RELIABILITY

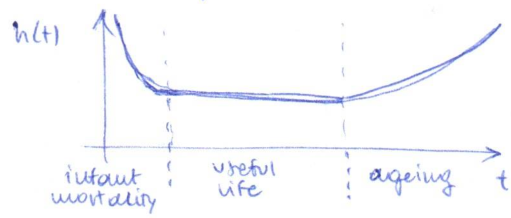
- ability of an item to perform a required function under stated conditions for a stated period of time
- quantify the ability to achieve the desired objective without failures
- no repairs
- $R(t)$, MTBF (Mean Time Between Failures)

T = time to failure, random variable:

- $F_T(t) = \mathbb{P}(T \le t)$ (cdf)
- $f_T(t)$ = density function (pdf)
- $R(t) = 1 - F_T(t) = \mathbb{P}(T > t)$ = reliability at time t (ccdf = complementary cumulative density fun.)
- $h_T(t) = \dfrac{f_T(t)}{R(t)}$ = hazard function (conditional density function: gives the $\mathbb{P}$ of failing in the next dt given that the system has not failed yet)

probability of functioning at least till time t

3 distinct phases:



EXPONENTIAL DISTRIBUTION

- $h_T(t) = \lambda$ $\quad t \ge 0$ (only distr. with constant hazard rate (failure rate))
- $F_T(t) = 1 - e^{-\lambda t}$
- $f_T(t) = \lambda e^{-\lambda t}$ $\quad t \ge 0$
- $\mathbb{E}[T] = \frac{1}{\lambda}$ = MTTF (Mean Time To Failure)
- $var(T) = \frac{1}{\lambda^2}$
- $\mathbb{P}(t_1 < T < t_2 \mid T > t_1) = 1 - e^{-\lambda(t_2 - t_1)}$ (memoryless)

WEIBULL DISTRIBUTION

- $F_T(t) = 1 - e^{-\lambda t^{\alpha}}$
- $f_T(t) = \lambda \alpha t^{\alpha - 1} e^{-\lambda t^{\alpha}}$ $\quad t \ge 0$
- $\mathbb{E}[T] = \frac{1}{\lambda} \Gamma\left(\frac{1}{\alpha} + 1\right)$
- $Var(T) = \frac{1}{\lambda^2}\left[\Gamma\left(\frac{2}{\alpha} + 1\right) - \Gamma\left(\frac{1}{\alpha} + 1\right)\right]^2$

$$\Gamma(k) = \int_0^{\infty} x^{k-1} e^{-x}\, dx \qquad k > 0$$

- $\begin{cases} \alpha > 1 & \text{decreasing hazard rate} \\ \alpha = 1 & \text{constant failure/hazard rate } (\sim \mathcal{E}) \\ \alpha < 1 & \text{aging period} \end{cases}$

RELIABILITY of a system of N components (with known reliability $R_i(t)$ $i = 1, \dots, N$)

- SERIES: all components must function
  $R(t) = \prod_{i=1}^{N} R_i(t)$ = $\mathbb{P}$(the system doesn't fail until time t)
- PARALLEL: all components must fail for the system to fail
  $R(t) = 1 - \prod_{i=1}^{N} (1 - R_i(t))$ = $\mathbb{P}$(at least one does not fail until time t)
- r OUT OF N: N parallel component, at least r needed
  $R(t) = \sum_{k=r}^{N} \binom{N}{k} e^{-\lambda k t} (1 - e^{-\lambda t})^{N-k}$ (EXPONENTIAL)
- COLD STAN-BY: $N-1$ substitute components which cannot fail
  The system fails when all the subst. comp. fail!
  $T = \sum_{i=1}^{N} T_i$, $R(t) = 1 - \int_0^t f_T(x)\,dx$, $\tilde{f}_T(s) = \prod_{i=1}^{N} \tilde{f}_{T_i}(s)$, $\text{MTTF} = \int_0^{\infty} t\, f_T(t)\, dt$
- HOT STAND-BY: second component which can deteriorate
  $$R(t) = \underbrace{R_1(t)}_{\text{either the main works till } t} + \int_0^t \underbrace{f_1(\tau)}_{\text{the main fails at } \tau} \underbrace{R_S(\tau)}_{\text{the second is not failed at } \tau} \underbrace{R_2(t-\tau)}_{\text{the second work from } \tau \text{ to } t}\, d\tau$$

EXPONENTIAL CASE :

- SERIES :

$$R(t) = e^{-\lambda t} \qquad \lambda = \sum_i^N \lambda_i = \text{system failure rate (constant)}$$

$$\mathbb{E}[T] = \frac{1}{\lambda} = \text{MTTF}$$

- PARALLEL :

$$R(t) = 1 - \prod_{i=1}^N \left(1 - e^{-\lambda_i t}\right)$$

$$\mathbb{E}[T] = \sum_{i=1}^N \frac{1}{\lambda_i} - \sum_{i=1}^{N-1} \sum_{j=i+1}^N \frac{1}{\lambda_i + \lambda_j} + \dots + (-1)^{N-1} \frac{1}{\sum_{i=1}^N \lambda_i} = \text{MTTF}$$

$$= \sum_{i=1}^N \frac{1}{i \lambda_i}$$ IF THEY'RE IDENTICAL ($\lambda_i = \lambda_j \ \forall i, j$)

- r OUT OF N :

$$R(t) = \sum_{k=r}^N \binom{N}{k} \underbrace{e^{-\lambda k t}}_{k \text{ functioning}} \underbrace{\left(1 - e^{-\lambda t}\right)^{N-k}}_{N-k \text{ not}}$$

$$\mathbb{E}[T] = \sum_{k=r}^N \frac{1}{k\lambda} = \text{MTTF} \quad \text{(IF THEY'RE IDENTICAL)}$$

- COLD STAND-BY

2 ELEMENTS : MAIN + STAND-BY

$$f_T(t) = \int_0^t f_{T_1}(\tau) f_{T_2}(t-\tau)\, d\tau = \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1} \left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)$$

$$\mathbb{E}[T] = \left(\frac{1}{\lambda_2}\right)^2 - \left(\frac{1}{\lambda_1}\right)^2 = \text{MTTF}$$

N ELEMENTS : MAIN + (N-1) STAND-BY

$$\tilde{f}_T(s) = \prod_{i=1}^N \tilde{f}_{T_i}(s) \longrightarrow f_T(t)$$

$$R(t) = 1 - \int_0^t f_T(x)\, dx$$

$$\mathbb{E}[T] = \int_0^\infty t f_T(t)\, dt$$

- HOT STAND-BY

2 ELEMENTS :

$$R(t) = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_1 + \lambda_s - \lambda_2} \left[e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_s) t}\right]$$

N ELEMENTS:

$$R(t) = R_1(t) + \int_0^t f_1(\tau) R_s(\tau) R_2(t-\tau)\, d\tau$$

TIME-DEPENDENT

parallel system of 2 that share a load:

- both functioning: $f_A(t)$, $f_B(t)$ $\quad (\longrightarrow F_A(t), F_B(t))$
- one not functioning, the other: $g_A(t)$, $g_B(t)$ $\quad (\longrightarrow G_A(t), G_B(t))$

$R(t) = \mathbb{P}(\text{surviving till time } t)$

$= \mathbb{P}(\text{both survive}) + \mathbb{P}(\text{one fails at time } \tau\text{, the other not}) + \mathbb{P}(\text{the other fails})$

$$= (1 - F_{T_A}(t))(1 - F_{T_B}(t)) + \int_0^t \underbrace{f_{T_A}(\tau)}_{\substack{\text{A fails}\\ \text{at time } \tau}} \underbrace{\left(1 - F_{T_B}(\tau)\right)}_{\substack{\text{B survives}\\ \text{till time } \tau}} \underbrace{\left(1 - G_{T_B}(t-\tau)\right)}_{\substack{\text{B survives}\\ \text{from } \tau \text{ to } t\\ \text{under more}\\ \text{stress}}} d\tau + \int_0^t f_{T_B}(\tau)\left(1 - F_{T_A}(\tau)\right)\left(1 - G_{T_A}(t-\right.$$

AVAILABILITY

- quantifies the ability to fulfill the assigned mission at any specific moment of the lifetime
- repairs
- $\dfrac{MTBF}{MTBF + MDT}$ (Mean Time Between Failures) (Mean Down Time)

- $X(t) = \begin{cases} 1 & \text{system is operating at time } t \\ 0 & \text{system is failed at time } t \end{cases}$
- $p(t) = \mathbb{P}(X(t)=1) = \mathbb{E}[X(t)]$ = istantaneous availability
- $q(t) = \mathbb{P}(X(t)=0) = 1 - p(t)$ = istantaneous unavailability
- Average availability descriptors
  - corrective maintenance
    $$p = \lim_{t\to\infty} p(t)$$
  - periodic maintenance
    $$p_T = \frac{1}{T}\int_0^T p(t)\,dt = \frac{\overline{T_U}}{T}$$ average time up

