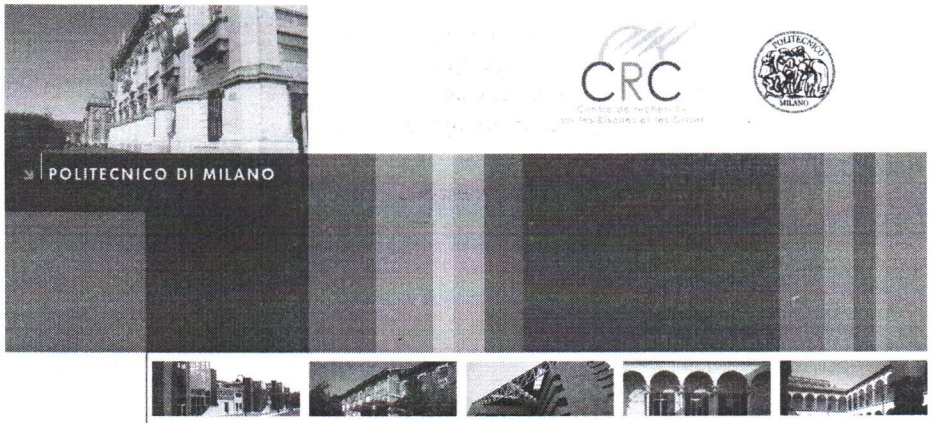
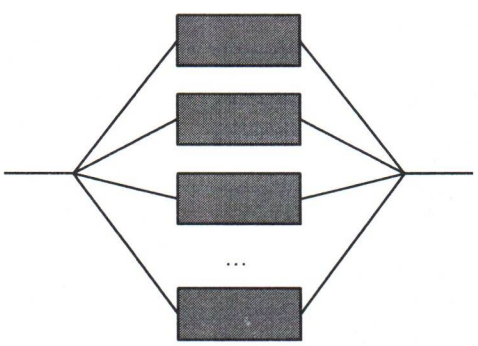


Dependent Failures

An Example

U_c=0.2 = unreliability of the component

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



$U_s=(U_c)^n$

$\Downarrow$

n=14 → U_s=1.6·10^{-10}

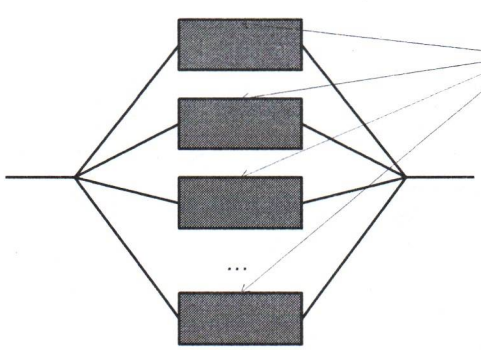
n=15 → U_s=0.3·10^{-10}

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}?

What if all of the components rely on the same power supply? They're **not** !!



Power Supply

$U_{PS}=10^{-5}$

$U_s=(U_c)^n$

$\Downarrow$

n=14 → U_s=1.6·10^{-10}

n=15 → U_s=0.3·10^{-10}

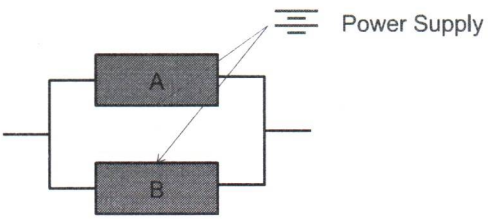
Ignoring dependent failure → gross underestimation of risk !!!

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 piece of hardware extenal to the system
   - Human Error (operational or maintenance)

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

multiple components that fail due to the same cause

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

which aims at identifying dependencies: once we identify them we want to model them to analyze their contribution to the risk / unreliability of the system

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 (it alarms that one component has a degradation → we check the other similar components on the redundant part and we see if they also have degradation
- 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)] these external events are so relevant (they account for the largest source of risk) that we do a dedicated risk assessment for them
- 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 precede 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

How the probability of failure of a system changes because of a dependence of an other system

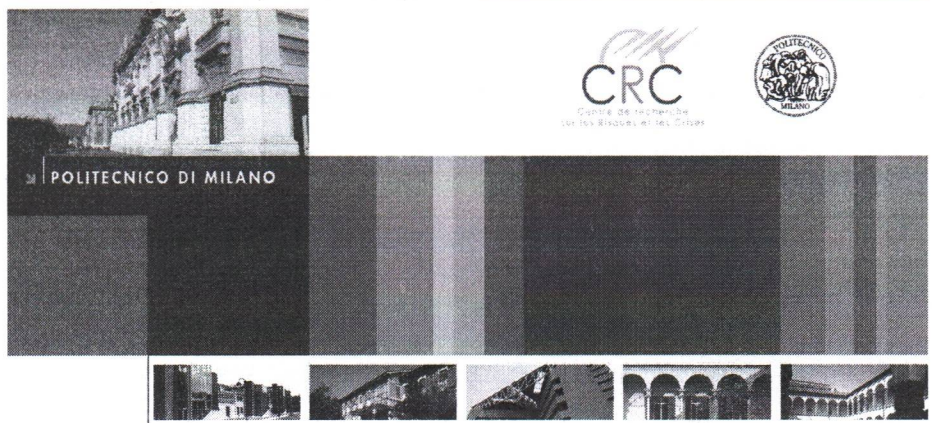
dependence among systems

dependence among components

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.



