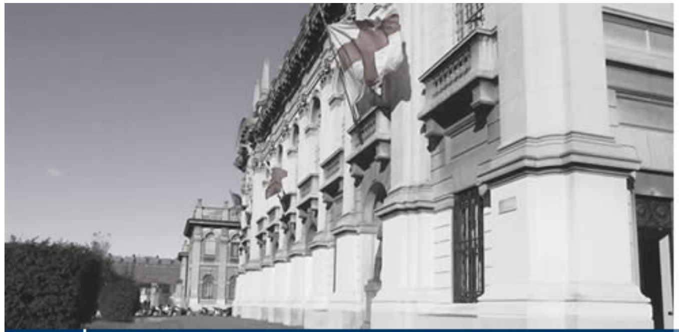


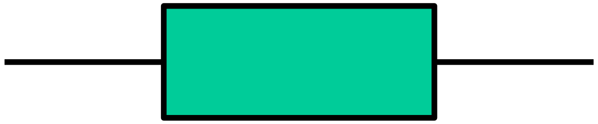
CRC
Centre de recherche
sur les Risques et les Crises

POLITECNICO
MILANO

POLITECNICO DI MILANO

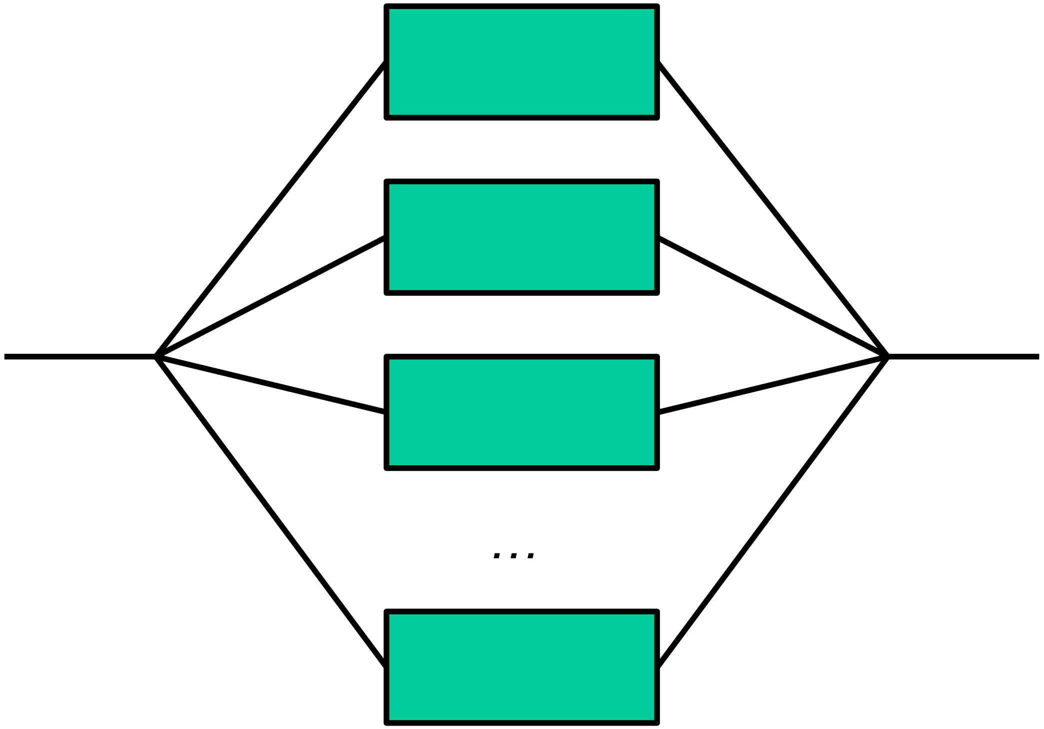
Dependent Failures

An Example



U_c=0.2

How many components should be added in parallel to achieve a system unreliability of the order of 10^{-10}?

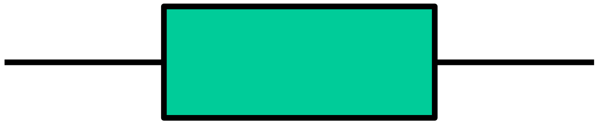


$U_s=(U_c)^n$

$\Downarrow$

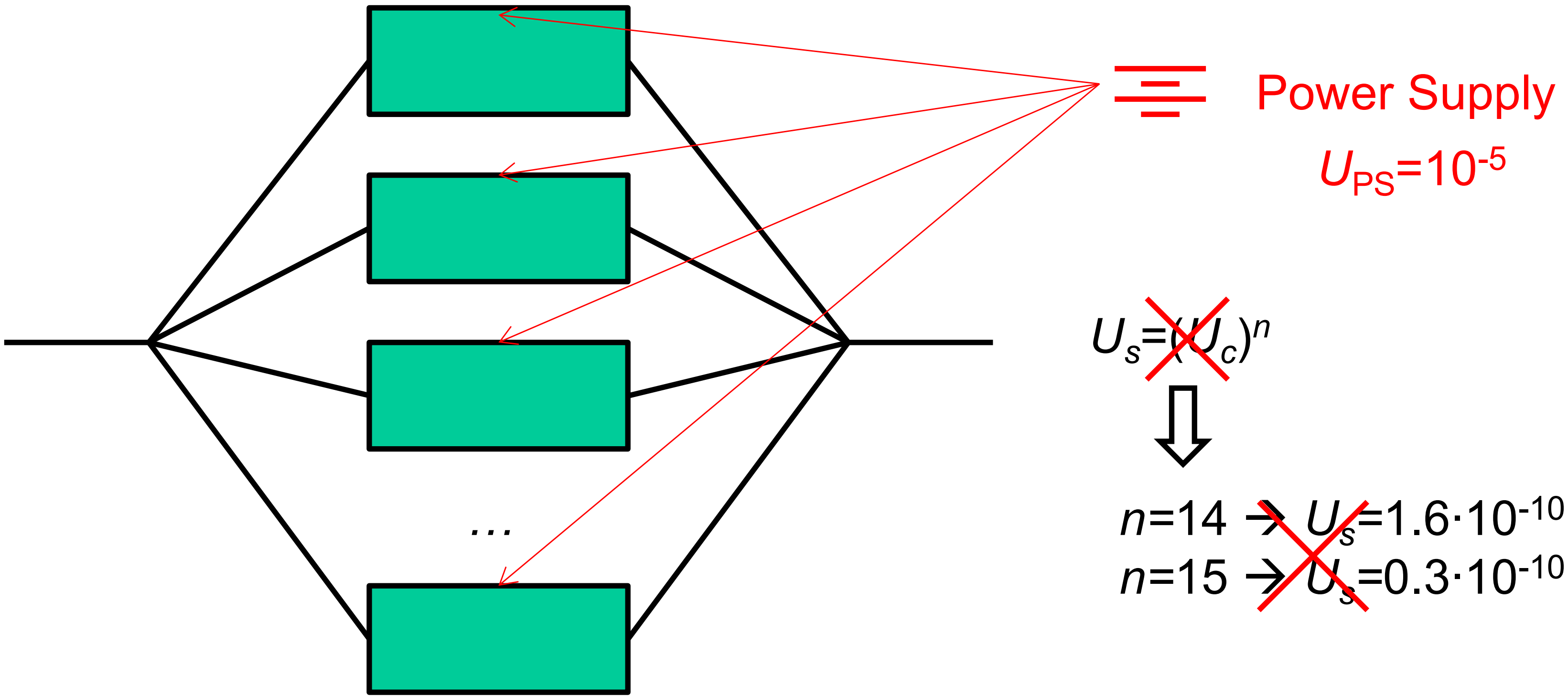
n=14 → $U_s=1.6\cdot10^{-10}$
n=15 → $U_s=0.3\cdot10^{-10}$

An Example: dependent failures



$U_c=0.2$

How many components should be added in parallel to achieve a system unreliability U_s lower than 10^{-10}?



$$\cancel{U_s=(U_c)^n}$$

$$\Downarrow$$

$$n=14 \rightarrow \cancel{U_s}=1.6\cdot10^{-10}$$
$$n=15 \rightarrow \cancel{U_s}=0.3\cdot10^{-10}$$

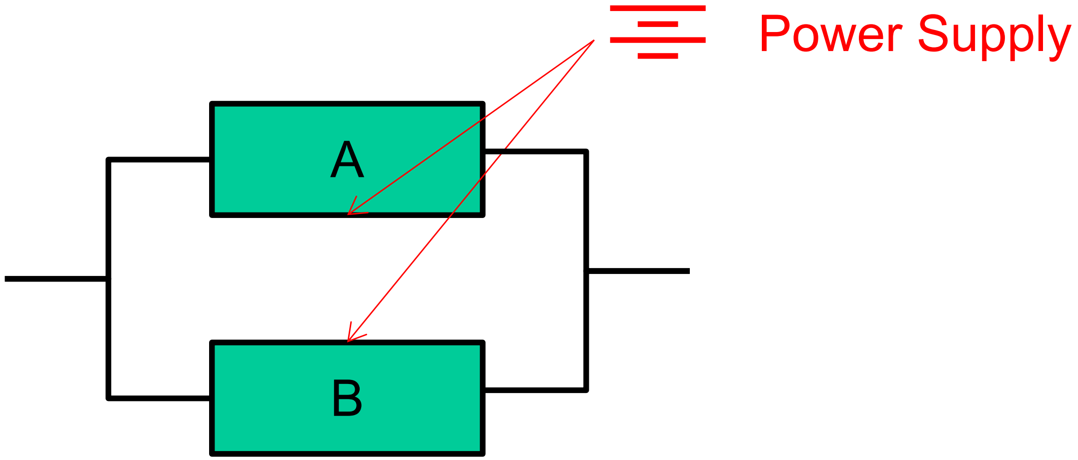
Ignoring dependent failure → gross underestimation of risk !!!

Why?

- All modern technological systems are highly redundant but still fail because of dependent failures. This is because dependent failures can defeat redundant protective barriers and thus contribute significantly to risk; quantification of such contribution is thus necessary to avoid gross underestimation of risk.
- The modeling of this kind of failures is still a critical issue in PSA (Probabilistic Safety Assessment).

