REAL AVAILABILITY 2005

Common Cause Failures:

Failures of multiple components involving a shared dependency

KEY POINTS OF THE SESSION

Component Arrangements

Common Cause Failures

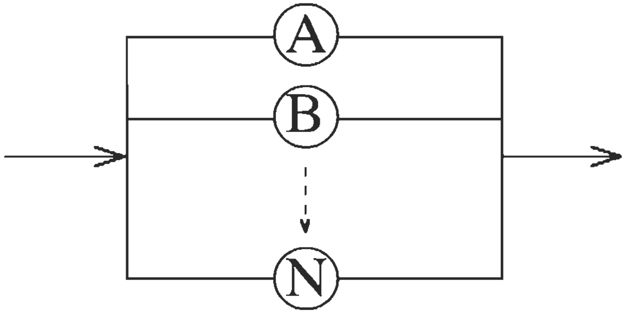
B Factor Method

Data Center Common Cause Failures

Dual Path and Dual Cord

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

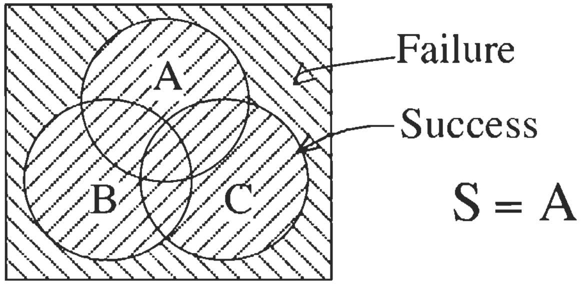
COMPONENT ARRANGEMENTS



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

$$P_{\substack{\text{system}\\\text{success}}} = \underbrace{1 - \prod_i q_i}_{Q_{\text{system}}}, \quad q_i = \text{Failure Probability of i - th Component}$$

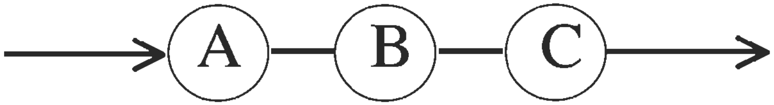
Three Component System



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

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

COMPONENT ARRANGEMENTS

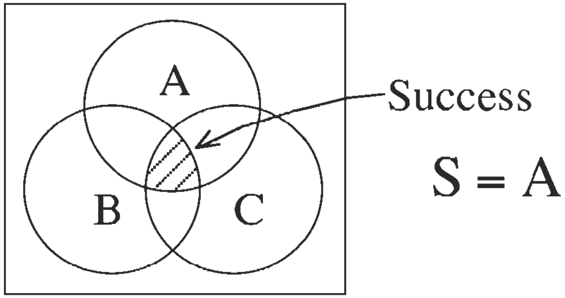


Series: Success of Every Component is Necessary for System Success (e.g., the links of a chain)

$$P_{\substack{\text{system}\\\text{success}}} = \prod_i p_i \,, \quad p_i = \text{Success Probability of } i\text{ - th Component}$$

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

Three Component Series



$$S = A \cdot B \cdot C = 1 - \left(\overline{A} + \overline{B} + \overline{C}\right)$$

EXAMPLE OF COMMON CAUSE FAILURE SOURCES POTENTIALLY ABLE TO AFFECT DATA CENTERS SERIOUSLY

Support System

- Fuel Quantity
- Fuel Quality
- Cooling
- Lubrication
- Ventilation
- Human Error
- Control Power
- Interfacing Switchgear

Environmental (Exceeding Allowable Envelope)

- Temperature
- Pressure
- Vibration
- Noise
- Air Quality
- Electromagnetic Pulse

Structural

- Manufacturing Flaw
- Faulty Maintenance Procedure
- Component Design Error

External

- Earthquake
- Hurricane
- Tornado
- Flood
- Explosion
- Labor Strike
- Terrorist Action

