Common Cause Failures:
Failures of multiple components involving a shared dependency
KEY POINTS OF THE SESSION

Component Arrangements

Common Cause Failures

B Factor Method

Data Center Common Cause Failures

Dual Path and Dual Cord

Fault Tree Analysis of Single-Cord, Dual Path, and Dual Cord Service
COMPONENT ARRANGEMENTS

Parallel: Success of One Component is Sufficient for System Success (e.g., backup power sources)

$$P_{\text{system success}} = 1 - \prod_{i} q_i$$, \quad q_i = \text{Failure Probability of } i\text{-th Component}

Three Component System

$$S = A + B + C = 1 - \overline{A} \cdot \overline{B} \cdot \overline{C}$$

(Note: Adding Components Increases $P_{\text{system success}}$)
COMPONENT ARRANGEMENTS

Series: Success of Every Component is Necessary for System Success (e.g., the links of a chain)

\[ P_{\text{success}} = \prod p_i, \quad p_i = \text{Success Probability of } i\text{-th Component} \]

(Note: Adding Components Decreases \( P_{\text{success}} \))

Three Component Series

\[ S = A \cdot B \cdot C = 1 - (\overline{A} + \overline{B} + \overline{C}) \]
## EXAMPLE OF COMMON CAUSE FAILURE SOURCES POTENTIALLY ABLE TO AFFECT DATA CENTERS SERIOUSLY

<table>
<thead>
<tr>
<th>Support System</th>
<th>Environmental (Exceeding Allowable Envelope)</th>
<th>Structural</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuel Quantity</td>
<td>Temperature</td>
<td>Manufacturing Flaw</td>
<td></td>
</tr>
<tr>
<td>Fuel Quality</td>
<td>Pressure</td>
<td>Faulty Maintenance Procedure</td>
<td></td>
</tr>
<tr>
<td>Cooling</td>
<td>Vibration</td>
<td>Component Design Error</td>
<td></td>
</tr>
<tr>
<td>Lubrication</td>
<td>Noise</td>
<td>Earthquake</td>
<td></td>
</tr>
<tr>
<td>Ventilation</td>
<td>Air Quality</td>
<td>Hurricane</td>
<td></td>
</tr>
<tr>
<td>Human Error</td>
<td>Electromagnetic Pulse</td>
<td>Tornado</td>
<td></td>
</tr>
<tr>
<td>Control Power</td>
<td></td>
<td>Flood</td>
<td></td>
</tr>
<tr>
<td>Interfacing Switchgear</td>
<td></td>
<td>Explosion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Labor Strike</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terrorist</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Action</td>
<td></td>
</tr>
</tbody>
</table>
# TYPES OF COMMON CAUSE FAILURES AND THEIR ASPECTS

<table>
<thead>
<tr>
<th>Description of Failure Cause</th>
<th>DEPENDENT</th>
<th>STRUCTURAL*</th>
<th>ENVIRONMENTAL</th>
<th>EXTERNAL*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of an interfacing system, action or component</td>
<td>Failure of a component due to a design flaw which simultaneously affects all components population</td>
<td>Faulty materials</td>
<td>A change in the operational environment which affects all members of a component population simultaneously</td>
<td>An event originating outside the system which affects all members of a component population simultaneously</td>
</tr>
</tbody>
</table>

### Hardware Examples
- Loss of electrical power
- A manufacturer provides defective replacement parts that are installed in all components of a given class
- Incorrect training
- Poor management
- Poor motivation
- Low pay
- Common cause psf’s
- New disease
- Hunger
- Fear
- Noise
- Radiation in control room
- Explosion
- Toxic substance
- Severe Weather
- Earthquake
- Concern for families

### Human Examples
- Following a mistaken leader
- An erroneous maintenance procedure is repeated for all components of a given class
- An erroneous maintenance procedure is repeated for all components of a given class

### Easy to Anticipate?:
- Component failure: High
- Human error: Medium

### Easy to Mitigate?:
- Component failure: Very Low, hard to design for mitigation
- Human error: Low, the factors making CCF likely also discourage being prepared for correction

* Usually there are no precursors
COMMON CAUSE (i.e., DEPENDENT) FAILURES

Let CC Be a Common Cause Failure Event Causing Dependent Failures of Components A, B, C and D. The Component A Can Fail By