Definition of dependent failures

$$P(A \cap B) = P(A|B) \cdot P(B) \neq P(A) \cdot P(B)$$



General Classification

i. Common Cause Failures (CCF): multiple failures that result directly from a common or shared root cause

- Extreme enviromental conditions
- Failure of a shared piece of hardware external to the systems
- Human Error (operational or maintenance)

e.g. fire at Browns Ferry Nuclear Power Plant (1975)

ii. Cascading Failures: several component share a common load → 1 component failure may lead to increase load on the remaining ones → increased likelihood of failure

e.g. 2003 northeast Blackout

Identification of dependent failures

~~Traditional techniques (FMEA)~~

↓

Dedicated analysis

Protection from dependent failures

- Barriers (physical impediments that tend to confine and/or restrict a potentially damaging condition)
- Personnel training (ensure that procedures are followed in all operation conditions)
- Quality control (ensure the product is conforming with the design and its operation and maintenance follow the approved procedures and norms)
- Preventive maintenance
- Monitoring, testing and inspection (including dedicated tests performed on redundant components following observed failures)
- Diversity (equipment diversity as for manufacturing, functional diversity as for the physical principle of operation)

Types of probabilistic dependence

- Common Cause initiating event (external event, e.g. fires, floods, earthquakes, loss of off-site power, aircraft crashes, gas clouds)
- Intersystem dependences (the conditional probability of failure for a given system along an accident sequence depends from the success or failure of the system that precedes it in the sequence)
  - Fuctional: System 2 functions only if system 1 fails
  - Shared-equipment dependences: components in different systems fed by the same electrical bus
  - Physical interactions: failure of one system to provide cooling results in excessive temperature which causes the failure of a set of sensors.
  - Human interaction dependences: operator turns off a system after failing to correctly diagnose the conditions of a plant
- Intercomponent dependences
  - same cases of intersystem dependences

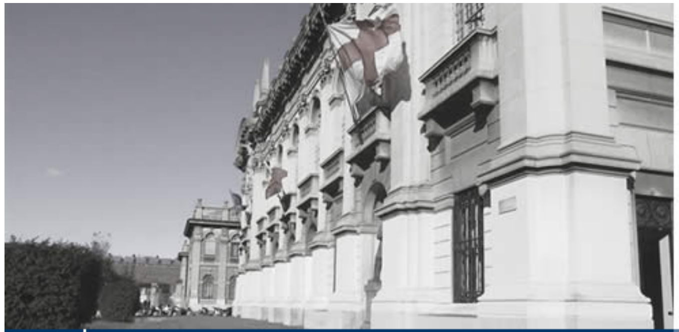
Methods for dependent-failure analysis

- **Explicit methods:**

  Involve the identification and treatment of specific root causes of dependent failures at the system level, in the event and fault-tree logic.

- **Implicit methods**

  Multiple failure events, for which no clear root cause event can be identified and treated explicitly, can be modeled using implicit, parametric models.



POLITECNICO DI MILANO

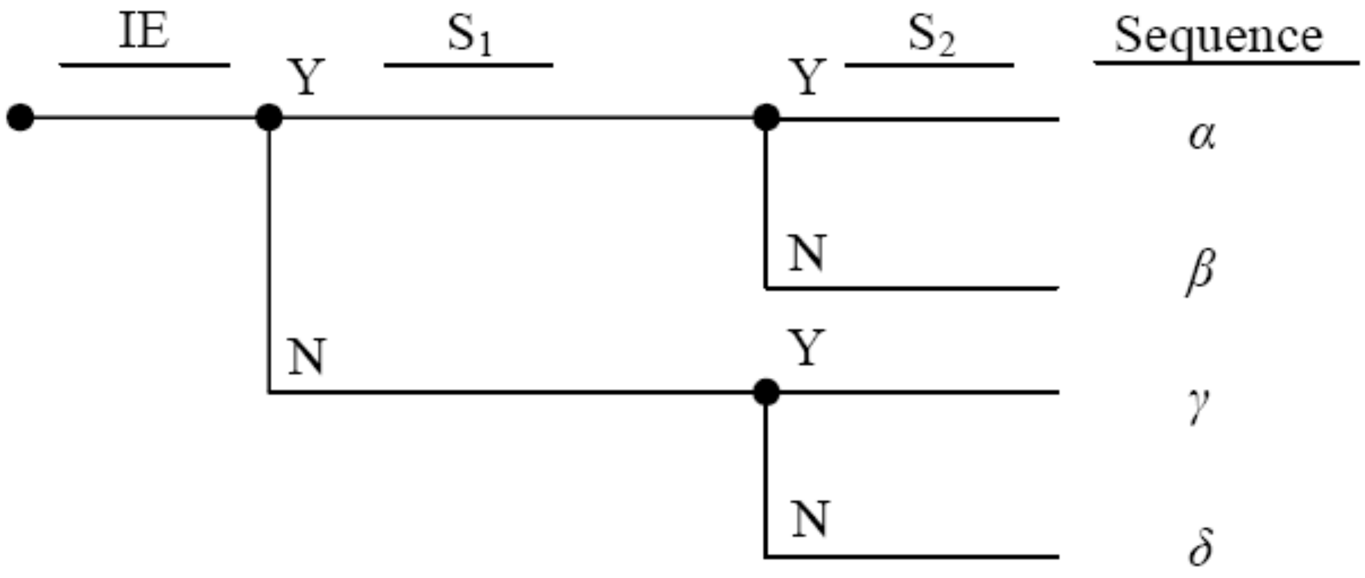
Explicit methods

1. Common Cause initiating events

- External events (earthquakes, fires and floods) are treated explicitly as initiating events in the risk analysis.

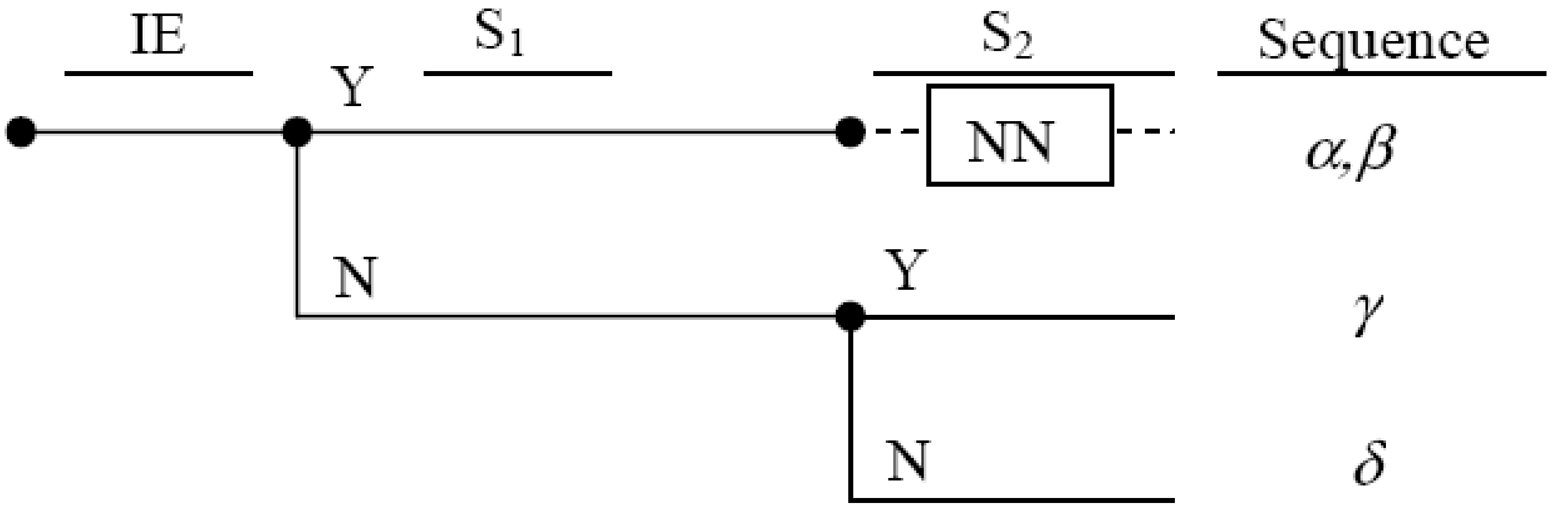
2. Intersystem dependences

- Two safety systems S1 and S2 are expected to intervene upon the occurrence of an initiating event (IE)