TYPES OF COMMON CAUSE FAILURES AND THEIR ASPECTS

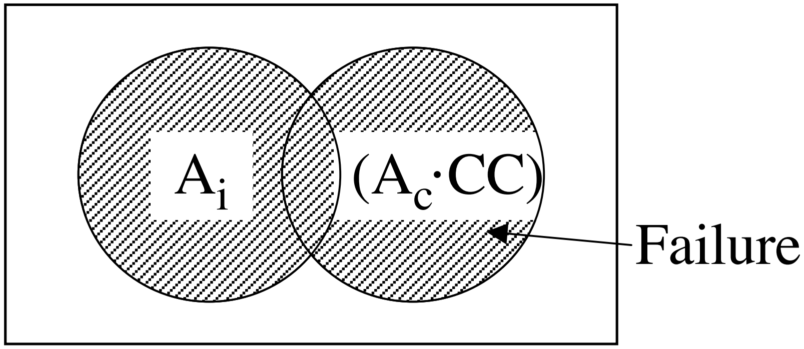
	DEPENDENT	STRUCTURAL*	ENVIRONMENTAL	EXTERNAL*
Description of Failure Cause	Failure of an interfacing system, action or component	A common material or design flaw which simultaneously affects all components population	A change in the operational environment which affects all members of a component population simultaneously	An event originating outside the system which affects all members of a component population simultaneously
Hardware Examples	• Loss of electrical power • A manufacturer provides defective replacement parts that are installed in all components of a given class	• Faulty materials • Aging • Fatigue • Improperly cured materials • Manufacturing flaw	• High pressure • High temperature • Vibration	
Human Examples	• Following a mistaken leader • An erroneous maintenance procedure is repeated for 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
Easy to Anticipate?:				
Component failure	High	Very Low	Medium	Medium
Human error	Medium	Very Low	Medium	Medium
Easy to Mitigate?:				
Component failure	High, if system designed for mitigation	Very Low, hard to design for mitigation	Low	Low
Human error	High, if feedback provided to identify the error promptly	Very Low, the factors making CCF likely also discourage being prepared for correction	Low	Low

* 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. = Prob.$[A_c|CC] \cdot$ Prob.(CC) = Prob.(CC)



$$\text{Prob.[Failure of Component A]} = \text{Prob.}(A_i) + \text{Prob.}\ (A_c \cdot CC) - \underbrace{\text{Prob.}(A_i) \cdot \text{Prob.}\ (A_c \cdot CC)}_{\text{Neglect, as Usually is of Small Value}}$$

COMMON CAUSE (i.e., DEPENDENT) FAILURES

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

$$\text{Prob.}\left[\text{4 Component Failures}\right] = \text{Prob.}\left[A \cdot B \cdot C \cdot D\right]$$

$$= \text{Prob.}\left[A \middle| \left(B \cdot C \cdot D\right)\right] \text{Prob.}\left[B \middle| \left(C \cdot D\right)\right] \text{Prob.}\left[C \middle| D\right] \text{Prob.}\left(D\right)$$

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

Then $\text{Prob.}\left(A \cdot B \cdot C \cdot D\right) \cong q_A q_B q_C q_D$

$$+ \text{Prob.}\left[A_c \middle| \left(B_c \cdot C_c \cdot D_c\right)\right] \text{Prob.}\left[B_c \middle| \left(C_c \cdot D_c \cdot CC\right)\right] \text{Prob.}\left[C_c \middle| \left(D_c \cdot CC\right)\right]$$

$$\underbrace{\cdot \text{Prob.}\left(D_c \middle| CC\right) \text{Prob.}\left(CC\right)}_{\text{Prob.}\left(D_c \cdot CC\right)}$$

Or $\text{Prob.}\left(A \cdot B \cdot C \cdot D\right) \cong \underbrace{q_A q_B q_C q_D}_{\text{Independent}} + \underbrace{1 \cdot q_{cc}}_{\text{Dependent}}$

COMMON CAUSE (i.e., DEPENDENT) FAILURES

Often $\quad \text{Order}\left(q_{CC}\right) = \text{Order}\left(q_{A,B,C,D}\right) >> q_A q_B q_C q_D$

$$\Rightarrow \text{Prob.}\left(A \cdot B \cdot C \cdot D\right) \cong q_{CC}$$

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

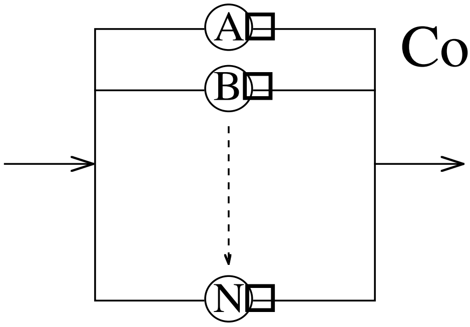
Then $\text{Prob.}\left(A \cdot B \cdot C \cdot D\right) \cong \text{Prob.}\left(A_i \cdot B_i \cdot C_i \cdot D_i\right) + \text{Prob.}\left(A_{cc} \cdot B_{cc} \cdot C_{cc} \cdot D_{cc} \cdot CC\right)$