AVAILABILITY OF :

- UNATTENDED COMPONENT (NO REPAIR) $\rightarrow$ istantaneous availability = reliability
  $$q(t) = F(t)$$
  $$p(t) = 1 - q(t) = R(t)$$

- CONTINUOUSLY MONITORED COMPONENT
  we can repair a failed component : T_R = time repair $\sim g(t)$
  suppose that we have N components

$$\underbrace{N\,p(t+\Delta t)}_{\text{expected number of available comp. at time } t+\Delta t} = \underbrace{N\,p(t)}_{\text{available at time } t} - \underbrace{N\,p(t)\,\overset{\mathbb{P}(\text{fail in }\Delta t)}{\lambda\,\Delta t}}_{\text{failed in the interval }\Delta t} + \int_0^t \underbrace{N\,p(\tau)\,\lambda\,\Delta\tau}_{\text{failed in }(\tau,\tau+\Delta\tau)}\ \underbrace{g(t-\tau)\,\Delta t}_{\text{repaired from }\tau\text{ before }t+\Delta t}$$

From this we obtain $(/N,\ /\Delta t,\ \Delta t \to \infty)$

$$\begin{cases} p'(t) = -\lambda p(t) + \int_0^t \lambda p(\tau)\, g(t-\tau)\, d\tau \\ p(0) = 1 \end{cases}$$

(a new component is available at $t=1$)

Laplace transform :

$$s\tilde{p}(s) - 1 = -\lambda\tilde{p}(s) + \lambda\tilde{p}(s)\tilde{g}(s)$$

$$\Longrightarrow \tilde{p}(s) = \frac{1}{s+\lambda(1-\tilde{g}(s))} \longrightarrow p(t) = \mathcal{L}^{-1}(\tilde{p}(s))$$

Asymptotic availability:

$$p = \lim_{t\to\infty} p(t) \overset{\text{zero-value theorem (Laplace)}}{=} \lim_{s\to 0} s\,\tilde{p}(s) = \lim_{s\to 0}\frac{s}{s+\lambda(1-\tilde{g}(s))}$$

First order approx. of $\tilde{g}(s)$ as $s\to 0$:

$$\tilde{g}(s) = 1 - s\,\overline{\tau}_R \qquad \text{where } \overline{\tau}_R = \mathbb{E}[T_R]$$

$$\Longrightarrow p = \frac{1}{1+\lambda\overline{\tau}_R} = \frac{1/\lambda}{1/\lambda + \overline{\tau}_R} = \frac{MTTF}{MTTF + MTTR} = \frac{\text{uptime}}{\text{overall time}} = \mathbf{A}$$

(Mean Time To Repair)

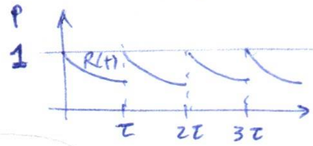
Unavailability of a system :

- series : $q_S = \sum_{i=1}^N q_i$ $\longrightarrow$ with stand-by (suppose comp 1 has the stand-by while comp 2 and 3 don't): $q_S = q_1^2 + q_2 + q_3$
  (component 1 has 2 stand-by?): $q_S = q_1^3 + q_2 + q_3$
- parallel : $q_P = \prod_{i=1}^N q_i$
- networks : we have to consider all the possible paths

- COMPONENT UNDER PERIODIC MAINTENANCE

We perform maintenance every τ.

→ suppose the testing time negligible:



the function between two successive inspections is the reliability function

average time down

average time up

$$q_\tau = \frac{\overline{T}_D}{\tau} = \frac{\int_0^\tau F_T(t)\,dt}{\tau} \quad , \quad p_\tau = 1 - q_\tau = \frac{\overline{T}_U}{\tau} = \frac{\int_0^\tau R(t)\,dt}{\tau}$$

average unavailability over a period τ — average availability over a period τ

→ suppose a repair time (always after test) τ_R:

$$q_{\tau+\tau_R} \cong \frac{\tau_R + \int_0^\tau F_T(t)\,dt}{\tau} \quad , \quad p_{\tau+\tau_R} \cong \frac{\int_0^\tau R(t)\,dt}{\tau}$$

→ realistic case:

- component initially working: $p(0)=1$, $q(0)=0$
- random failure: $T \sim f_T$
- on-line switching failure $\sim Q_0$
- maintenance disabling component $\sim \gamma_0$

average unavailability $[0,T]$?
(//// maintenance)

$\boxed{OA}$ $\quad q_{OA}(t) = Q_0 + (1-Q_0)\,F_T(t) \qquad = \mathbb{P}(\text{online failure}) + \mathbb{P}(\text{not online failure}, \text{random failing} \le t)$

$$\overline{T}_{D(OA)} = \int_0^\tau q_{OA}(t)\,dt = Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)\,dt$$

cycle repeated $k = \dfrac{T}{\tau+\tau_R}$ times (the time of OA is usually neglected)

$\boxed{AB}$ $\quad q_{AB}(t) = 1$

$$\overline{T}_{D(AB)} = \tau_R$$

$\boxed{BC}$ $\quad q_{BC}(t) = \gamma_0 + (1-\gamma_0)\,Q_0 + (1-\gamma_0)(1-Q_0)\,F_T(t)$

$= \mathbb{P}(\text{disabled at maint.}) + \mathbb{P}(\text{not disabled at maint}, \text{online failure}) + \mathbb{P}(\text{not dis. at maint}, \text{not online failure}, \text{random failing} \le t)$

$$\overline{T}_{D(BC)} = \int_0^\tau q_{BC}(t)\,dt = \gamma_0\tau + (1-\gamma_0)\left[Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)\,dt\right]$$

Total expected downtime:

$$\overline{T}_D = \underbrace{\left[Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)\,dt\right]}_{OA} + \frac{T}{\tau+\tau_R}\left[\underbrace{\tau_R}_{AB} + \underbrace{\left[\gamma_0\tau + (1-\gamma_0)\left[Q_0\tau + (1-Q_0)\int_0^\tau F_T(t)\,dt\right]\right]}_{BC}\right]$$

The average unavailability:

$$\overline{q}_T = \frac{\overline{T}_D}{T}$$

simplifying: $$\overline{q}_{0T} \cong \frac{\tau_R}{\tau} + \gamma_0 + (1-\gamma_0)\left[Q_0 + \frac{(1-Q_0)}{\tau}\int_0^\tau F_T(t)\,dt\right]$$

If the component is EXPONENTIAL:

$$\overline{q}_{0T} \cong \frac{\tau_R}{\tau} + \gamma_0 + Q_0 + \frac{1}{2}\lambda\tau$$

FAULT TREE ANALYSIS (FTA)

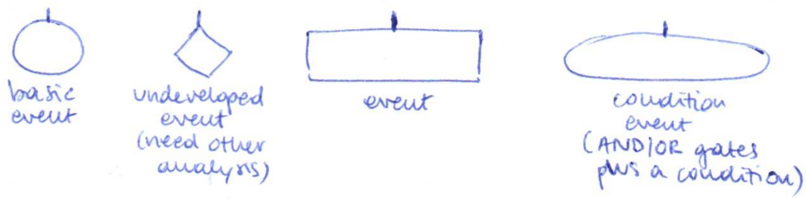
- calculate the probability of failure of the system given the probability of failure of its components
- deduce the combinations of failure of the elements that make the system fail
- systematic, quantitative, deductive

→ system diagram
→ fault tree
→ boolean algebra equation
→ minimal cut sets
→ probabilistic terms

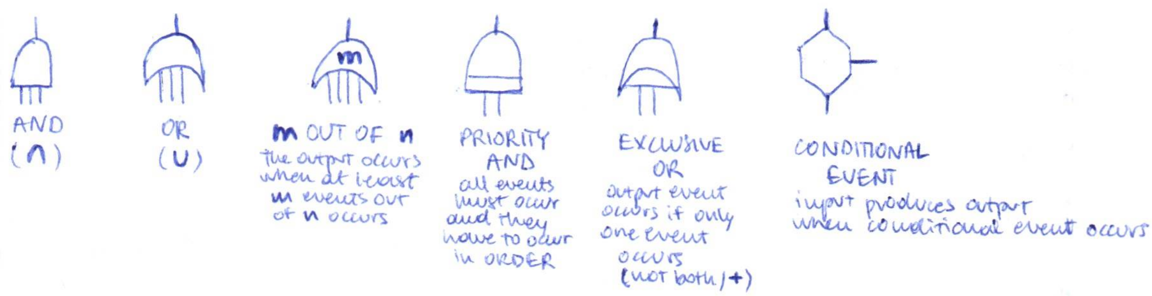
PROCEDURE:

1. Define the top event (system failure)
2. Decompose the top event by identifying sub-events that can cause it
3. Decompose each subevent in more elementary sub-events which can cause it
4. Stop decomposing when subevent probabilities are available
   (we stop at events which are ⫫ and characterizable in terms of failure/repair)

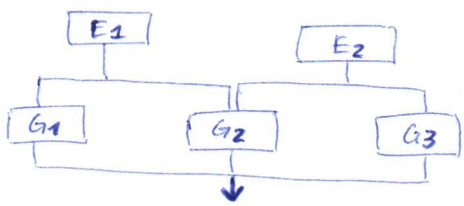
EVENTS:



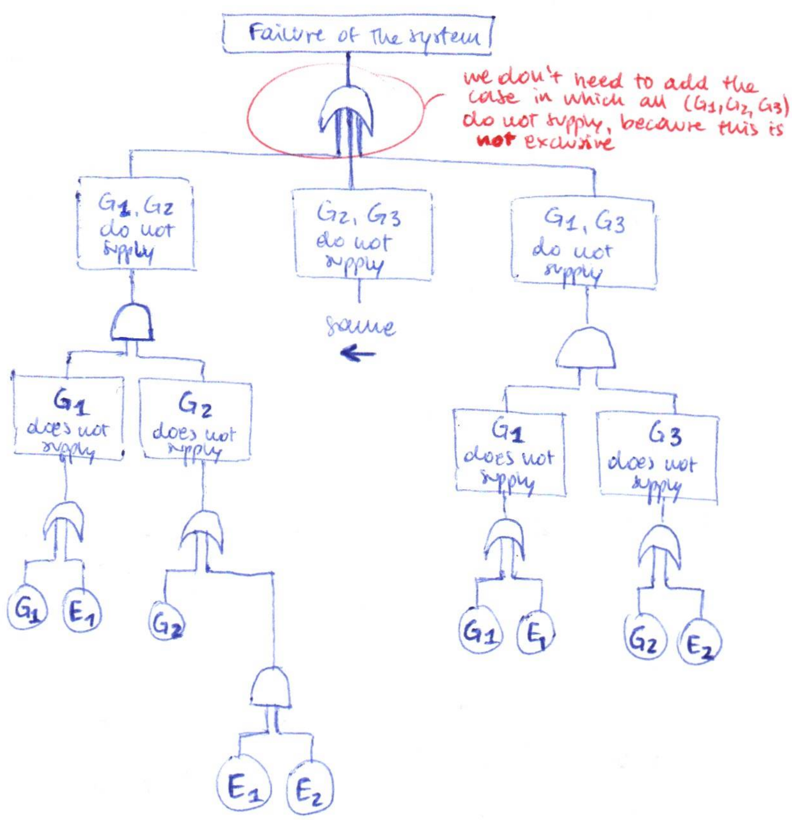
GATES:



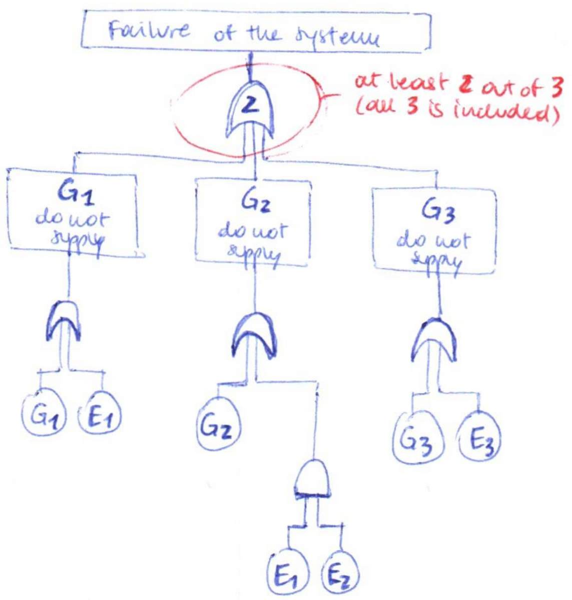
EXAMPLE 1:



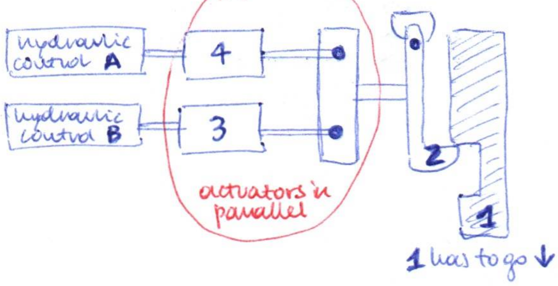
Solution 1.



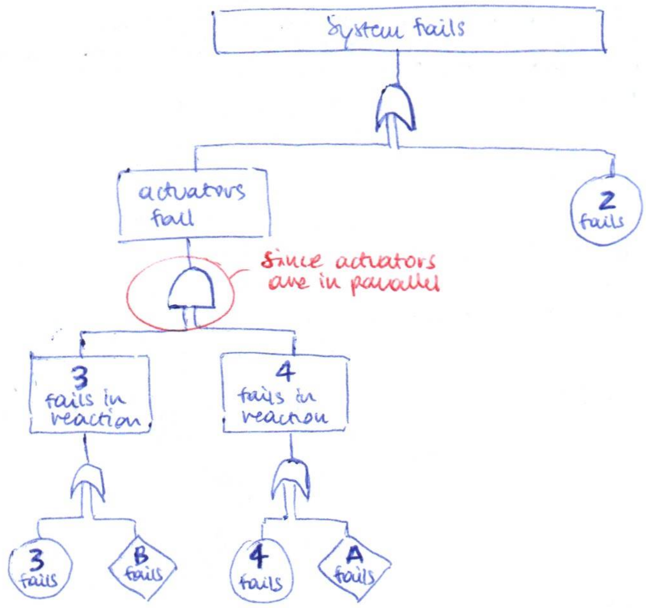
Solution 2.



EXAMPLE 2:



Solution:



QUALITATIVE ANALYSIS (no P involved)

→ Look for minimal combinations of failures that make the system fail

- $X_i = \begin{cases} 1 & \text{failure event} = \text{true} \\ 0 & \text{failure event} = \text{false} \end{cases}$: we have an indicator for any event
- $X_T = \phi(X_1, \dots, X_n)$ = state of the top event (given all the states $X_1, \dots, X_n$ and the logic represented by $\phi(\cdot)$, $X_T = \mathbb{1}\{\text{top event occurs}\}$)
- Structure function $\phi(\cdot)$:
  - can be written uniquely as the union of fundamental products
  - $\phi(\underline{1}) = 1$
  - $\phi(\underline{0}) = 0$
  - $\phi(\underline{X}) \geq \phi(\underline{Y})$ if $\underline{X} \geq \underline{Y}$ monotonically increasing in each variable (i.e. the repairing of 1/+ component/s cannot make the system not working)
  - cut sets: $\underline{X}$ s.t. $\phi(\underline{X}) = 0$
  - minimal cut sets: $\underline{X}$ s.t. $\phi(\underline{X}) = 0$ but if one of the events is not verified then the top event is not verified
- Fundamental laws:
  - $XX = X$
  - $X + X = X$
  - $X(X+Y) = X + XY = X$
  - $(X+Y)(X+Z) = X + YZ$
  - $X + \bar{X}Y = X + Y$
  - $\bar{X}(X+Y) = \bar{X}\bar{Y}$
  - OR GATE (X if A or B)
    $X = 1 - (1-A)(1-B)$
  - AND GATE (X if A and B)
    $X = AB$

EXAMPLE 2:

$$
\begin{aligned}
X_T &= 1 - (1 - X_2)(1 - X_{actuators}) \\
&= 1 - (1 - X_2)(1 - X_{3\_react} X_{4\ react}) \\
&= 1 - (1 - X_2)(1 - [1 - (1 - X_3)(1 - X_B)][1 - (1 - X_4)(1 - X_A)]) \\
&= 1 - (1 - X_2)(1 - [\cancel{1} \cancel{-1} + X_3 + X_B - X_3 X_B][\cancel{1} \cancel{-1} + X_4 + X_A - X_4 X_A]) \\
&= 1 - (1 - X_2)(1 - (X_3 + X_B - X_3 X_B)(X_4 + X_A - X_4 X_A))
\end{aligned}
$$

⟹ minimal cut sets: $M_1 = X_2$, $M_2 = X_3, X_4$, $M_3 = X_3, X_A$, $M_4 = X_B, X_4$, $M_5 = X_B, X_A$

Another method: "AND" → columns, "OR" → rows
(MOCUS)

