Bruno Castanier – ISTIA – Bureau E43 – Bruno.Castanier@univ-angers.fr

Les outils d'évaluation de la Sûreté de Fonctionnement

Formation Alstom

Institut des Sciences et Techniques de l'Ingénieur d'Angers

Sommaire

- Journée 1 :
  - Quelques rappels sur les lois de durée de vie
  - Les outils d'analyse statique
    - Les diagrammes de fiabilité
    - Les arbres de défaillance
    - Les arbres d'événements (à confirmer)
    - Les facteurs d'importance
  - Un modèle d'analyse dynamique : les processus de Markov
- Journée 2 : Etudes de cas
  - Estimation des performances d'une rame de tramway vis-à-vis de la défaillance des portes
  - Estimation des performances d'un tramway vis-à-vis de ses bogies

Quelques rappels sur les lois de durées de vie

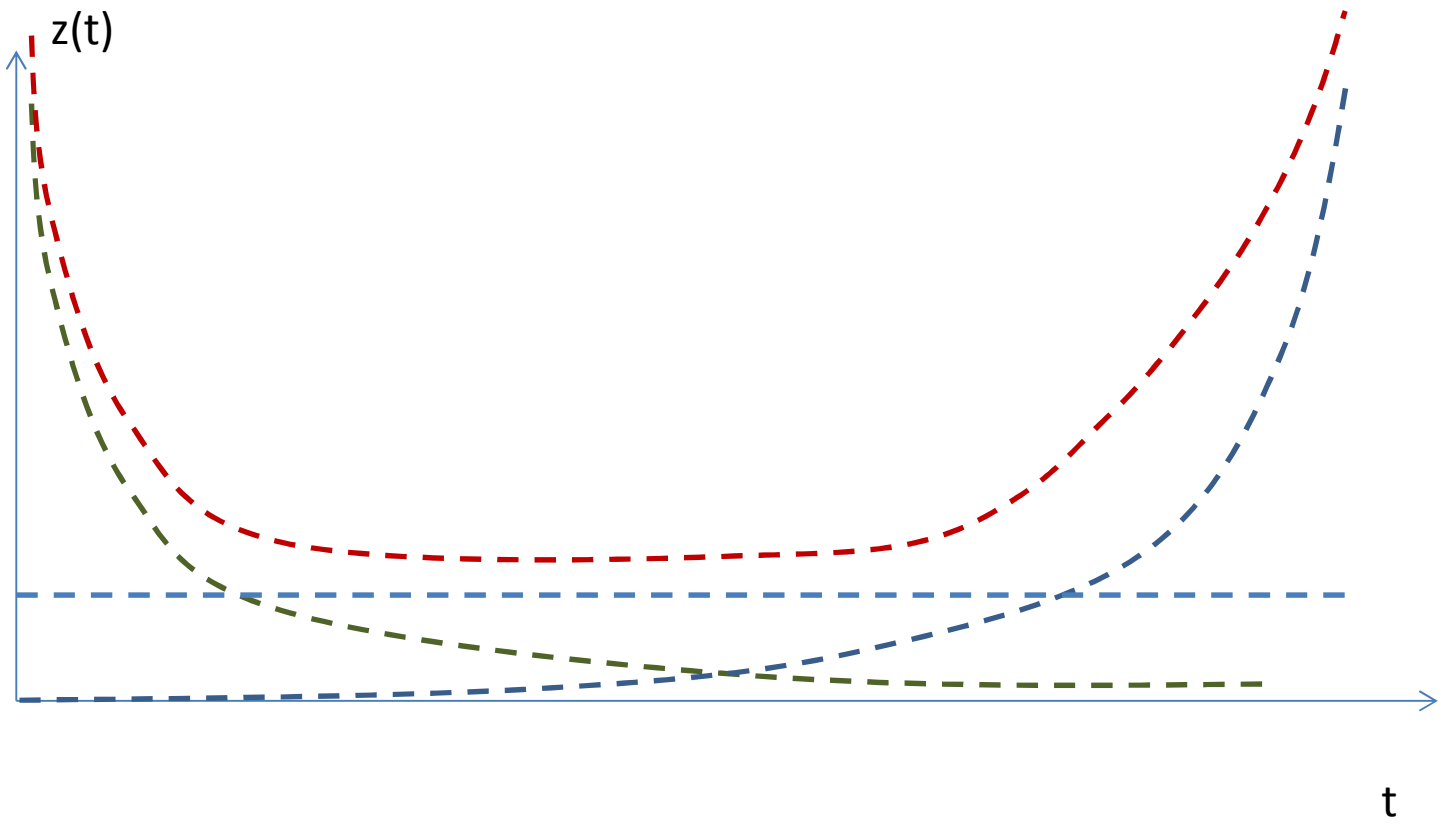
- Les métriques en fiabilité

Expressed by	$F(t)$	$f(t)$	$R(t)$	$z(t)$
$F(t) =$	–	$\int_0^t f(u)\,du$	$1 - R(t)$	$1 - \exp\left(-\int_0^t z(u)\,du\right)$
$f(t) =$	$\frac{d}{dt}F(t)$	–	$-\frac{d}{dt}R(t)$	$z(t) \cdot \exp\left(-\int_0^t z(u)\,du\right)$
$R(t) =$	$1 - F(t)$	$\int_t^\infty f(u)\,du$	–	$\exp\left(-\int_0^t z(u)\,du\right)$
$z(t) =$	$\frac{dF(t)/dt}{1 - F(t)}$	$\frac{f(t)}{\int_t^\infty f(u)\,du}$	$-\frac{d}{dt}\ln R(t)$	–

Quelques rappels sur les lois de durées de vie

- Quelques mesures complémentaires
  - MTTF
  - $R(x|t) = \frac{R(t+x)}{R(t)}$
  - $MRL(t) = \int_0^{+\infty} R(x|t)dx = \frac{1}{R(t)} \int_t^{+\infty} R(x)dx$
  - $L_{10} = \{t > 0 | R(t) = 0.90\}$

Taux de défaillance d'un système en phase d'exploitation



Etude de quelques lois et leur contexte d'application

- Lois discrètes :
- Lois binomiale et géométrique
  - Processus de Poisson
  - Lois continues :
  - Loi exponentielle
  - Loi de Weibull
  - Loi gamma
  - Loi normale
  - Loi Lognormale
  - Distribution de Birnbaum-Saunders
  - Les distributions des valeurs extrêmes

La loi exponentielle

- Hypothèse : Fonction du taux de défaillance constante
- Calculer la durée de vie résiduelle moyenne d'une carte électronique pour laquelle on suppose un taux de défaillance $\lambda_1 = 4.28 \cdot 10^{-4} h^{-1}$. Conclure
- Si on rajoute une seconde carte avec un taux λ_2. Quelle est la probabilité qu'elle soit défaillante avant la carte 1 ?
- Le taux de défaillance d'une population issue d'un mélange de lois exponentielles n'est pas constant.

La loi de Weibull

- Hypothèse : fonction du taux de défaillance monotone et continue en fonction du temps

$$z(t) = \alpha t^{\beta}, t \geq 0$$

- On peut alors retrouver

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$

- Et les autres métriques de fiabilité de la loi de Weibull à 2 paramètres.
- Tracer le taux de défaillance d'une loi de Weibull dont le paramètre d'échelle vaut 1 pour des paramètres de forme $\beta = 0.5, 1, 2\ et\ 3$.

Nota : $MTTF = \eta\Gamma\left(1 + \frac{1}{\beta}\right)$ et $\mathrm{Var(T)} = \eta^2\left[\Gamma\left(1 + \frac{2}{\beta}\right) - \Gamma^2\left(1 + \frac{1}{\beta}\right)\right]$

La loi Gamma

- Supposons qu'un système tombe en panne au *k*ème choc sachant que les intervalles entre chocs sont exponentiellement distribués, alors

$$T \sim gamma(\alpha, \beta)$$

$$f(t) = \frac{\beta}{\Gamma(\alpha)}(\beta t)^{\alpha-1}e^{-\beta t}, MTTF = \frac{\alpha}{\beta}, Var(t) = \frac{\alpha}{\beta^2}$$

Le taux de défaillance est croissant pour $\alpha \geq 1$ et tend asymptotiquement vers β

- Cas spécifiques :
  - $\beta = 1$, loi exponentielle
  - $\beta = {}^{n}/_{2}\ et\ \alpha = {}^{1}/_{2}$, loi du Khi-Deux avec *n* degrés de liberté
  - $\alpha \in \mathbb{N}$, loi de Erlang

La loi normale

La modélisation d'une durée de vie par une loi normale impose une troncature à gauche en 0 (T>0).

