ENGINEERING RELIABILITY

FAULT TREES AND RELIABILITY BLOCK DIAGRAMS

Harry G. Kwatny

Department of Mechanical Engineering & Mechanics
Drexel University
OUTLINE

RELIABILITY BLOCK DIAGRAMS
- RBD Definition
- RBDs and Fault Trees
- System Structure

QUALITATIVE ANALYSIS
- Structure Functions
- Paths and Cutsets

QUANTITATIVE ANALYSIS
- Reliability
- Redundancy
A reliability block diagram (RBD) provides a success oriented view of the system.

RBDs provide a framework for understanding redundancy.

RBDs facilitate the computation of system reliability from component reliabilities.

RBDs and fault trees provide essentially the same information.

Below is the RBD for the backup power supply.
A reliability block diagram (RBD) is defined as follows:

- A reliability block diagram is a graph whose edges are the system components.
- There are a pair of nodes called *terminal nodes* – (a) and (b) in the backup power supply diagram.
- If there is a path between the terminal nodes which contains only edges with functional components, the entire system is functional. Otherwise it is not functional.
In the serial configuration, failure of either component, $A_1$ or $A_2$ causes system failure.

In the parallel configuration, both components must fail in order for the system to fail – redundancy.
Example: Fire Pump System

- The reliability block diagram for the fire pump system is shown below.
- The redundancy of the pumps is clearly evident.
Notice that the fault tree takes a failure perspective, whereas the reliability block diagram takes a success perspective.
A simple serial parallel composition.
A system composed of $n$ subsystems is called a **series structure** if the failure of any one component causes failure of the complete system.
A system composed of \( n \) subsystems is called a parallel structure if it operates if any one or more of its components operates.
A system that is functioning if and only if at least $k$ of its $n$ components is functioning is called a \textit{k-out-of-n} structure.

A 1-out-of-$n$ structure is a parallel structure.
A system with \( n \) components is called a system of order \( n \).

- \( x_i \) denotes the state of component or subsystem \( i \),
  \[
  x_i = \begin{cases} 
  1 & \text{the component is functioning} \\
  0 & \text{the component is failed}
  \end{cases}, \quad i = 1, \ldots, n
  \]

- \( x \) denotes the state of the entire system,
  \[
  x = \begin{cases} 
  1 & \text{the system is functioning} \\
  0 & \text{the system is failed}
  \end{cases}
  \]

- The **structure function** is a function \( \phi \left( x_1, \ldots, x_n \right) \) associated with a given system, such that
  \[
  x = \phi \left( x_1, \ldots, x_n \right)
  \]
Structure Functions

- serial structure
  \[ \phi(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n \]

- parallel structure
  \[ \phi(x_1, \ldots, x_n) = 1 - (1 - x_1)(1 - x_2) \ldots (1 - x_n) = 1 - \prod_{i=1}^{n} (1 - x_i) \]
  \[ \phi(x_1, \ldots, x_n) = \max_{i \in \{1, \ldots, n\}} x_i \]

- k-out-of-n structure
  \[ \phi(x_1, \ldots, x_n) = \begin{cases} 1 & \sum_{i=1}^{n} x_i \geq k \\ 0 & \sum_{i=1}^{n} x_i < k \end{cases} \]
A component is irrelevant if it has no effect on the functioning of the system, i.e., the \(i^{th}\) component is irrelevant if
\[
\phi(x_1, \ldots x_{i-1}, 0, x_{i+1}, \ldots, x_n) = \phi(x_1, \ldots x_{i-1}, 1, x_{i+1}, \ldots, x_n)
\]
for all \(x_1, \ldots x_{i-1}, x_{i+1}, \ldots, x_n\)

Otherwise it is called relevant.

Assumption: the system will not run worse if a failed component is replaced by a functional component
\(\Rightarrow \phi(x_1, \ldots, x_n)\) is a nondecreasing function of each of the variables \(x_1, \ldots, x_n\).

A system is coherent if all of its components are relevant and its structure function is nondecreasing.

By focusing on coherent structures we rule out certain pathologies.
The set of components of a system of order $n$ is

$$C = \{1, 2, \ldots, n\}$$

A path set, $P$, is a subset of $C$ which by functioning ensures that the system is functioning. A path set is minimal if it cannot be reduced without losing its status as a path set.