Explicit methods

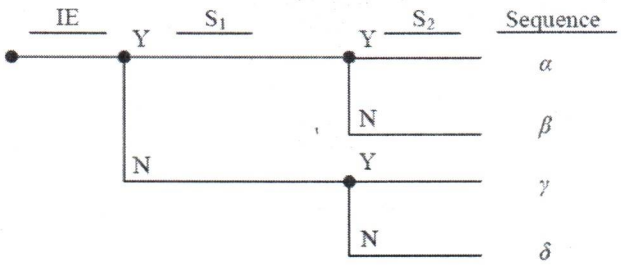
event trees / fault trees
(it's just about understanding the logic of the system and being able to represent the system model)

1. Common Cause initiating events

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

2. Intersystem dependences

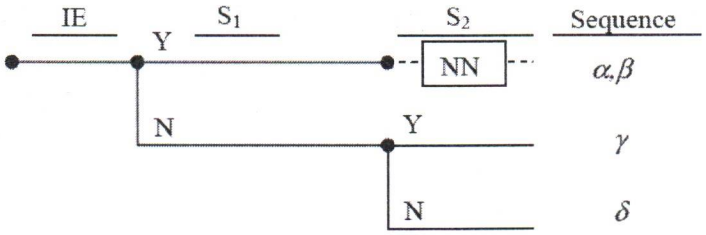
- Two safety systems S1 and S2 are expected to intervene upon the occurrence of an initiating event (IE)



2.A: Functional dependences

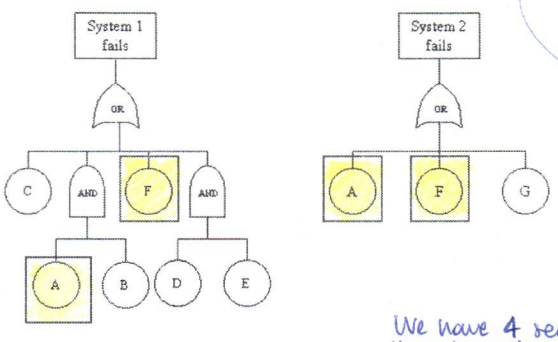
≠

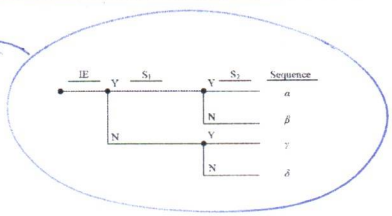
System 2 is not needed (NN) unless system 1 fails



2.B Shared equipment

Given this we look at the systems and they may have something in common (shared)!





We have 4 sequences, we need to account the shared equipment. If system 1 fails and it fails because of the common equip. then system 2 fails too? They're not ⊥!

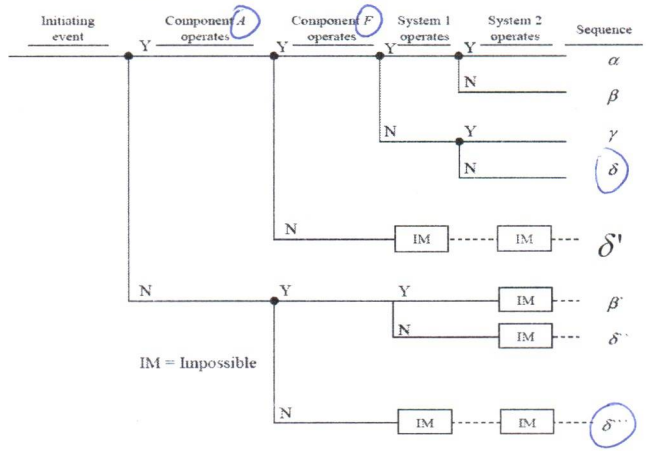
How can we account for the dependencies?

Method of the 'event trees with boundary conditions'

(also called "large event trees")

We take out the shared components: we explicitly represent them, with the right logic, in the system.

1. Develop the event tree

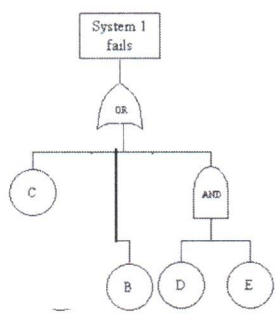


For example (previous case) here we had to take out both A and F

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}

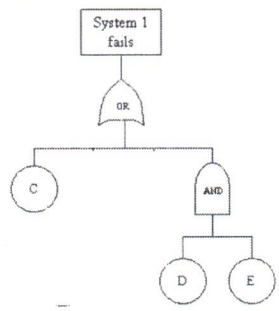


Method of the 'event trees with boundary conditions'

- 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}



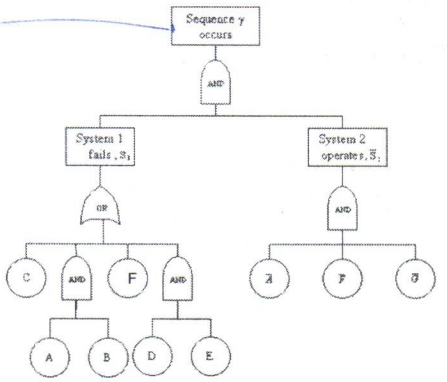
Method of 'Fault tree link"

(also called "large fault trees")