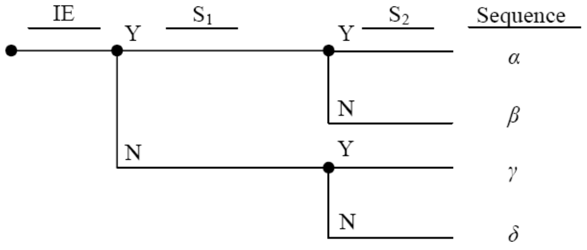


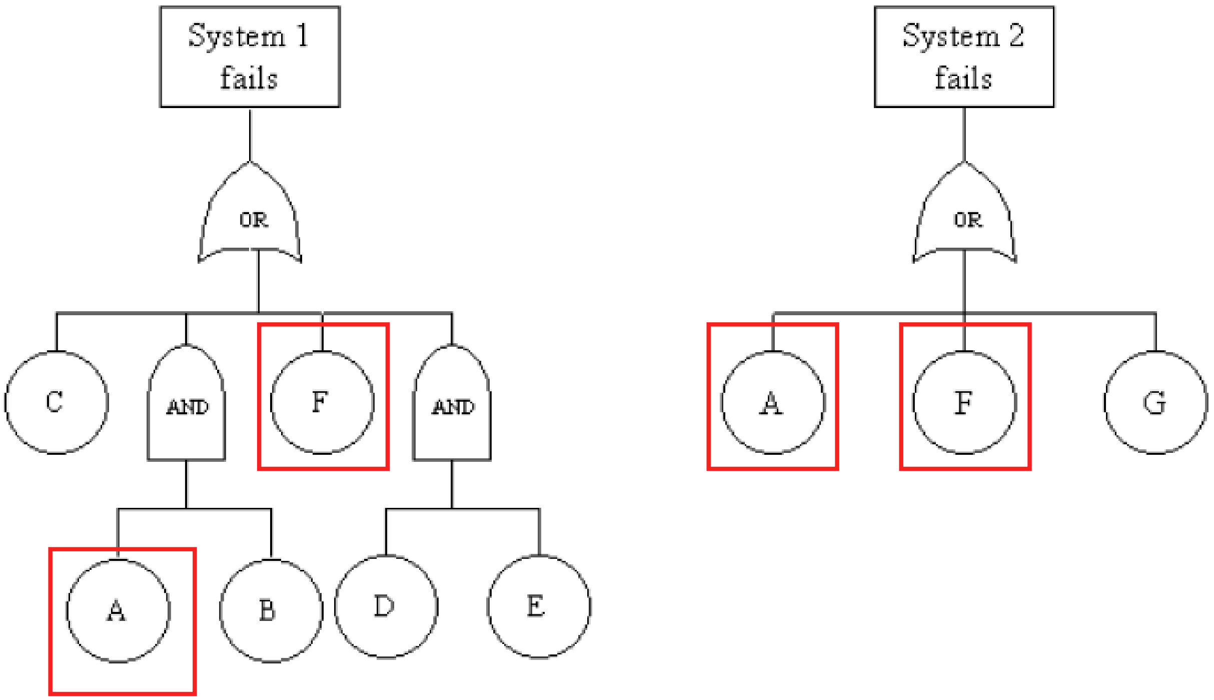
2.A: Functional dependences

System 2 is not needed (NN) unless system 1 fails



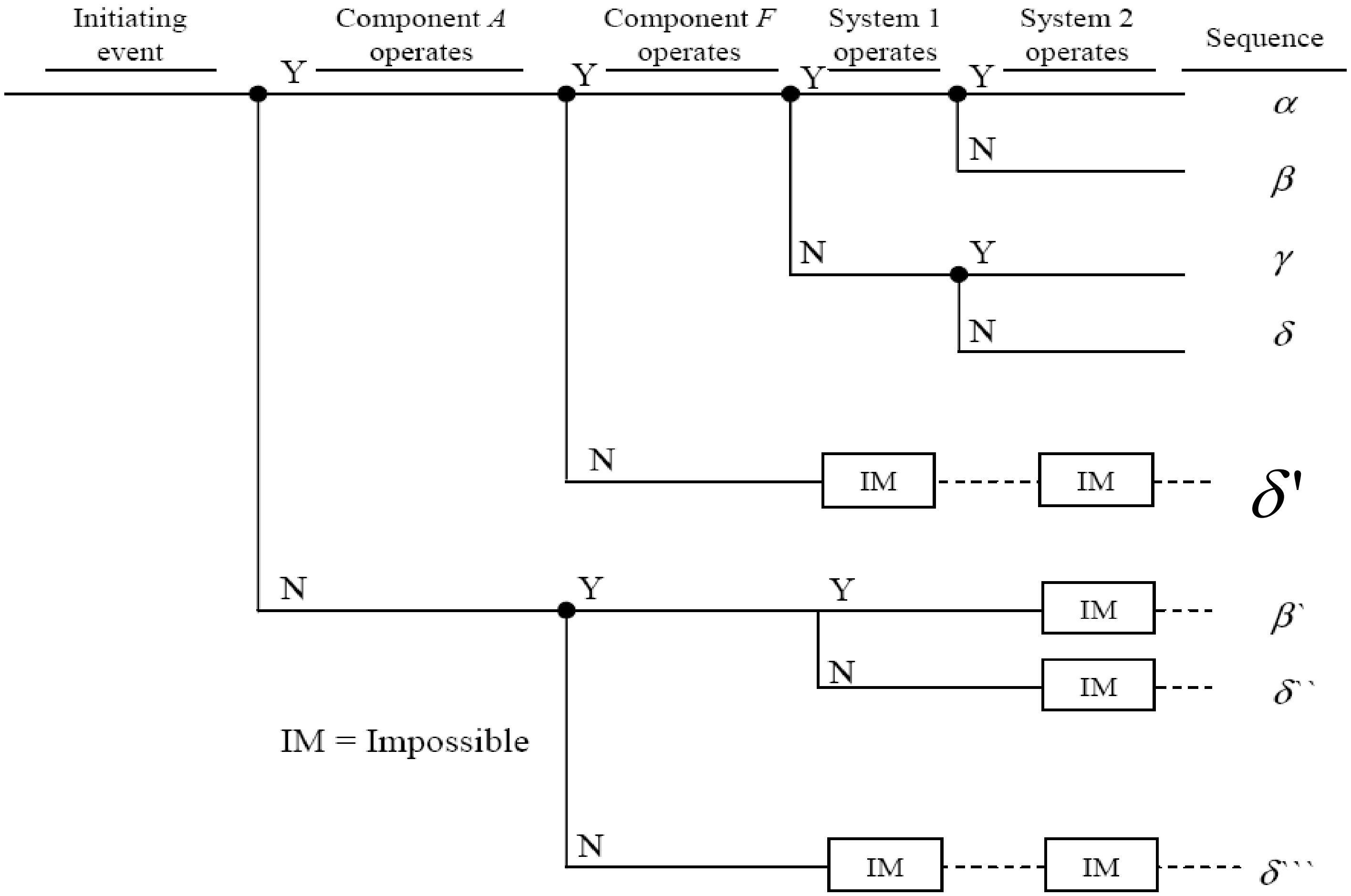
2.B Shared equipment





Method of the ‘event trees with boundary conditions’

1. Develop the event tree

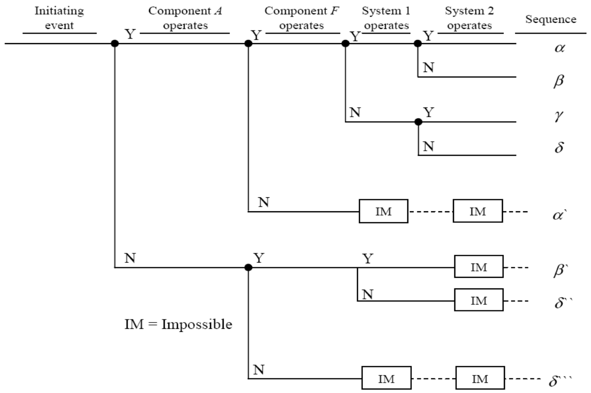


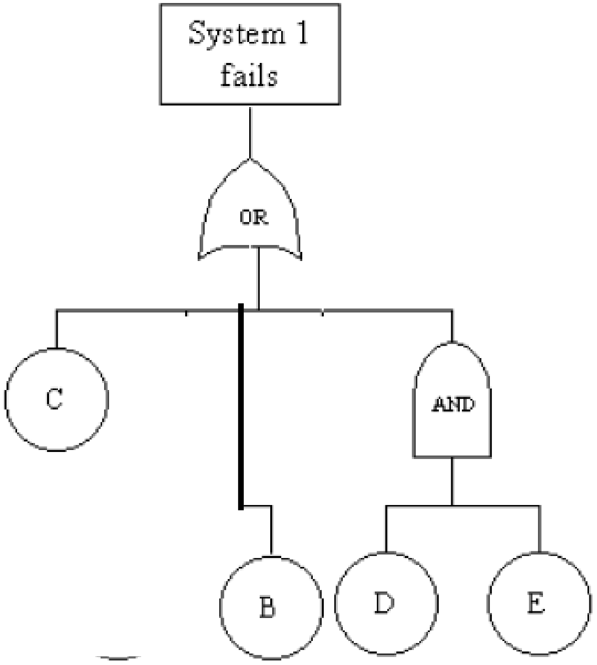
IM = Impossible

Method of the 'event trees with boundary conditions'

- 2. To evaluate the probabilities, develop the conditional fault trees
  - sequence δ'' (P(A)=1, P(F)=0) →

system 1 mcs= {C,B,DE}



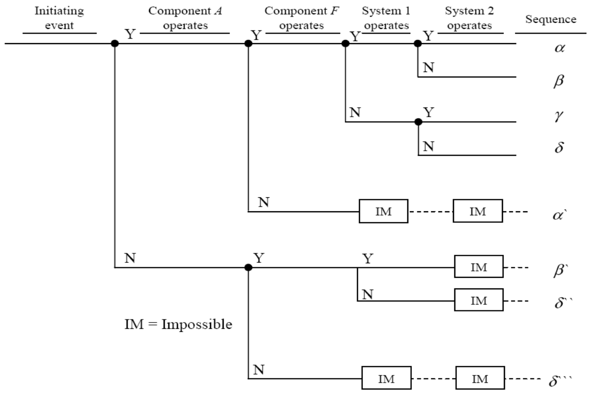


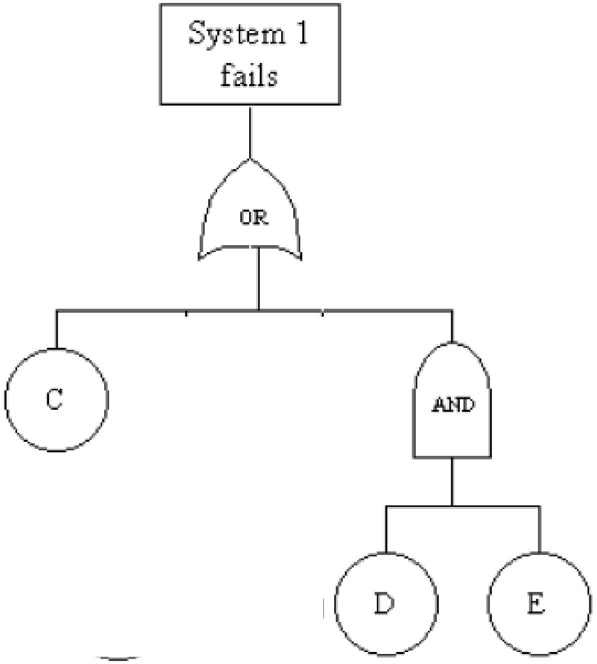
Method of the ‘event trees with boundary conditions’

- 2. To evaluate the probabilities, develop the conditional fault trees
  - sequence δ'' (P(A)=1, P(F)=0) →

    system 1 mcs= {C,B,DE}
  - sequence δ (P(A)=0, P(F)=0) →

    system 1 mcs= {C,DE}

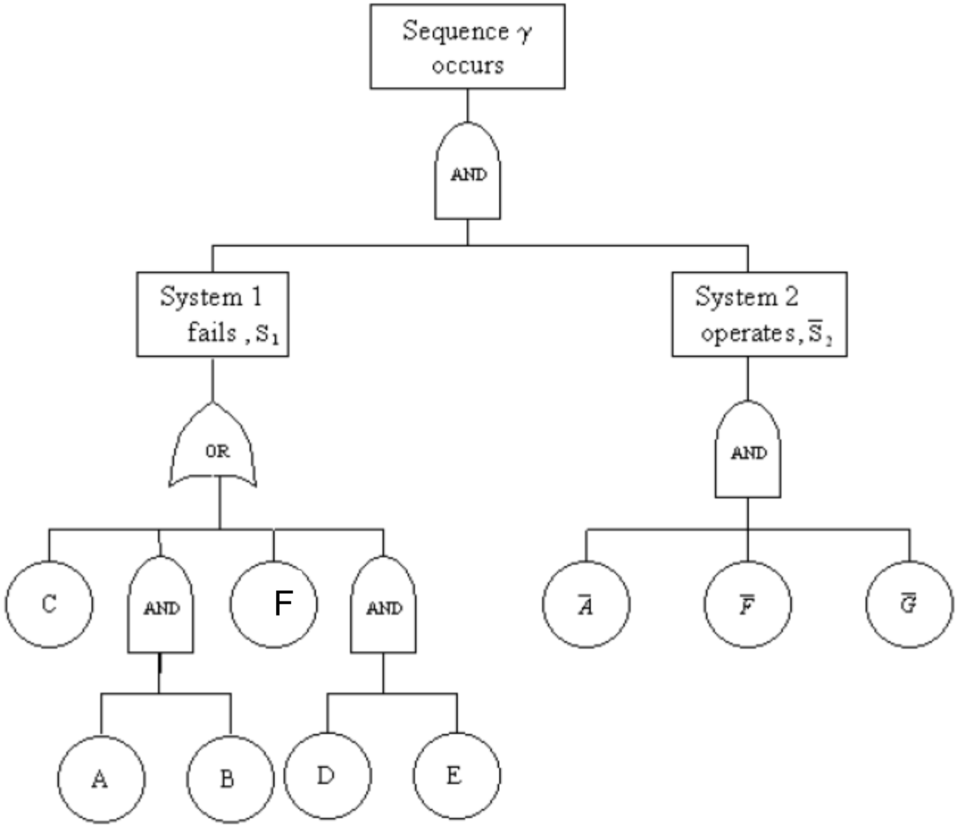




Method of ‘Fault tree link”

The fault trees of systems S1 and S2 are linked together, thus developing a single large fault tree for each accident sequence

- Sequence γ = “S1 fails and S2 operates”