On peut montrer que, pour t >0 :

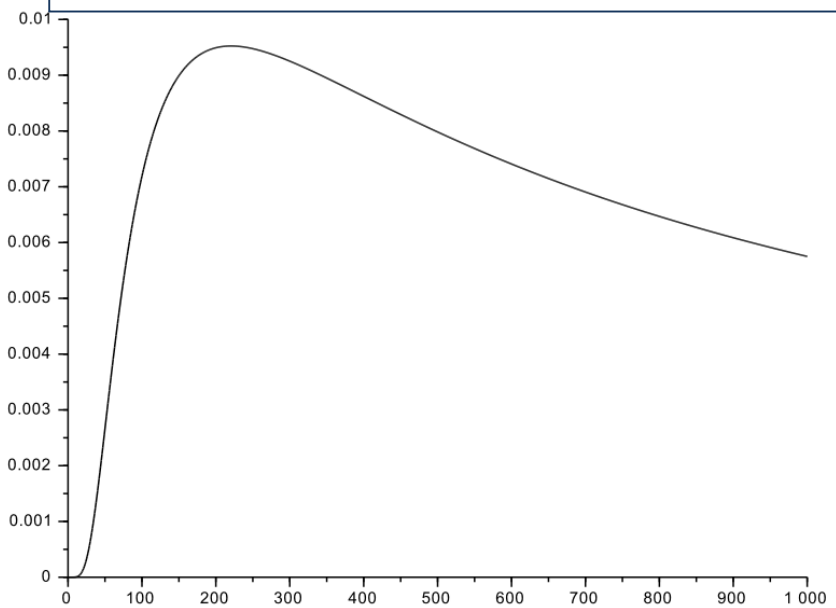
- $R(t) = \frac{\Phi((\mu - t)/\sigma)}{\Phi(\mu/\sigma)}$
- $\mathrm{z}(t) = \frac{1}{\sigma} \frac{\phi((t-\mu)/\sigma)}{1-\Phi((t-\mu)/\sigma)}$

La loi Lognormale

$$T \sim Lognormal(\mu, \sigma^2)\ si\ Y = \ln T \sim normal\ (\mu, \sigma^2)$$

$$MTTF = e^{-\mu + \sigma^2/2}\ ;\ R(t) = \Phi\left(\frac{\mu - \ln t}{\sigma}\right)$$

$$z(t) = \frac{\phi(\frac{\mu - \ln t}{\sigma})/\sigma t}{\Phi(\frac{\mu - \ln t}{\sigma})}$$



Cas d'applications :

- Les durées de maintenance
- En fiabilité mécanique, relation avec la courbe de Whöler

La distribution de Birnbaum-Saunders

- Supposons que la fatigue ne puisse pas être liée à des cycles de stress sinusoïdaux mais quelle reste la somme cumulée de fatigues partielles aléatoires (μ, σ^2) liées à chacun des *n* cycles.
- La défaillance est liée à un seuil de fatigue ω.
- Si *N* est le cycle d'observation de la défaillance, on a

$$\Pr(N \leq n) \approx \Phi\left(\frac{\omega - n\mu}{\sigma\sqrt{n}}\right)$$

En introduisant $\alpha = \sigma/\sqrt{\mu\omega}$ et $\lambda = \mu/\omega$, dans un contexte continu, on trouve

$$F(t) \approx \Phi\left(\frac{1}{\alpha}\left(\sqrt{\lambda t} - \frac{1}{\sqrt{\lambda t}}\right)\right)$$

On peut alors retrouver les autres caractéristiques.

Les distributions des valeurs extrêmes

- Définition : Si T_i sont des v.a. i.i.d. avec des distributions continues, la loi des valeurs extrêmes est la loi des v.a. suivantes :
  - $T_{(1)} = \min(T_1, T_2, \dots, T_n)$
  - $T_{(n)} = \max(T_1, T_2, \dots, T_n)$
- Question : et si *n* est très grand ?
- Les lois les plus utilisées
  - La loi de Gumbel pour le plus petit extrême
  - La loi de Gumbel pour le plus grand extrême
  - La loi de Weibull pour le plus petit extrême

Modélisation en fonction du stress

- Exemple d'un stress sur la loi de Weibull
  - On considère un système dont la défaillance sous condition nominale peut être modélisée par une loi de Weibull
  - On suppose un effet multiplicatif d'un stress (température notée *s*) sur la durée de vie. On peut alors montrer :

$$\beta(s) = \beta$$
$$\eta(s) = \eta(0).s^b$$

D'où

$$\Pr(T < t; s) = 1 - e^{-\left(\frac{t}{\eta(0)s^b}\right)^\beta}$$

Comment choisir sa loi ?

- Première approche :
  - L'expertise en fonction des contextes d'utilisation et en analysant les tendances des taux de défaillance
- Deuxième approche :
  - Test d'adéquation graphique
  - Test d'adéquation de type Chi-Deux
  - Critère de type AIC

Evaluation statique de la fiabilité

- Diagramme de fiabilité
- Les arbres de défaillance
- Les arbres d'événements (à confirmer)
- Les facteurs d'importance

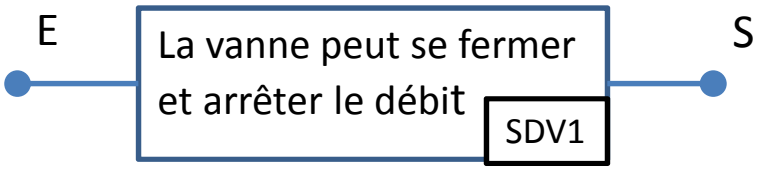
Diagramme de fiabilité

- Problématique :
  - Caractérisation individuelle des modes de défaillances et des composants
  - Quid de la performance globale du « système » ?
- Hypothèses :
  - $R_S(t) = f_S(t; x_1(t), x_2(t), \dots, x_n(t))$

  Où
    - $x_i(t)$ est l'état de réalisation de la fonction i, supposé indépendant des autres états $x_j, j \neq i$
    - $f_s(t; \cdot)$ est la fonction fiabilité qui est fonction du niveau de réalisation de l'ensemble de ses fonctions et de la structure (architecture) même du système

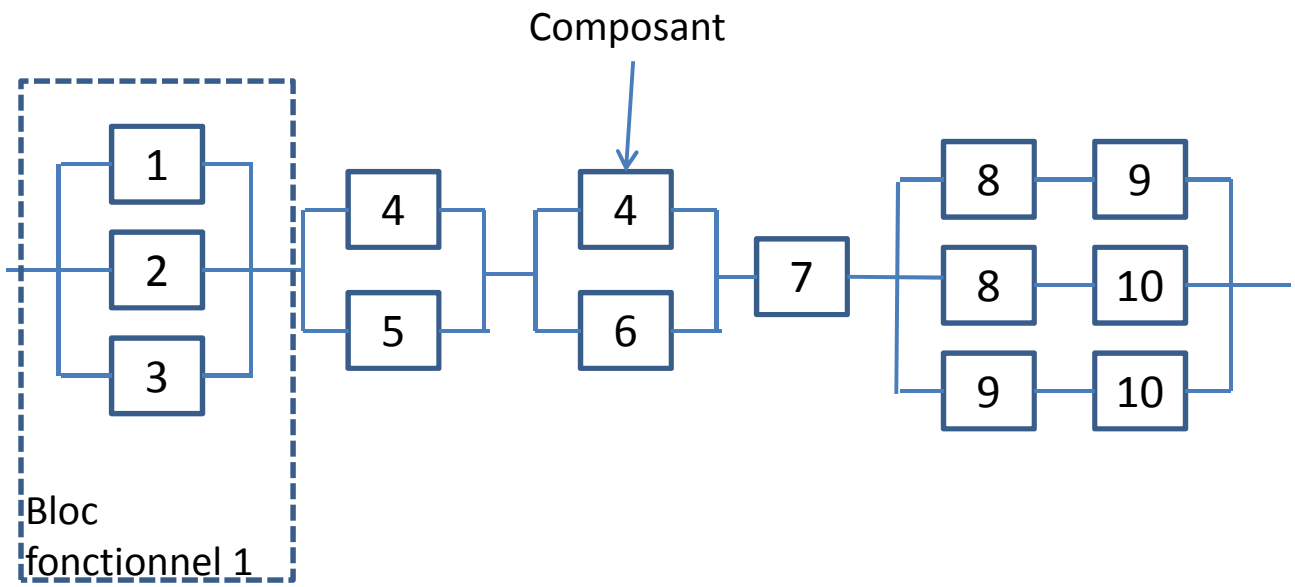
Diagramme de fiabilité

- Définition
  - Un diagramme (ou bloc diagramme) de fiabilité est un graphe orienté succès illustrant de manière logique comment le fonctionnement de différents blocs fonctionnels assure la mission/fonction globale du système. La structure du diagramme de fiabilité est décrite mathématiquement par des **fonctions de structure**, qui permettent d'évaluer des indices de fiabilité du système (complexe).
- Modélisation d'une fonction



Modélisation de systèmes complexes

- Décomposition en bloc fonctionnel du système



Les architectures classiques

- Structure « Série »
  - Un système qui fonctionne si et seulement si tous ces *n* composants fonctionnent est appelé une structure/système série.

- Structure « Parallèle »
  - Un système qui fonctionne si au moins un de ces *n* composants fonctionne est appelé structure/système parallèle.

- Structure « *k*-sur-*n* »
  - Un système qui fonctionne si au moins *k* de ces *n* composants fonctionnent est appelé structure/système *k*-sur-*n* (*koon*)

Exemple

- On considère 2 vannes de sécurité indépendantes V1 et V2 qui sont physiquement installées en série.

