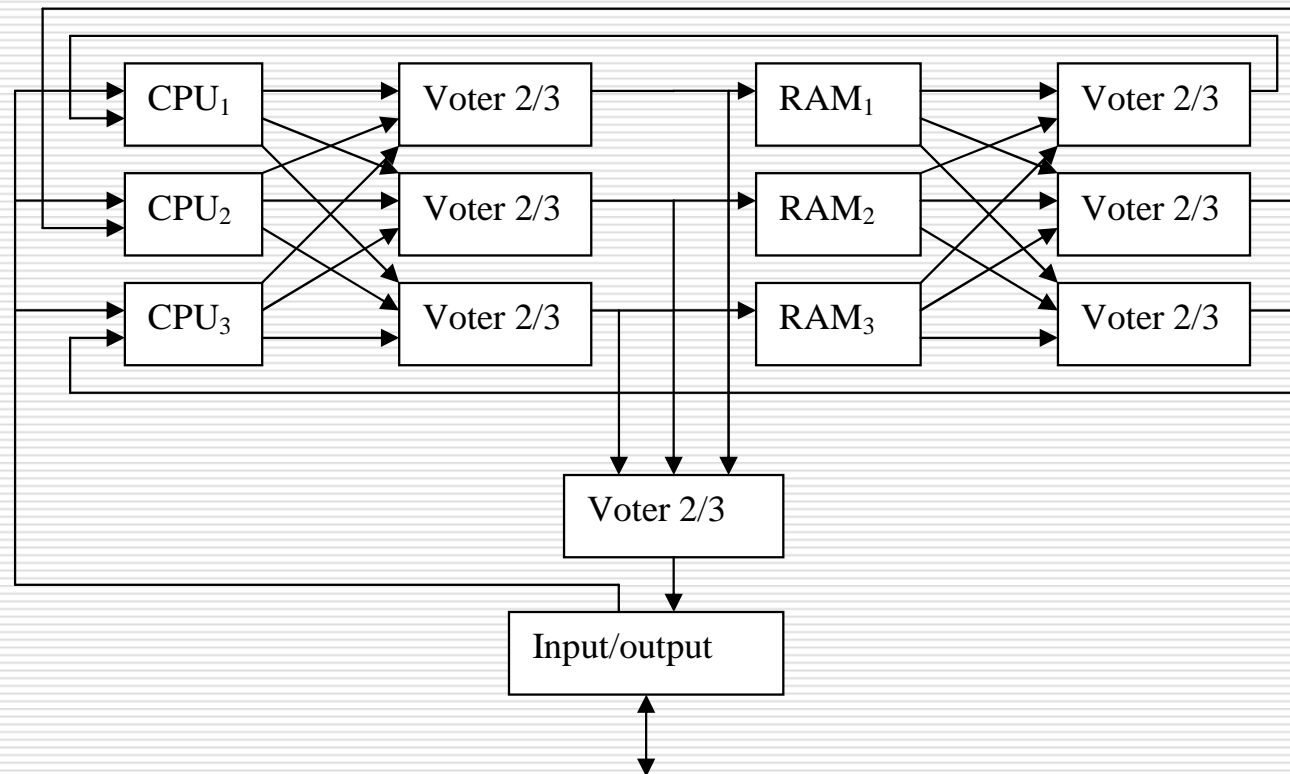
# Схемы с резервированием мажоритарара (три выхода)

---



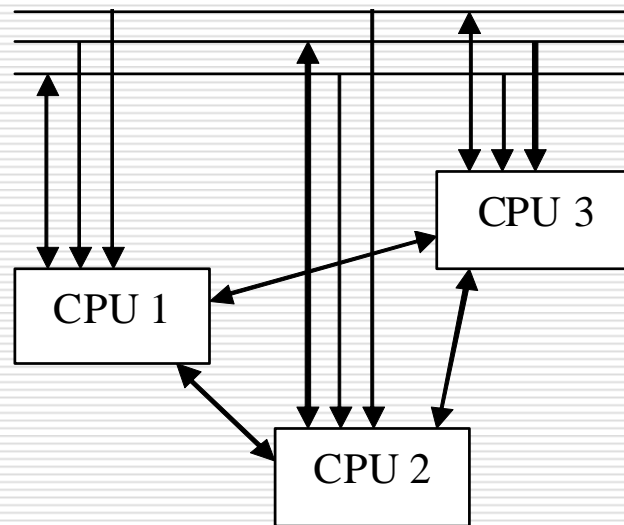
- ❑ Позволяет защититься от отказа мажоритарара
- ❑ Проблема - система имеет 3 результата