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"

it's a sequence tree



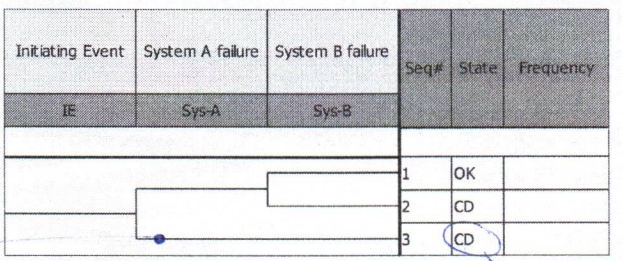
$$\gamma = S1 \cap \overline{S_2} = [(A \cap B) \cup C \cup (D \cap E) \cup F] \cap [\overline{A} \cap \overline{F} \cap \overline{G}] =$$
$$= [(A \cap B) \cap (\overline{A} \cap \overline{F} \cap \overline{G})] \cup [C \cap (\overline{A} \cap \overline{F} \cap \overline{G})] \cup$$
$$\cup [(D \cap E)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

$$mcs = \{\overline{AFGC}; \overline{AFGDE}\}$$

Example of Method of 'Fault tree link"

The event tree and the fault trees can be linked together, thus develop a entire system fault tree

- The event tree:



completely damaged

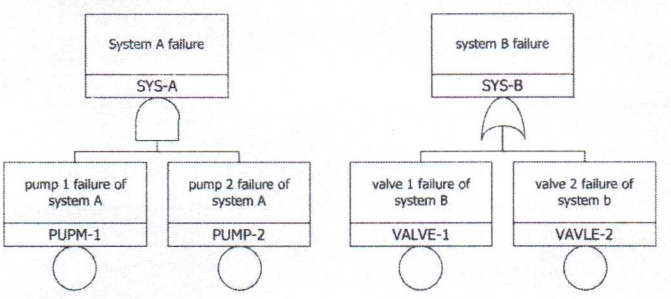
if system A fails B cannot function

- 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"

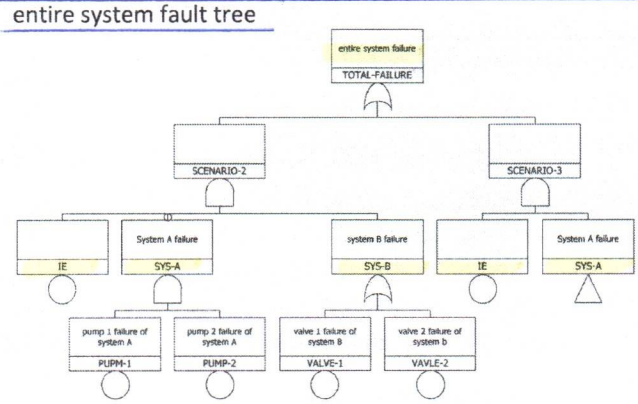
The fault trees of Sys-A and Sys-B

$Sys-A$ $Sys-B$



Example of Method of 'Fault tree link"

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



we don't have to worry of the shared equipment, but the fault tree that we get is much longer

- 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:

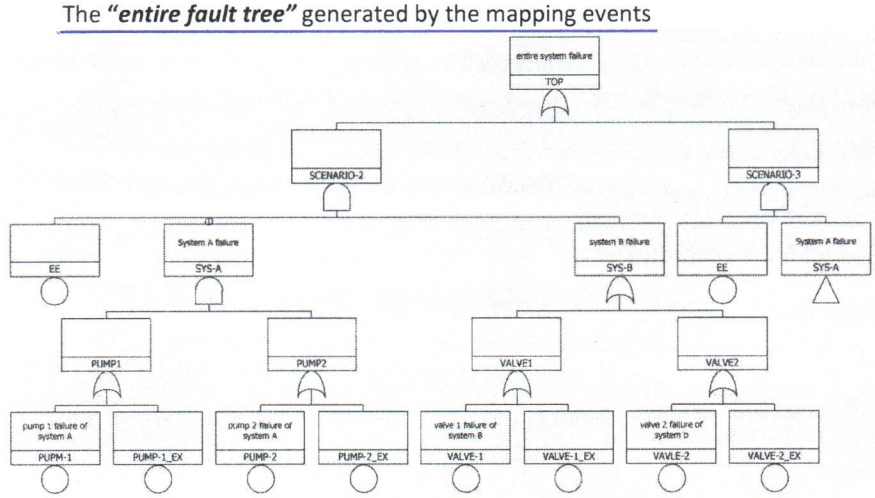
- IE -> EE
- PUMP-1 -> PUMP-1 +PUMP-1_EX
- PUMP-2 -> PUMP-2 +PUMP-2_EX
- VALVE-1 -> VALVE-1 + VALVE-1_EX
- VALVE-1 -> VALVE-1 + VALVE-1_EX

now each component can fail because of internal reason or because of the external event

"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



Example of Method of 'Fault tree link"

To model fire risk by using the mapping method.

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

we have one fire in the location of system B and one fire in the location of system A

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}

every component can fail independently (internally) or due to the fire (the fire of the corresponding zone)

- *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"

To insert the mapping fire events into the ***"entire fault tree"*** and, obtain the minimal cut sets:

- Total Failure = $(F_1 + F_2)$*(PUMP-1 + F_2*CF_{21})*(PUMP-2 + F_2*CF_{22})
  + $(F_1 + F_2)$*(VALVE-1 + F_2*CF_{11})
  + $(F_1 + F_2)$*(VALVE-2 + F_2*CF_{12})

both fires and failures due to fires or internal

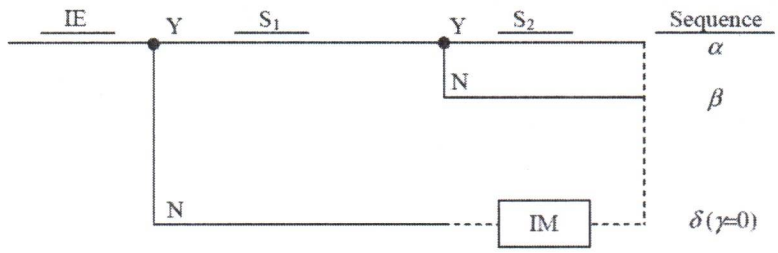
- Assuming exclusiveness among fire initiating events (F_1*F_2=0)
- Total Failure = $(F_1 + F_2)$*PUMP-1*PUMP-2
  + F_2*(CF_{21}*PUMP-2 + CF_{21}*F_2*CF_{22})
  + $(F_1 + F_2)$*VALVE-1 + $(F_1 + F_2)$* VALVE-2
  + F_2*CF_{11} + F_2*CF_{12}

