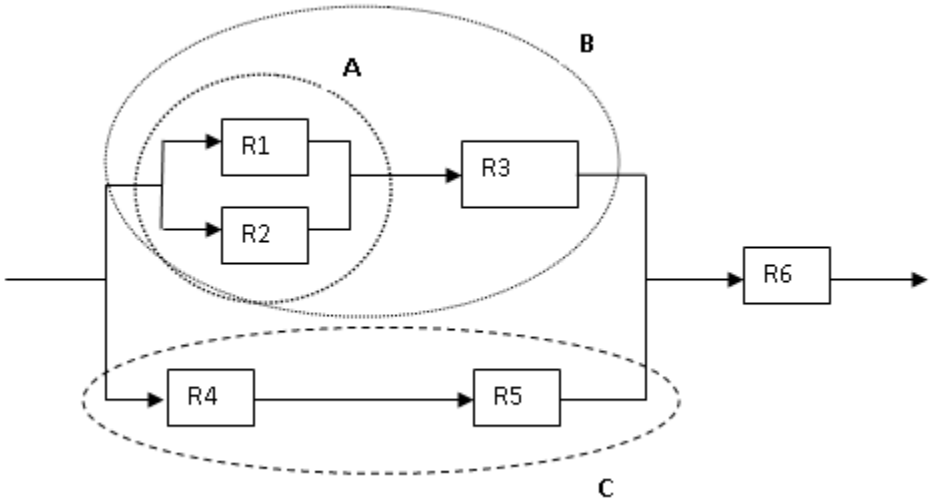
Reliability of Technical Systems

Main Topics

1. Short Introduction, Reliability Parameters: Failure Rate, Failure Probability, etc.
2. Some Important Reliability Distributions
3. Component Reliability
4. Introduction, Key Terms, Framing the Problem
5. System Reliability I: Reliability Block Diagram, Structure Analysis (Fault Trees), State Model.
6. System Reliability II: State Analysis (Markovian chains)
7. System Reliability III: Dependent Failure Analysis
8. Data Collection, Bayes Theorem, Static Redundancy
9. Combined Redundancy, Dynamic Redundancy; Advanced Methods for Systems Modeling and Simulation I: Petri Nets
10. Advanced Methods for Systems Modeling and Simulation II: Object-oriented modeling and MC modeling
11. Human Reliability Analysis
12. Software Reliability, Fault Tolerance
13. Case study: Building a Reliable System

Combined Series-Parallel System

- Most technical systems contain components both in both series and parallel.
- Such systems need to be broken down in series and parallel subsystems.
- Finally the reliability of the system may be obtained based on the relationship among the subsystems.



Try to compute the reliability of system :

$R_A=[1-(1-R1)(1-R2)]$

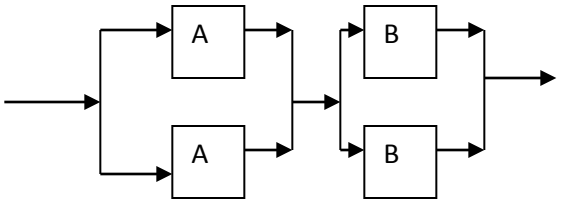
$R_B = R_A\ R3$

$R_C= R4R5$

$R_S=[1-(1-R_B)(1-R_C)]R6$

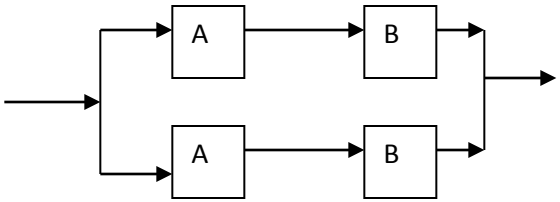
Combined Series-Parallel System

• **Low Level Redundancy**: Each component comprising the system may have one or more parallel components.
- Assume each component has reliability R



$$R_{low} = [1-(1-R)^2]^2 = (2R-R^2)^2$$

• **High Level Redundancy**: The entire system may be placed in parallel with one or more identical system.
- Assume each component has reliability R



$$R_{high} = [1-(1-R^2)^2] = 2R^2 - R^4$$

Combined Series-Parallel System

• By comparing the two reliability, it may be said that the reliability of low level redundancy is greater than the reliability of the high-level redundancy. It may be seen below:

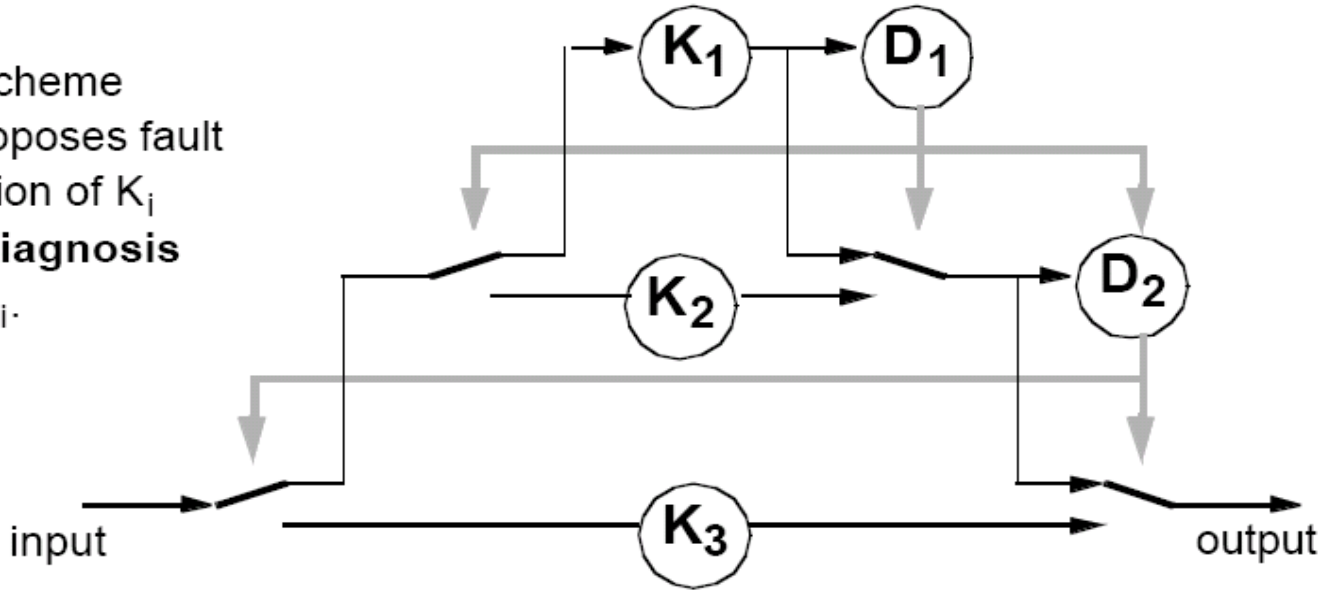
$$(R_{low} - R_{high}) = (2R - R^2)^2 - (2R^2 - R^4)$$
$$= 2R^2(R^2\text{-}2R + 1) = 2R^2(R\text{-}1)^2 \geq 0$$

Dynamic Redundancy

Dynamic Unused Redundancy

First, only the primary component K_1 is in operation.
When K_1 becomes faulty, it is replaced by the **spare** component K_2.
When K_2 becomes faulty, it is replaced by the **spare** component K_3.
etc.

This scheme presupposes fault detection of K_i by a **diagnosis unit** D_i.



Dynamic Redundancy

Activation of Redundancy

Use of redundant means/resources for fault tolerance.

Recall, **static redundancy** denotes redundant means/resources, which perform the specified function during the whole time of operation.

Example: 2-out-of-3 system.

Dynamic redundancy: denotes redundant means/resources, which perform the specified function after fault occurrence
(and detection and a possible exceptional operation).