X_2
$\boxed{X_{actuators}}$

→

X_2	
$\boxed{X_{3\_react}}$	$X_{4\text{-}react}$

→

X_2	
X_3	$\boxed{X_{4\text{-}react}}$
X_B	$\boxed{X_{4\text{-}react}}$

→

X_2		M_1
X_3	X_4	M_2
X_3	X_A	M_3
X_B	X_4	M_4
X_B	X_A	M_5

QUANTITATIVE ANALYSIS

→ we have to introduce probabilities

- using the laws of probability theory at the fault tree gate
  (from $X_T = \Phi(X_1, .., X_n)$ to $\mathbb{P}(X_T = 1) = \Phi(\mathbb{P}(X_1 = 1), .., \mathbb{P}(X_n = 1))$)
- using the mcs from the qualitative analysis

$$\mathbb{P}(\Phi(\underline{X}) = 1) = \sum_{j=1}^{mcs} \mathbb{P}(M_j) - \sum_{i=1}^{mcs-1} \sum_{j=i+1}^{mcs} \mathbb{P}(M_i M_j) + .. + (-1)^{mcs+1} \mathbb{P}(M_1 M_2 \cdots M_{mcs})$$

Rare events (overestimate) approximation:

$$\mathbb{P}(\Phi(\underline{X}) = 1) \leq \sum_{j=1}^{mcs} \mathbb{P}(M_j)$$

EXAMPLE 2:

$$\mathbb{P}(X_T = 1) = 1 - (1 - \mathbb{P}(X_2 = 1))\,(1 - (\mathbb{P}(X_3 = 1) + \mathbb{P}(X_B = 1) - \mathbb{P}(X_3 = 1)\mathbb{P}(X_B = 1))\,(\mathbb{P}(X_4) + \mathbb{P}(X_A) - \mathbb{P}(X_4)\mathbb{P}(X_A)))$$

$$= 1 - (1 - 0.01)(1 - (0.2 - 0.1^2)^2)$$

$$= 0.0457$$

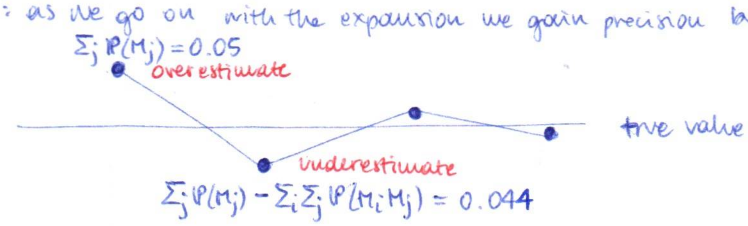
(reliability of the system: $1 - 0.0457$)

Approximation:

$$\mathbb{P}(M_1) = \mathbb{P}(X_2) = 0.01$$
$$\mathbb{P}(M_2) = \mathbb{P}(X_3, X_4) = 0.1^2 = 0.01$$
$$\mathbb{P}(M_3) = \mathbb{P}(X_3, X_A) = 0.1^2 = 0.01$$
$$\mathbb{P}(M_4) = \mathbb{P}(X_B, X_4) = 0.1^2 = 0.01$$
$$\mathbb{P}(M_5) = \mathbb{P}(X_B, X_A) = 0.1^2 = 0.01$$

$$\longrightarrow \mathbb{P}(X_T = 1) \leq \sum_j \mathbb{P}(M_j) = 0.05$$

Note: as we go on with the expansion we gain precision but:



EVENT TREE ANALYSIS (ETA)

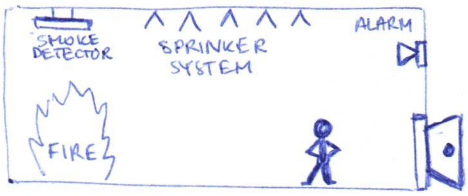
- systematic, quantitative, inductive
- identification of possible scenarios developing from a given accident initiator
- computation of accident sequence probability

PROCEDURE :

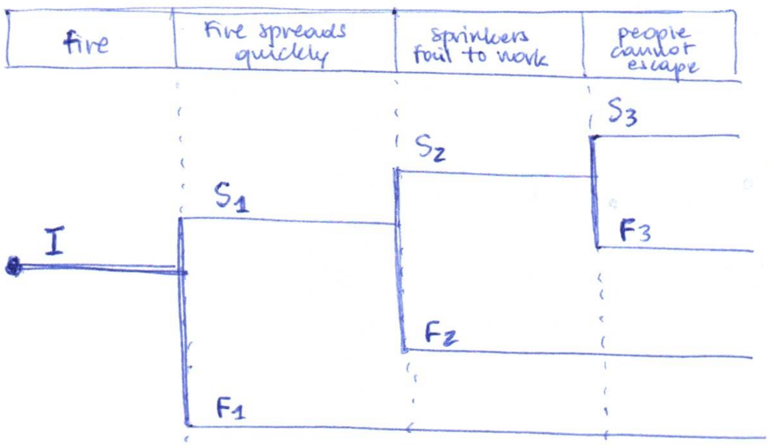
1. Define accident initiator I (system failure)
2. Identify safety/protection systems (S_k) demanded by I
3. Specify failure/success of S_k
4. Combine the states of all S_k to generate accident sequences

It's important to list in time and logic sequence of intervention

EXAMPLE :



Solution :



$\mathbb{P}(S_3|S_2,S_1,I)\ \mathbb{P}(S_2|S_1,I)\ \mathbb{P}(S_1|I)\ \mathbb{P}(I)$ multiple fatalities

$\mathbb{P}(F_3|S_2,S_1,I)\ \mathbb{P}(S_2|S_1,I)\ \mathbb{P}(S_1|I)\ \mathbb{P}(I)$ loss/damage

$\mathbb{P}(F_2|S_1,I)\ \mathbb{P}(S_1|I)\ \mathbb{P}(I)$ fire controlled

$\mathbb{P}(F_1|I)\ \mathbb{P}(I)$ fire contained (it estinguishes itself)

$\underbrace{\qquad\qquad\qquad\qquad}_{\text{all conditional } \mathbb{P}(\cdot)s}$

MARKOV

we want to describe the stochastic process of the system evolution which occurs as a consequence of the stochastic process of random transitions of the components in time

BASIC

- The system occupies a finite number of states $(N)^{+1}$
- States are mutually exclusive (the system is in 1! state) and exhaustive (always in one state)
- Transitions occur stochastically
- $X(t) = k$ = the system occupies state k at time t

DISCRETE-TIME FINITE-STATE MC

- The time interval is so small that only one event can occur within it
- $X(n) = k$ = the system occupies state k at time $t_n = n \cdot \Delta t$
- Objective : $\mathbb{P}(X(n)=j) \quad \forall n = 1, .., T, \quad \forall j = 1, .., N$
- Markov Process:

$$\mathbb{P}(X(n+1)=j \mid X(n)=i, \cancel{.., X(0)=x_0}) = \mathbb{P}(X(n+1)=j \mid X(n)=i) \qquad \text{(no memory)}$$

- Transition probability:

$$p_{ij}(m,n) = \mathbb{P}(X(n)=j \mid X(m)=i) \; ;$$

1. $p_{ij}(m,n) \geq 0$
2. $\sum_{j=1}^{N} p_{ij}(m,n) = 1$
3. $\boxed{p_{ij}(m,n) = \sum_k p_{ik}(m,r)\, p_{kj}(r,n)}$

- Homogeneous Markov Process (transition prob. are stationary) : $p_{ij}(m, m+k) = p_{ij}(k) \quad \perp\!\!\!\perp m$
  - → We need to know only the stationary one-step trans. prob. $p_{ij}(1) = p_{ij} = \mathbb{P}(i \to j)$
- Stochastic matrix $\underline{\underline{A}}$: (transition probability matrix)

$$\underline{\underline{A}} = \begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0N} \\ p_{10} & p_{11} & \cdots & p_{1N} \\ \vdots & & & \vdots \end{bmatrix}$$

- $\dim(\underline{\underline{A}}) = (N+1) \times (N+1)$
- $0 \leq p_{ij} \leq 1$
- $\sum_{j=0}^{N} p_{ij} = 1$ (by rows)

- $\mathbb{P}(X(n)=j) = P_j(n) \longrightarrow \underline{P}(n) = [P_0(n), P_1(n), .., P_N(n)]$

$$\underline{P}(0) = [C_0, C_1, .., C_N] = [1, 0, .., 0]$$

the initial state is the perfect functioning state

$$P_j(1) = \sum_{i=0}^{N} \mathbb{P}(X(1)=j \mid X(0)=i)\, \mathbb{P}(X(0)=i) = \sum_{i=0}^{N} p_{ij}\, C_i \quad ; \quad \underline{P}(1) = \underline{C} \cdot \underline{\underline{A}}$$

$$P_j(2) = \sum_{i=0}^{N} \mathbb{P}(X(2)=j \mid X(1)=i)\, \mathbb{P}(X(1)=i) = \sum_{i=0}^{N} p_{ij}\, P_i(1) \quad ; \quad \underline{P}(2) = \underline{P}(1) \cdot \underline{\underline{A}} = \underline{C} \cdot \underline{\underline{A}}^2$$