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

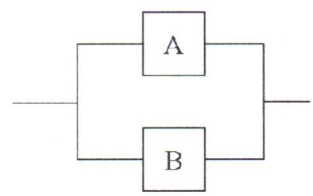
2.C Physical interactions

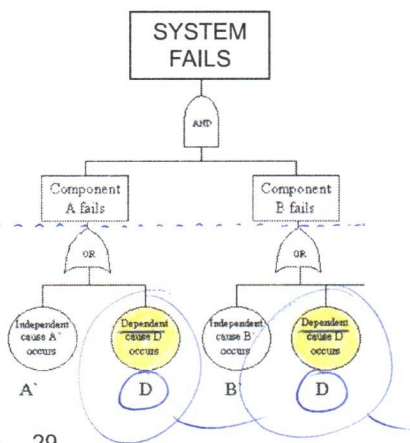
- System S2 can operate only if system S1 operates successfully. When system S1 fails a physical interaction takes place, which inhibits system S2 → Sequence γ is impossible



3. Intercomponent dependences (common cause failure)

- Parallel system





we would stop here without intercomponent dependences

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

This is the explicitation of the dependence at the component level

Numerical example (Parallel)

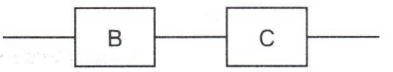
Parameter	A, B (parallel configuration ≡ mcs)	
	Case 1	Case 2
	No common cause	Common causes shared by components A and B
$P(A')$	1.0×10^{-3}	9.9×10^{-4}
$P(B')$	1.0×10^{-3}	9.9×10^{-4}
$P(D)$	0	1.0×10^{-5}
Q	1.0×10^{-6}	1.1×10^{-5}

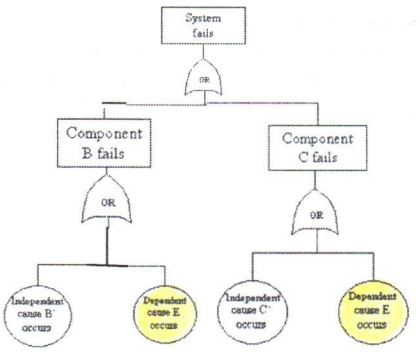
Notice that the probability of failure at the component level is still the same:
I. $\mathbb{P}(A) = \mathbb{P}(A') = 1.0 \cdot 10^{-3}$
II. $\mathbb{P}(A) = \mathbb{P}(A') + \mathbb{P}(D) = 1.0 \cdot 10^{-3}$

If there is a dependence and we take into account it, the overall probability of failure is a little higher (actually a whole order of magnitude, it's **not** small)

If there is no dependence the probability of the overall failure is the product of the two failure prob.

- Series System





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

Numerical example (Series)

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

at least this time it's the same order of magnitude ⇒ it doesn't impact so much

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)

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 $\Rightarrow P(A \mid B) \ge P(A)$

the failure of one component increases the failure of the other

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

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

the probability that we lose A and B together is bounded:
- lower bound: $\mathbb{P}(A)\,\mathbb{P}(B)$ (independent events)
- upper bound: $\min\{\mathbb{P}(A), \mathbb{P}(B)\}$

Square root method (2)

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

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* : $U_c = 10^{-2}$

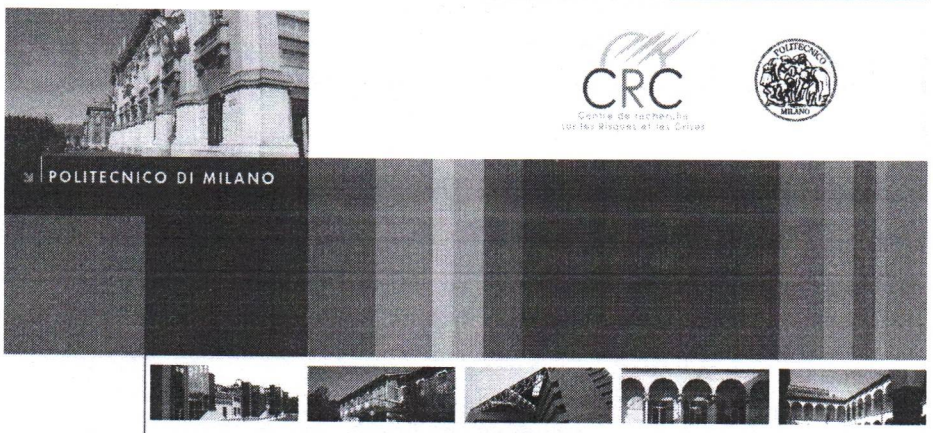
Estimate the system unavailability at time *t*

$$P_L = \prod_{i=1}^{n} P(A_i) = (U_c)^n$$
$$P_U = \min[P(A_1), P(A_2), \ldots, P(A_n)] = U_c$$
$$\Rightarrow U_s = \sqrt{P_L \cdot P_M} = (U_c)^{\frac{n+1}{2}}$$

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



A methodological framework for Common Cause Failures (CCF) analysis

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

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.