# Схемы с резервированием мажоритарара (один выход)



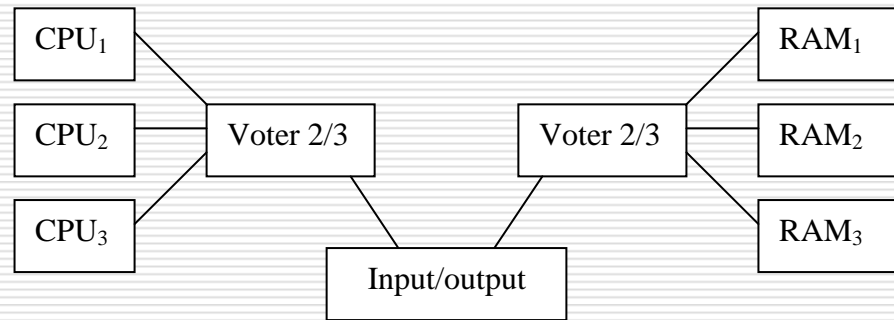
# Схемы с резервированием мажоритарара (общая шина)

---

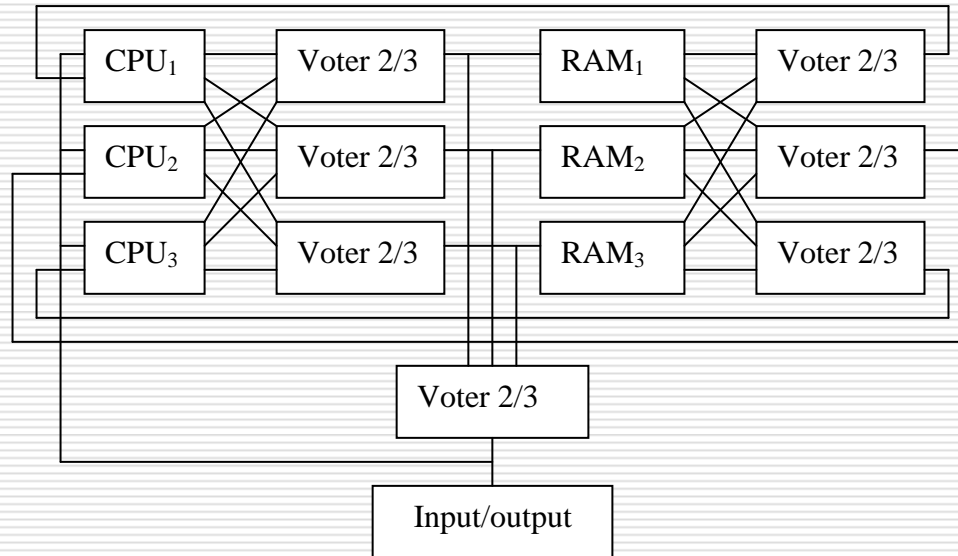


- На входе каждого узла – мажоритар

# Эффект от резервирования мажоритары



- $P_{cpu} = 95\%$
- $P_{ram} = 97\%$
- $P_{vot} = 99.5\%$
- $P_{io} = 99\%$



# Эффект от резервирования мажоритарара

---

## □ Вариант без резервирования

- $P_{sys} = P_{vot}^2 * P_{io} (3P_{cpu}^2 - 2P_{cpu}^3) (3P_{ram}^2 - 2P_{ram}^3)$

- Ответ  $P_{sys} = 97.0\%$

## □ Вариант с резервированием

- $P_{sys} = (3P_{cpu}^2 P_{vot}^2 - 2P_{cpu}^3 P_{vot}^3) (3P_{ram}^2 P_{vot}^2 - 2P_{ram}^3 P_{vot}^3) P_{vot} P_{io}$