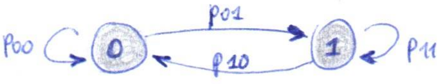
$\vdots$

$$\underline{P}(n) = \underline{P}(0) \cdot \underline{\underline{A}}^n = \underline{C} \cdot \underline{\underline{A}}^n \qquad \text{where} \qquad [\underline{\underline{A}}^n]_{ij} = p_{ij}(n) = \mathbb{P}(X(n)=j \mid X(0)=i)$$

example:

$$\underline{\underline{A}} = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} , \quad \underline{\underline{A}}^2 = \begin{bmatrix} p_{00}^2 + p_{01}p_{10} & p_{00}p_{01} + p_{01}p_{11} \\ p_{10}p_{00} + p_{11}p_{10} & p_{10}p_{01} + p_{11}^2 \end{bmatrix}$$

- Markov diagram (e.g. 2 states) :



- SOLUTION TO THE FUNDAMENTAL EQUATION :

$$\begin{cases} \underline{P}(n) = \underline{P}(0) \cdot \underline{\underline{A}}^n \\ \underline{P}(0) = \underline{C} \end{cases}$$

1. Find eigenvalues:
   $\underline{V} \cdot \underline{\underline{A}} = w\, \underline{V} \;\rightarrow\; \det(\underline{\underline{A}} - w\underline{\underline{I}}) = 0 \;\rightarrow\; w_j$
2. Find eigenvectors:
   $\underline{V}_j \underline{\underline{A}} = w_j \underline{V}_j$
3. Rewrite $\underline{C}$ as : $\underline{C} = \sum_{j=0}^{N} c_j \underline{V}_j$
4. $\boxed{\alpha_j = c_j w_j^n} \longrightarrow \underline{P}(n) = \sum_{j=0}^{N} \alpha_j \underline{V}_j$

- QUANTITY OF INTEREST
  - → Steady state probabilities π_j (asymptotic)
    - if we have eigen - :
      $$\lim_{n\to\infty} \underline{P}(n) = c_0 \underline{V}_0 = \underline{\Pi}$$
    - If we don't have:
      $$\begin{cases} \underline{P}(n) = \underline{P}(n-1)\underline{\underline{A}} \\ \underline{P}(n) = \underline{P}(n-1) = \underline{\Pi} \end{cases} \Rightarrow \begin{cases} \underline{\Pi} = \underline{\Pi} \cdot \underline{\underline{A}} \\ \sum_{j=1}^{N} \pi_j = 1 \end{cases} \quad [\pi_1 \cdots \pi_N] = [\pi_1 \cdots \pi_N] \ \underline{\underline{A}}$$
  - → First passage random time
    $$T_{ij} = \begin{cases} \min\{n \geq 1 : X(n) = j \mid X(0) = i\} & \text{if } \exists n \geq 1 \\ +\infty & \text{otherwise} \end{cases}$$
    $$\{T_{ij} = n\} = \{X(n) = j, X(n-1) \neq j, \dots, X(1) \neq j \mid X(0) = i\}$$
    $\mathbb{P}(T_{ij} = n) = f_{ij}(n)$ = $\mathbb{P}$ that the system goes to j for the 1st time after n steps
    $\neq p_{ij}(n)$ = $\mathbb{P}$ that the system goes to j from after n steps (here we're not counting first times)

    Renewal equation:
    $$f_{ij}(k) = p_{ij}(k) - \sum_{\ell=1}^{k-1} f_{ij}(k-\ell)\, p_{jj}(\ell)$$
    $$p_{ij}(k) = f_{ij}(k) + \sum_{\ell=1}^{k-1} f_{ij}(k-\ell)\, p_{jj}(\ell)$$
  - → Recurrent, transient, absorbing states:
    $$q_{ij}(m) = \sum_{n=1}^{m} f_{ij}(n)$$
    $q_{ij}(\infty) = \lim_{m\to\infty} q_{ij}(m)$ = $\mathbb{P}$ that the system reaches j from i eventually
    $f_{ii} = q_{ii}(\infty)$ = $\mathbb{P}$ that the system returns to i from i eventually

    Recurrent state $\Longleftrightarrow$ $f_{ii} = 1$ $(\pi_i \neq 0)$
    Transient state $\Longleftrightarrow$ $f_{ii} < 1$ $(\pi_i = 0)$
    Absorbient state $\Longleftrightarrow$ $p_{ii} = 1$
  - → Sojourn time in a state
    S_i = time spent in i
    $$\mathbb{P}(S_i = n) = p_{ii}^{\,n}(1 - p_{ii})$$
    $$S_i \sim Geom(1 - p_{ii})$$
    $\mathbb{E}[S_i] = \dfrac{1}{1 - p_{ii}}$ = average number of steps before the system exit the state

CONTINUOUS-TIME FINITE-STATE MC

- Objective: $\mathbb{P}(X(t) = j) \quad t \in [0, T], \ \forall j = 1, \dots, N$
- Markov assumption:
  the probability of the future depends only on the present:
  $$\mathbb{P}(X(t+\vartheta) = j \mid X(t) = i, X(u) = x(u) : 0 \leq u < t) = \mathbb{P}(X(t+\vartheta) = j \mid X(t) = i)$$
- Transition probabilities:
  $$p_{ij}(t, t+\vartheta) = \mathbb{P}(X(t+\vartheta) = j \mid X(t) = i) = p_{ij}(\vartheta)$$
  where $\vartheta = dt$ so small that only 1 event can occur
  → α_{ij} = transition rate from i to j
- Transition rate matrix: $\underline{\underline{A}}$:
  $$\boxed{\frac{d\underline{P}}{dt} = \underline{P}(t) \cdot \underline{\underline{A}}}, \quad \underline{\underline{A}} = \begin{bmatrix} -\sum_{j=1}^{N} \alpha_{0j} & \alpha_{01} & \cdots & \alpha_{0N} \\ \alpha_{10} & -\sum_{\substack{j=0 \\ j\neq 1}}^{N} \alpha_{1j} & \cdots & \alpha_{1N} \\ \vdots & \vdots & & \vdots \end{bmatrix}$$
- SOLUTION TO THE FUNDAMENTAL EQUATION:
  $$\begin{cases} \dfrac{d\underline{P}}{dt} = \underline{P}(t) \cdot \underline{\underline{A}} \\ \underline{P}(0) = \underline{C} \end{cases}$$
  1. $\boxed{\tilde{\underline{P}}(s) = \underline{C} \cdot \left[s \cdot \underline{\underline{I}} - \underline{\underline{A}}\right]^{-1}}$
  2. $\underline{P}(t) = \mathcal{L}^{-1}(\tilde{\underline{P}}(s))$

  where:
  $$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{\det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

– QUANTITY OF INTEREST

→ steady state probabilities π_j

$$\begin{cases} \underline{\pi} \cdot \underline{\underline{A}} = \underline{0} \\ \sum_{j=0}^{N} \pi_j = 1 \end{cases}$$

at steady state:

→ Frequency of departure from i to j : $v_{ij}^{dep}(t) = \alpha_{ij} P_i(t) = \alpha_{ij}\pi_i$

Total frequency of departure from i : $v_i^{dep}(t) = -\alpha_{ii} P_i(t) = -\alpha_{ii}\pi_i$

Arrivals to state i : $v_i^{arr}(t) = \sum_{k \neq i} \alpha_{ki} P_k(t) = \sum_{k \neq i} \alpha_{ki}\pi_k$

→ System failure intensity
(expected number of failures per unit of time)

$$W_f(t) = \sum_{i \in S} P_i(t)\, \lambda_{i \to F}$$

System repair intensity
(expected number of repairs per unit of time)

$$W_r(t) = \sum_{j \in F} P_j(t)\, \mu_{j \to S}$$

S = set of success states
F = set of failures states

→ Sojourn time in a state

T_i = time spent in i

$\mathbb{P}(T_i > t+s \mid T_i > t) = \mathbb{P}(T_i > s)$ memoryless

$T_i \sim \mathcal{E}(-\alpha_{ii})$

$\mathbb{E}[T_i] = \frac{1}{-\alpha_{ii}}$ = average time of occupancy of state i

→ $\pi_i = v_i^{dep}(\infty) \cdot \mathbb{E}[T_i]$ the mean proportion of time (π_i) that the system spends in the state i is equal to the visit frequency to state i multiplied by the mean duration of one visit in state i