- En régime normal, les vannes sont ouvertes et se ferment automatiquement et coupent le débit en cas d'urgence.
- Questions :
  - Identifiez les fonctions du système
  - Définissez le diagramme de fiabilité

Fonction de structure

- Soit un système formé de *n* composants indépendants pour lesquels on définit le vecteur d'état $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$ avec :

$$x_i = \begin{cases} 1 & si\ le\ composant\ i\ fonctionne \\ 0 & s'il\ est\ dans\ l'état\ de\ panne \end{cases}$$

- La fonction binaire $\phi(\boldsymbol{x}) = \phi(x_1, x_2, \dots, x_n)$ telle que

$$\phi(\boldsymbol{x}) = \begin{cases} 1 & si\ le\ système\ fonctionne \\ 0 & s'il\ est\ dans\ l'état\ de\ panne \end{cases}$$

est appelée **fonction de structure du système** ou simplement **structure**.

Exercice

- Ecrire la fonction de structure :
  - D’un système série
  - D’un système parallèle
  - D’un système *2*-sur-*3*

Analyse de structure des systèmes

- Un composant *i* est appelé **non-pertinent** si $\phi(1_i, \boldsymbol{x}) = \phi(0_i, \boldsymbol{x})$ pour tout $(\cdot_i, \boldsymbol{x})$ où $(\cdot_i, \boldsymbol{x})$ est le vecteur pour lequel l'état du composant *i* vaut 1 ou 0
- Un système est dit **cohérent** si tous ses composants sont pertinents et que sa fonction de structure est non-décroissante en ses arguments
  - Théorèmes :
    - $\phi(\mathbf{0}) = 0$ et $\phi(\mathbf{1}) = 1$
    - $\prod_{i=1}^{n} x_i \leq \phi(\boldsymbol{x}) \leq \coprod_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{x_i}$
    - $\phi(\boldsymbol{x} \sqcup \boldsymbol{y}) \geq \phi(\boldsymbol{x}) \sqcup \phi(\boldsymbol{y})$
    - $\phi(\boldsymbol{x} \cdot \boldsymbol{y}) \leq \phi(\boldsymbol{x}) \cdot \phi(\boldsymbol{y})$

Calcul de fiabilité

- L'état du composant *i* à l'instant *t* est une variable aléatoire notée $X_i(t)$
- On définit alors :
  - La fiabilité du composant *i* :
    $r_i(t) = P(X_i(t) = 1) = E(X_i(t))$
  - La fiabilité du système *S*

$$R_S(t) = P\big(\phi\big(\boldsymbol{X}(t)\big) = 1\big) = E\left(\phi\big(\boldsymbol{X}(t)\big)\right)$$
$$= h(\boldsymbol{r}(t))$$

si indépendance des composants

Système série irréparable

- Calcul de la fiabilité pour un système à *n* composants indépendants

$$R_S(t) = E\left(\phi\big(\boldsymbol{X}(t)\big)\right) = E\left(\prod_{i=1}^{n} X_i(t)\right) = \prod_{i=1}^{n} E(X_i(t))$$

$$= \prod_{i=1}^{n} r_i(t) = e^{-\int_0^t \boxed{\sum_{i=1}^{n} z_i(u)} du}$$

Fonction de taux de défaillance du système

- On peut remarquer que :

$$R_S(t) \leq \min_i (r_i(t))$$

- Application :

  Quelle est la fiabilité d'un système série à *n* composants à taux de défaillance constants ? Quel est son MTTF ?

Exercices

- On rappelle la fonction de fiabilité pour une loi de Weibull à 2 paramètres (α, λ) :

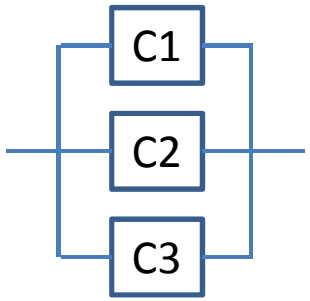
$$R(t) = e^{-(\lambda.t)^{\alpha}}$$

Montrer que la loi de durée de vie d'un système série de *n* composants indépendants distribués suivant une loi de Weibull est aussi une loi de Weibull. En déduire son MTTF.

- On considère un système présentant 3 modes de défaillance indépendants, chacun des modes entrainant la défaillance du système.
  - Le premier mode présentant un taux de défaillance décroissant, est modélisé par une loi de Weibull avec un paramètre de forme $\alpha_1 = 0{,}5$,
  - le second présentant un taux de défaillance constant est modélisé par une loi exponentielle,
  - le troisième présentant un taux de défaillance croissant est modélisé par une loi de Weibull avec un paramètre de forme $\alpha_3 = 3$.

  1. Déterminez la fonction du taux de défaillance du système global.
  2. Tracez cette fonction en fonction du temps pour des valeurs arbitraires des λ_i
  3. Commentez

Système parallèle irréparable



- Calcul de la fiabilité pour un système à *n* composants indépendants

$$R_S(t) = E\left(\phi\big(\boldsymbol{X}(t)\big)\right) = E\left(\prod_{i=1}^{n} X_i(t)\right) = 1 - \prod_{i=1}^{n}\big(1 - E(X_i(t))\big)$$

$$= 1 - \prod_{i=1}^{n}\big(1 - r_i(t)\big) = \prod_{i=1}^{n} r_i(t)$$

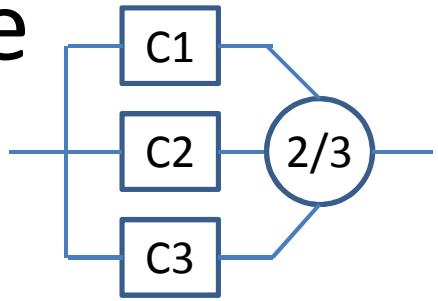
- La fiabilité pour un système parallèle à *n* composants à taux de défaillance constants s'écrit alors :

$$R_S(t) = 1 - \prod_{i=1}^{n}\left(1 - e^{-\lambda_i \cdot t}\right)$$

- Application :

  Quels sont la fonction de fiabilité, le MTTF et le taux de défaillance d'un système parallèle à *n* composants si $\lambda_i = \lambda$?

Structure *2*-sur-*3* non réparable



La fonction de structure 2 sur 3 est donnée par

$$\phi(\boldsymbol{X}(t)) = X_1(t)X_2(t) + X_1(t)X_3(t) + X_2(t)X_3(t) - 2X_1(t)X_2(t)X_3(t)$$

D'où la fonction de fiabilité

$$R_S(t) = R_1(t)R_2(t) + R_1(t)R_3(t) + R_2(t)R_3(t) - 2R_1(t)R_2(t)R_3(t)$$

Si $z_i(t) = \lambda$,

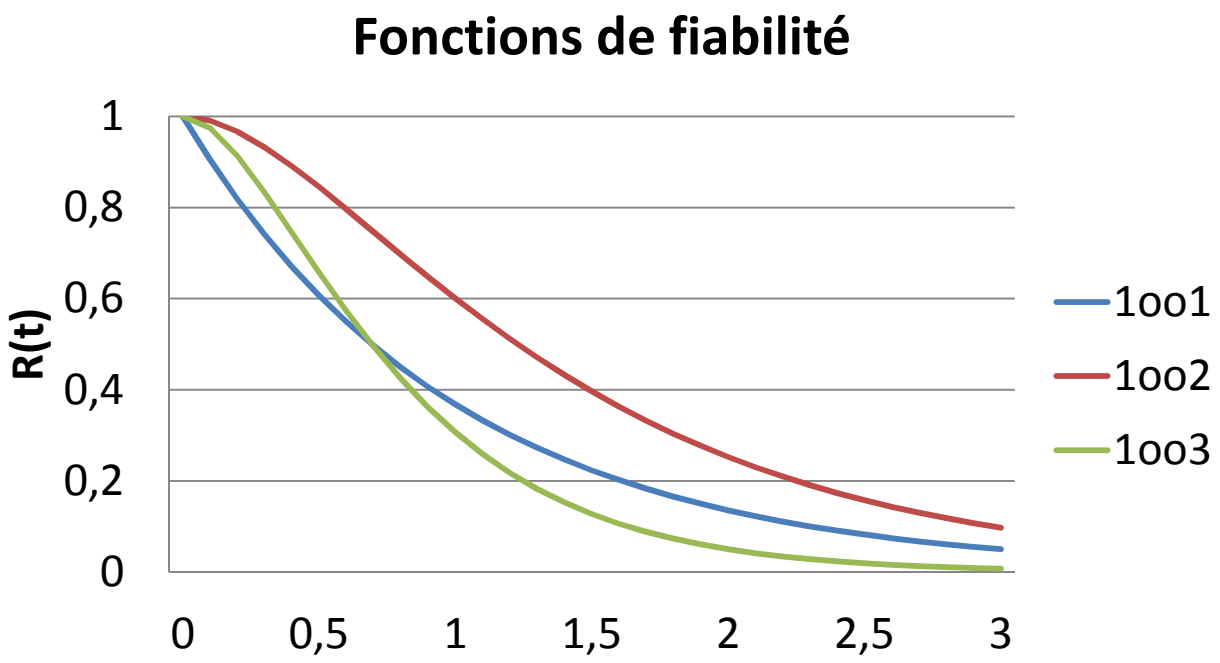
$$R_S(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

$$z_S(t) = \frac{6\lambda\left(e^{-2\lambda t} - e^{-3\lambda t}\right)}{3e^{-2\lambda t} - 2e^{-3\lambda t}} \xrightarrow{t\to\infty} 2\lambda$$

$$MTTF = \int_0^\infty R_S(t)dt = \frac{5}{6}\frac{1}{\lambda}$$

Discussion

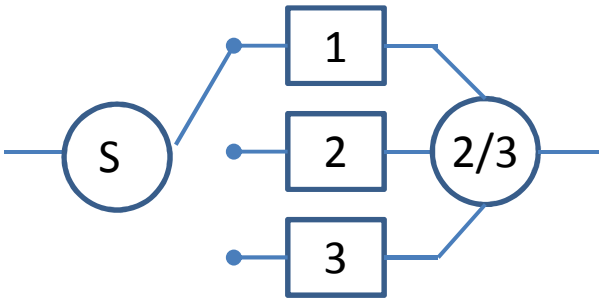
Structure	Fonction de fiabilité	MTTF
1oo1	$e^{-\lambda t}$	$\frac{1}{\lambda}$
1oo2	$2e^{-\lambda t} - e^{-2\lambda t}$	$\frac{3}{2}\frac{1}{\lambda}$
2oo3	$3e^{-2\lambda t} - 2e^{-3\lambda t}$	$\frac{5}{6}\frac{1}{\lambda}$