- Ответ  $P_{sys} = 97.3\%$

## □ Чем менее надежен мажоритар, тем более полезно его резервирование

---

# Высоконадежные мажорированные системы

---

- ❑ В некоторых случаях надежность системы с простым мажоритаром (три входа) оказывается недостаточной
- ❑ Могут применяться схемы со сложным мажоритаром "М из N"



# Сложные мажоритары

---

- На входе мажоритары  $N$  результатов
- Алгоритм абсолютного большинства
  - верными считаются  $M > N/2$  совпавших результатов
- Алгоритм относительного большинства
  - верными считаются совпавшие результаты, образующие группу максимального размера
- Деградация
  - если устройство систематически дает неверные результаты, оно выключается, система переходит в режим с  $N-1$  устройством

# Пример

---

- ❑ Система включает 4 процессора и мажоритар
- ❑ Мажоритар считается абсолютно надежным
- ❑ Интенсивность отказов процессора 0.05 отказов в год
- ❑ Система может деградировать до конфигурации с двумя процессорами (после этого очередной отказ приводит к отказу системы)
- ❑ Одновременный отказ двух и более устройств считается невозможным.
- ❑ Рассчитать вероятность безотказной работы системы за 5 лет

# Решение

---

- $F = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$
- $F = x_1(x_2 + x_3 + x_4) + x_1'(x_2x_3 + x_2x_4 + x_3x_4)$
- $F = x_1(x_2'x_3'x_4')' + x_1'x_2(x_3 + x_4) + x_1'x_2'x_3x_4$
- $F = x_1(x_2'x_3'x_4')' + x_1'x_2(x_3'x_4')' + x_1'x_2'x_3x_4$
- $P(S) = p(1 - (1-p)^3) + p(1-p)(1 - (1-p)^2) + p^2(1-p)^2$
- $P(S) = 3p^4 - 8p^3 + 6p^2$
- $p = 77.9\% \quad P(S) = 96.4\%$
- для сравнения  $P_3(S) = 87.5\%$

# Адаптивные алгоритмы голосования

---

- Позволяют принять решение в ситуации, когда есть два ответа, за которых проголосовало одинаковое количество устройств (самый простой вариант: 1+1)
- Используют
  - диагностическую информацию о состоянии устройства, сформированную независимой системой диагностики
  - статистическую информацию о количестве неверных результатов ранее
  - в зависимости от этого один из результатов объявляется правильным

# Пример

---

- 3 процессора, 1 мажоритар, вероятность успешной диагностики отказа процессора 80%, интенсивность отказов 0.05/год
- Найти вероятность безотказной работы системы за 5 лет