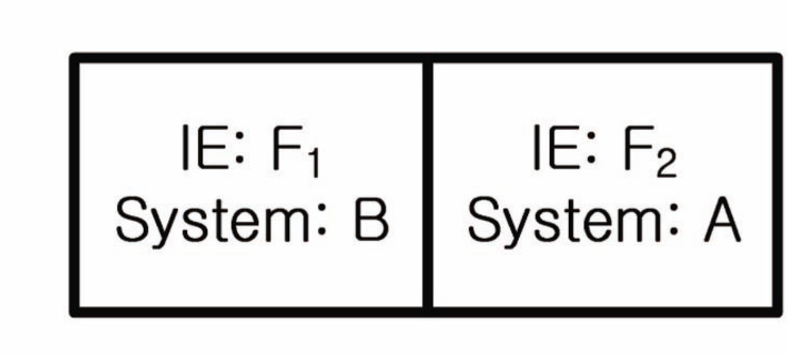


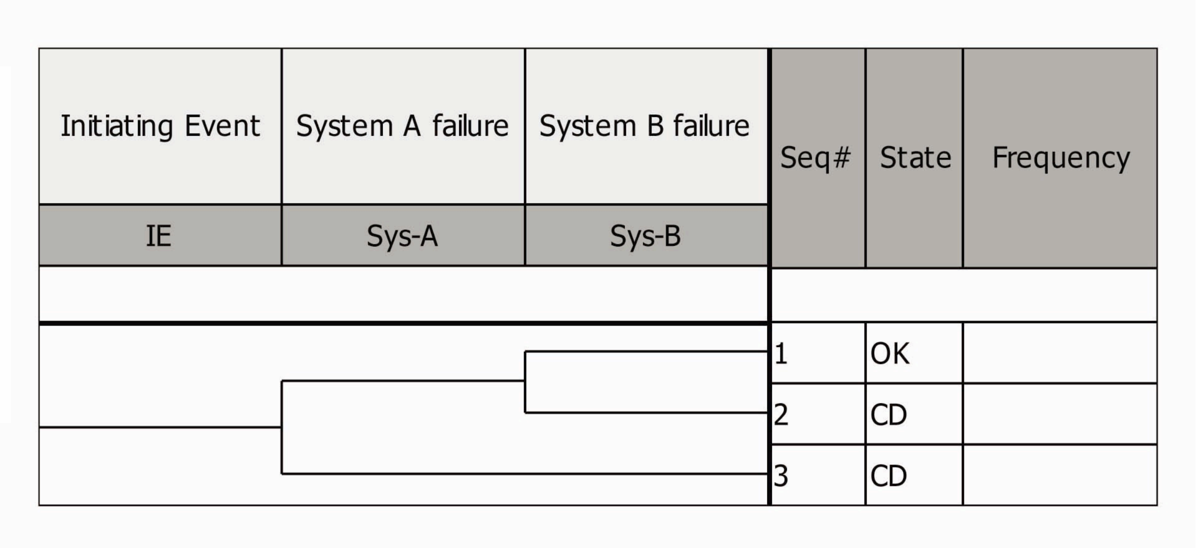
$$\gamma = S1 \cap \overline{S_2} = [(A \cap B) \cup C \cup (D \cap E) \cup F] \cap [\bar{A} \cap \bar{F} \cap \bar{G}] =$$
$$= [(A \cap B) \cap (\bar{A} \cap \bar{F} \cap \bar{G})] \cup [C \cap (\bar{A} \cap \bar{F} \cap \bar{G})] \cup$$
$$\cup [(D \cap E) \cap (\bar{A} \cap \bar{F} \cap \bar{G})] \cup [F \cap (\bar{A} \cap \bar{F} \cap \bar{G})] =$$
$$= [C \cap (\bar{A} \cap \bar{F} \cap \bar{G})] \cup [(D \cap E) \cap (\bar{A} \cap \bar{F} \cap \bar{G})]$$

$$mcs = \left\{ \bar{\mathrm{A}}\bar{\mathrm{F}}\bar{\mathrm{G}}\mathrm{C}; \bar{\mathrm{A}}\bar{\mathrm{F}}\bar{\mathrm{G}}\mathrm{DE} \right\}$$

Example of Method of 'Fault tree link"

Two different fire events occur in two fire compartments, and the fire events follow the accident sequences in the event tree.





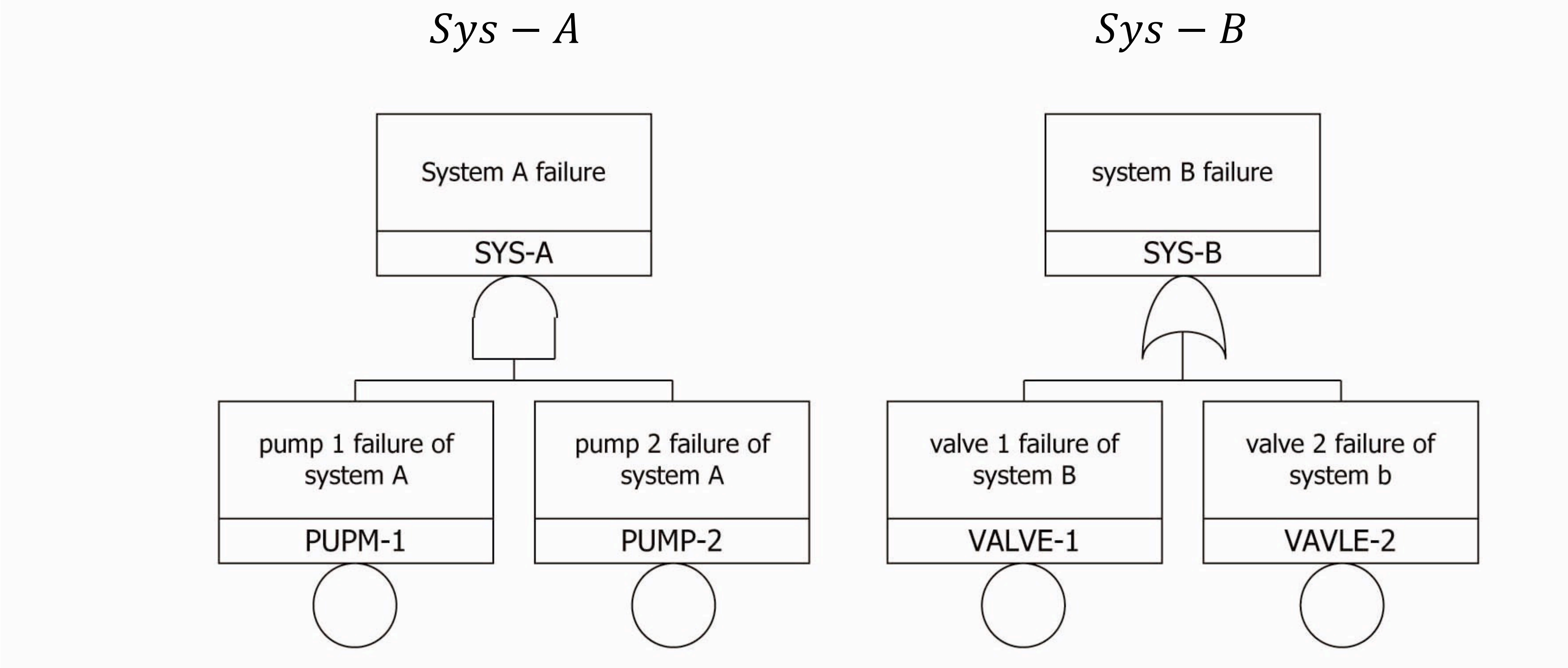
Initiating Event	System A failure	System B failure	Seq#	State	Frequency
IE	Sys-A	Sys-B			
			1	OK	
			2	CD	
			3	CD	

- Safety scenario: $IE * \overline{Sys-A} * \overline{Sys-B}$ 1
- Accident scenarios: $IE * \overline{Sys-A} * Sys-B$ 2

  $IE * Sys-A$ 3

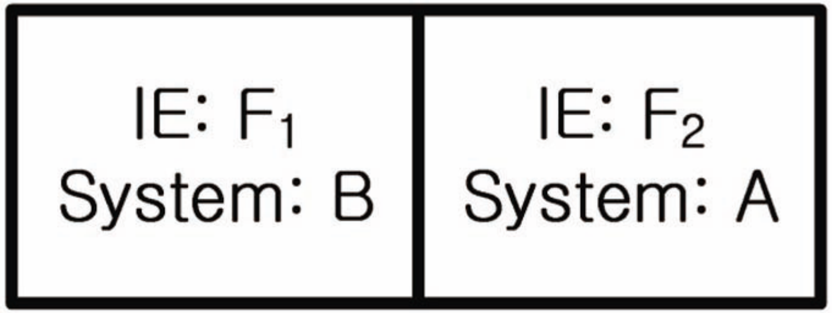
Example of Method of ‘Fault tree link”

The fault trees of Sys-A and Sys-B


$Sys - A$
$Sys - B$
System A failure
SYS-A
system B failure
SYS-B
pump 1 failure of system A
PUPM-1
pump 2 failure of system A
PUMP-2
valve 1 failure of system B
VALVE-1
valve 2 failure of system b
VAVLE-2

Example of Method of ‘Fault tree link”

To model fire risk by using the mapping method.



IE: F_1
System: B

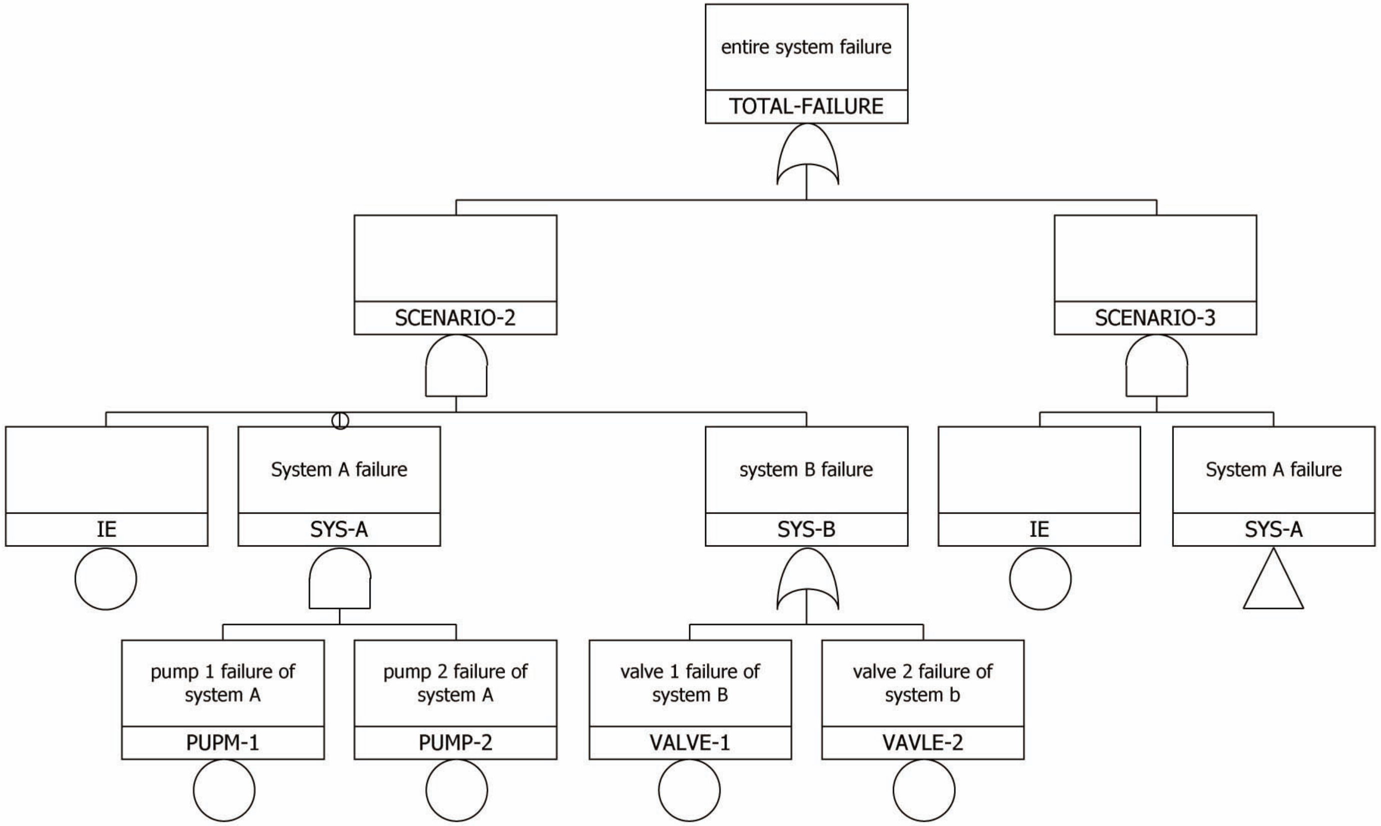
IE: F_2
System: A

- Map the fire initiating events
- IE -> $F_1 + F_2$
- PUMP-1 -> PUMP-1 + $F_2 * CF_{21}$, PUMP-2 -> PUMP-2 + $F_2 * CF_{22}$
- VALVE-1 -> VALVE-1 + $F_1 * CF_{11}$, VALVE-2 -> VALVE-2 + $F_1 * CF_{12}$