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

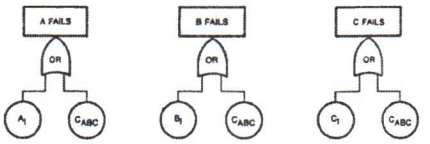
- Check-list:
  - Similarity of component type
  - Similarity of component use
  - Similarity of component manufacturer
  - Similarity of component internal conditions (pressure, temperature, chemistry)
  - Similarity of component boundaries and system interfaces
  - Similarity of component location 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

if we find a malfunctioning then we should check similar components (maybe the malfunctioning is due to the design or something that characterize all the comps.)

- 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

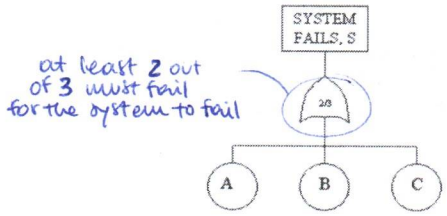
STEPS:

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)



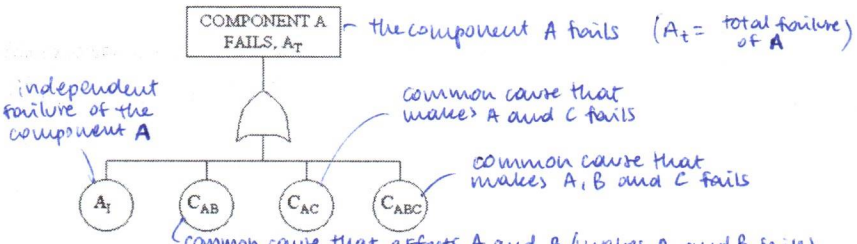
at least 2 out of 3 must fail for the system to fail

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



the component A fails (A_t = total failure of A)

independent failure of the component A

common cause that makes A and C fails

common cause that makes A, B and C fails

common cause that affects A and B (makes A and B fails)

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 β factor model)
  - Multi-parameter model
- Classification (taxonomy 2):
  - Shock models: the binomial failure rate model 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. basic parameter model
    - Indirect models – estimate the probabilities of the common cause events through the introduction of other parameters

The basic parameter model

- Non-shock, direct model ← it uses the probabilities of the common cause events
- 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: (*)

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

- Other assumptions:

  Q_k = probability of a basic event involving k specific components

$$P(A_I)=P(B_I)=P(C_I)=Q_1$$
$$P(C_{AB})=P(C_{AC})=P(C_{BC})=Q_2$$
$$P(C_{ABC})=Q_3$$

- 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:

$$Q_S = 3Q_1^2 + 3Q_2 + Q_3$$ ← based on the mcs

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 ⟹ less parameters to estimate

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

semplification:

$$Q_t = Q_I + Q_m$$

- 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

$$Q_1 = (1-\beta)Q_t$$
$$Q_2 = 0$$
$$Q_3 = \beta Q_t$$

$$\Rightarrow \quad Q_s = 3(1-\beta)^2 Q_t^2 + \beta Q_t$$

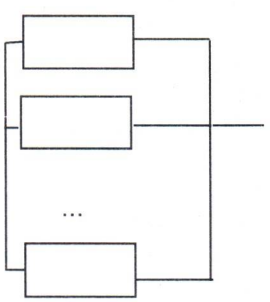
now we have only 2 parameters to estimate

- 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.



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

Example

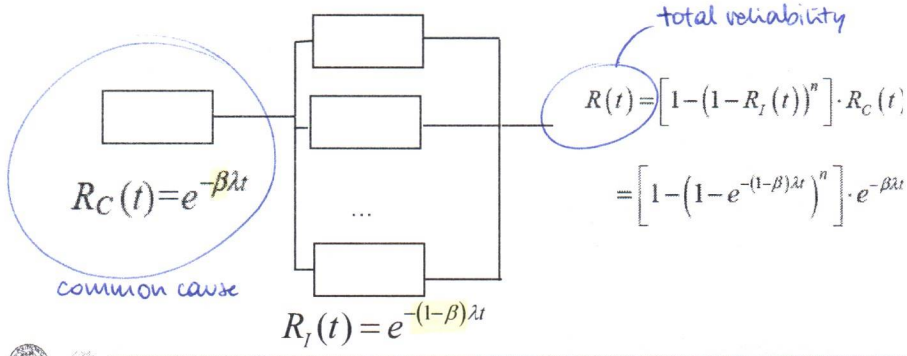
- A parallel structure of *n* identical components with failure rate λ.
- Components non repairable.
- An external event can cause simultaneous failure of all components in the system. β = fraction of the total failure rate of a component attributable to the external event.

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

if this component fails then also all the other fail

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.



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. (the failure process is exponential in time)
  - 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*:

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

$\mathbb{P}$(*i* components fail)

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 1 unit in a common cause failure group of multiplicity *m* :

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

= either one component (out of m) failed internally **or** the shock arrived and only **1** component failed

Binomial failure rate (BFR) model

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

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

= the failure rate of i units is only due to the shock, and so it's μ times the probability of having i components failed during the shock

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

Data classification and screening

- Data sources available are typically of two kinds:
  - generic raw data (NUREG, ...)
  - plant specific data (rarity of common cause failure + limited experience of specific plant -→ very limited)
  - ***Binary Impact Vector*** for each event that has occurred in a group of size *m*

$$I = [I_0, I_1, \ldots, I_m]$$

e.g. , 2 components have failed in a group of size 3:

$$I = [0,0,1,0]$$ = [1{0 failed}, 1{1 comp. failed}, 1{2 comp failed}, 1{3 failed}]

  - Event descriptions are not clear → classification of the event requires establishing hypotheses representing different interpretations of the event. Probability are associated to the hypotheses.