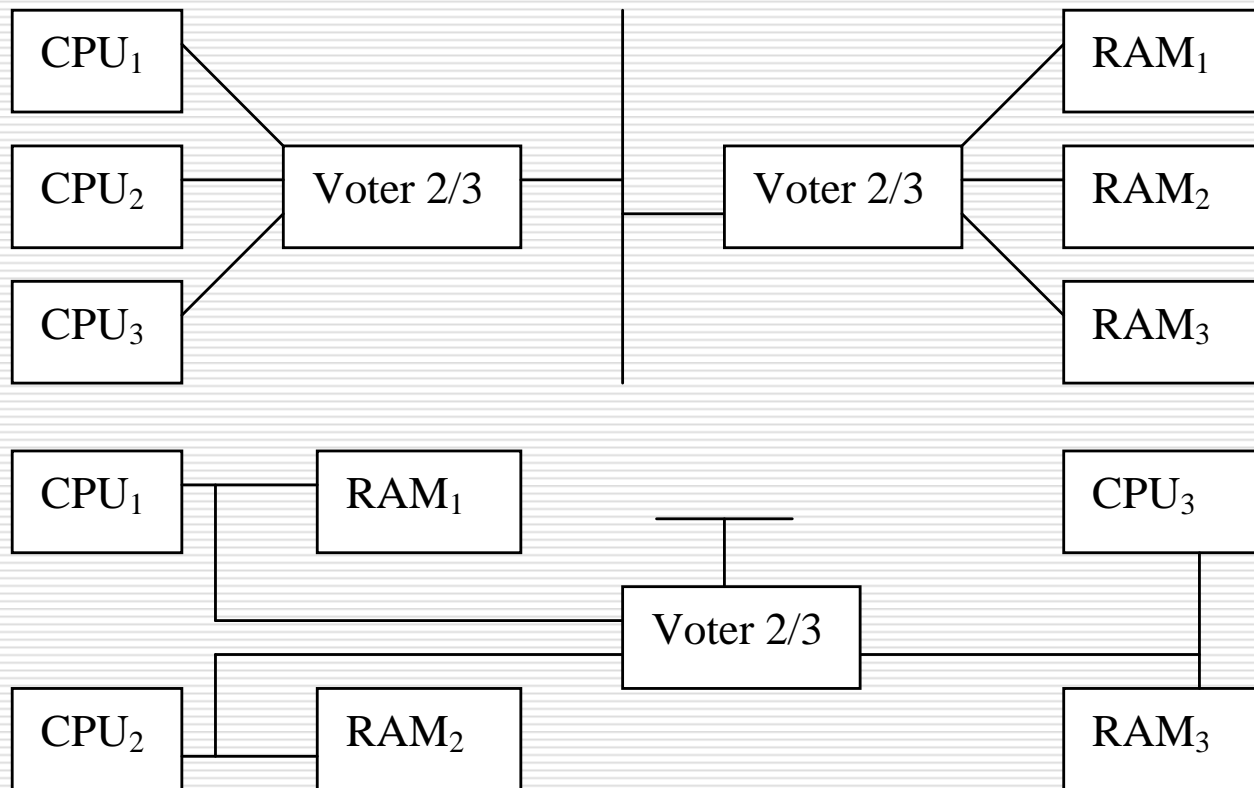
# Решение

---

- $F = dx_1 + dx_2 + dx_3 + x_1x_2 + x_1x_3 + x_2x_3$
- $F = d(x_1 + x_2 + x_3) + d'(x_1x_2 + x_1x_3 + x_2x_3)$
- $F = d(x_1'x_2'x_3')' + d'x_1(x_2 + x_3) + d'x_1'x_2x_3$
- $F = d(x_1'x_2'x_3')' + d'x_1(x_2'x_3')' + d'x_1'x_2x_3$
- $P(S) = r(1 - (1-p)^3) + p(1-r)(1 - (1-p)^2) + p^2(1-p)(1-r)$
- $P(S) = 3p^2 - 2p^3 + r(3p - 6p^2 + 3p^3)$
- $p = 77.9\% \quad r = 80\% \quad P(S) = 96.6\%$

# Выбор уровня мажорирования

---



# Выбор уровня мажорирования

---

- Критерий: требуемая надежность при минимальной стоимости. Или (реже): максимальная надежность при ограниченной стоимости.
- Выбор из небольшого числа вариантов: путем перебора
  - начинаем с самого дешевого, проверяем его надежность
  - если недостаточна, смотрим более дорогие



# Пример

---

- $P_{cpu} = 95\%$
- $P_{ram} = 97\%$
- $P_{vot} = 99.5\%$
- Требуется  $P_{sys} = 98\%$