- *F_i – the frequency of the fire event in the compartment i*
- *CF_{ij} – a conditional failure of component j by F_i*

Example of Method of ‘Fault tree link”

Link the event tree with the fault trees of Sys-A and Sys-B, to generate a entire system fault tree



- Minimal Cut Sets: IE*VALVE-1

  IE*VALVE-2

  IE*PUMP-1*PUMP-2

Example of Method of ‘Fault tree link”

Assume an external event follows the same accident sequences in the event tree, and the systems (Sys-A and Sys-B) have an additional failure event caused by the external event

The mapping events due to the external event:

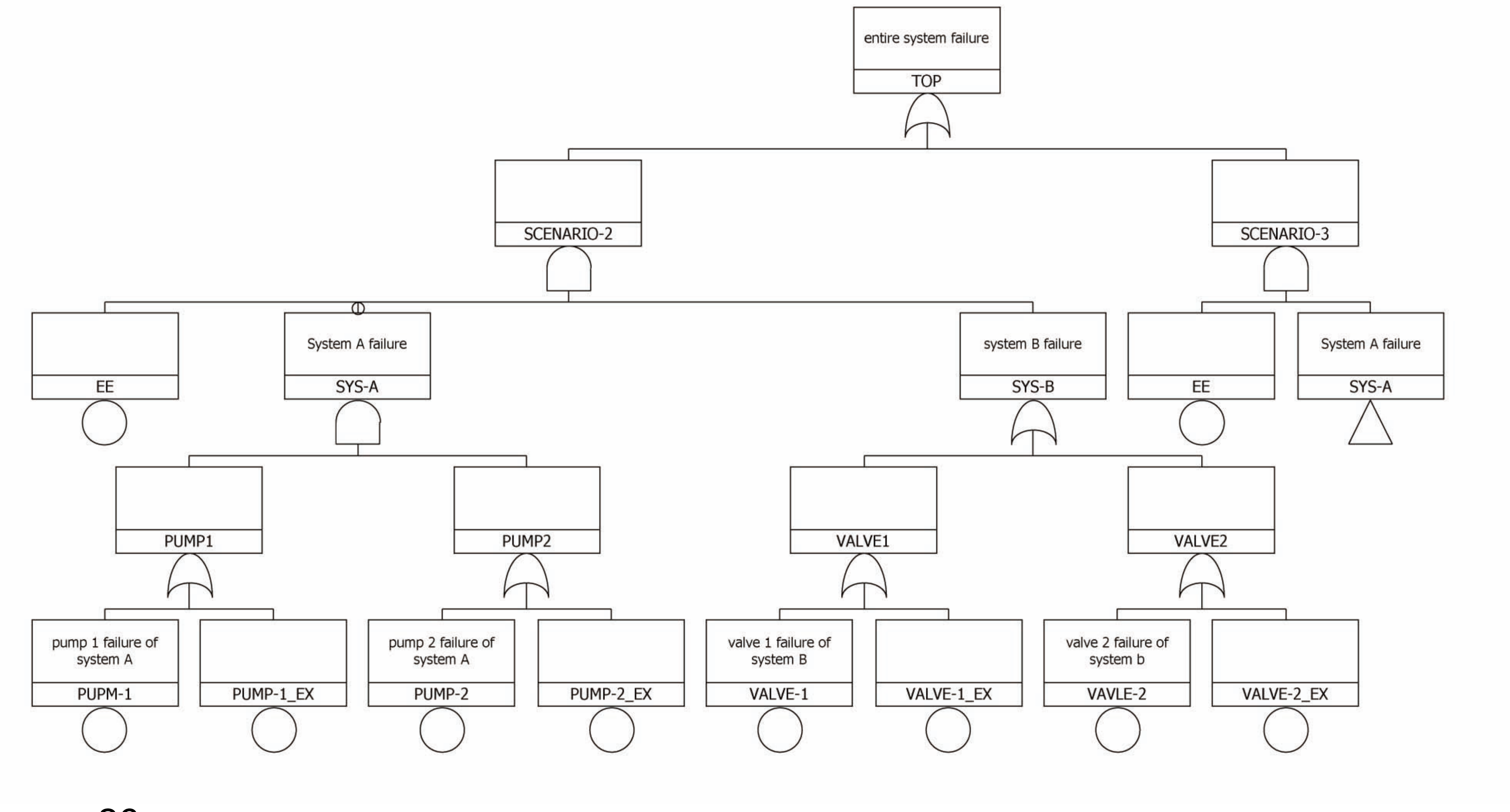
- IE -> EE
- PUMP-1 -> PUMP-1 +PUMP-1_EX
- PUMP-2 -> PUMP-2 +PUMP-2_EX
- VALVE-1 -> VALVE-1 + VALVE-1_EX
- VALVE-1 -> VALVE-1 + VALVE-1_EX

“EE” – an external initiating event.

“_EX” – a component failure caused by an external event.

Example of Method of ‘Fault tree link”

The ***“entire fault tree”*** generated by the mapping events

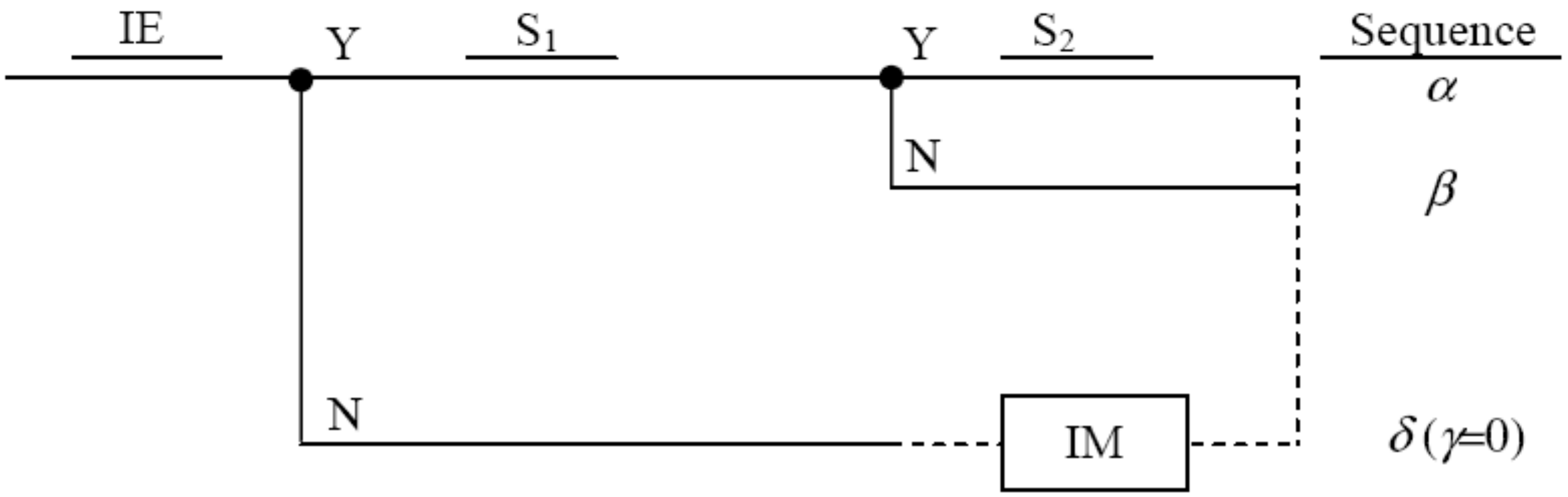


2.B Shared equipment: comments

- Methods:
  - Event tree with boundary conditions (analyst must explicitly recognize the shared equipment dependence)
  - Fault tree links (share equipment dependence is automatically accounted for in the mcs)
- Correctly applied → Same results

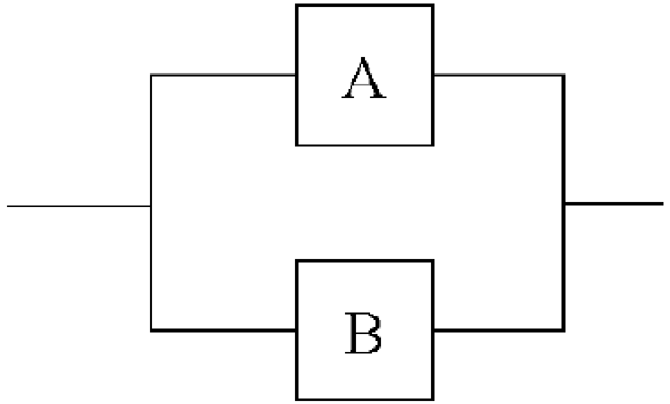
2.C Physical interactions

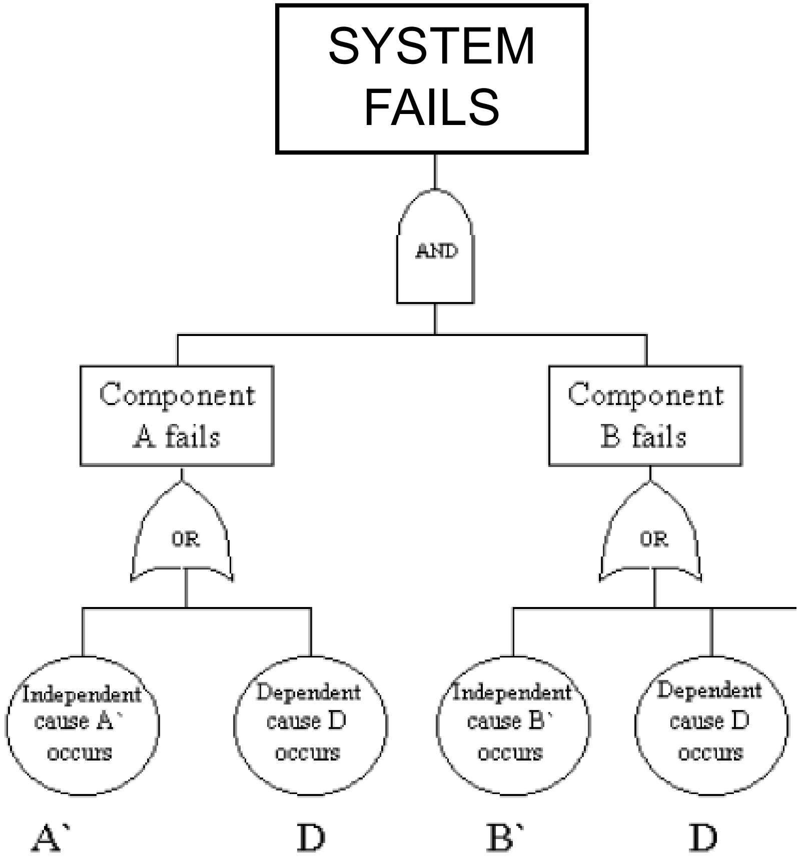
- System S2 can operate only if system S1 operates successfully. When system S1 fails a physical interaction takes place, which inhibits system S2 → Sequence γ is impossible