→ System AVAILABILITY

$$p(t) = \sum_{i \in S} P_i(t) = 1 - \sum_{i \in F} P_i(t) \leftarrow \tilde{p}(s) = \sum_{i \in S} \tilde{P}_i(s) = \frac{1}{s} - \sum_{i \in F} \tilde{P}_i(s)$$

System RELIABILITY

- No repairs allowed:

$$R(t) = p(t) \leftarrow \tilde{R}(s) = \sum_{i \in S} \tilde{P}_i(s)$$

$$MTTF = \int_0^\infty R(t)\,dt = \tilde{R}(0) = \sum_{i \in S} \tilde{P}_i(0) = \left[\frac{1}{s} - \sum_{i \in F} \tilde{P}_i(s)\right]_{s=0}$$

- Repairs allowed:

1. Exclude all the failed states $i \in F$: $\underline{\underline{A}} \to \underline{\underline{A}}'$
2. Solve the reduced problem:

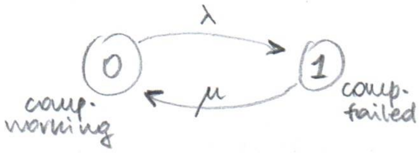
$$\frac{d\underline{P}^*}{dt} = \underline{P}^*(t) \cdot \underline{\underline{A}}'$$

3. $R(t) = \sum_{i \in S} P_i^*(t)$

$$MTTF = \int_0^\infty R(t)\,dt = \sum_{i \in S} \tilde{P}_i^*(0) = \tilde{R}(0)$$

EXAMPLE 1

One component, one repair-man : λ = failure rate, μ = repair rate



$$\longrightarrow \quad \underline{\underline{A}} = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

→ Time dependent state probabilities?

$$\underline{\tilde{P}}(s) = \underline{c}(s\underline{\underline{I}} - \underline{\underline{A}})^{-1} = [1 \ 0] \cdot \begin{bmatrix} s+\lambda & -\lambda \\ -\mu & s+\mu \end{bmatrix}^{-1} = [1 \ 0] \cdot \frac{1}{s^2+s\lambda+s\mu} \begin{bmatrix} s+\mu & \lambda \\ \mu & s+\lambda \end{bmatrix}$$

$$= \left[\frac{s+\mu}{s(s+\lambda+\mu)}, \frac{\lambda}{s(s+\lambda+\mu)} \right]$$

$$\underline{P}(t) = \Bigg[\underbrace{\frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}}_{\text{istantaneous availability}}, \underbrace{\frac{\lambda}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}}_{\text{istantaneous unavailability}} \Bigg] = [P_0(t), P_1(t)]$$

→ Steady state probabilities?

$$\underline{\Pi} = [\pi_0, \pi_1] = \lim_{t\to\infty} \underline{P}(t) = \left[\frac{\mu}{\lambda+\mu}, \frac{\lambda}{\lambda+\mu} \right] = \left[\frac{\overset{\text{MTBF}}{1/\lambda}}{1/\mu + 1/\lambda}, \frac{\overset{\text{MTTR}}{1/\mu}}{1/\mu + 1/\lambda} \right]$$

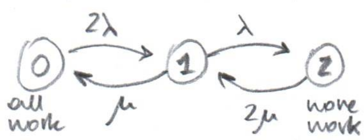
→ Failure/repair intensities?

$$W_f(t) = \lambda P_0(t) = \frac{\lambda\mu}{\lambda+\mu} + \frac{\lambda^2}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

$$W_r(t) = \mu P_1(t) = \frac{\lambda\mu}{\lambda+\mu} + \frac{\lambda\mu}{\lambda+\mu} e^{-(\lambda+\mu)t}$$

EXAMPLE 2

Two components, two repair-men : λ = failure rate, μ = repair rate



$$\longrightarrow \quad \underline{\underline{A}} = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & 2\mu & -2\mu \end{bmatrix}$$

→ Parallel logic ($F = \{2\}$); system reliability?

$$\underline{\underline{A}}' = \begin{bmatrix} -2\lambda & 2\lambda \\ \mu & -(\lambda+\mu) \end{bmatrix}$$

$$\underline{\tilde{P}}(s) = [1 \ 0] \begin{bmatrix} s+2\lambda & 2\lambda \\ \mu & s+\lambda+\mu \end{bmatrix}^{-1} = \frac{1}{s^2+(3\lambda+\mu)s+2\lambda^2} [s+\lambda+\mu, 2\lambda]$$

$$s^2+(3\lambda+\mu)s+2\lambda^2 = 0 \implies w_{0/1} = \frac{-(3\lambda+\mu) \pm \sqrt{\lambda^2+\mu^2+6\lambda\mu}}{2}$$

$$\underline{\tilde{P}}(s) = \left[\frac{s+\lambda+\mu}{(s-w_0)(s-w_1)}, \frac{2\lambda}{(s-w_0)(s-w_1)} \right]$$

$$\tilde{R}(s) = \sum P_i(s) = \frac{s+3\lambda+\mu}{(s-w_0)(s-w_1)} = \frac{s+3\lambda+\mu}{s^2+(3\lambda+\mu)s+2\lambda^2}$$

$$R(t) = \mathcal{L}^{-1}(\tilde{R}(s)) = \frac{-(w_1+3\lambda+\mu)e^{w_1 t} + (w_0+3\lambda+\mu)e^{w_0 t}}{w_0 - w_1}$$

→ MTTF?

$$\tilde{R}(0) = \frac{3\lambda+\mu}{2\lambda^2}$$

MONTE CARLO

SAMPLING

- Uniform $\mathcal{U}([0,1])$

  $R \sim \mathcal{U}([0,1]) \implies x_i = (a x_{i-1} + c) \bmod m \quad , \quad a, c \in [0, m-1] , \quad r_i = \frac{x_i}{m}$

- Inverse transform technique
  - continuous distribution

    $R \sim \mathcal{U}([0,1]) \ , \quad X = F_X^{-1}(R)$ $\qquad \mathbb{P}(X \le x) = \mathbb{P}(F_X^{-1}(R) \le x) = \mathbb{P}(R \le F(x)) = F(x)$

    → Exponential

    $T \sim \mathcal{E}(\lambda)$

    $F_T(t) = 1 - e^{-\lambda t} \quad \sim \mathcal{U}([0,1])$

    $F_T^{-1}(r) = -\frac{1}{\lambda} \ln(1-r) = t$

    → Weibull

    $T \sim \text{Weibull}(\alpha, \beta)$

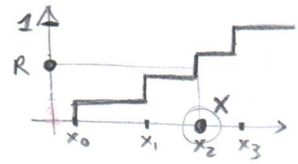
    $F_T(t) = 1 - e^{-\beta t^\alpha} \quad \sim \mathcal{U}([0,1])$

    $F_T^{-1}(r) = \left(-\frac{1}{\beta} \ln(1-r)\right)^{1/\alpha} = t$

  - Discrete distribution

    $R \sim \mathcal{U}([0,1]) , \quad X \in \{x_0, \dots, x_n, \dots\} \ , \quad F_n = \mathbb{P}(X \le x_n) = \sum_{i=0}^{n} \mathbb{P}(X = x_i)$

    $\mathbb{P}(F_{n-1} < R \le F_n) = F_n - F_{n-1} = \mathbb{P}(X = x_k)$



- Rejection method
  1. Normalize the distribution (dividing by the maximum) : $h(x) = \frac{f(x)}{f_M}$
  2. Sample $X \sim \mathcal{U}([0,1])$ and calculate $h(X)$
  3. Sample $R \sim \mathcal{U}([0,1])$:

     if $R \le h(X) \implies X$ accepted → $\boxed{\text{realization of } f(x)}$

     $R > h(X) \implies X$ rejected

  Efficiency $\varepsilon = \mathbb{P}(\text{accepted}) = \frac{1}{f_M} = \frac{1}{\max H(x)}$

  more generally
  1. $X \sim f(x) = g(x) H(x)$

     $h(x) = \frac{H(x)}{\max H(x)}$
  2. Sample $X' \sim g(x)$

     calculate $h(X')$
  3. $R \sim \mathcal{U}([0,1])$,

     accept if $R \le h(X')$

EVALUATION OF INTEGRALS (definite integrals)

- Analog case

  $$G = \int_a^b g(x) f(x)\, dx \xrightarrow[\substack{f(x) \text{ pdf} \\ f(x) \ge 0 \\ \int f(x) dx = 1}]{} G = \mathbb{E}[g(X)] \approx \underbrace{\frac{1}{N} \sum_{i=1}^{N} g(x_i)}_{x_i \text{ sampled from } f(x)}$$

- Biased case (variance reduction method)

