**Stand-by Redundancy**

- When primary component fails, standby component is started up.
- Stand-by spares are cold spares => unpowered
- Switching equipment assumed failure free

Let $X_i$ denote the lifetime of the i-th component from the time it is put into operation until its failure.

System lifetime:

$$X_{sys} = \sum_{i=1}^{n} X_i$$

---

**Stand-by Redundancy**

- **MTTF**
  $$E(X) = \frac{n}{\lambda}$$
  
  - gain is linear as a function of the number of components, unlike the case of parallel redundancy
  - added complexity of detection and switching mechanism
**M-of-N System**

Starting with \( N \) components, we need any \( M \) components operable for the system to be operable.

Example: TMR

\[
R_{\text{TMR}}(t) = R_1(t)R_2(t)R_3(t) + R_1(t)R_2(t)(1 - R_3(t)) \\
+ R_1(t)(1 - R_2(t))R_3(t) + (1 - R_1(t))R_2(t)R_3(t)
\]

Where \( R_i(t) \) is the reliability of the \( i \)-th component

if \( R_1(t) = R_2(t) = R_3(t) = R(t) \) then

\[
R_{\text{TMR}}(t) = R^3(t) + 3R^2(t)(1 - R(t)) \\
= R^3(t) + 3R^2(t) - 3R^3(t) \\
= 3R^2(t) - 2R^3(t)
\]

---

**M-of-N System**

The probability that exactly \( j \) components are not operating is

\[
\binom{N}{j} Q^j(t) R^{N-j}(t) \quad \text{with} \quad \binom{N}{j} = \frac{N!}{j!(N-j)!}
\]

then

\[
R_{MofN}(t) = \sum_{i=0}^{N-M} \binom{N}{i} Q^i(t) R^{N-i}(t)
\]
Reliability Block Diagram

- Series Parallel Graph
  - a graph that is recursively composed of series and parallel structures.
  - therefore it can be “collapsed” by applying series and/or parallel reduction
  - Let $C_i$ denote the condition that component $i$ is operable
    » 1 = up, 0 = down
  - Let $S$ denote the condition that the system is operable
    » 1 = up, 0 = down
  - $S$ is a logic function of $C$’s

- Example:

\[
S = (C_1 + C_2 + C_3)(C_4 C_5)(C_6 + C_7 C_8)
\]

+ => parallel (1 of N)
. => series (N of N)
**K of N system**

- Example 2-of-3 system

\[ S = (C_1C_2 + C_1C_3 + C_2C_3) \]

may abbreviate

\[ S = \frac{2}{3} (C_1C_2C_3) \]

draw as parallel

![Diagram of 2-of-3 system](image)

---

**Example: Bus-Guardian**

- assume \( \lambda \) for transistor & logic \( \lambda = 2 \times 10^{-5} \)
- 50/50 split: fail-on/fail-off

Two failure states for system

- \( Q_A = \) failed active (babbling) with \( \lambda_A \)
- \( Q_P = \) failed passive with \( \lambda_P \)
Example: Bus-Guardian

\[ \lambda = 2 \times 10^{-5} \]
\[ \lambda_A = 1 \times 10^{-5} \]
\[ \lambda_p = 1 \times 10^{-5} \]

\[ MTTF = \frac{1}{\lambda} = 5 \times 10^4 \]
\[ MTTF_A = \frac{1}{\lambda_A} = 10^5 \]
\[ MTTF_p = \frac{1}{\lambda_p} = 10^5 \]

for each stage

Example: Bus-Guardian

◆ Active Failure
  - if any one bus guardian is correct then no babble possible
  - thus we use 1-of-N parallel system model

\[ Q(t) = \prod_{i=1}^{3} Q_i(t) \]

with \[ Q_i(t) = 1 - e^{-\lambda_i t} \]
Example: Bus-Guardian

- Solution - Parallel
  » if any one bus guardian is correct then no babble possible
  » 1-of-N parallel system model

\[ Q(t) = (1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t}) \]
\[ = 1 - 3e^{-\lambda_A t} + 3e^{-2\lambda_A t} - e^{-3\lambda_A t} \]

e.g. with \( \lambda_A = 10^{-5} / h \) and \( t = 1000h \)
\[ \lambda_A t = 0.01 \]