For dynamic structural redundancy we distinguish:

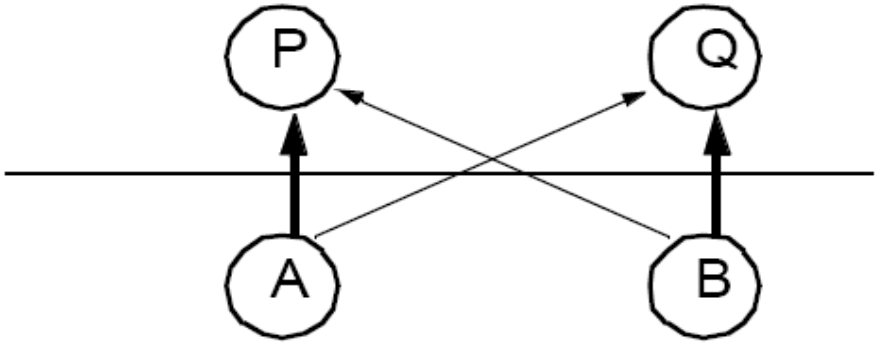
- **Primary** component
- **Spare** or **stand-by** component — so-called hot stand-by
  — so-called cold stand-by

Dynamic Redundancy

Use of Spare Components

Before spare components are activated on fault occurrence they can be used for different purposes:

- **Unused redundancy**: no further use.
- **use-outside redundancy**: Spare components perform the functions of a different subsystem.
- **Mutual redundancy**: The components can substitute each other. This enables **graceful degradation**.

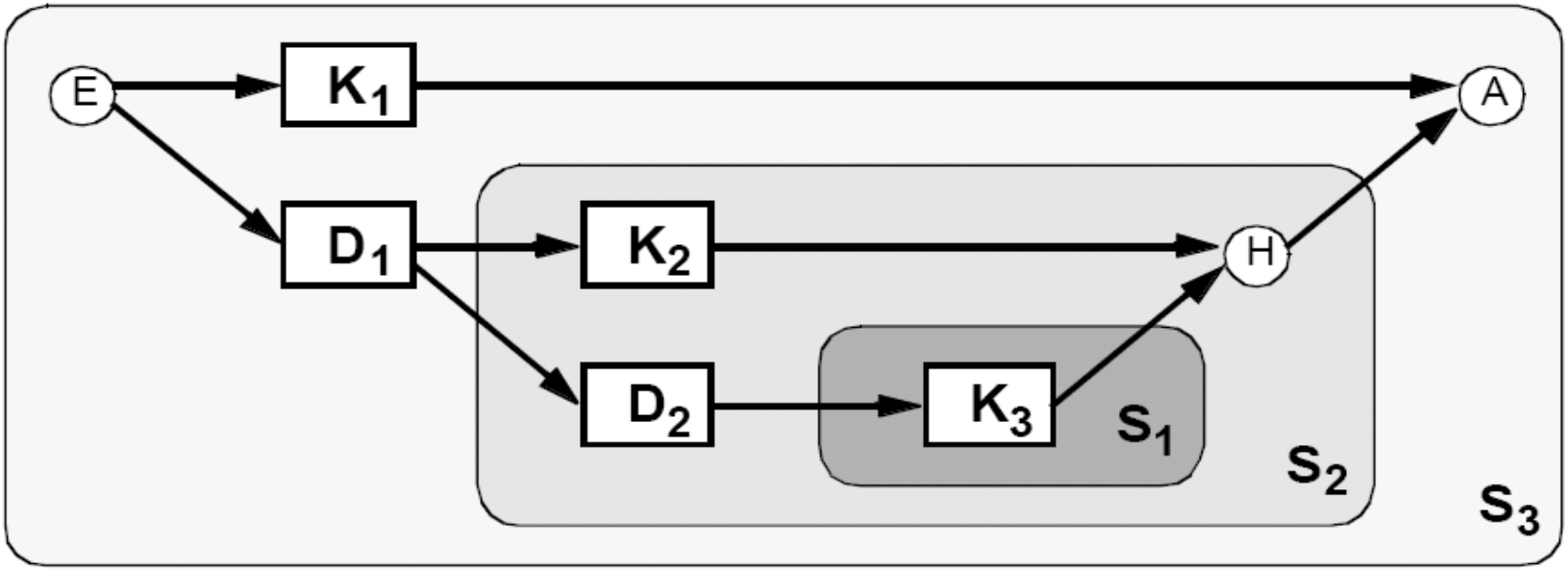


A and B are mutually redundant

Dynamic Redundancy

Dynamic Unused Redundancy

Reliability diagram: It should be noticed that a fault can occur in a spare component even before it is activated.