i + independent failure

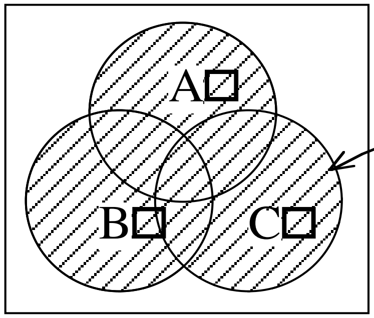
c + dependent, or common cause failure

COMPONENT ARRANGEMENTS

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



Three Component Systems

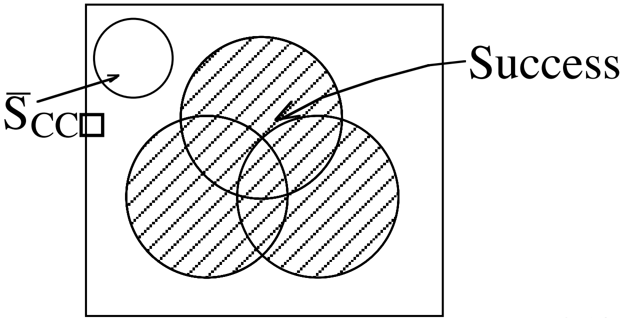


$$S = A + B + C = 1 - \underbrace{\overline{A} \cdot \overline{B} \cdot \overline{C}}_{\text{Failure}}$$

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

$$P_{system} = 1 - Q_{independent} - Q_{\substack{common\\cause}} + \left(Q_{independent} \cdot Q_{cc}\right)$$

$$= 1 - \left(\prod_{i=1}^{N} q_i + q_{cc} - \underbrace{q_{cc} \cdot \prod_{i=1}^{N} q_i}_{\substack{\text{Typically}\\\text{is small}}} \right)$$



COMMON CAUSE FAILURE – β FACTOR METHOD

- N components, each of which has an independent failure probability q_I;
- Common cause failure factor β;
  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.

NO COMMON CAUSE FAILURE

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.

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

$$k = 0, 1, 2, \ldots, 10$$

COMMON CAUSE FAILURE: β FACTOR METHOD (continued)

- If $\beta \neq 0$, X has the following distribution:

$$P(X=0) = P(X=0 \mid C)P(C) + P(X=0 \mid \overline{C})\,P(\overline{C})$$

$$= 1 \times \beta q_I + \binom{10}{0}(1-q_I)^0\, q_I^{10} \times (1-\beta) = \beta q_I + (1-\beta)q_I^{10} \approx \beta q_I$$

$k \neq 0$

$$P(X=k) = P(X=k \mid C)\,P(C) + P(X=k \mid \overline{C})P(\overline{C})$$

$$= 0 \times \beta q_I + \binom{10}{k}(1-q_I)^k\, q_I^{10-k} \times (1-\beta q_I) = (1-\beta q_I) \times \binom{10}{k}(1-q_I)^k\, q_I^{10-k}$$

$$\approx \binom{10}{k}(1-q_I)^k\, q_I^{10-k}$$

COMMON CAUSE FAILURE: β 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 β = 0 (no common cause failure), the probability that all 10 components will fail is $\binom{10}{0}(1-0.01)^{0}0.01^{10\square} = 0.01^{10\square} = 10^{-20}$
  - If β = 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 β = 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}.