A cut set, $K$, is a subset of $C$ which by failing causes the system to fail. A cut set is minimal if it cannot be reduced without losing its status as a cut set.
A system with \( n \) components is called a system of order \( n \).

\( A_i \) denotes the event that the component or subsystem \( i, i = 1, \ldots, n \) is functioning at time \( t \).

\( A \) denotes the event that the entire system is functioning at time \( t \).

\( P (A_i) = R_i (t) \) is the reliability of the \( i^{th} \) subsystem.

\( P (A) = R (t) \) is the reliability of the entire system.
SERIES STRUCTURE

Note:

- $A = A_1 \cap A_2 \cap \cdots \cap A_n \iff A^c = A_1^c \cup A_2^c \cup \cdots \cup A_n^c$
- $A \subset A_i, \ i = 1, \ldots, n \Rightarrow R(t) \leq R_i(t)$

- A serial system reliability is no greater than the reliability of any subsystem!

- Suppose that the failure events $A_i$ are mutually independent, then

$$R(t) = P(A) = P(\cap_{i=1}^{n} A_i) = \prod_{i=1}^{n} P(A_i) = \prod_{i=1}^{n} R_i(t)$$
PARALLEL STRUCTURE

- $A = A_1 \cup A_2 \cup \cdots \cup A_n$

- If the subsystem failure events are independent:
  - $A^c = A_1^c \cap A_2^c \cap \cdots \cap A_n^c$
  - $P(A^c) = P(A_1^c) P(A_2^c) \cdots P(A_n^c)$
  - $P(A) = 1 - P(A^c) = 1 - \prod_{i=1}^{n} P(A_i^c) = 1 - \prod_{i=1}^{n} [1 - P(A_i)]$

- Consequently, for independent events:
  $$R(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t))$$
Consider identical components,

- The probability failure of failure over a specified time period for a single component is $p$, so the component reliability is $r = 1 - p$.

Let $M$ denote the number of components that fail in the specified time period, then

\[
P(M = m) = \binom{n}{m} p^m (1 - p)^{n-m} = \binom{c}{m} (1 - r)^m r^{n-m}
\]

# ways to get $m/n$ failures

$n-m$ survivors

The $k/n$ system will survive if there are no more than $n - k$ failures, so

\[
R = \sum_{m=0}^{n-k} \binom{n}{m} (1 - r)^m r^{n-m}
\]
 Definitions

- Redundancy is the duplication of critical components in a system in order to improve reliability.
- Redundancy is normally a parallel connection of identical components – can be active or standby.
Consider a redundant (parallel) combination of two identical components.

Let $T_1$, $T_2$, $T$ denote the failure times of component 1, component 2, and the system, respectively.

- the units are identical, so $R_1(t) = R_2(t)$
- assume the failures of the two units are independent events.

The system reliability of the active parallel structure is

$$R_a(t) = P(T_1 > t \cup T_2 > t)$$

$$= P(T_1 > t) + P(T_2 > t) - P(T_1 > t)P(T_2 > t)$$

$$R_a(t) = R_1(t) + R_2(t) - R_1(t)R_2(t)$$
The standby system does not start operating until the primary unit fails.

The system can survive until time $t$ if the primary unit survives until time $t$ or the primary unit fails before time $t$, but the second unit survives until time $t$:

$$R_s(t) = P(T_2 > t | T_2 > T_1) = P(T_1 > t) + P(T_1 < t \cap T_2 > t)$$

The two possibilities can be restated as $T_1 > t$ or $T_1$ occurs at $\tau < t$ and $T_2 > t - \tau$. Notice that

$$P(\tau < T_1 < \tau + d\tau) = f_1(\tau) \, d\tau$$
$$P(\tau < T_1 < \tau + d\tau \cap T_2 > t) = R_2(t - \tau) \, f_1(\tau) \, d\tau$$
$$P(T_1 < t \cap T_2 > t) = \int_0^t R_2(t - \tau) \, f_1(\tau) \, d\tau$$

$$R_s(t) = R_1(t) + \int_0^t R_2(t - \tau) \, f_1(\tau) \, d\tau$$
Example: Constant Failure Rate