# Решение

---

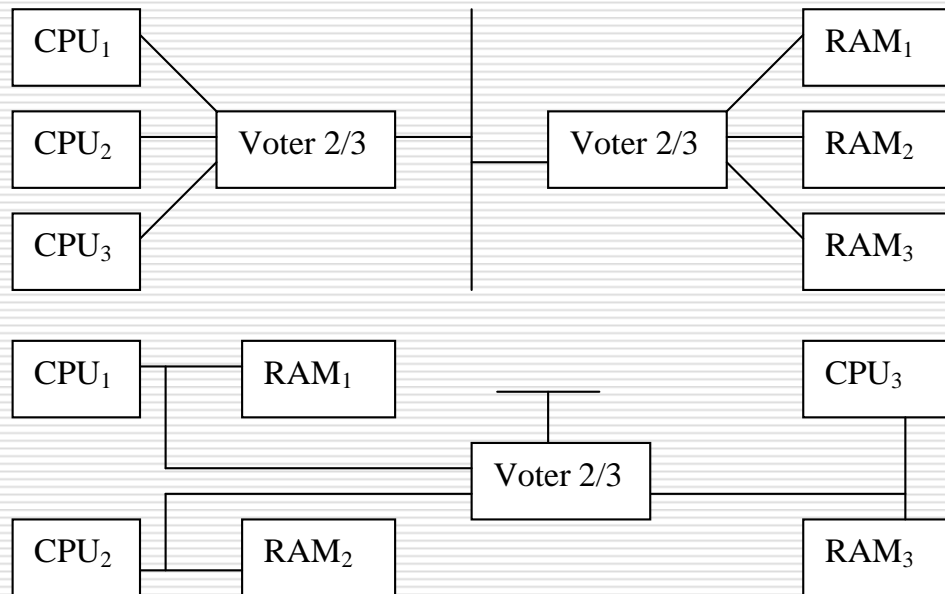
## □ Общее резервирование

- $P_{c+r} = P_{cpu} P_{ram} = 92.2\%$
- $P_{sys} = P_{vot} (3P_{c+r}^2 - 2P_{c+r}^3) = 97.8\%$
- недостаточно

## □ Групповое резервирование

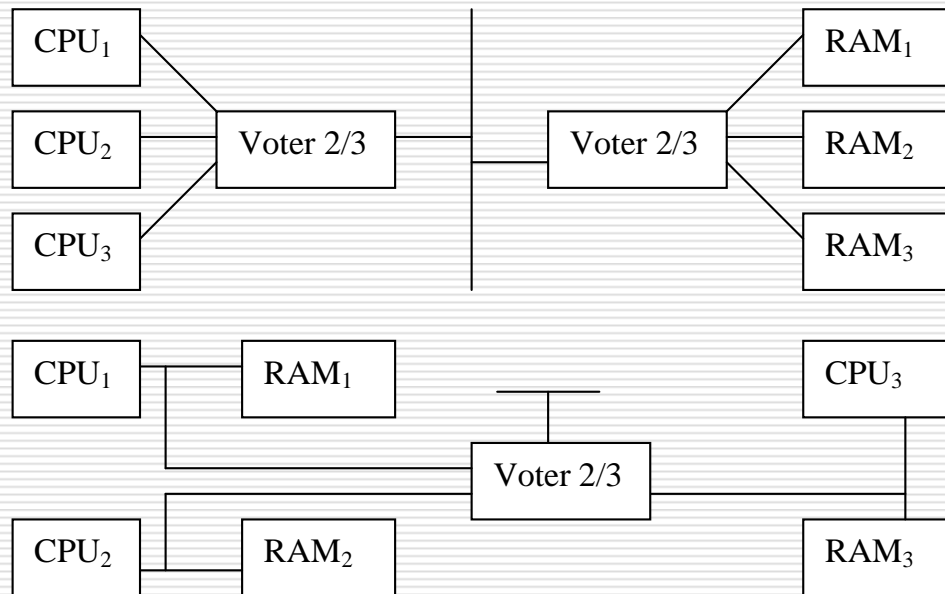
- $P_{sys-c} = P_{vot} (3P_{cpu}^2 - 2P_{cpu}^3) = 98.8\%$
- $P_{sys-r} = P_{vot} (3P_{ram}^2 - 2P_{ram}^3) = 99.2\%$
- $P_{sys} = P_{sys-c} P_{sys-r} = 98.0\%$
- достаточно

# Выбор уровня для адаптивного мажоритарара



- $P_{cpu} = 95\%$
- $P_{ram} = 97\%$
- $P_{vot} = 99.5\%$
- $P_{cpu\_diag} = 60\%$
- $P_{ram\_diag} = 90\%$
- Надо  $P_{sys} = 99\%$

# Выбор уровня для адаптивного мажоритарара



- $P_{cpu} = 95\%$
- $P_{ram} = 97\%$
- $P_{vot} = 99.5\%$
- $P_{cpu\_diag} = 60\%$
- $P_{ram\_diag} = 90\%$
- Надо  $P_{sys} = 99\%$