S_i denotes a dynamically redundant system consisting of i components.

Dynamic Redundancy

Dynamic Unused Redundancy

Assumptions: All components $K_1, \ldots, K_n$ have the **same** function probability $\varphi(K_i) = \phi$. All diagnosis units $D_1, \ldots, D_{n-1}$ have the function probability, i. e. the **fault coverage**, $\varphi(K_i) = \delta$.

The **system function probability** can be obtained by recursive binary distinction of fault cases: $\varphi(S_i) = \phi + \bar{\phi}\delta S_{i-1}$, where $\varphi(S_1) = \phi$.

Here: $\varphi(S_2) = \phi + \bar{\phi}\delta\phi$ $\varphi(S_3) = \phi + \bar{\phi}\delta(\phi + \bar{\phi}\delta\phi) = \phi + \bar{\phi}\delta\phi + \bar{\phi}^2\delta^2\phi$

In general: $\varphi(S_n) = \phi \sum_{i=0}^{n-1} \bar{\phi}^i \delta^i$

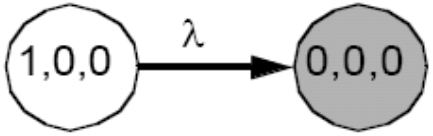
Calculation of the **reliability**:
Components: $\phi = e^{-\lambda t}$ **time dependent**. Fault coverage: δ **constant**.

$R_S(t) = e^{-\lambda t} \cdot \sum_{i=0}^{n-1} (1 - e^{-\lambda t})^i \delta^i$ Negative gradient: $\frac{dR_S(0)}{dt} < 0$.

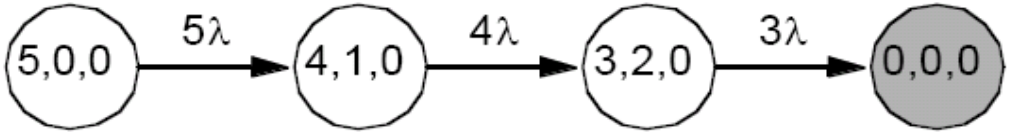
Redundancy

Simple State Models for Comparison Purpose

non-redundant **simplex system**:



purely statically redundant **n-out-of-m system** with n = 3 and m = 5:



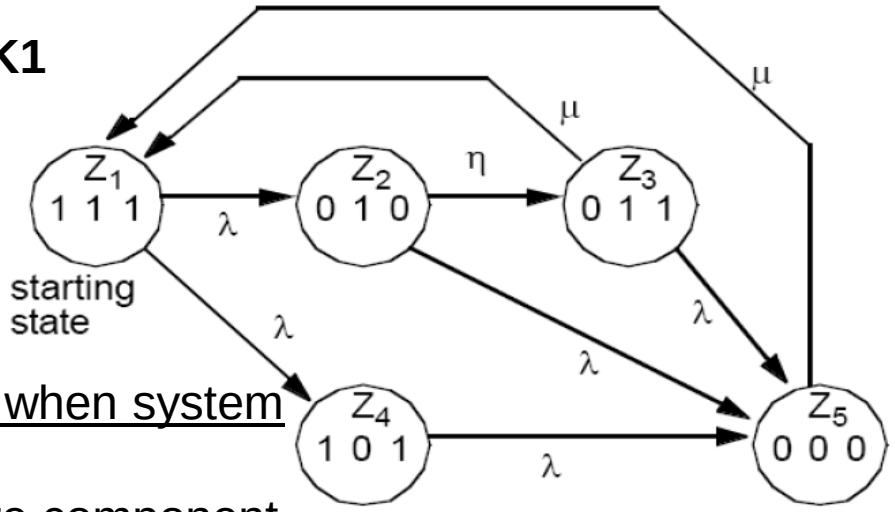
There are no spare components.

The different failed states of the system are not distinguished here.