Les différents types de redondance

- L'amélioration des performances fiabilistes pour une fonction critique est :
  - La recherche de l'amélioration de la performance fiabiliste intrinsèque à la fonction (choix de composants très fiables)
  - L'introduction de **redondances** dites **actives** ou **passives**.
- Si les composants fonctionnent en parallèle (en même temps), on parle de redondance active. Les composants partagent alors la charge de la fonction jusqu'à la défaillance d'un des 2 items.
- Si un composant est mis en attente (standby) de manière à assurer la fonction dès la défaillance du premier composant, on parle de redondance passive.
  - Si le composant en standby n'assure aucune fonction et qu'on peut considérer qu'il n'est soumis à aucune défaillance dans cet intervalle, on parle de **redondance froide (cold standby)**
  - Si le composant en standby assure une charge de fonctionnement réduite, on parle de **redondance partiellement chargée (partly loaded)**.

Analyse de performance des redondances passives



- Redondance passive, changement parfait, pas de réparation
- Redondance passive froide, changement imparfait, pas de réparation
- Redondance passive partiellement chargée, changement imparfait, pas de réparation

Optimisation en fiabilité

- Les objectifs en conception peuvent être liée à une maximisation de la fiabilité sur un horizon de temps donné. Cette maximisation pourra être effectuée tout en cherchant à respecter un budget ou encore à minimiser les dépenses. D'autres critères peuvent être associés (minimisation du poids) et des contraintes ajoutées (volume, design, …).
- Cette optimisation revient à trouver le meilleur compromis entre l'amélioration de la fiabilité et les autres critères. On pourra faire alors appel à des techniques d'optimisation multi-objectif (Recherche Opérationnelle) pour résoudre un tel problème.

$$\max_{n \in \mathbb{N}^k} f^i(n), i \in \{1, \dots, m\}$$

- Problème 1 :
  - On cherche à définir la structure optimale d'un système série devant assurer un ensemble *k* de sous-fonctions. On cherche à maximiser la fiabilité sur un intervalle *t* fixé à budget d'investissement maximal fixé $Cmax$.
  - Hypothèse :
    - Chacune des sous-fonctions peut être assurée par un composant spécifique de coût unitaire donné c_k. On considère que les composants ont un taux de défaillance constant λ_k.
- Ceci revient à chercher le vecteur $\boldsymbol{n}^* = ({n_1}^*, {n_k}^*, \dots, {n_k}^*)$ tel que

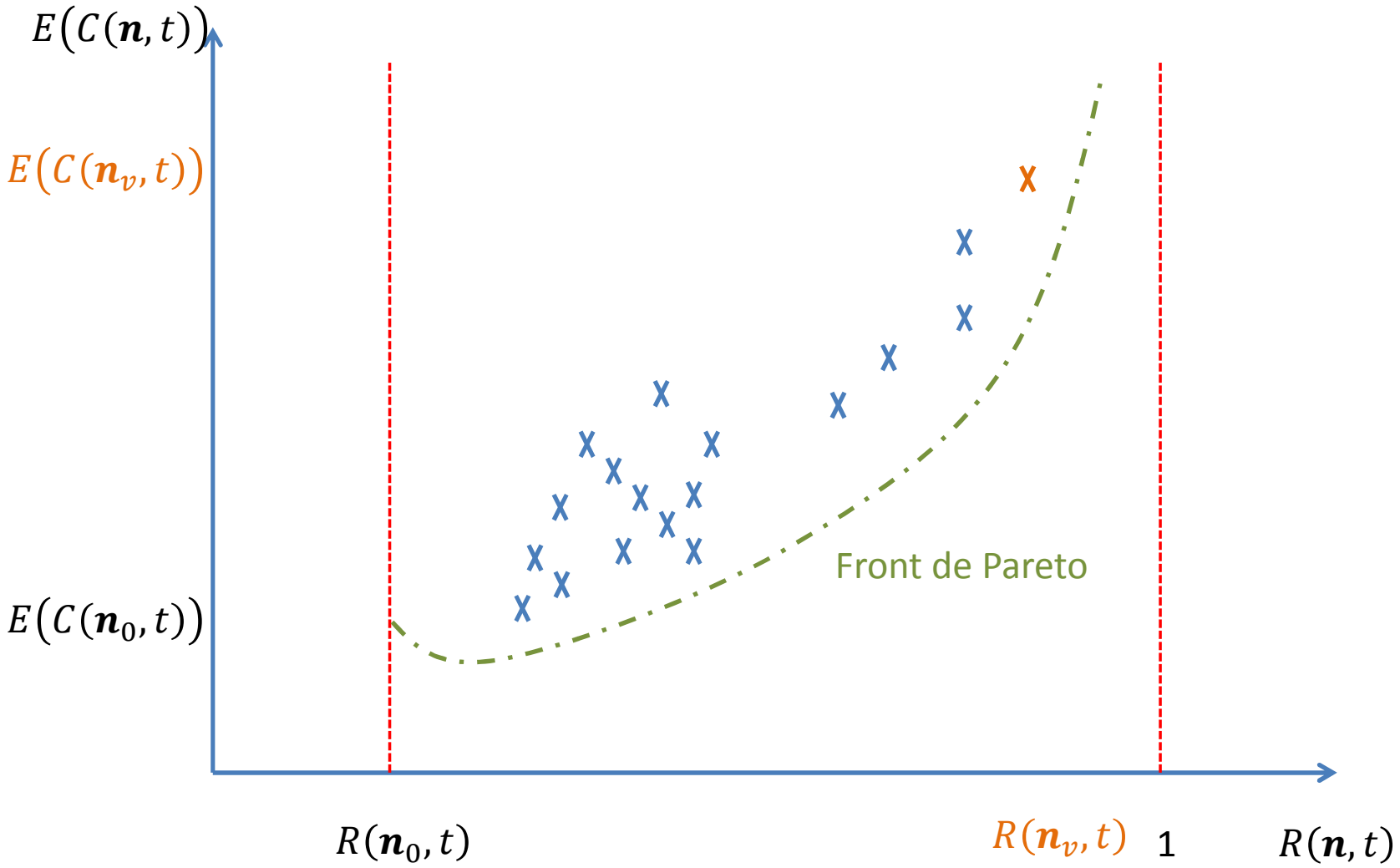
$$R(\boldsymbol{n}^*, t) = \max_{\boldsymbol{n} \in \mathbb{N}^k} \left\{ R(\boldsymbol{n}, t) \middle| \sum_{i=1}^{k} n_i c_i \leq C_{max} \right\}$$

Avec $\mathrm{R}(\boldsymbol{n}, t) = \prod_{i=1}^{k} \left[1 - (1 - e^{-\lambda_i . t})^{n_i}\right]$

- Problème 2 :
  - On cherche à définir la structure optimale d'un système série devant assurer un ensemble *k* de sous-fonctions. On cherche à maximiser la fiabilité sur un intervalle *t* fixé à coût minimal.
  - Hypothèse :
    - Chacune des sous-fonctions peut être assurée par un composant spécifique de coût unitaire donné c_k et de coût de fonctionnement par unité de temps g_k. On considère que les composants en nombre fini ont un taux de défaillance constant λ_k.
- Heuristique pour maximiser la fiabilité et minimiser le coût :
  - Step 0 : Définir les fonctions objectifs de la structure série initiale :

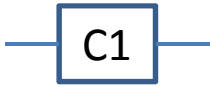
$$\left\{R(\boldsymbol{n}_0,t)=e^{-\sum_{i=1}^{k}\lambda_i\cdot t},E\big(C(\boldsymbol{n}_0,t)\big)=\sum_{i=1}^{k}[c_i+g_i\cdot E(\min(T_S,t))]\right\}$$