3. Intercomponent dependences (common cause failure)

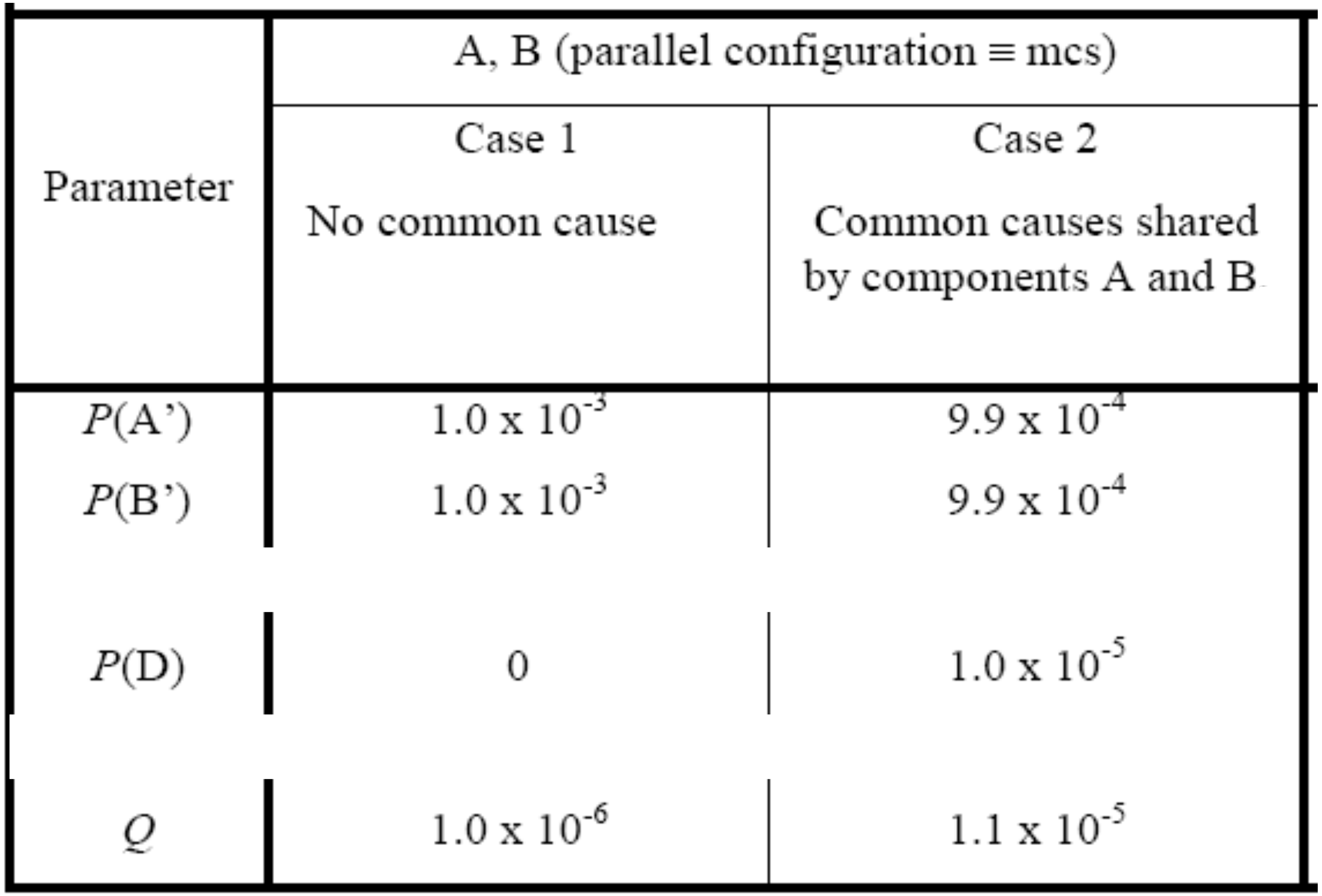
- Parallel system





Minimal cut sets	
Without common causes of failures	With common causes of failures
$A \cap B$	$A' \cap B'$ D

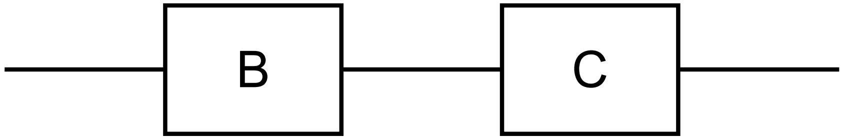
Numerical example (Parallel)

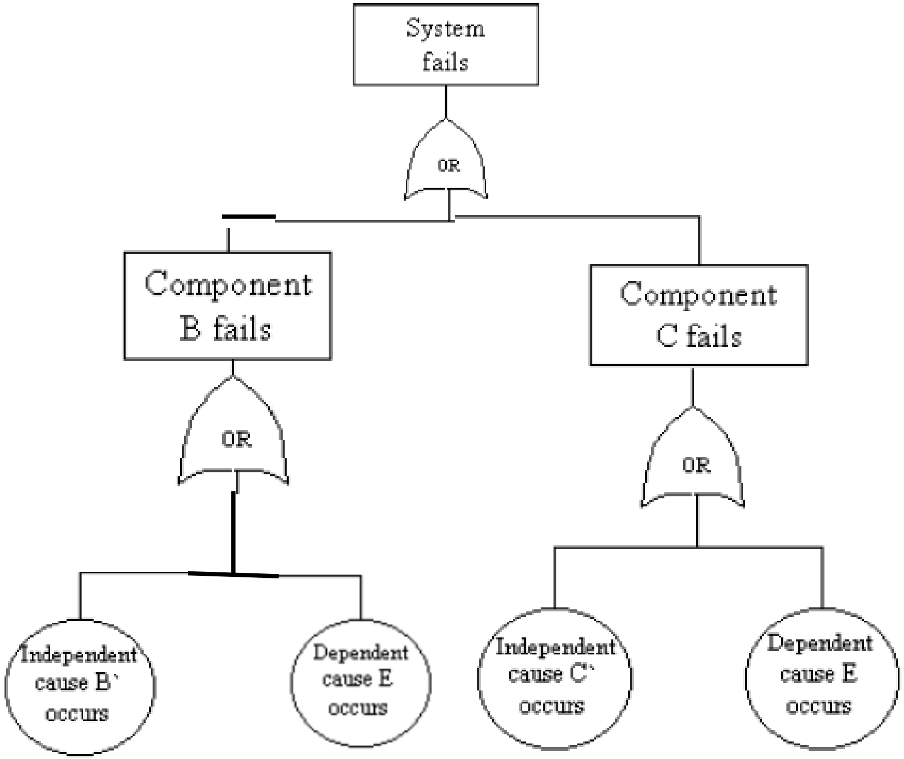


Parameter	A, B (parallel configuration ≡ mcs)	
	Case 1 No common cause	Case 2 Common causes shared by components A and B
P(A’)	1.0×10^{-3}	9.9×10^{-4}
P(B’)	1.0×10^{-3}	9.9×10^{-4}
P(D)	0	1.0×10^{-5}
Q	1.0×10^{-6}	1.1×10^{-5}

3. Intercomponent dependences

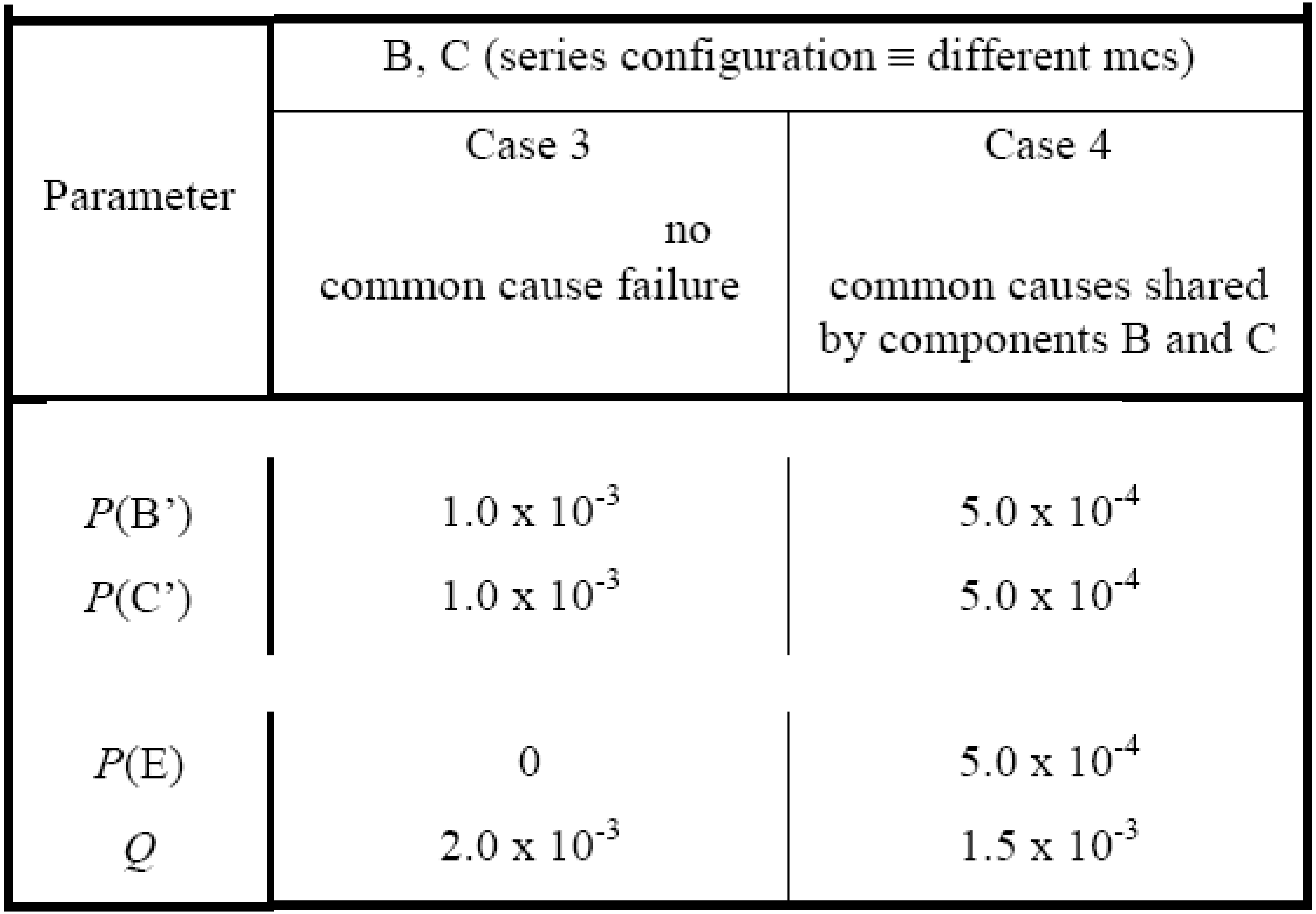
- Series System





Minimal cut sets	
Without common causes of failures	With common causes of failures
B C	B' C' E