Data classification and screening

we introduce probabilities instead of 0/1

Component Group Size	Hypothesis	Hypothesis Probability	I_0	I_1	I_2	I_3	Shock type	Fault Mode
3	H_1	0.9	0	0	1	0	Non lethal	Failure during operation
	H_2	0.1	0	0	0	1		
	Average Impact Vector ($\bar{I}$)		P_0	P_1	P_2	P_3		
			0	0	0.9	0.1		

Hp. 1 (H_1): there are 2 components involved in the accident

Hp. 2 (H_2): there are 3 components involved in the acc.

$P(H_1) = 0.9$
$P(H_2) = 0.1$

- ***Average impact vector*** (not binary): for a given event: $I = [P_0, P_1, \ldots, P_m]$
- Several events → computation of n_k = the total number of events involving the failure of *k* similar components in the group

$$n_k = \sum_j P_k(j)$$

Parameter estimation

- Impact vectors → number of events in which 1,2,3,....m components failed → $n_k = \sum_j P_k(j)$

•Basic event probabilities directly (within the basic parameter model)
E.g. Safety system: number of demands = N → $Q_k = \frac{n_k}{N}$

•the parameters of the common cause failure models (beta factor, BFR)

Beta-factor estimation for a two-train redundant standby safety system tested for failures

- Available recorded evidence:
  - n_1 failures of single components
  - n_2 failures of both components
  - Q_t : total single component failure probability

probability of all components failing / (total) probability of failure of 1 component

$$\beta = \frac{Q_2}{Q_t} = \frac{Q_2}{Q_1 + Q_2} = \frac{\boxed{N_2}}{\boxed{n_1}\boxed{N} + \frac{n_2}{\boxed{N_2}}}$$

number of tests for common-cause failures

Unknown!

where the component can fail alone or in pair

number of single-component demands to start

probability of failing by itself

Beta-factor estimation for a two-train redundant standby safety system tested for failures (TEST STRATEGY I)

- Estimation of N (number of single-component demands to start)

Total number of failures

$$Q_t = \frac{\boxed{n_1 + 2n_2}}{N} \Rightarrow N = \frac{n_1 + 2n_2}{Q_t}$$

n_1 : failures of single components
n_2 : failures of both components

N_2: number of tests for common-cause failures

- Estimation of N_2 → surveillance testing strategy
  - Both components are tested at the same time

Tests = Demands to start

S = successful, F = fail

we test the components separately

	Day 0	Day 15	Day 30	Day 45	Day 60
Comp. 1	S	S	F	F	S
Comp. 2	S	F	S	F	S
N	2	4	6	8	10
N_2	1	2	3	4	5
n_1	0	1	2	2	2
n_2	0	0	0	1	1

cumulative!

overall test till the day (in this case = 2 because we tested 2 components on the day 0)

tests of 2 components (here = 1 because on day 0 we tested both once)

Beta-factor estimation for a two-train redundant standby safety system tested for failures (TEST STRATEGY I)

- Estimation of N (number of single-component demands to start)

Total number of failure

$$Q_t = \frac{n_1 + 2n_2}{N} \Rightarrow N = \frac{n_1 + 2n_2}{Q_t}$$

- Estimation of N_2 → surveillance testing strategy
  - Both components are tested at the same time $\Longrightarrow N = \frac{1}{2} N_2$ (from the previous table)

$$N_2 = \frac{N}{2} \longrightarrow Q_2 = \frac{n_2}{N/2} \longrightarrow \beta = \frac{Q_2}{Q_t} = \frac{\frac{n_2}{N/2}}{\frac{n_1}{N} + \frac{n_2}{N_2/2}} = \frac{2n_2}{n_1 + 2n_2}$$

Beta-factor estimation for a two-train redundant standby safety system tested for failures (TEST STRATEGY II)

- The components are tested at staggered intervals, if there is a failure, the second component is tested immediately. N_2 is known. N is linked to N_2 from:

Number of single-component demands to start

Number of tests for common-cause failures

Number of failures of a single component

Number of failures involving both components

$$N = N_2 + n_1 + n_2$$

Tests = Demands to start

	Day 0	Day 15	Day 30	Day 45	Day 60
Comp. 1	S	S	T	T	S
Comp. 2	NO TEST	NO TEST	S	T	NO TEST
N	1	2	4	6	7
N_2	1	2	3	4	5
n_1	0	0	1	1	1
n_2	0	0	0	1	1

we test the second comp. only if the first fails

overall number of tests: here we tested only the first comp.

we go from 2 to 4 because on day 30 we test both comp.s

Beta-factor estimation for a two-train redundant standby safety system tested for failures (TEST STRATEGY II)

- The components are tested at staggered intervals, if there is a failure, the second component is tested immediately. N_2 is known. N is linked to N_2 from:

Number of single-component demands to start

$$N = N_2 + n_1 + n_2$$

$$Q_2 = \frac{n_2}{N_2} \approx \frac{n_2}{N} \quad (n_1 \text{ and } n_2 << N)$$

$$\beta = \frac{Q_2}{Q_t} \cong \frac{\frac{n_2}{N}}{\frac{n_1 + n_2}{N}} = \frac{n_2}{n_1 + n_2}$$