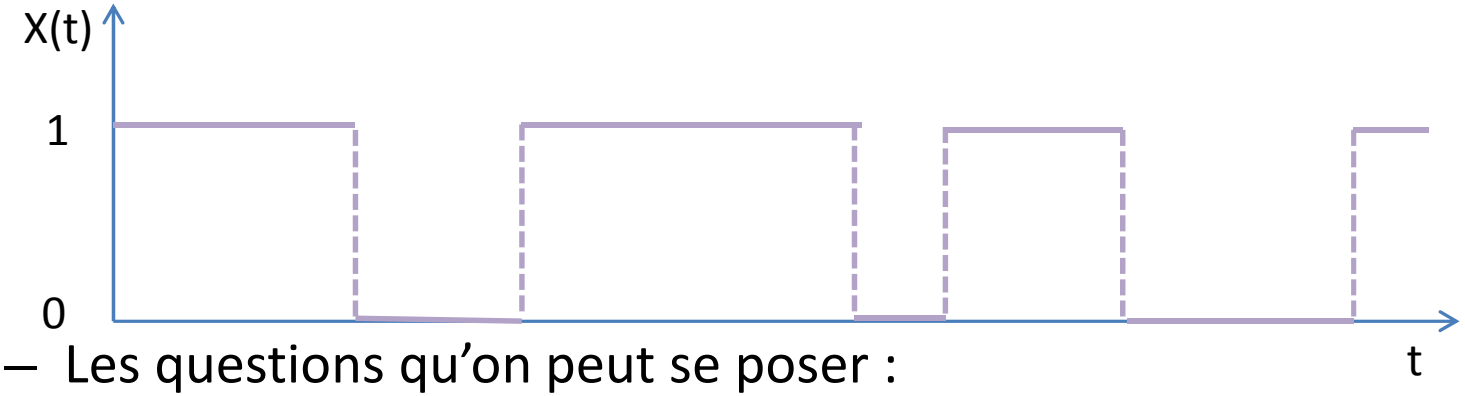
  - Step *v*
    - Ajouter un composant à l'étage *a* le moins fiable ${n_a}^v={n_a}^{v-1}+1$ et ${n_i}^v={n_i}^{v-1}, i\neq a$
    - Évaluer la fonction de fiabilité de l'étage *a,* $R_a\big({n_a}^v,t\big)=1-(1-e^{-\lambda_a\cdot t})^{n_a}$
    - Calculer la fiabilité du système $R(\boldsymbol{n}_v,t)=\prod_{i\neq a}R_i({n_i}^{v-1},t)\cdot R_a({n_a}^v,t)$
    - Évaluer le temps moyen de fonctionnement avant *t :* $E\big(\min({T_S}^v,t)\big)=\int_0^t R(\boldsymbol{n}_v,u)du$
    - Calculer la fonction coût moyen $E\big(C(\boldsymbol{n}_v,t)\big)=\sum_{i=1}^{k}\left[{n_i}^v\big(c_i+g_i\cdot E\big(\min({T_S}^v,t)\big)\big)_i\right]$
    - Dessiner $\{R(\boldsymbol{n}_v,t),E\big(C(\boldsymbol{n}_v,t)\big)\}$


$E(C(\boldsymbol{n},t))$
$E(C(\boldsymbol{n}_v,t))$
$E(C(\boldsymbol{n}_0,t))$
Front de Pareto
$R(\boldsymbol{n}_0,t)$
$R(\boldsymbol{n}_v,t)$
1
$R(\boldsymbol{n},t)$

Analyses des systèmes réparables

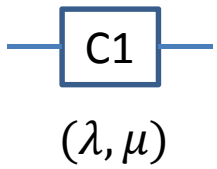
- Un système réparable est un système qui se dégrade et se répare pour revenir dans des états plus favorables.
- Exemple :
  - Pour un système simple





  - Les questions qu'on peut se poser :
    - A une date donnée, quelle est la probabilité que le système fonctionne ?
    - Quelle est la durée moyenne de fonctionnement sur un horizon de temps donné ?
    - Quelle est la proportion de temps où le système n'est pas disponible ?

Cas : un seul élément



- A l'instant t :
  - $p_0(t)$: probabilité de fonctionnement ($p_0(t=0)=1$)
  - $p_1(t)$: probabilité de défaillance ($p_1(t=0)=0$)
- Pour que le système fonctionne à l'instant $t+\delta t$ ($p_0(t+\delta t)$), il faut :
  - Soit qu'il fonctionne à l'instant t et qu'il n'y ait pas de défaillance dans l'intervalle $(t, t+\delta t)$
  - Soit qu'il soit en réparation à l'instant t et qu'il soit remis en état dans l'intervalle $(t, t+\delta t)$
- On a donc

$$p_0(t+\delta t) = p_0(t)\cdot(1-\lambda\cdot\delta t) + \big(1-p_0(t)\big)\cdot\mu\cdot\delta t$$

  - D'où, en divisant par δt et en faisant tendre δt vers 0,

$$p_0'(t) + (\lambda+\mu)p_0(t) = \mu$$

  - Équation différentielle du premier ordre dont la solution est

$$p_0(t) = \frac{1}{\lambda+\mu}\left(\mu+\lambda e^{-(\lambda+\mu)t}\right)$$

- D'où :
  - La disponibilité (instantanée) à l'instant t :

$$A(t) = \frac{1}{\lambda + \mu}\left(\mu + \lambda e^{-(\lambda+\mu)t}\right)$$

  - La disponibilité asymptotique ($t \to \infty$) ou « moyenne » :

$$A_\infty = \frac{\mu}{\lambda + \mu} = \frac{MTTF}{MTTF + MTTR}$$

  - La disponibilité moyenne sur un intervalle (t_1, t_2)

$$A_{av}(t_1, t_2) = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} A(t)dt$$

  - La disponibilité moyenne depuis la mise en service

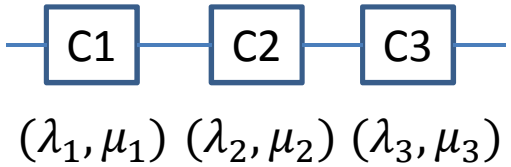
$$A_{av}(\tau) = \frac{1}{\tau}\int_{0}^{\tau} A(t)dt$$

  - La disponibilité moyenne asymptotique

$$A_{av} = \lim_{\tau\to\infty} A_{av}(\tau) = \lim_{\tau\to\infty}\frac{1}{\tau}\int_{0}^{\tau} A(t)dt$$

  - Par ailleurs,
    - L'indisponibilité asymptotique est définie par $\bar{A}_\infty = 1 - A_\infty = \frac{\lambda.MTTR}{1+\lambda.MTTR} \approx \lambda.MTTR$
    - Le nombre moyen de défaillances sur un intervalle : $W(t) \approx \frac{t}{MTTF+MTTR}$
    - L'indisponibilité opérationnelle :
      $\bar{A}_{OP} = 1 - A_{OP} = \frac{Moyenne\ des\ temps\ d'arrêts\ planifiés + Moyenne\ des\ temps\ d'arrêts\ non\ planifiés}{Durée\ de\ la\ mission}$

Cas : Structure série



- La disponibilité instantanée s'écrit

$$A_S(t) = E\big(\phi(\boldsymbol{X}(t))\big) = \prod_{i=1}^{n} A_i(t) = \prod_{i=1}^{n} \left[\frac{1}{\lambda_i + \mu_i}\left(\mu_i + \lambda_i e^{-(\lambda_i+\mu_i)t}\right)\right]$$

- Et donc, on a la disponibilité asymptotique

$$A_S = \prod_{i=1}^{n} \left[\frac{\mu_i}{\lambda_i + \mu_i}\right]$$

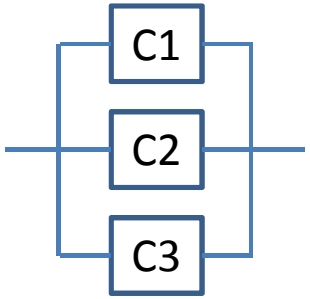
- On peut prouver que :

$$MTTR_S = \sum_{i=1}^{n} \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} MTTR_i = \frac{\sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}}{\sum_{i=1}^{n} \lambda_i}$$

- La fiabilité du système revient à traiter le cas non-réparable
- Les taux de défaillance et de réparation asymptotique sont respectivement:

$$\lambda_s = \sum_{i=1}^{n} \lambda_i \qquad \text{et} \qquad \mu_s = \frac{1}{MTTR_S} = \frac{\sum_{i=1}^{n} \lambda_i}{\sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}}$$

Cas : Structure parallèle



(λ_i, μ_i)

- La disponibilité instantanée s'écrit

Uniquement si indépendance

$$A_S(t) = E\big(\phi(\boldsymbol{X}(t))\big) = 1 - \prod_{i=1}^{n}[1 - A_i(t)]$$

$$= 1 - \prod_{i=1}^{n}\left[\frac{1}{\lambda_i + \mu_i}\left(\lambda_i + \mu_i e^{-(\lambda_i+\mu_i)t}\right)\right]$$

- Et donc, on a la disponibilité asymptotique

$$A_S = 1 - \prod_{i=1}^{n}\left[\frac{\lambda_i}{\lambda_i + \mu_i}\right]$$

Résolution du cas à 2 redondances actives identiques et un réparateur

- On définit le graphe de transition d'états où Ei représente l'événement « i composants fonctionnent »
- On construit la matrice de transition

$$M = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ \mu & -(\lambda+\mu) & \lambda \\ 0 & \mu & -\mu \end{bmatrix}$$

Qui donne l'équa-diff $\frac{dP}{dx}(t) = P(t)M$ que l'on résout par transformée de Laplace.