Redundancy

Application of the State Model:
Calculation of the availability or similar measures (Example)

System consists of a primary component **K1** and a spare component **K2.**
System is faultless (b=1) or not (b=0)
Each state is defined by (K1, K2, b).



Z_2 : models the failure after occurrence of a fault where error processing fails.
Z_3 : models the successful reconfiguration when system becomes faultless again.
Z_4 : models an undetected fault in the spare component.
Z_5 : models the failure of the system when both components fail
*Assume same failure rate **λ**, and repair rate **μ** for both components.*
***η** stands for reconfiguration rate.*

What is the probability of the faultless operation: P1+ P3 + P4 ?

Redundancy

Application of the State Model: Calculation of the availability or similar measures (Example)

This simple example shows that the state model has a bigger modeling power than the reliability diagram:

A fault in the primary component is modeled by two states:
- With the failure in the primary component also the system fails.
- After a reconfiguration has evacuated the application process to the spare component, faultless operation is continued (fault tolerance was successful).

In this simple model we assume that repair of the failed model begins after reconfiguration.

As a further simplification we assume that a fault in the spare component remains undetected as long as the spare component is not activated. Moreover, the repair of two failed components takes the same time as the repair of only one.

Redundancy

Application of the State Model: Calculation of the availability or similar measures (Solution)

$$
\begin{aligned}
Z_1: &\quad \mu \cdot P_3 + \mu \cdot P_5 &&= 2 \cdot \lambda \cdot P_1 \\
Z_2: &\quad \lambda \cdot P_1 &&= \eta \cdot P_2 + \lambda \cdot P_2 \\
Z_3: &\quad \eta \cdot P_2 &&= \lambda \cdot P_3 + \mu \cdot P_3 \\
Z_4: &\quad \lambda \cdot P_1 &&= \lambda \cdot P_4 \\
Z_5: &\quad \lambda \cdot P_2 + \lambda \cdot P_3 + \lambda \cdot P_4 &&= \mu \cdot P_5 \\
&\quad P_1 + P_2 + P_3 + P_4 + P_5 &&= 1
\end{aligned}
$$

Solution:

$$P_1 = \frac{\mu \cdot (\eta + \lambda)}{2\mu(\eta + \lambda) + \lambda\mu + 2\lambda(\eta + \lambda)} \qquad P_2 = \frac{\lambda}{\eta + \lambda} \cdot P_1 \qquad P_3 = \frac{\eta}{\lambda + \mu} \cdot P_2$$

$$P_4 = P_1 \qquad P_5 = \frac{2\lambda}{\mu} \cdot P_1 - P_3$$

For $\lambda = \frac{1}{\text{Std}}$ and $\eta = \mu = \frac{4}{\text{Std}}$ we obtain $P_1 + P_3 + P_4 = 0.8$

Redundancy

Coarse Comparison of the Redundancy Types

Static redundancy:

- highest reliability and availability for short durations of operation

Dynamic redundancy:

- high reliability and availability for longer durations of operation
- cost-optimal realization: mutual redundancy

Repair (of both statically and dynamically systems):

- high availability for any duration of operation

Combination: **repairable system with hybrid redundancy**

State Models to Evaluate Combined Redundancy

Examples:

$P_{ff} = 3$,
$P_{fy} = 0$,
$E = 2$

system failed if $P_{ff} = P_{fy} = E = 0$

Each state is expressed by the triple **(P_{ff}, P_{fy}, E)** where

P_{ff} number of faultless primary components in normal operation,

P_{fy} number of faulty primary components in normal operation,

E number of spare components

spare components which have been activated (by reconfiguration) are taken as (new) **primary** components.

rates:

λ failure rate,

η reconfiguration rate (reciprocal of the reconfiguration duration),

ω recovery rate (reciprocal of sum of durations of reconfiguration, backward recovery and repetition operation)

no repair assumed

probability: δ **fault coverage** by absolute tests

Advantages of Redundacy*:*

- Improves system reliability
- Can be implemented in different ways

Disadvantages:

- Cost and complexity increase
- Inefficient by common mode failures
- Security weak points are multiplied

General Objectives of System Design