Estimates of β are based on the assumptions on the testing strategies

Binomial failure rate model parameter estimation

- Parameter to be estimated: p, μ (we should also estimate λ, the individual comp. failure rate (we estimate it with max. likelihood estimation))
- μ is not directly available because:
  - Shocks that do not cause any failure are not observable
  - Single failures from common-cause shocks may not be distinguishable from single independent failures

(we observe failures, not shocks)

- Data available for the estimation:
  - N_i = number of observations of *i* concurrent failures (certain number of realizations in which, in our test, we observe *i* concurrent failures)
  - $N_+ = \sum_{i=2}^{m} N_i$ number of observations of dependent failures of any multiplicity order

Binomial failure rate model parameter estimation

- Rate of dependent failures of any multiplicity:

$$\lambda_+ = \sum_{i=2}^{m} \lambda_i = \mu\left[1-(1-p)^m - mp(1-p)^{m-1}\right]$$

(rate of having an event with 2 or more failures (look at slide 61))

- Method for the estimation: maximizing the likelihood:

$$P_T\left[N_1 = n_1, N_2 = n_2, \ldots, N_m = n_m\right] = P_1\left[N_1 = n_1\right] \cdot P_+\left[N_+ = n_+\right] \cdot P_m\left[N_2 = n_2, \ldots, N_m = n_m\right]$$

- For a given observation time T, the variables N_1 and N_+ have Poisson distributions with parameters $\lambda_1 T$ and $\lambda_+ T$, respectively. Maximizing the likelihoods P_1 and P_+ →

$$\hat{\lambda}_1 = \frac{n_1}{T}$$

(= estimate of the rates of single failures)

$$\hat{\lambda}_+ = \frac{n_+}{T}$$

Binomial failure rate model parameter estimation

- The likelihood, P_m, follows a multinomial distribution. From the total number of unit failing:

$$S = \sum_{i=2}^{m} i \cdot n_i$$

(e.g. 5 events where 2 units fail: we have a total amount of 10 failures ($2 \cdot 5 = i \cdot n_i$))

- The estimate of the value of *p* which maximizes P_m is found from:

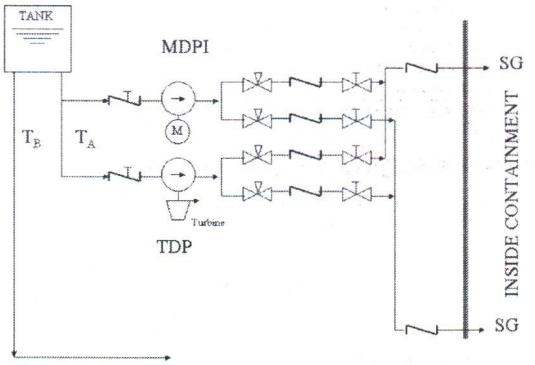
$$S = \frac{m n_+ p\left[1-(1-p)^{m-1}\right]}{1-(1-p)^m - mp(1-p)^{m-1}}$$

Valid for $m > 2$

- From λ_1, λ_+ and *p* it is possible to estimate μ from:

$$\lambda_+ = \sum_{i=2}^{m} \lambda_i = \mu\left[1-(1-p)^m - mp(1-p)^{m-1}\right]$$

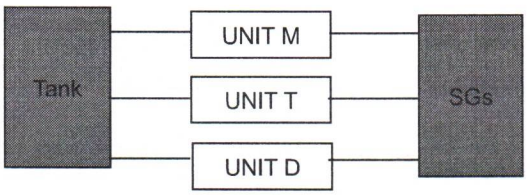
EXAMPLE: Auxiliary Feedwater System (AFWS) of a nuclear Pressurized Water Reactor



T_A,T_B = Trains A and B
MDP = electrical motor-driven-pump
TDP = steam turbine-driven pump
SG = steam generator (1 to 4)

TRAIN ≡ UNIT

EXAMPLE: Auxiliary Feedwater System (AFWS) of a nuclear Pressurized Water Reactor



DATA FROM US PWR PLANT:
•Different number of units
•Different type of units (M,T, D)

Instances of multiple failures in PWR auxiliary feedwater systems

Plant	Date	Number of failures and failed train type	Number of trains		
			M	T	D
Calvert Cliffs Unit 1	5/76	2/T,T *	0	2	0
Haddam Neck	7/76	2/T,T *	0	2	0
Kewaunee Unit 1	8/74	2/M,M	2	1	0
	10/75	2/M,T	2	1	0
	11/75	3/M,M,T *	2	1	0
Point Beach Unit 1	4/74	2/M,M	2	1	0
Robert E. Ginna	12/73	2/M,M	2	1	0
Trojan Unit	1/76	2/T,D *	0	1	1
	12/77	2/T,D *	0	1	1
Turkey Point Unit 3	5/74	3/T,T,T *	0	3	0
Turkey Point Unit 4	6/73	2/T,T	0	3	0

Plant with 2 units

* Failure of the system (6)

N_e = n. of multiple failure events= 11
N_c = n. of unit failure in multiple failure events = 24

EXAMPLE: Auxiliary Feedwater System (AFWS) of a nuclear Pressurized Water Reactor

Sum of number of systems times length of service	1874 system-months
Contribution to above by multiple-unit systems	1641 system-months
Contribution to above by 2-units systems	474 system-months
Contribution to above by 3-units systems	1167 system-months
Sum of number of units times length of service	4682 unit-months
Contribution to above by multiple-unit systems	4449 unit-months
Total number of single failures	69
Number of single failures in multiple-unit systems (N_i)	68
Number of multiple-unit failure events (N_e)	11
Number of unit failures in dependent-failure occurrences (N_c)	24