Numerical example (Series)



Parameter	B, C (series configuration ≡ different mcs)	
	Case 3 no common cause failure	Case 4 common causes shared by components B and C
P(B’)	1.0 x 10^{-3}	5.0 x 10^{-4}
P(C’)	1.0 x 10^{-3}	5.0 x 10^{-4}
P(E)	0	5.0 x 10^{-4}
Q	2.0 x 10^{-3}	1.5 x 10^{-3}

3. Intercomponent dependencies

Neglecting the causes of dependent failures (i.e., assuming independence in the component unavailabilities) leads to:

- Optimistic predictions of system availability for components in the same mcs (i.e., in parallel)
- Conservative predictions of system availability for components in different mcs (i.e. in series)

Implicit methods

Multiple failure events, for which no clear root cause event can be identified and treated explicitly, can be modeled using implicit, parametric models

Square root method (1) [Reactor safety study, WASH 1400]

- Parallel system of 2 component $A, B \Rightarrow \ U = P(A \cap B)$

$$\left.\begin{array}{l} P(A \cap B) \le P(A) \\ P(A \cap B) \le P(B) \end{array}\right. \Rightarrow P(A \cap B) \le \min\left[P(A), P(B)\right] \qquad (1)$$

- If A and B are independent $\Rightarrow P(A \cap B) = P(A) \cdot P(B)$

  If A and B are positively dependent $\Rightarrow P(A \mid B) \ge P(A)$

⇒

$$P(A \cap B) = P(A \mid B) \cdot P(B) \ge P(A) \cdot P(B) \qquad (2)$$

- Combining (1)+(2) $\Rightarrow \underbrace{P(A) \cdot P(B)}_{P_L} \le P(A \cap B) \le \underbrace{\min\left[P(A), P(B)\right]}_{P_U}$

Square root method (2)

$$\underbrace{P(A)\cdot P(B)}_{P_L} \le P(A\cap B) \le \min\underbrace{\left[P(A), P(B)\right]}_{P_U}$$

Estimate $P(A\cap B)$ by using the geometric average of P_L and P_U (no proven theoretical foundation)

$$P_M(A\cap B) = \sqrt{P_L \cdot P_U}$$

Example (1)

- System of *n* identical component   in parallel
- Unavailability of the single component at time *t* : $U_c = 10^{-2}$

Estimate the system unavailability at time *t*

$$P_L = \prod_{i=1}^{n} P(A_i) = (U_c)^n$$

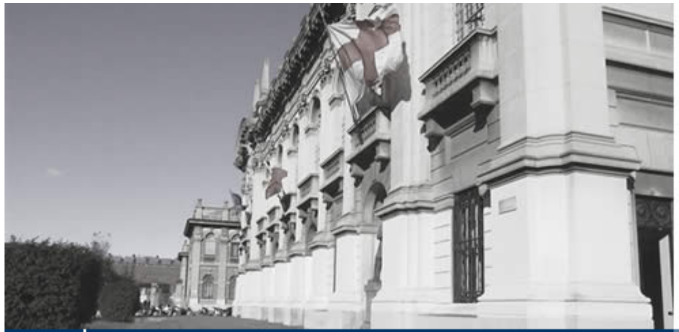
$$P_U = \min[P(A_1), P(A_2), \ldots, P(A_n)] = U_c$$

$$\Rightarrow U_s = \sqrt{P_L \cdot P_M} = (U_c)^{\frac{n+1}{2}}$$

Example (2)

n	Independent components $U_s = (U_c)^n$	Square root method $U_s = (U_c)^{\frac{n+1}{2}}$
1	10^{-2}	10^{-2}
2	10^{-4}	10^{-3}
3	10^{-6}	10^{-4}
4	10^{-8}	10^{-5}
5	10^{-10}	10^{-6}

Note how the difference in the system unavailability under the dependence and independence assumptions increases as the number of components *n* increases



POLITECNICO DI MILANO

A methodological framework for Common Cause Failures (CCF) analysis

CCF in PSA

i. System logic model development

ii. Identification of common-cause component groups

iii. Common-cause modeling and data analysis

iv. System quantification and interpretation of results

CCF in PSA

i. System logic model development

ii. Identification of common-cause component groups

iii. Common-cause modeling and data analysis

iv. System quantification and interpretation of results

System logic model development

OBJECTIVE:

identify and understand the physical and functional links in the system, the functional dependences and interfaces and to develop the corresponding logic models of the system (fault trees and event trees), which include the proper representation of the identified dependences

STEPS:

- System familiarization (*particular attention must be paid to identifying those elements of design, operation, maintenance, and test procedures that could increase the chance of multiple component failures*).
- Problem definition, e.g. physical and functional boundaries of the system, functional dependencies on other systems, functional interfaces with other systems, system success criteria (*root causes of common failures to be included in the analysis*)
- Logic model development, i.e. relationship between the system state and component states, e.g. fault tree.

CCF in PSA

- i. System logic model development
- ii. Identification of common-cause component groups
- iii. Common-cause modeling and data analysis
- iv. System quantification and interpretation of results

Identification of common-cause component groups

OBJECTIVES:

- Identifying group of components potentially involved in dependent failures and thus to be included in the CCF analysis
- Prioritizing the groups for the best resource allocation of the successive analysis
- Providing engineering arguments for data analysis related to common cause failure events and for the identification of defense alternatives to protect against dependent failures

DEFINITION OF COMMON CAUSE COMPONENT GROUPS:

"a group of similar or identical components that have a significant likelihood of experiencing a common cause event"

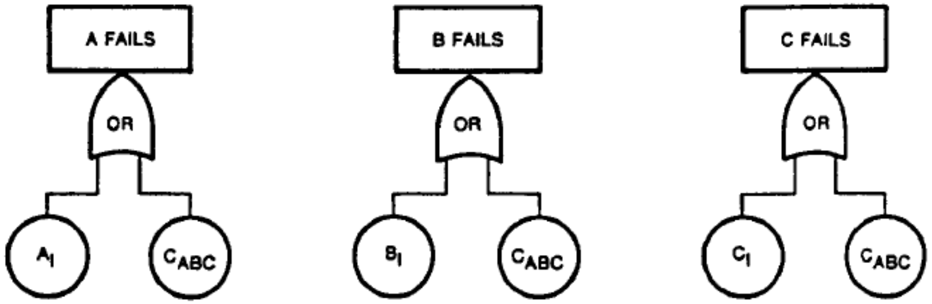
Qualitative screening

- Check-list:
- Similarity of component type
- Similarity of component use
- Similarity of component manufacturer
- Similarity of component internal conditions (pressure, temperature, chemistry)
- Similarity of component boundaries and system interfaces
- Similarity of component location name and/or code
- Similarity of component external environmental conditions (humidity, temperature, pressure)
- Similarity of component initial conditions and operating characteristics (standby, operating)
- Similarity of component testing procedures and characteristics
- Similarity of component maintenance procedures and characteristics

- Practical guidelines to be followed in the assignment of component groups:
- Identical components providing redundancy in the system should always be assigned to a common cause group
- Diverse redundant components which have piece parts that are identically redundant, should not be assumed fully independent in spite of their diversity
- Susceptibility of a group of components to CCFs not only depends on their degree of similarity but also on the existence/lack of defensive measures (barriers) against CCFs.

Quantitative Screening

- A complete quantitative common cause analysis except that a conservative and very simple quantification model is used. The following steps are carried out:
  - The fault trees are modified to explicitly include a single CCF basic event for each component in a common cause group that fails ***all*** members of the group, e.g. if component A,B and C are in the same common cause group



  - The fault trees are solved to obtain the minimal cut sets
  - Numerical values for the probabilities of the CCF basic events can be estimated by the beta factor model (conservative regardless of the number of components in the CCF basic event) :

    $P(C_{ABC}) = \beta P(A)$ β=0.1 for screening

    P(A) = total failure probability in absence of common cause
  - Those common cause failure events which are found to contribute little to the overall system failure probability are screened out

CCF in PSA

i. System logic model development

ii. Identification of common-cause component groups

iii. Common-cause modeling and data analysis

iv. System quantification and interpretation of results

Common cause failure modeling and data analysis

OBJECTIVE:

complete the system quantification by incorporating the effects of common cause events for those component groups that survive the screening

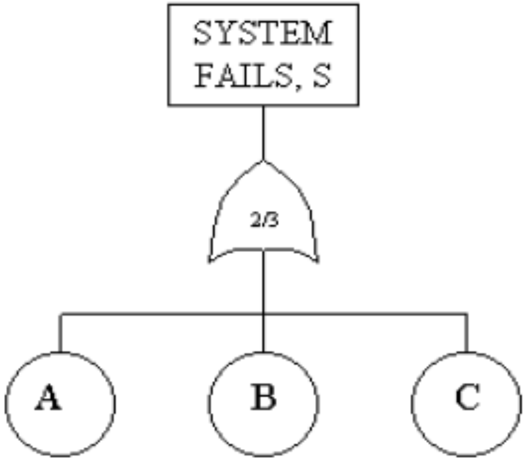
STEPS:

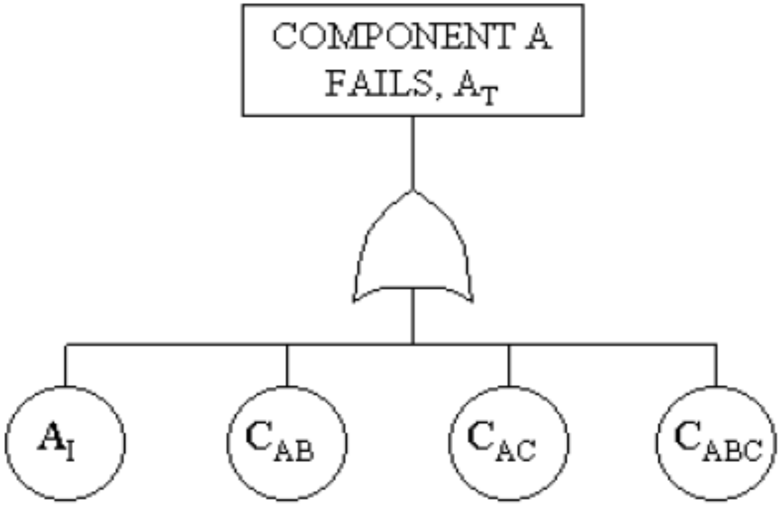
1. Definition of common cause basic events
2. Selection of implicit probability models for common cause basic events
3. Data classification and screening
4. Parameter estimation

Definition of common cause basic events (an example)

Component level ⇨ Common cause impact level

(each component basic event becomes a sub tree)





mcs: $\{A \cap B\}, \{A \cap C\}, \{B \cap C\}$

$$S = (A \cap B) \cup (A \cap C) \cup (B \cap C)$$
$$= A \cdot B + A \cdot C + B \cdot C$$