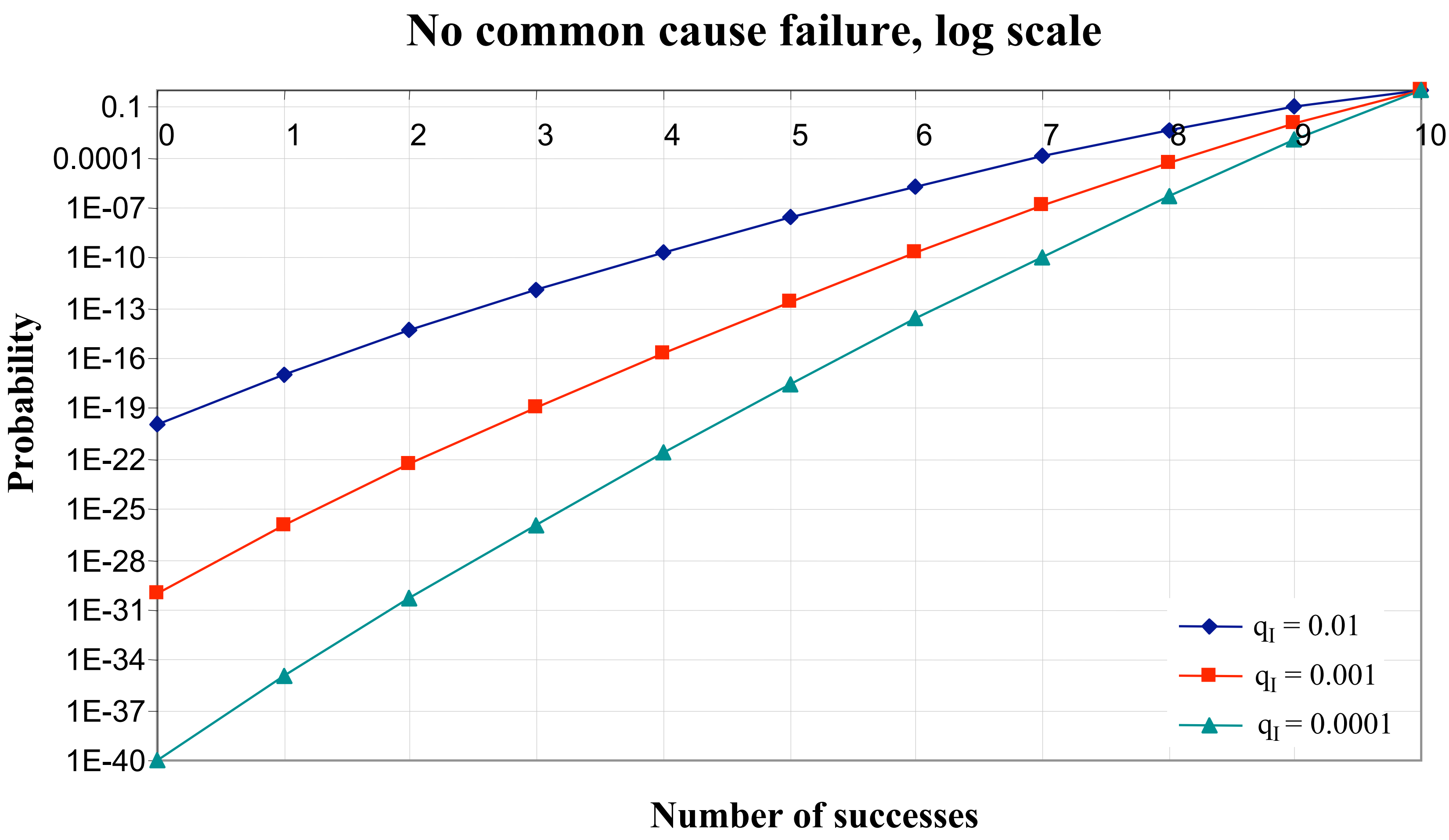
COMMON CAUSE FAILURE: β FACTOR METHOD

(continued)