Example: Bus-Guardian

compute: \[ Q(t) = 1 - 3e^{-\lambda_A t} + 3e^{-2\lambda_A t} - e^{-3\lambda_A t} \]

\[ Q(1000h) = 1 - 3(0.9900498) + 3(0.9801987) - (0.9704455) \]
\[ = 1.2 \times 10^{-6} \]

compute:
\[ Q(t) = (1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t}) \]
\[ = (1 - e^{-\lambda_A t})^3 \]
\[ Q(1000h) = 0.9851243 \times 10^{-6} \]

in general: danger of cancellation
=> catastrophic results,
=> legal issues (even though one should realize what the fail rates really mean)
**Example: Bus-Guardian**

\[ \text{MTTF}_A = \int_0^\infty R(t)dt = \int_0^\infty 1 - Q(t)dt \]

\[ = \int_0^\infty (3e^{-\lambda_A t} - 3e^{-2\lambda_A t} + e^{-3\lambda_A t})dt \]

\[ = \left[ -\frac{3}{\lambda_A} e^{-\lambda_A t} + \frac{3}{2\lambda_A} e^{-2\lambda_A t} - \frac{1}{3\lambda_A} e^{-3\lambda_A t} \right]_0^\infty \]

simplification:

\[ e^{-\lambda_A t} = 0 \text{ as } t \to \infty \]

\[ e^{-\lambda_A t} = 1 \text{ with } t = 0 \]

\[ \text{MTTF}_A = \frac{3}{\lambda_A} - \frac{3}{2\lambda_A} + \frac{1}{3\lambda_A} \]

3 drivers result in approx. MTTF of twice and not three times that of single driver

\[ = (3 - \frac{3}{2} + \frac{1}{3}) \times 10^5 \]

\[ = 1.83 \times 10^5 \text{ h} \]

---

**Example: Bus-Guardian**

- **Passive Failure**
  - any one of \( N \) bus guardians can take out subsystem
  - thus we use series system model

\[ R(t) = \prod_{i=1}^3 R_i(t) \]

\[ = e^{-\sum_{i=1}^3 \lambda_i t} \]

\[ = e^{-3\lambda t} \]

Given \( \lambda = 1 \times 10^{-5} \)

\[ t = 1000 \text{h} \]

\[ R(t) = e^{-3\lambda t} = 0.9704455 \]

\[ \Rightarrow \text{MTTF} = \frac{1}{\lambda_{\text{sys}}} = 33333 \text{h} \]
**Example: Bus-Guardian**

- summary
  - active failure $\Rightarrow$ parallel $\Rightarrow Q_A$
  - passive failure $\Rightarrow$ series $\Rightarrow Q_P$
  - whole system fails if either mode occurs $\Rightarrow$ series

![Diagram of series and parallel systems]

$$Q_A \quad Q_P$$

---

**Example: Bus-Guardian**

- summary

<table>
<thead>
<tr>
<th></th>
<th>Simplex</th>
<th>Triplex</th>
</tr>
</thead>
<tbody>
<tr>
<td>$MTTF_A$</td>
<td>$1 \times 10^5 h$</td>
<td>$1.8 \times 10^5 h$</td>
</tr>
<tr>
<td>$MTTF_P$</td>
<td>$1 \times 10^5 h$</td>
<td>$0.33 \times 10^5 h$</td>
</tr>
<tr>
<td>$MTTF$</td>
<td>$0.5 \times 10^5 h$</td>
<td>$0.28 \times 10^5 h$</td>
</tr>
</tbody>
</table>

$$MTTF = \frac{MTTF_A \times MTTF_P}{MTTF_A + MTTF_P}$$
What is the unreliability $Q_A$?

- Two approaches to compute $Q(t)$ at 1000h

1) $$Q(t) = (1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t})(1 - e^{-\lambda_A t})$$
   $$= 1 - 3e^{-\lambda_A t} + 3e^{-2\lambda_A t} - e^{-3\lambda_A t}$$

2) $MTTF_A = 1.8333 \times 10^5$
   
   using $MTTF = \frac{1}{\lambda}$ we compute $\lambda$ and use
   $$Q(t) = (1 - e^{-\lambda t})$$

Now we compute $Q(1000)$ and ...

What is wrong?