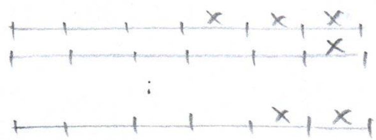
  $$G = \underbrace{\int_a^b \left[\frac{f(x)}{f_1(x)} g(x)\right] f_1(x)\, dx = \int_a^b g_1(x) f_1(x)\, dx}_{\text{we change the density from which we sample}} \longrightarrow G \approx \underbrace{\frac{1}{N} \sum_{i=1}^{N} g_1(x_i)}_{x_i \text{ sampled from } f_1(x)}$$

SIMULATION OF SYSTEM TRANSPORT

→ $\underbrace{K(t, k \mid t', k')\, dt}_{\text{probability that the system next transition occurs at } t \text{ and makes the system enters in } k \text{ given that the last trans. occurred at } t' \text{ and brought the syst. in } k'} = \underbrace{T(t \mid t', k)\, dt}_{\text{conditional prob. of a transition at } t \in dt \text{, given that the syst. was at } k' \text{ and the trans. bringing the system at } k' \text{ occurred at } t'} \ \underbrace{C(k \mid k', t)}_{\text{conditional prob. of entering } k \text{ given that there is a transition at } t \text{ and that the starting state is } k'}$ } gives the fully stochastic description of the process of transition

→ $\Psi(t; k)$ = (unconditioned) probability that the system has a transition at time t in which it enters at state k

- Reliability estimation **1**
  - we simulate M random walks (realizations of the system life generated by the underlying state-transition stochastic process)
  - calculate $C^R(t)$ = count of how many systems have failed before ($\leq$) t



$C^R(t)$ 0 0 0 1 2 3

  - calculate the unreliability of the system: $\hat{F_T}(t) = \frac{C^R(t)}{M}$ = cumulative distr. of the failure time of the system

- Ways to simulate
  - **Indirect** Monte Carlo (system)
    at each time step, the equivalent system transition rate is computed as the sum of transition rates of the components out of their current states
  - **Direct** Monte Carlo (component-wise)
    each component transition time is directly sampled and then, the next system transition time is defined as the first occurring component transition time

Each trial of a MC simulation consists in generating a random walk which guides the system from one configuration to another, at different times. During a trial, starting from a given system configuration k' at t', we need to determine when the next transition occurs and what is the new configuration reached by the system as a consequence of the transition. This can be done in 2 ways.

- Reliability estimation **2**

$$\underbrace{G(t)}_{\text{unreliability at time } t} = \underbrace{\sum_{k \in \Gamma} \int_0^t \psi(\tau, k) R_k(\tau, t) \, d\tau}$$

probability that the system enters a failed state (Γ = set of failed states, $\psi(\tau, k)$ = density function / prob. to enter k at time τ) and that remain in the failed state from the entering (τ) till t ($R_k(\tau, t)$)

- Boltzmann transport equation

$$\psi(t,k) = \underbrace{\psi^0(t,k)}_{\substack{0^{th} \text{ transition directly to } k \text{ at time } t \\ \text{(already be there)}}} + \sum_{k'} \int_{t_0}^{t} \underbrace{\psi(t',k')}_{\text{go to } k' \text{ at time } t'} \underbrace{K(t,k \mid t',k')}_{\substack{\text{go to } k \text{ at time } t \text{ starting from } k' \\ \text{reached at time } t' \text{ (transport kernel)}}} \, dt'$$

- Monte Carlo solution to the transport equation

$$\psi^1(t_1,k_1) = K(t_1,k_1 \mid t_0,k_0)$$

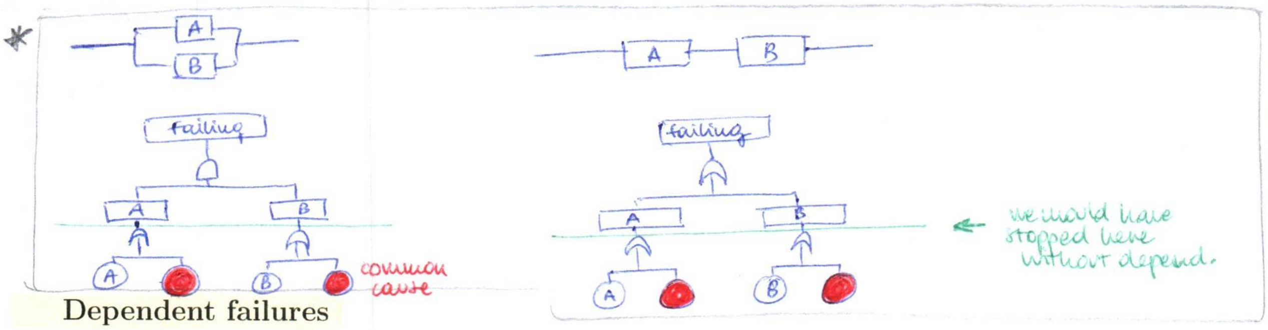
$$\psi^2(t_2,k_2) = \sum_{k_1} \int_{t_0}^{t_2} \psi^1(t_1,k_1) K(t_2,k_2 \mid t_1,k_1) \, dt_1$$

$$= \sum_{k_1} \int_{t_0}^{t_2} K(t_1,k_1 \mid t_0,k_0) K(t_2,k_2 \mid t_1,k_1) \, dt_1$$

$\vdots$

$$\psi^n(t_n,k_n) = \sum_{k_1,\dots,k_{n-1}} \int_{t_0}^{t_n} \int_{t_0}^{t_{n-1}} \cdots \int_{t_0}^{t_2} \underbrace{K(t_1,k_1 \mid t_0,k_0) \cdots K(t_n,k_n \mid t_{n-1},k_{n-1}) \, dt_1 \cdots dt_{n-1}}$$

we're going to sample from this, we're sampling the full path $x = (t_1, k_1, t_2, k_2, \dots)$



Dependent failures

Ignoring dependent failures leads to underestimation of risk: $\mathbb{P}(A \cap B) = \mathbb{P}(A|B) \cdot \mathbb{P}(B) \neq \mathbb{P}(A) \cdot \mathbb{P}(B)$.
There might be *common cause failures* (CCF): multiple failures derive directly from a common/shared root cause. Or *cascading failures*: if several components share a common load and one component fails, there is an increased load on the remaining ones, and so an increased likelihood of failure.

Explicit methods: identification and treatment of specific root causes of dependent failures at the system level in the event/fault-tree logic.

1. **Common cause initiating event**: external events are treated explicitly as initiating events in the risk analysis
2. **Intersystem dependences**: dependences among systems (two safety systems S_1 and S_2 are expected to intervene upon the occurrence of an initiating event (IE))

   2.A. **Functional dependences**: S_2 is not needed (NN) unless S_1 fails

   2.B. **Shared equipment**

   – **Event trees with boundary conditions**: take out the shared components and explicitly represent them in the system event tree, then, to evaluate the probabilities, develop the conditional fault trees

   – **Fault tree link**: faul trees of S_1 and S_2 are linked together, thus develop a single large fault tree for each accident sequence

   Event tree with boundary conditions have analysts which have to explicitly recognize the shared equipment dependences. Fault tree links have shared equipment denpendences automatically accounted in mcs.