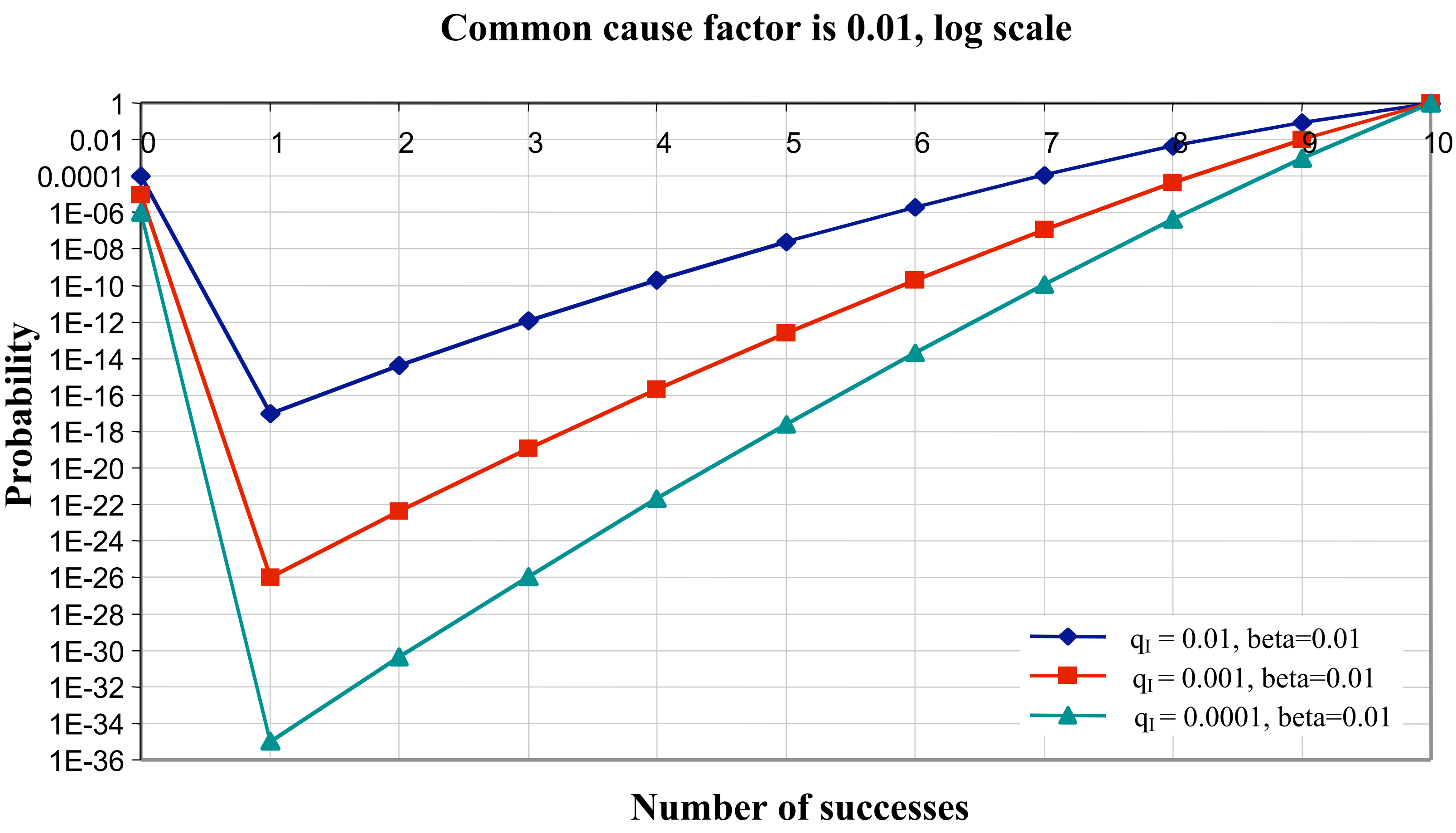
beta=0											
p \ k	0	1	2	3	4	5	6	7	8	9	10
0.01	1.0000E-20	9.9000E-18	4.4105E-15	1.1644E-12	2.0173E-10	2.3965E-08	1.9771E-06	1.1185E-04	4.1524E-03	9.1352E-02	9.0438E-01
0.001	1.0000E-30	9.9900E-27	4.4910E-23	1.1964E-19	2.0916E-16	2.5074E-13	2.0874E-10	1.1916E-07	4.4641E-05	9.9104E-03	9.9004E-01
0.0001	1.0000E-40	9.9990E-36	4.4991E-31	1.1996E-26	2.0992E-22	2.5187E-18	2.0987E-14	1.1992E-10	4.4964E-07	9.9910E-04	9.9900E-01
beta=0.01											
p \ k	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
0.001	1.0000E-05	9.9899E-27	4.4910E-23	1.1964E-19	2.0916E-16	2.5074E-13	2.0874E-10	1.1916E-07	4.4641E-05	9.9103E-03	9.9003E-01
0.0001	1.0000E-06	9.9990E-36	4.4991E-31	1.1996E-26	2.0992E-22	2.5187E-18	2.0987E-14	1.1992E-10	4.4964E-07	9.9910E-04	9.9900E-01
beta=0.001											
p \ k	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
0.001	1.0000E-06	9.9900E-27	4.4910E-23	1.1964E-19	2.0916E-16	2.5074E-13	2.0874E-10	1.1916E-07	4.4641E-05	9.9103E-03	9.9004E-01
0.0001	1.0000E-07	9.9990E-36	4.4991E-31	1.1996E-26	2.0992E-22	2.5187E-18	2.0987E-14	1.1992E-10	4.4964E-07	9.9910E-04	9.9900E-01