- La transformée de Laplace est alors solution de l'équation :

$$(\mathcal{L}_1(p), \mathcal{L}_2(p), \mathcal{L}_3(p)) = (1,0,0)(pI - M)^{-1} = (1,0,0)\begin{bmatrix} p+2\lambda & -2\lambda & 0 \\ \mu & p+\lambda+\mu & -\lambda \\ 0 & -\mu & p+\mu \end{bmatrix}^{-1}$$

- La disponibilité est donnée par la somme des états de fonctionnement

$$\mathcal{L}D_S(p) = (1,0,0)\begin{bmatrix} p+2\lambda & -2\lambda & 0 \\ \mu & p+\lambda+\mu & -\lambda \\ 0 & -\mu & p+\mu \end{bmatrix}^{-1}\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \frac{\widetilde{M}_{11} + \widetilde{M}_{21}}{\Delta_M}$$

On ne donnera pas ici la comatrice mais seulement le déterminant de la matrice à inverser :

$$\Delta_M = p(p^2 + p(2\mu + 3\lambda) + \mu^2 + 2\lambda^2 + 2\lambda\mu) = p(p - S_1)(p - S_2)$$

$$\mathcal{L}D_S(p) = \frac{p^2 + p(2\mu + 3\lambda) + \mu^2 + 2\lambda\mu}{p(p - S_1)(p - S_2)} = \frac{A}{p} + \frac{B}{p - S_1} + \frac{C}{p - S_2}$$

Avec $\begin{cases} AS_1S_2 = \mu^2 + 2\lambda\mu \\ A + B + C = 1 \\ -(A+B)S_2 - (A+C)S_1 = 2\mu + 3\lambda \end{cases}$

- On revient ensuite dans l'espace temps en prenant la transformée de Laplace inverse

$$D_S(t) = \mathcal{L}^{-1}(\mathcal{L}D_S(p)) = \mathcal{L}^{-1}\left(\frac{A}{p}\right) + \mathcal{L}^{-1}\left(\frac{B}{p - S_1}\right) + \mathcal{L}^{-1}\left(\frac{C}{p - S_2}\right) = A + Be^{S_1 t} + Ce^{S_2 t}$$

Optimisation de structures

- L'optimisation de structures revient dans ce cadre à définir :
  - Le type de redondance à mettre en place
  - Le nombre de composants en redondance
  - Le nombre de réparateurs
- Le problème est un problème d'optimisation discrète complexe surtout au vu des dépendances liées à la disponibilité des réparateurs.
- Si la structure est complexe, une approche d'optimisation basée sur la simulation d'événements discrets (type MCMC ou RdPS généralisés) peut être employée.
- On peut chercher à analyser la pertinence de l'approximation (temps de réparation faible devant le temps de fonctionnement) et on utilise les formules précédentes

Analyse des Arbres de Défaillance

ADD : Objectifs

- Rechercher les différentes *combinaisons possibles* d'événements conduisant à *l'événement critique* : Scénarios de danger.
- *Représentation graphique* de ces combinaisons par le biais d'une *structure logique d'arbre.*
- L'étude d'un Arbre de Défaillance peut conduire à :
  - Une analyse qualitative
    - Meilleure compréhension du mécanisme de défaillance d'un système complexe
    - Identification des défaillances de cause commune
    - Opportunités de révéler et corriger les points faibles du système – développement de *barrières* ou *systèmes de protection.* ⇨ Défense en profondeur
  - Une analyse quantitative :
    - Evaluation de la *probabilité* de l'occurrence de l'événement sommet
    - Fiabilité, Disponibilité d'un système complexe
    - Métriques de Sûreté et d'analyse de risque

Facteurs d'Importance probabilistes

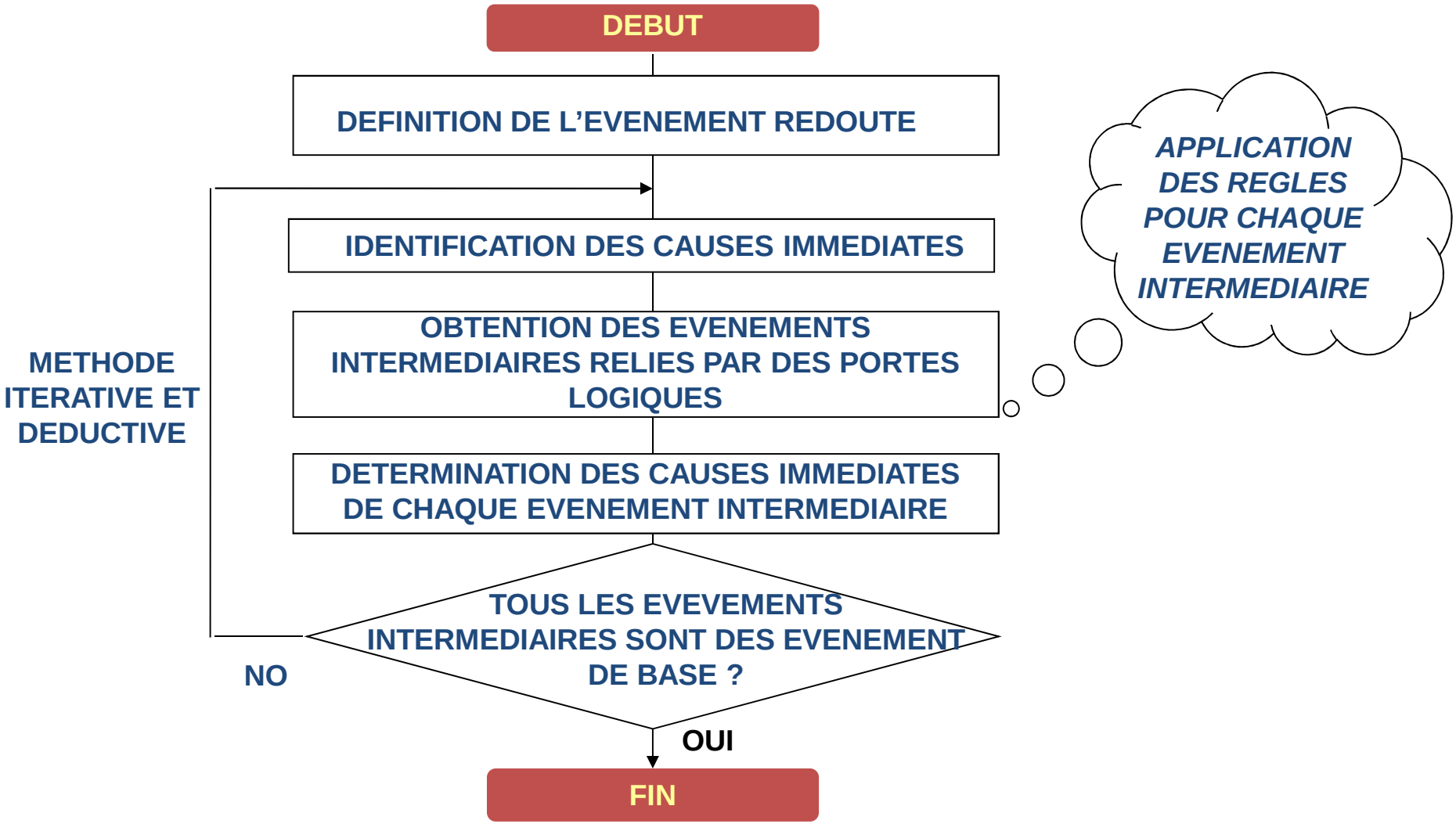
Analyse d'Arbre de Défaillance

- 6 étapes :
  1. Définition du problème et des conditions limites
  2. Construction de l'Arbre de Défaillance
  3. Identification des coupes minimales (ou des chemins de succès)
  4. Analyse qualitative de l'Arbre
  5. Analyse quantitative de l'Arbre
  6. Définition des éventuels plans d'action ou d'amélioration

1. Problème et conditions aux limites

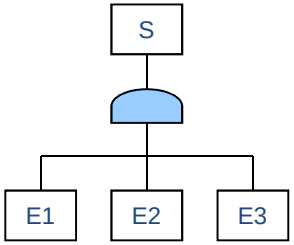
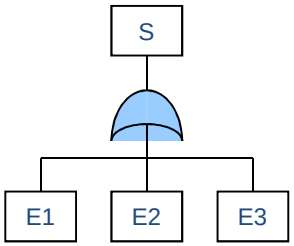
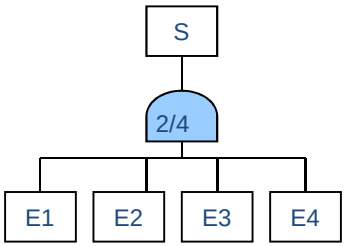
- Définition de l'événement critique (l'accident) = l'événement sommet:
  - QUOI : décrit quel type d'événement critique apparait (le feu)
  - OU: décrit le lieu où l'événement redouté peut se produire (dans le réacteur d'oxydation)
  - QUAND : décrit les conditions opératoires durant lesquelles l'événement redouté est étudié (en conditions normales d'utilisation)
- Définition des conditions aux limites :
  - **Les limites physiques du système**. Quels ensembles du système font partie de l'analyse et lesquels n'en font pas partie ?
  - **Les conditions initiales**
    - Quel est l'état de fonctionnement du système pour l'analyse de l'occurrence de l'événement sommet ?
    - Le système fonctionne-t-il à capacité réduite ou à pleine capacité ?
    - Quelles sont les vannes ouvertes et fermées ? Quelles pompes sont en fonction ? etc.
  - **Les conditions environnementales**. Quel type d'événements externes (sabotage, coupure de courant, tremblement de terre, etc.) doivent être inclus dans l'analyse ?
  - **Le niveau de résolution**
    - A quel niveau de détail doit être pris pour analyser les causes potentielles des états de défaillance ? (« défaillance de la vanne » ? Ou défaillances de la soupape, la tige ou l'actionneur ? Ou ...)