Assumption: one complete (i.e., all units) system demand for each calendar month

From real data:

•System per-demand failure probability: $\frac{6 \text{ system failures}}{1641 \text{ system months of operation}} = 3.7 \cdot 10^{-3}$ = multiple-unit system demands

•Two-component per-demand failure probability (1 out of 2) :

$\frac{4 \text{ system failures}}{474 \quad \text{system months of operation}} = 8.4 \cdot 10^{-3}$ = two-unit system demands

•Three-component per-demand failure probability (1 out of 3): $\frac{2 \text{ system failures}}{1641-474} = 1.7 \cdot 10^{-3}$ = three-unit system demands

Example: Beta-factor model

n. of unit failures in multiple(dependent)-failure events

$$\hat{\beta} = \frac{\lambda_m}{\lambda_m + \lambda_i} = \frac{N_c / T}{N_c / T + N_i / T} = \frac{2n_2 + 3n_3}{n_1 + 2n_2 + 3n_3} = \frac{24}{24 + 68} = 0.26$$

• $Q_S = Q_{1\text{-}2}$ per-demand probability of failure-to-start for a 1-out-of-2 system is:

$$\left.\begin{aligned} Q_1 &= (1-\beta) Q_t \\ Q_2 &= \beta Q_t \end{aligned}\right\} \Rightarrow Q_s = Q_{1\text{-}2} = (1-\beta)^2 Q_t^2 + \beta Q_t = \underbrace{(1-\beta)^2 \lambda_{tot}^2}_{\text{multiple independent failures}} + \underbrace{\beta \lambda_{tot}}_{\text{common cause failures}} \qquad (6.57)$$

•With:

λ_{tot} = probability of failure on demand of a single unit $= \frac{n_1 + 2n_2 + 3n_3}{N} = \frac{N_i + N_c}{T \cdot 1 (\equiv N)} = \frac{68 + 24}{4682} = 0.02$

$$Q_{1\text{-}2} = \left[(1-0.26)(0.02)\right]^2 + (0.026)(0.02) = 2 \cdot 10^{-4} + 5.2 \cdot 10^{-3} = 5.4 \cdot 10^{-3}$$

From data = 8.4 10^{-3}

Example: Beta-factor model

- $Q_S = Q_{1\text{-}3}$ per-demand probability of failure-to-start for a 1-out-of-3 system is:

$$Q_{1\text{-}3} = (1-\beta)^3 \lambda_{tot}^3 + \beta \lambda_{tot} = 5.2 \cdot 10^{-3}$$

negligible

From data: $= 1.7 \cdot 10^{-3}$

Example: Binomial failure-rate model

Number of observed single failures in multi-unit systems

$$\hat{\lambda}_1 = \frac{N_1}{T \cdot 1} = \frac{68}{1641} = 0.0414$$

n. of system demand for each calendar month

System month of operation

Number of observed multiple failures

$$\lambda_+ = \frac{N_t}{T \cdot 1} = \frac{11}{1641} = 0.0067$$

Example: Binomial failure-rate model

Estimation of p (for 3-unit systems)

- $n_+ = 7$ multiple failure events in 3-unit systems
- S : total number of units failing in 7 multiple failures in 3-units systems : S=16)

$$\hat{p} = \frac{3 \cdot (S - 2n_+)}{2S - 3n_+} = \frac{3 \cdot (16 - 2 \cdot 7)}{2 \cdot 16 - 3 \cdot 7} = 0.55$$

$$1 - \hat{p} = 0.45$$

$$\lambda_+ = \sum_{i=2}^{m} \lambda_i = \mu \left[1 - (1-p)^m - mp(1-p)^{m-1} \right]$$

$$0.0067 = \mu \left[1 - (0.45)^3 - 3(0.55)(0.45)^2 \right]$$

$$\hat{\mu} = 0.0118$$

Example: Binomial failure-rate model

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

the per-demand system failure probabilities for 2-out-of-3 units failing is

$$Q^{(2)}_{1\text{-}3} = (0.0118) \binom{3}{2} (0.55)^2 (0.45)^{3-2} = 4.8 \cdot 10^{-3}$$

and for 3-out-of-3 units failing is (Three-component per-demand failure probability)

$$Q_{1\text{-}3} = (0.0118) \binom{3}{3} (0.55)^2 (0.45)^{3-3} = 1.9 \cdot 10^{-3}$$

From data: $= 1.7 \cdot 10^{-3}$

- The Beta-factor model requires the estimation of 2 parameters: λ, β
- The Binomial Failure Rate model requires the estimation of 3 parameters: λ, μ, p

Then, the Beta-factor model is less data-demanding but also applicable to multiple unit systems.

- With both models, one should keep in mind that we are trying to describe the complex reality of multiple failures by means of quite simple models. In certain cases, the models may be inadequate and one should then resort to more complicated (but also more data-demanding) models.

- In the example, the beta factor model estimates the system failure probabilities:
  Q_{1-2} in 2-unit systems
  Q_{1-3} in 3-unit systems
  whereas it does not estimate the probability of 2 components failing in the 1-3 system, $Q_{1-3}^{(2)}$ (but compensates by overestimating Q_{1-3}).

- The BFR estimates p from data only taken from three-unit systems and that is why it fits direct estimates by three units data almost perfectly ($1.9 \cdot 10^{-3}$ against $1.7 \cdot 10^{-3}$).