- Components with constant failure rate $\lambda$ have reliability
  
  $$R(t) = e^{-\lambda t}$$

- An active parallel structure has reliability
  
  $$R_a(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

- A standby parallel structure has reliability
  
  $$R_s(t) = (1 + \lambda t) e^{-\lambda t}$$
High- and Low-Level Redundancy

High (SYSTEM)-level Redundancy

Low (COMPONENT)-level Redundancy

Diagram showing high and low levels of redundancy.
Consider a system with state vector \( \mathbf{x} = \{x_1, \ldots, x_n\} \) and structure function \( \phi_1(\mathbf{x}) \), and a second system with state vector \( \mathbf{y} = \{y_1, \ldots, y_m\} \) and structure function \( \phi_2(\mathbf{y}) \).

- If these systems are connected in series then the whole system is of order \( n + m \), and its structure function is

\[
\phi(\mathbf{x}, \mathbf{y}) = \phi_1(\mathbf{x}) \phi_2(\mathbf{y})
\]

- If these systems are connected in parallel then the whole system is of order \( n + m \), and its structure function is

\[
\phi(\mathbf{x}, \mathbf{y}) = \max\{\phi_1(\mathbf{x}), \phi_2(\mathbf{y})\}
\]
Suppose the two systems in the parallel structure are identical, i.e., we have a system level redundant configuration. In this case,

\[
\phi_S(x, y) = \max \{\phi_1(x), \phi_1(y)\} \leq \phi_1(x_1y_1, \ldots, x_ny_n)
\]

Consider a component level redundant configuration of system one, the structure function is

\[
\phi_C(x, y) = \phi_1(\max \{x_1, y_1\}, \ldots, \max \{x_n, y_n\})
\]

But, for coherent systems,

\[
\phi_1(\max \{x_1, y_1\}, \ldots, \max \{x_n, y_n\}) \geq \phi_1(x_1y_1, \ldots, x_ny_n)
\]

So,

\[
\phi_C(x, y) \geq \phi_S(x, y)
\]

Thus, in general, we get a better (more reliable?) system through component redundancy rather than system redundancy.
Consider a system with $K$ minimal cutsets, $A_1, A_2, \ldots, A_K$.

For a system level redundant configuration, place an identical system with cutsets labeled $B_1, B_2, \ldots, B_K$ in parallel with the original. The redundant system cutsets are all combinations $A_i \cap B_j$, $i, j = 1, \ldots, K$.

A component level redundant system has cut sets $A_i \cap B_i$, $i = 1, \ldots, K$.

Consequently, $R_C \geq R_S$. 

<table>
<thead>
<tr>
<th>$A_1 \cap B_1$</th>
<th>$A_1 \cap B_2$</th>
<th>$A_1 \cap B_3$</th>
<th>$\cdots$</th>
<th>$A_1 \cap B_K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A_2 \cap B_1$</td>
<td>$A_2 \cap B_2$</td>
<td>$A_2 \cap B_3$</td>
<td>$\cdots$</td>
<td>$A_2 \cap B_K$</td>
</tr>
<tr>
<td>$A_3 \cap B_1$</td>
<td>$A_3 \cap B_2$</td>
<td>$A_3 \cap B_3$</td>
<td>$\cdots$</td>
<td>$A_3 \cap B_K$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\ddots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$A_K \cap B_1$</td>
<td>$A_K \cap B_2$</td>
<td>$A_K \cap B_3$</td>
<td>$\cdots$</td>
<td>$A_K \cap B_K$</td>
</tr>
</tbody>
</table>
Example: System vs Component Redundancy

Engineering Reliability

Reliability Block Diagrams
RBD Definition
RBDs and Fault Trees
System Structure

Qualitative Analysis
Structure Functions
Paths and Cutsets

Quantitative Analysis
Reliability Redundancy
Redundancy Limitations

▶ **Common-mode** failures are caused by dependencies that cause redundant components to fail simultaneously.
  ▶ common power supply
  ▶ shared environmental stresses
  ▶ common maintenance issues

▶ Load sharing can cause reliability degradation in active parallel systems.
  ▶ failure of one unit can cause increased stress on remaining units, e.g., engines, pumps, etc.,

▶ switching failures can occur in standby parallel systems