2. Construction

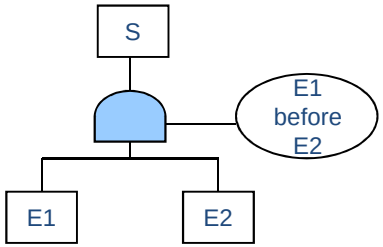
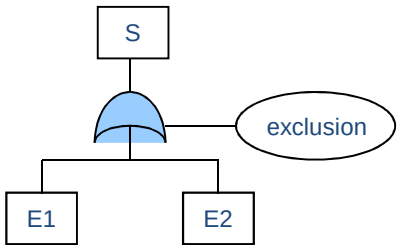
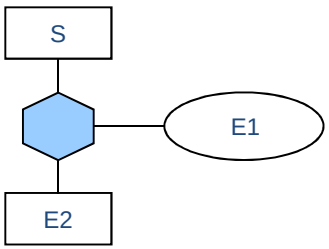


2. Construction

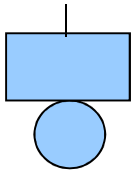
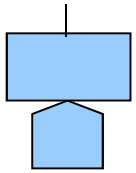
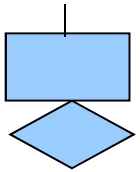
Logic gates

Symbol	Name	Description
	AND-gate	The AND-gate indicates that the output event S occurs only when all the input events Ei occur simultaneously.
	OR-gate	The OR-gate indicates that the ouput event S occurs if any of the input events Ei occur.
	K/N-gate (e.g., 2/4)	The K/N-gate indicates that the output event S occurs only when at least K input events Ei among N occur (e.g., 2 among 4)

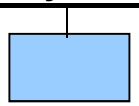
Conditional logic gates

Symbol	Name	Description
	AND-gate with condtion	The AND-gate with condition indicates that the output event S occurs only when all the input events Ei occur with the condition (E1 before E2).
	Exclusive OR-gate	The exclusive OR-gate indicates that the ouput event S occurs if only one of the input events Ei occur (only E1 or E2).
	Inhibit gate	The inhibit gate indicates that the output event S occurs if both the conditional event E1 and the input event E2 occur.

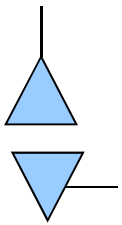
Input events

Symbol	Name	Description
	BASIC event	The Basic event represents a basic equipment fault or failure that requires no further development into more basic faults or failures.
	HOUSE event	The House event represents a condition of an event which is TRUE (ON) or FALSE (OFF) (not true).
	UNDEVELOPED event	The Undeveloped event represents a fault that is not examined further because information is unavailable or because its consequence is insignificant

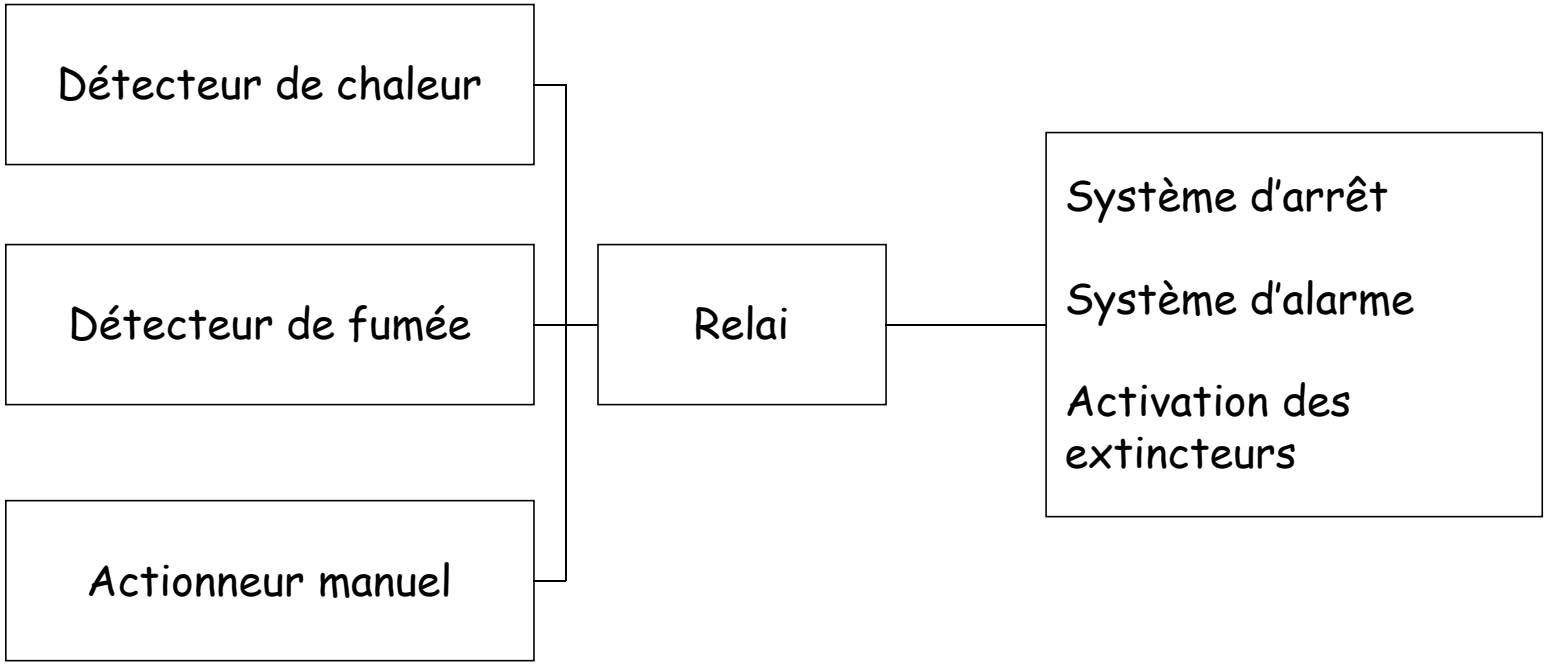
Description of State

Symbol	Name	Description
	COMMENT rectangle	The Comment rectangle is for supplementary information.