1. Independent Failure, Event $A_i$, Prob. = $q_A$
2. Dependent Failure, Event ($A_c \cdot CC$), Prob. = $\text{Prob.}[A_c|CC] \cdot \text{Prob.}(CC) = \text{Prob.}(CC)$

$$\text{Prob.}[\text{Failure of Component A}] = \text{Prob.}(A_i) + \text{Prob.}(A_c \cdot CC) - \text{Prob.}(A_i) \cdot \text{Prob.}(A_c \cdot CC)$$

Neglect, as Usually is of Small Value
COMMON CAUSE (i.e., DEPENDENT) FAILURES

Consider Failure of Four Components: A, B, C, D

\[
\text{Prob.}[\text{4 Component Failures}] = \text{Prob.}[A \cdot B \cdot C \cdot D] = \text{Prob.}[A|(B \cdot C \cdot D)] \cdot \text{Prob.}[B|(C \cdot D)] \cdot \text{Prob.}[C|D] \cdot \text{Prob.}(D)
\]

Now Consider Events A, B, C, D Each to Have an Independent Version and a Version Dependent Upon Event CC, \( \text{Prob.}(CC) = q_{cc} \)

Then

\[
\text{Prob.}(A \cdot B \cdot C \cdot D) \approx q_A \cdot q_B \cdot q_C \cdot q_D + \text{Prob.}[A_c|(B_c \cdot C_c \cdot D_c)] \cdot \text{Prob.}[B_c|(C_c \cdot D_c \cdot CC)] \cdot \text{Prob.}[C_c|(D_c \cdot CC)] \cdot \text{Prob.}(D_c|CC) \cdot \text{Prob.}(CC) \]

\[
\frac{\text{Prob.}(D_c|CC) \cdot \text{Prob.}(CC)}{\text{Prob.}(D_c \cdot CC)}
\]

Or

\[
\text{Prob.}(A \cdot B \cdot C \cdot D) \approx \underbrace{q_A \cdot q_B \cdot q_C \cdot q_D}_{\text{Independent}} + \frac{1 \cdot q_{cc}}{\text{Dependent}}
\]
COMMON CAUSE (i.e., DEPENDENT) FAILURES

Often
\[ \text{Order}(q_{cc}) = \text{Order}(q_{A,B,C,D}) \gg q_A q_B q_C q_D \]
\[ \Rightarrow \text{Prob.}(A \cdot B \cdot C \cdot D) \equiv q_{cc} \]

In This Situation Redundancy of Components is of Little Benefit in Reducing Values of \( \text{Prob.}(A \cdot B \cdot C \cdot D) \)

Then
\[ \text{Prob.}(A \cdot B \cdot C \cdot D) \equiv \text{Prob.}(A_i \cdot B_i \cdot C_i \cdot D_i) + \text{Prob.}(A_{cc} \cdot B_{cc} \cdot C_{cc} \cdot D_{cc} \cdot CC) \]

i + independent failure

cc + dependent, or common cause failure
COMPONENT ARRANGEMENTS

Parallel – Used When Success of a Single Component is Sufficient for System Success

Three Component Systems

\[ S = A + B + C = 1 - A \cdot B \cdot C \]

Failure

\[ P_{\text{system}} = 1 - \prod_{i=1}^{N} q_i, \text{ for Independent Failures} \]

\[ P_{\text{system}} = 1 - Q_{\text{independent}} - Q_{\text{common}} + \left( Q_{\text{independent}} \cdot Q_{\text{cc}} \right) \]

Typically is small

\[ = 1 - \left( \prod_{i=1}^{N} q_i \cdot q_{\text{cc}} \right) \prod_{i=1}^{N} q_i \]

Typically is small

4-10
COMMON CAUSE FAILURE — $\beta$ FACTOR METHOD

- N components, each of which has an independent failure probability $q_i$;
- Common cause failure factor $\beta$;
  Let $C$ be the event that common failure happens, $P(C) = \beta q_i$;
- If $C$ happens, none of the N components can succeed;

NOTE: Sometimes sharing a common cause among N components will result in $m$ ($m \leq N$) failing upon occurrence of the common cause.
If there is no common cause failure, i.e. $\beta = 0$.