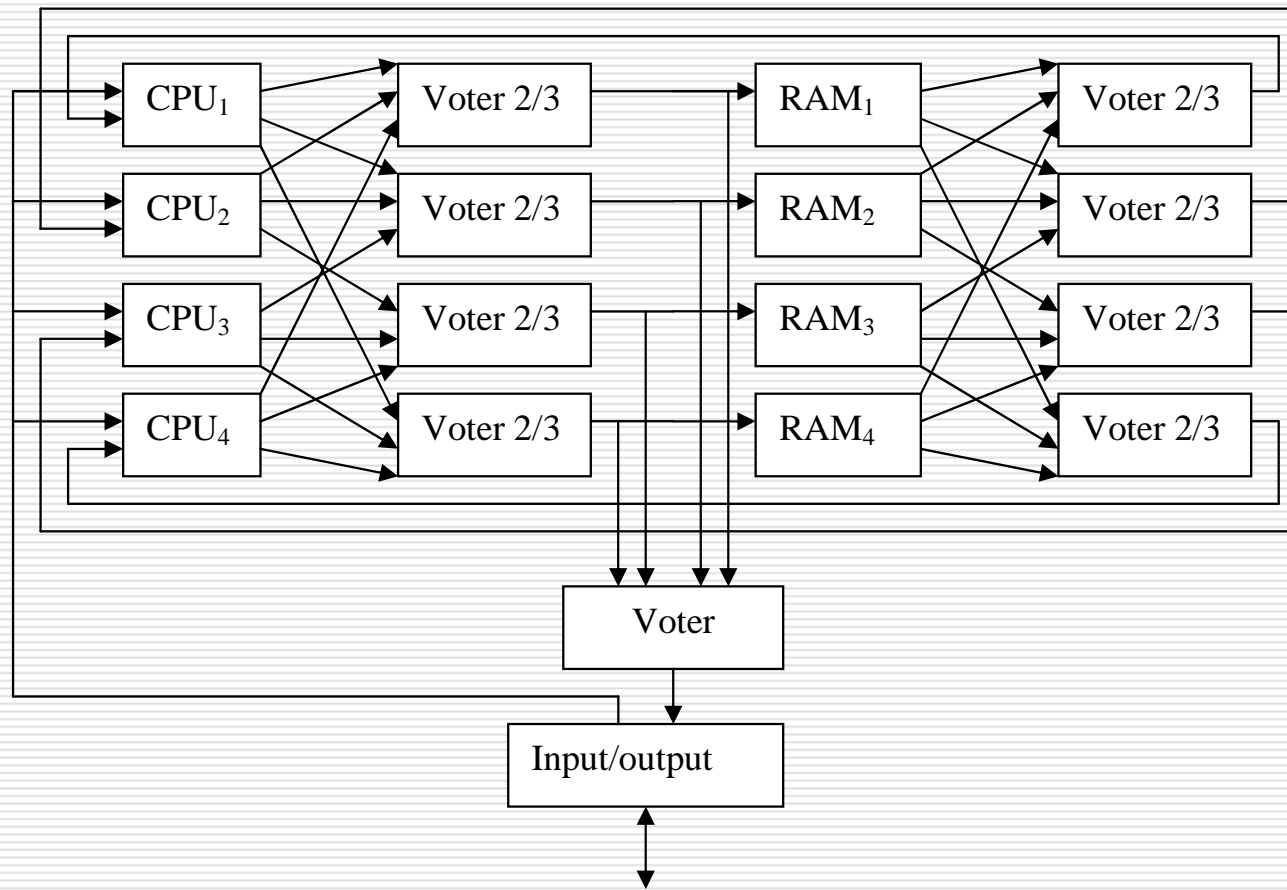
Попробуйте решить самостоятельно

# Масштабируемая система с резервированием

---

- ❑ Идея: добавлять устройства в систему, не усложняя мажоритар, но увеличивая общую надежность
- ❑ Реализация: на вход мажоритары подключаются не все имеющиеся устройства, а только часть из них (например, 3 процессора из 4)
- ❑ Соединение устройств и мажоритаров идет «по кольцу» (2: 1, 2, 3; 3: 2, 3, 4; 4: 3, 4, 1; 1: 4, 1, 2) - присоединяется устройство с тем же номером и соседние

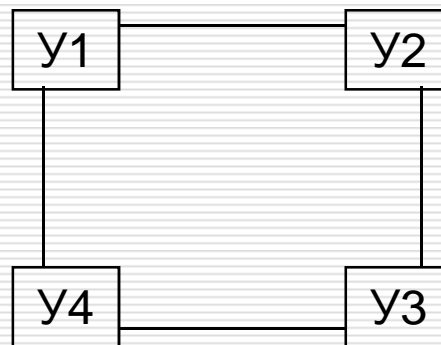
# Масштабируемая система с резервированием