*In the above table, q means q_I,

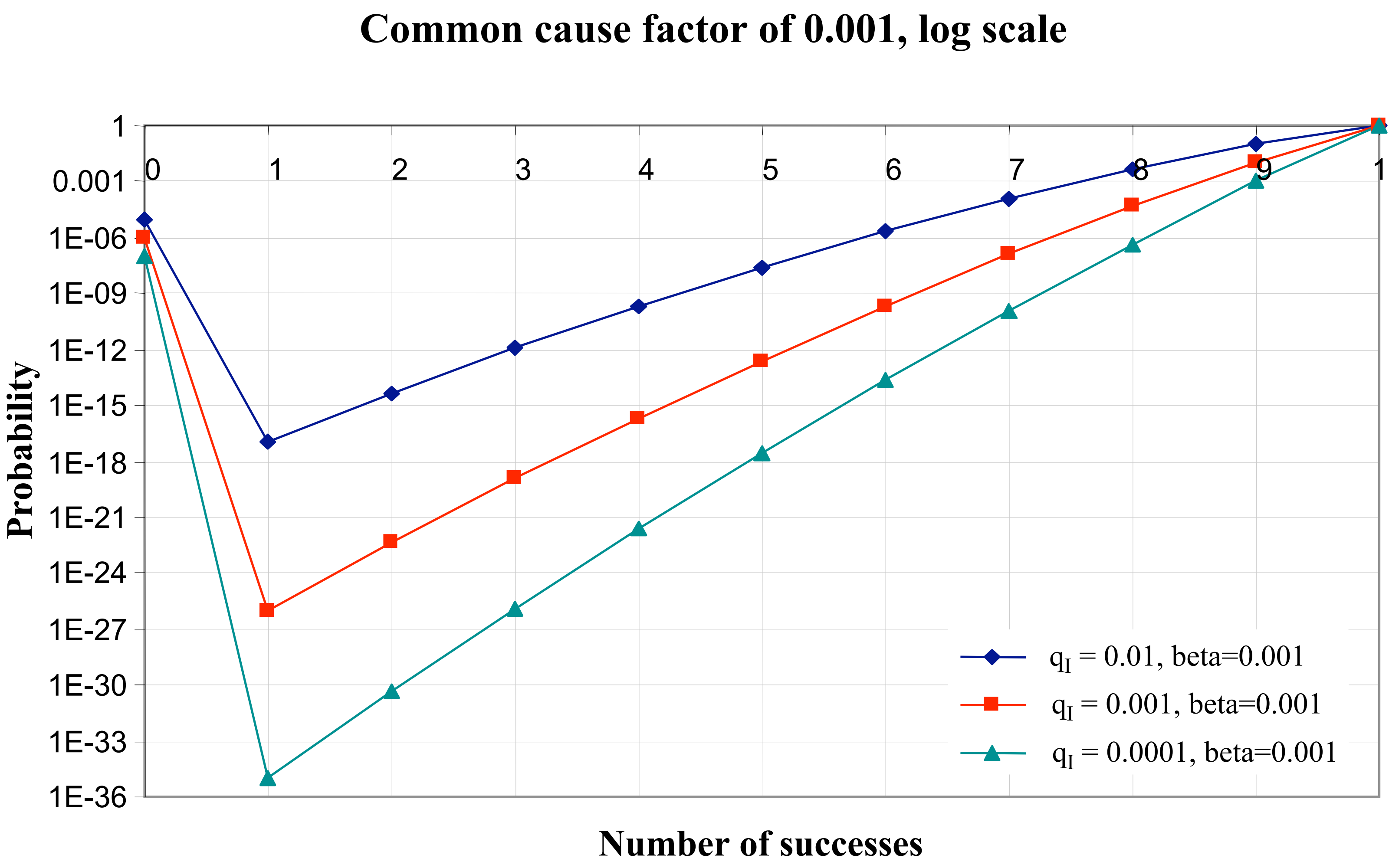
COMMON CAUSE FAILURE – β FACTOR METHOD (continued)



COMMON CAUSE FAILURE – β FACTOR METHOD
(continued)



COMMON CAUSE FAILURE – β FACTOR METHOD
(continued)


Common cause factor of 0.001, log scale
Probability
1E-06
1E-09
1E-12
1E-15
1E-18
1E-21
1E-24
1E-27
1E-30
1E-33
1E-36
Number of successes
q_I = 0.01, beta=0.001
q_I = 0.001, beta=0.001
q_I = 0.0001, beta=0.001