With $N = 10$, we obtain the following binomial distribution for $X$ — the number of successful components.

$$P(X = k) = \binom{10}{k} (1 - q_I)^k q_I^{10-k},$$

$k = 0, 1, 2, \ldots, 10$
If $\beta \neq 0$, $X$ has the following distribution:

$$\begin{align*}
P(X = 0) &= P(X = 0 | C)P(C) + P(X = 0 | \bar{C})P(\bar{C}) \\
&= 1 \times \beta q_I + \binom{10}{0} (1 - q_I)^0 q_I^0 \times (1 - \beta) = \beta q_I + (1 - \beta) q_I^{10} \approx \beta q_I
\end{align*}$$

$k \neq 0$

$$\begin{align*}
P(X = k) &= P(X = k | C)P(C) + P(X = k | \bar{C})P(\bar{C}) \\
&= 0 \times \beta q_I + \binom{10}{k} (1 - q_I)^k q_I^{10-k} \times (1 - \beta q_I) = (1 - \beta q_I) \times \binom{10}{k} (1 - q_I)^k q_I^{10-k} \\
&\approx \binom{10}{k} (1 - q_I)^k q_I^{10-k}
\end{align*}$$
COMMON CAUSE FAILURE:  
\( \beta \) FACTOR METHOD  
(continued)

- Common cause failure increased the probability that all components will fail dramatically. Take \( N = 10, q_I = 0.01 \) as an example:

  - If \( \beta = 0 \) (no common cause failure), the probability that all 10 components will fail is \( \binom{10}{0} (1-0.01)^0 0.01^{10} = 0.01^{10} = 10^{-20} \)

  - If \( \beta = 0.01 \), the probability the common cause failure happens is \( P(C) = \beta q_I = 0.01 \times 0.01 = 10^{-4} \). The probability that all 10 components will fail is \( \beta q_I + (1-\beta)q_I^{10} = 0.01 \times 0.01 + (1-0.01) \times 0.01^{10} \approx 10^{-4} \)

  - With \( \beta = 0.01 \), we have all components failure probability of \( 10^{-4} \) while without common cause failure, we have \( 10^{-20} \), which is far less than \( 10^{-4} \).
**COMMON CAUSE FAILURE: \( \beta \) FACTOR METHOD**

(continued)

| \( \beta \) = 0 |
|-----------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| \( p \)  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 0.01 | 1.0000E-20 | 9.9000E-18 | 4.4105E-15 | 1.1644E-12 | 2.0173E-10 | 2.3965E-08 | 1.9771E-06 | 1.1185E-04 | 4.1524E-03 | 9.1352E-02 | 9.0438E-01 |

| \( \beta \) = 0.01 |
|-----------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| \( p \)  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 0.01 | 1.0000E-04 | 9.8990E-18 | 4.4100E-15 | 1.1642E-12 | 2.0170E-10 | 2.3963E-08 | 1.9769E-06 | 1.1184E-04 | 4.1519E-03 | 9.1343E-02 | 9.0429E-01 |

| \( \beta \) = 0.001 |
|-----------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| \( p \)  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 0.01 | 1.0000E-05 | 9.8999E-18 | 4.4104E-15 | 1.1643E-12 | 2.0172E-10 | 2.3965E-08 | 1.9771E-06 | 1.1185E-04 | 4.1523E-03 | 9.1351E-02 | 9.0437E-01 |

*In the above table, \( q \) means \( q_I \).*
COMMON CAUSE FAILURE – $\beta$

FACTOR METHOD

(continued)

No common cause failure, log scale

<table>
<thead>
<tr>
<th>Number of successes</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1E-40</td>
</tr>
<tr>
<td>1</td>
<td>1E-39</td>
</tr>
<tr>
<td>2</td>
<td>1E-38</td>
</tr>
<tr>
<td>3</td>
<td>1E-37</td>
</tr>
<tr>
<td>4</td>
<td>1E-36</td>
</tr>
<tr>
<td>5</td>
<td>1E-35</td>
</tr>
<tr>
<td>6</td>
<td>1E-34</td>
</tr>
<tr>
<td>7</td>
<td>1E-33</td>
</tr>
<tr>
<td>8</td>
<td>1E-32</td>
</tr>
<tr>
<td>9</td>
<td>1E-31</td>
</tr>
<tr>
<td>10</td>
<td>1E-30</td>
</tr>
</tbody>
</table>

- $q_I = 0.01$
- $q_I = 0.001$
- $q_I = 0.0001$
COMMON CAUSE FAILURE — $\beta$
FACTOR METHOD
(continued)

Common cause factor is 0.01, log scale

- $q_I = 0.01$, $\beta = 0.01$
- $q_I = 0.001$, $\beta = 0.01$
- $q_I = 0.0001$, $\beta = 0.01$
COMMON CAUSE FAILURE — $\beta$
FACTOR METHOD
(continued)

Common cause factor of 0.001, log scale

Number of successes vs. Probability

- $q_l = 0.01$, $\beta=0.001$
- $q_l = 0.001$, $\beta=0.001$
- $q_l = 0.0001$, $\beta=0.001$