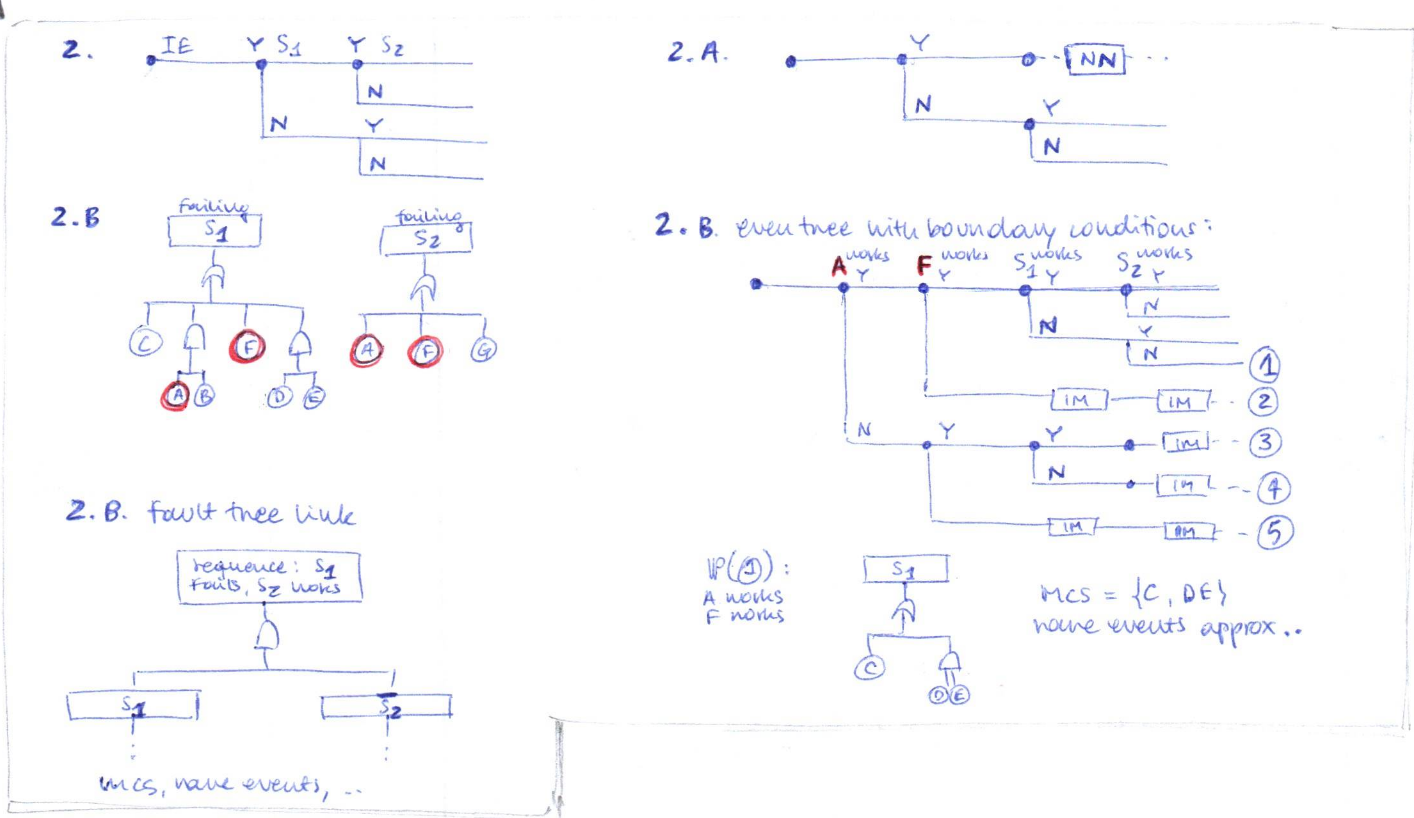
   2.C **Physical interactions**: S_2 can operate only if S_1 operates successfully (when S_1 fails, a physical interaction takes place and inhabits S_2)

3. **Intercomponent dependences**: dependences among components (if there is a dependence among components, the probability of failure of the overall system is a little higher when considering the dependence rather than when not considering it → neglecting dependences among failures leads to *optimistic prediction* in *parallel* and *conservative predictions* in *series*)

Implicit methods: multiple failure events for which no clear root cause event can be identified and treated explicitly are modeled using implicit and parametric models.

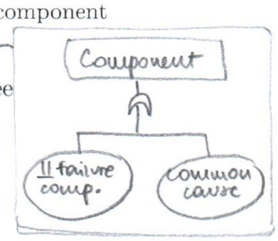
→ Square root method: (components positively dependent (the failure of one increases the probability of failing of the other))

$$\underbrace{\mathbb{P}(A)\,\mathbb{P}(B)}_{:= P_L} \le \mathbb{P}(A,B) \le \underbrace{\min\{\mathbb{P}(A), \mathbb{P}(B)\}}_{:= P_U} \Rightarrow \mathbb{P}(A,B) \simeq \sqrt{P_L P_U}$$



Methodological framework for Common Cause Failures (CCF) analysis

1. **System logic model development**
   Identify and understand the physical and functional links in the system, the functional dependences and interfaces, then develop the corresponding logic models of the system (fault trees and event trees), which include the proper representation of the identified dependencies
2. **Identification of common-cause component groups**
   → ***Qualitative screening***: identify group of components potentially involved in dependent failures (common cause component groups := group of similar/identical components that have a significant likelihood of experiencing a common cause event)
   → ***Quantitative screening***: modify the fault trees by explicitly including the CCF basic event for each component in a common cause group (numerical values for the probabilities of the CCF basic events can be estimated by the beta factor model)
3. **Common-cause modeling and data analysis**
   Complete the system quantification by incorporating the effects of common cause events for those component groups that survive the screening



   - **Definition of common cause basic events**: each component basic event becomes a sub-tree
   - **Selection of implicit probability models for common cause basic events**
     - Taxonomy 1
       * *Single-parameter model* - **Beta factor model**
       * *Multi-parameter model*
     - Taxonomy 2
       * *Shock models* - **Binomial failure rate model**
         assume that the system is subject to a common cause 'shock' which occurs at a certain rate
       * *Non-shock direct models*
         use the probabilities of common cause events directly
       * *Non-shock indirect models*
         estimate the $\mathbb{P}$'s of the common cause events through the introduction of other parameters
   - **Data classification and screening**
   - **Parameter estimation**
4. **System quantification and interpretation of results**

β-FACTOR MODEL

$Q_t = \mathbb{P}$(failure of a component in a common cause group of m components)

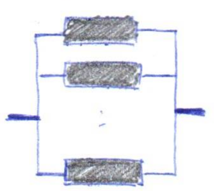
$$Q_t = \underbrace{Q_I}_{\parallel \text{ prob. of failure}} + \underbrace{Q_m}_{\mathbb{P}\text{ all comp. of the group fail}}$$

$$\beta = \frac{Q_m}{Q_t} \longrightarrow \begin{aligned} Q_m &= \beta Q_t \\ Q_I &= (1-\beta) Q_t \end{aligned}$$

External event can cause the simultaneous failure of all components in the system
β = % of the failure rate of a component attributable to the external event
→ factor model → hypotetical component C in series with the rest of the system

Ex. n identical component with failure rate λ:

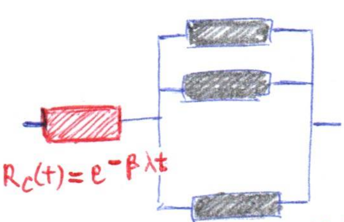
no dependence



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

$R_{TOT}(t) = 1-(1-R(t))^n$

dependence



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

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

$R_{TOT}(t) = (1-(1-R_I(t))^n)\, R_C(t)$

BINOMIAL FAILURE RATE (BFR)

- system of m components
- each component can fail at random time, $\parallel$ from the others, with failure rate λ
- a common shock hits the system with occurrence rate μ
- whenever a shock occurs, each of the m components may fail with probability p ($p=1 \Rightarrow \beta$-model)

- Failure rate for 1 unit:

$$\lambda_1 = \underbrace{m\lambda}_{\text{either fails a component }\parallel} + \underbrace{\mu\left[\binom{m}{1} p(1-p)^{m-1}\right]}_{\text{either fails a component because of the shock}}$$

- Failure rate for $i > 1$ units:

$$\lambda_i = \mu\left[\binom{m}{i} p^i (1-p)^{m-i}\right] \quad \text{(only due to the shock)}$$

$$f(t) \longrightarrow \tilde{f}(s) = \int_0^{+\infty} f(t)\, e^{-st}\, dt = \mathcal{L}(f(t))$$

$$\tilde{f}(s) \longrightarrow f(t) = \mathcal{L}^{-1}(\tilde{f}(s))$$

$f(t)$			$\tilde{f}(s)$		
e^{at}	e^{-at}	$\frac{1}{a}(1-e^{-at})$	$\frac{1}{s-a}$	$\frac{1}{s+a}$	$\frac{1}{s(s+a)}$
t^n			$\frac{n!}{s^{n+1}}$		
$\sin(at)$			$\frac{a}{s^2+a^2}$		
$\cos(at)$			$\frac{s}{s^2+a^2}$		
1			$\frac{1}{s}$		
$f'(t)$			$s\tilde{f}(s) - f(0)$		
$t^n e^{at}$			$\frac{n!}{(s-a)^{n+1}}$		

$$h(t) = \int_0^t f_1(t-\tau)\, f_2(\tau)\, d\tau \longrightarrow \tilde{h}(s) = \tilde{f}_1(s) \cdot \tilde{f}_2(s)$$

$$\tilde{f}(s) = \frac{2(s-1)}{s(s+1)(s+2)^2} \xrightarrow{\frac{A}{s} + \frac{B}{s+1} + \frac{C}{s+2} + \frac{D}{(s+2)^2}} \tilde{f}(s) = -\frac{1/2}{s} + \frac{4}{s+1} - \frac{7/2}{s+2} - \frac{3}{(s+2)^2}$$

$$f(t) = -\frac{1}{2}\mathbb{1}_{(t>0)} + 4e^{-t} - \frac{7}{2}e^{-2t} - 3te^{-2t}$$

$$\Gamma(\alpha) = \int_0^{+\infty} x^{\alpha-1}\, e^{-x}\, dx$$

$$\Gamma(n+1) = n!$$
$$\Gamma(\alpha+1) = \alpha\, \Gamma(\alpha)$$
$$\Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi}$$