$X \cup Y$ =union of events X and Y

A_i=Failure of component A from independent causes

$$S = (A \cap B) \cup (A \cap C) \cup (B \cap C)$$

$$A = A_T = A_I \cup C_{AB} \cup C_{AC} \cup C_{ABC}$$

…

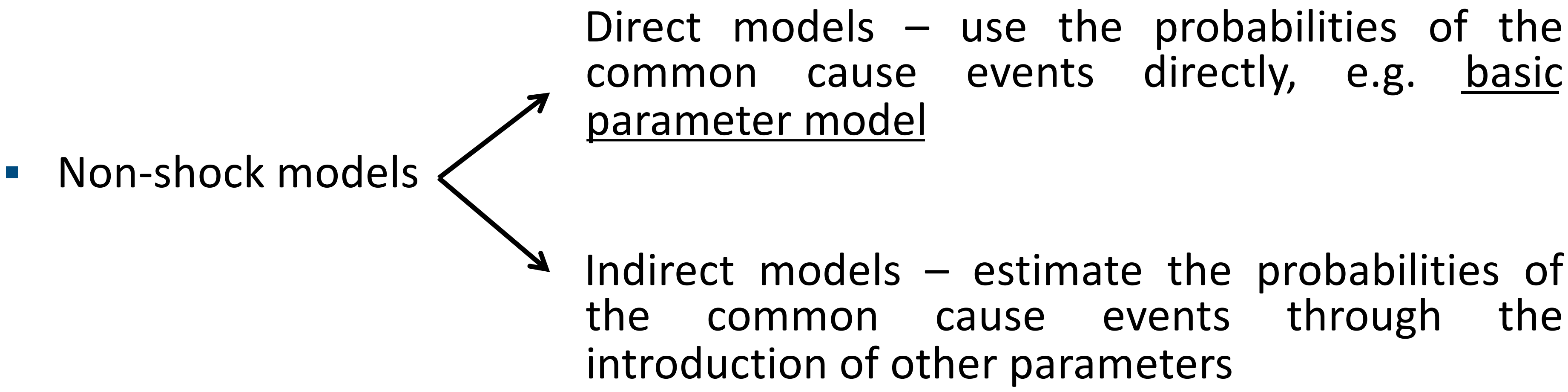
$$S = A_I \cdot B_I + A_I \cdot C_I + B_I \cdot C_I + C_{AB} + C_{AC} + C_{BC} + C_{ABC}$$

$$mcs = \{A_I \cap B_I\}, \{A_I \cap C_I\}, \{B_I \cap C_I\},$$
$$\{C_{AB}\}, \{C_{AC}\}, \{C_{BC}\}, \{C_{ABC}\}$$

Selection of implicit probability models for common cause basic events

- Classification (taxonomy 1):
  - Single-parameter models (the <u>β factor model</u>)
  - Multi-parameter model

- Classification (taxonomy 2):
  - Shock models: the <u>binomial failure rate model</u> which assumes that the system is subject to a common cause 'shock' which occurs at a certain rate



  - Non-shock models

Direct models – use the probabilities of the common cause events directly, e.g. <u>basic parameter model</u>

Indirect models – estimate the probabilities of the common cause events through the introduction of other parameters

The basic parameter model

- Non-shock, direct model
- Assumptions:
  - Rare event approximation
  - The probability of similar events involving similar types of components are the same
  - The probability of failure of any given basic event within a common cause component group depends only on the number and not on the specific components in that basic event (symmetry assumption)

The basic parameter model: example of the 2-out-of-3 system

- Rare event approximation:

$$P(\mathrm{S})=P(\mathrm{A_I})P(\mathrm{B_I})+P(\mathrm{A_I})P(\mathrm{C_I})+P(\mathrm{B_I})\,P(\mathrm{C_I})+P(\mathrm{C_{AB}})+P(\mathrm{C_{AC}})+P(\mathrm{C_{BC}})+P(\mathrm{C_{ABC}})$$

- Other assumptions:

  Q_k = probability of a basic event involving k specific components

$$P(\mathrm{A_I})=P(\mathrm{B_I})=P(\mathrm{C_I})=Q_I$$

$$P(\mathrm{C_{AB}})=P(\mathrm{C_{AC}})=P(\mathrm{C_{BC}})=Q_2$$

$$P(\mathrm{C_{ABC}})=Q_3$$

- Total probability of failure of a component - Q_t=P(A)=P(B)=P(C):

$$Q_t=Q_1+2Q_2+Q_3$$

- Probability of failure of the 2-out-of-3 logical system:

$$Q_S=3Q_1^2+3Q_2+Q_3$$

The basic parameter model: generalization to a common cause group of *m* components

- Total probability of failure of a component in a common cause group of *m* component:

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k$$

Number of different ways in which a component
can fail with (*k*-1) other components
in a group of *m* similar components

Criticality of the method: all the necessary data to estimate Q_k are normally not available

Models with more assumptions but less stringent requirement on the data

The β factor model

- Single parameter model. Used for "intercomponent physical interactions" and "human interactions"
- Assumption: common cause failure → all *m* components in the group fail

$$Q_t = Q_I + Q_m$$

- β factor:

$$\beta = \frac{Q_m}{Q_t} = \frac{Q_m}{Q_I + Q_m} \Rightarrow \begin{cases} Q_m = \beta Q_t \\ Q_I = (1-\beta) Q_t \end{cases}$$

The β factor model: Example of the 2 out of 3 system

- Basic parameter model: $Q_s = 3Q_1^{\,2} + 3Q_2 + Q_3$
- β factor model

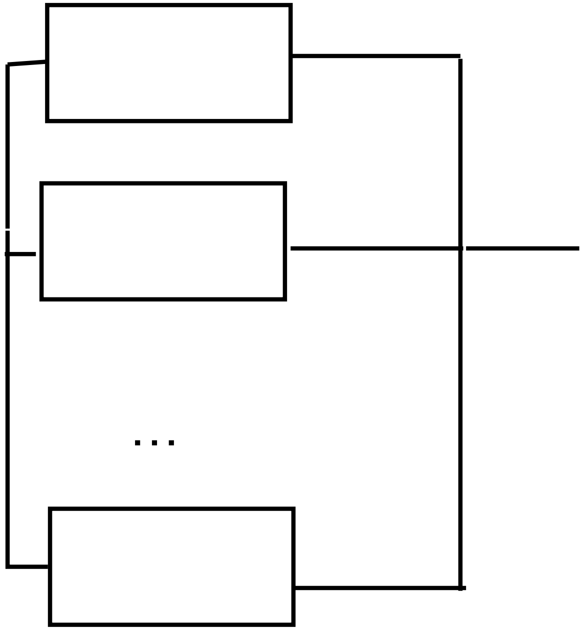
$$\begin{aligned} Q_1 &= (1-\beta)Q_t \\ Q_2 &= 0 \\ Q_3 &= \beta Q_t \end{aligned} \quad \Rightarrow \quad Q_s = 3(1-\beta)^2 Q_t^{\,2} + \beta Q_t$$

- Notice:
  - All units fail when a CCF occurs → conservative predictions
  - Parameter to be estimated from data: β, Q_t
  - Time dependent failure probability:

$$\beta = \frac{Q_m(t)}{Q_t(t)} = \frac{1-e^{-\lambda_m t}}{1-e^{-\lambda_t t}} \cong \frac{\lambda_m}{\lambda_t} \cong \frac{\lambda_m}{\lambda_I + \lambda_m}$$

Example

- A parallel structure of *n* identical components with failure rate λ.
- Components non repairable.



$$R_t(t) = e^{-\lambda t}$$

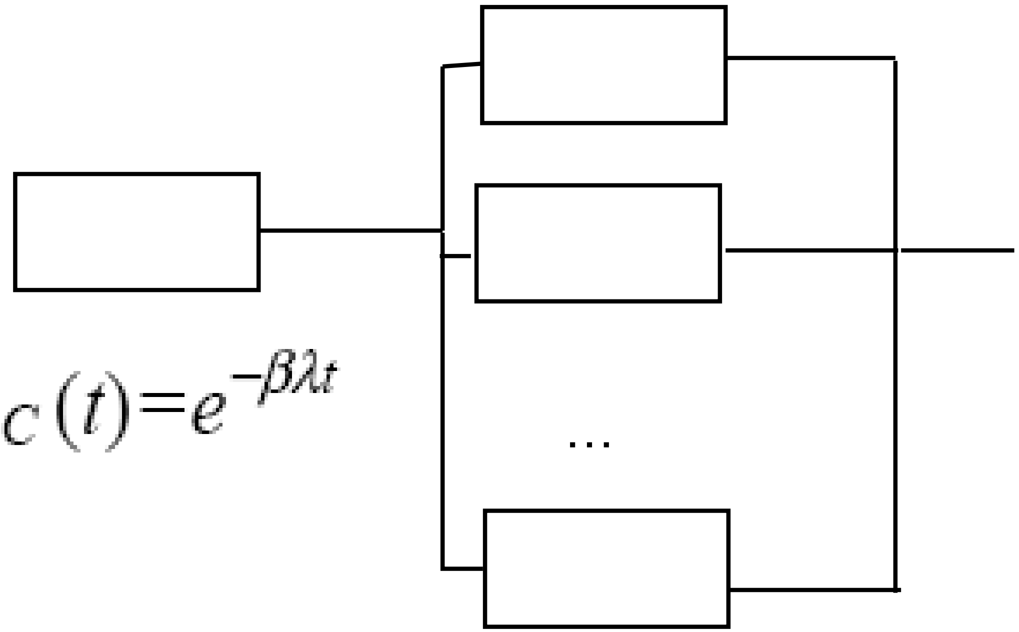
Example

- A parallel structure of *n* identical components with failure rate λ.
- Components non repairable.
- An external event can cause simultaneous failure of all components in the system. β = fraction of the total failure rate of a component attributable to the external event.

β factor model → External event = hypothetical component ***C*** in series with the rest of the system

Example

- A parallel structure of *n* identical components with failure rate λ.
- Components non repairable.
- An external event can cause simultaneous failure of all components in the system. β = fraction of the total failure rate of a component attributable to the external event.



$$R_C(t) = e^{-\beta\lambda t}$$

$$R(t) = \left[1-\left(1-R_I(t)\right)^n\right] \cdot R_C(t)$$

$$= \left[1-\left(1-e^{-(1-\beta)\lambda t}\right)^n\right] \cdot e^{-\beta\lambda t}$$

$$R_I(t) = e^{-(1-\beta)\lambda t}$$

Binomial failure rate (BFR) model

- System composed of *m* identical components.
  - Each component can fail at random times, independently of each other, with failure rate λ.
  - a common cause shock can hit the system with occurrence rate μ.
  - Whenever a shock occurs, each of the *m* individual components may fail with probability *p*, independent of the states of the other components (*p*=1→β-model)

number *I* of individual components failing as a consequence of the shock is binomially distributed with parameters *m* and *p*:

$$p[I=i]=\binom{m}{i}p^i(1-p)^{m-i} \qquad i=0,1,\dots,m$$

Binomial failure rate (BFR) model

- Additional assumptions:
  1. Shocks and individual failures occur independently of each other;
  2. All failures are immediately discovered and repaired, with negligible repair time
- Failure rate for <u>1 unit</u> in a common cause failure group of <u>multiplicity *m*</u> :

$$\lambda_1 = \underbrace{m\lambda}_{\text{Total contribution due to independent failures}} + \underbrace{\mu\left[\binom{m}{1}p\left(1-p\right)^{m-1}\right].}_{\text{Rate of single-unit failures from common cause shocks}}$$

Binomial failure rate (BFR) model

- Failure rate of *i* units in a common cause failure group of multiplicity *m* is:

$$\lambda_i = \mu\left[\binom{m}{i} p^i (1-p)^{m-i}\right]$$

- Parameters to be estimated from data: λ, μ and p