# Пример

---

- Рассмотрим систему на рисунке. Система считается работоспособной, когда в рабочем состоянии два соседних узла. Интенсивность отказов  $0.05/\text{год}$ . Рассчитать вероятность безотказной работы за 5 лет



# Решение

---

- $F = x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4$
- $F = x_1(x_2 + x_4) + x_1'x_3(x_2 + x_4)$
- $F = x_1(x_2'x_4')' + x_1'x_3(x_2'x_4')'$
- $P(S) = (p + p(1-p))(1 - (1-p)^2)$
- $P(S) = p^4 - 4p^3 + 4p^2$
- $p = 77.9\% \quad P(S) = 90.5\%$
- Для сравнения – система "2 из 3"
  - $P(S) = 87.5\%$



# Достоинства масштабируемой системы

---

- ❑ Сложность мажоритаров не увеличивается с ростом числа устройств в системе - мажоритары перестают быть слабым звеном
- ❑ Возможно увеличение кратности резервирования без изменения структуры существующих устройств

# Реализация мажоритаров

---

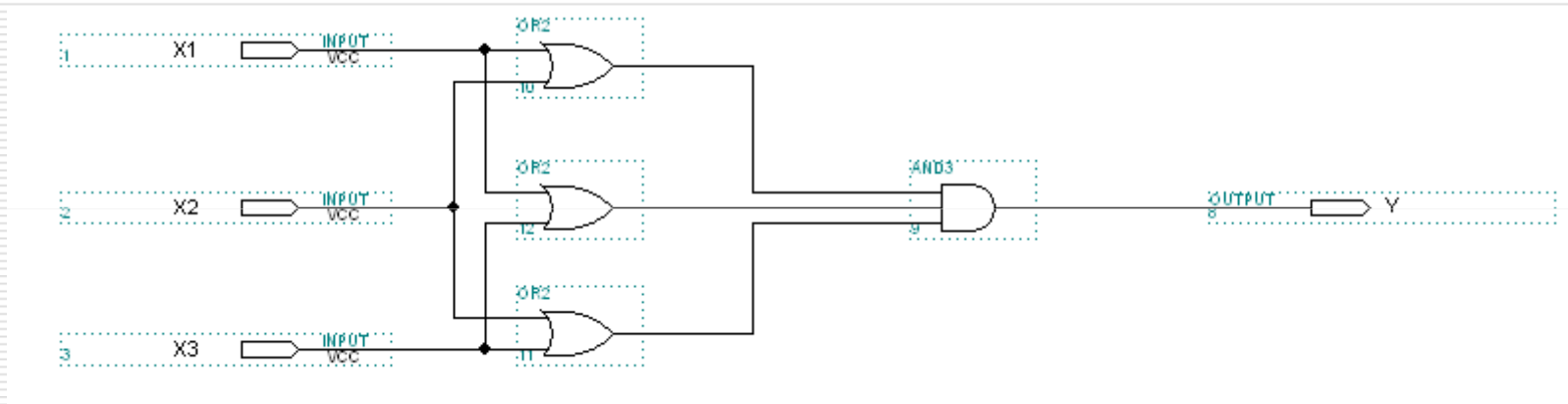
- Побитная – мажорируем каждый бит отдельно
- Шинная – мажорируем содержимое всей шины разом

# Реализация мажоритаров

---

- Побитная – мажорируем каждый бит отдельно
  - меньше затраты
  - но есть вероятность ошибки! Чему она равна?
  - применяется на низком уровне (регистровые передачи)
  
- Шинная – мажорируем содержимое всей шины разом
  - затраты выше
  - вероятность ошибки очень низка
  - применяется на высоком уровне (передачи между устройствами)

# Побитный мажоритар



# Шинный мажоритар

---

- Разрабатываем совместно

# Лабораторная работа №4

---

- Реализовать в среде Quartus II структуру сложного мажоритарара (например, "М из N", адаптивного, с выбором побитный/шинный)
- Промоделировать ее работу, используя готовый генератор сигналов и генератор ошибок