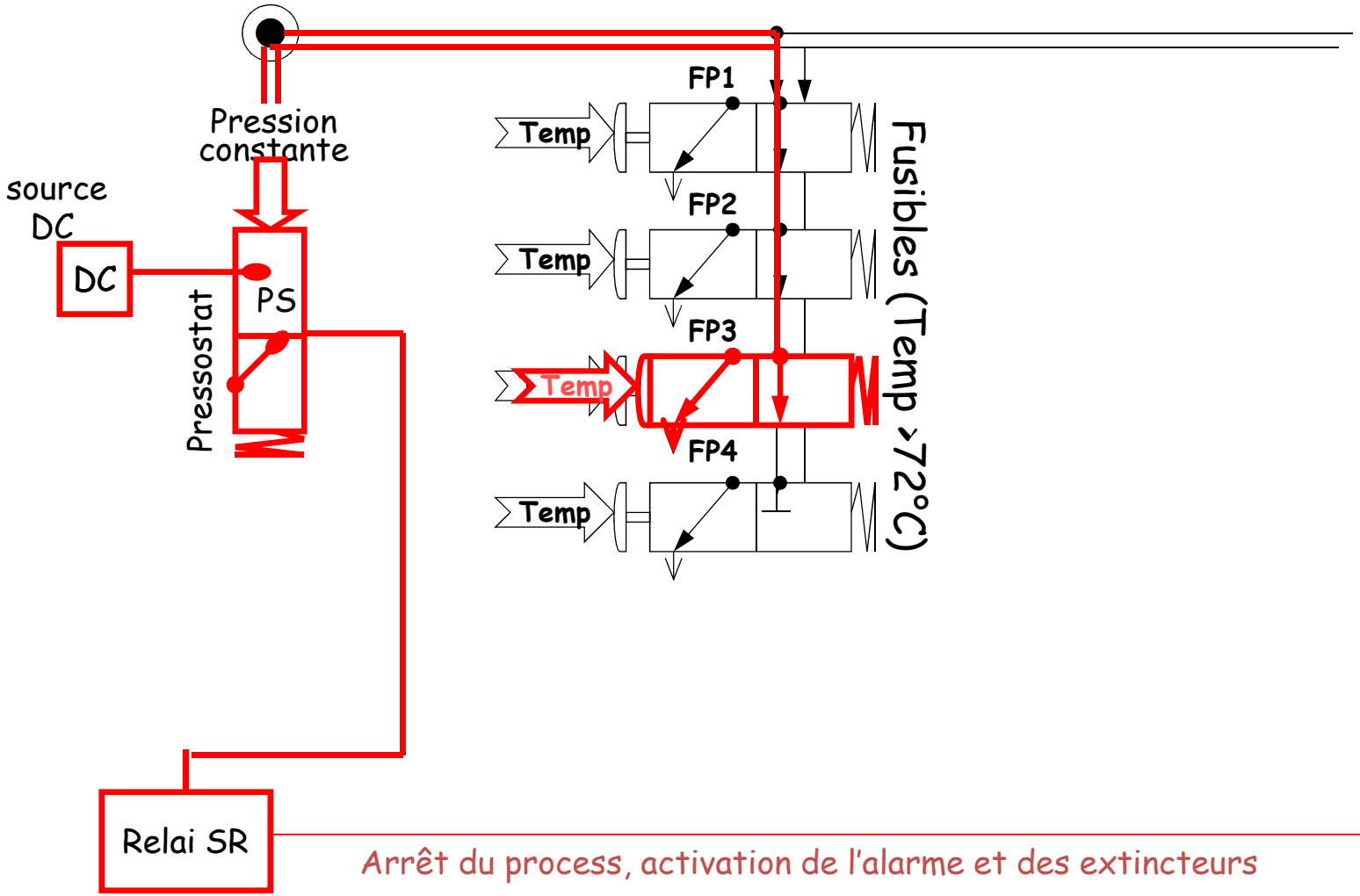
Transfert symbol

Symbol	Name	Description
	TRANSFERT down and TRANSFERT up	The Transfert down symbol indicates that the fault tree is developed further at the occurrence of the corresponding Transfert up symbol

Ex1: Système de détection d'incendie

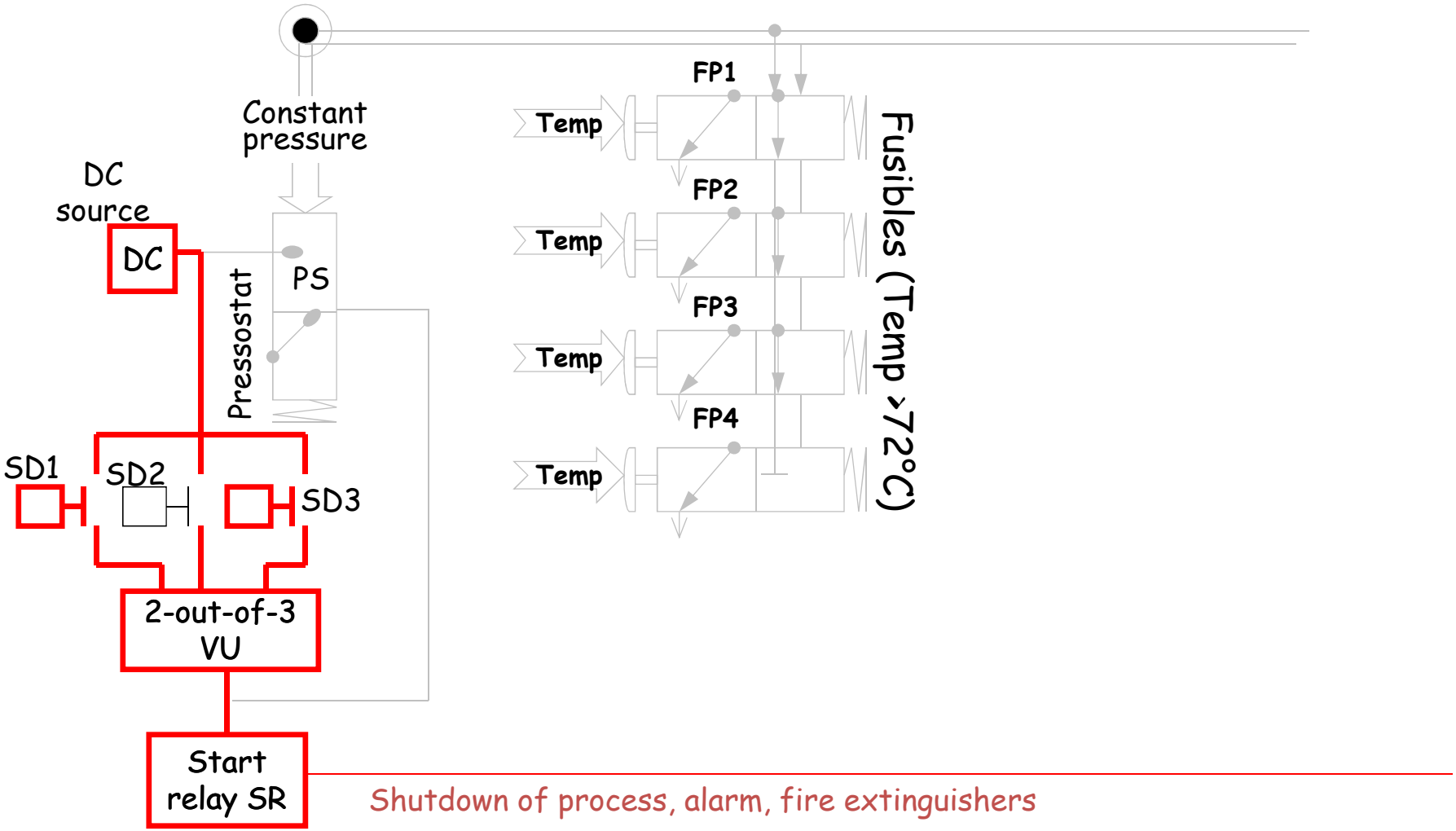


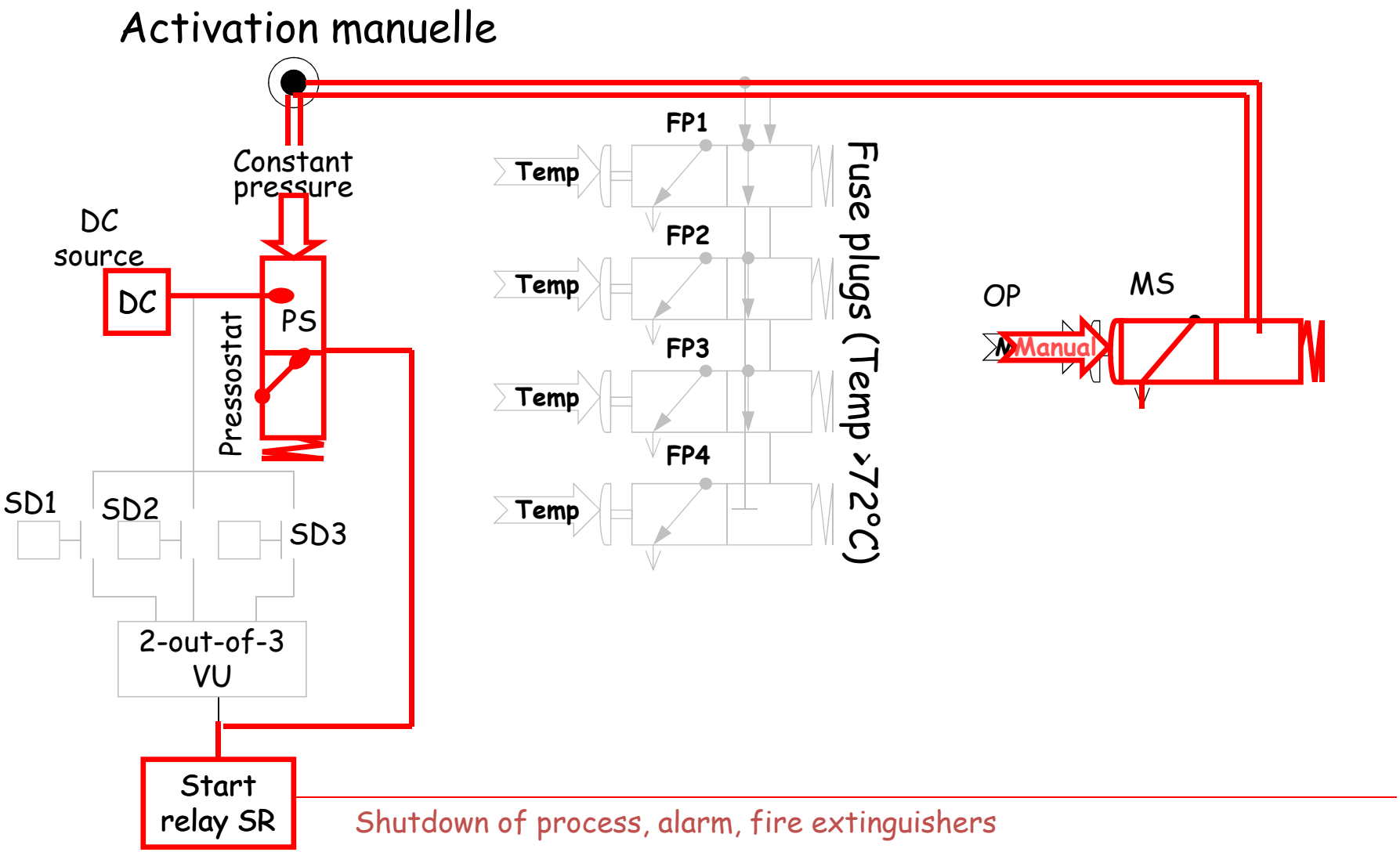
Détection de la chaleur



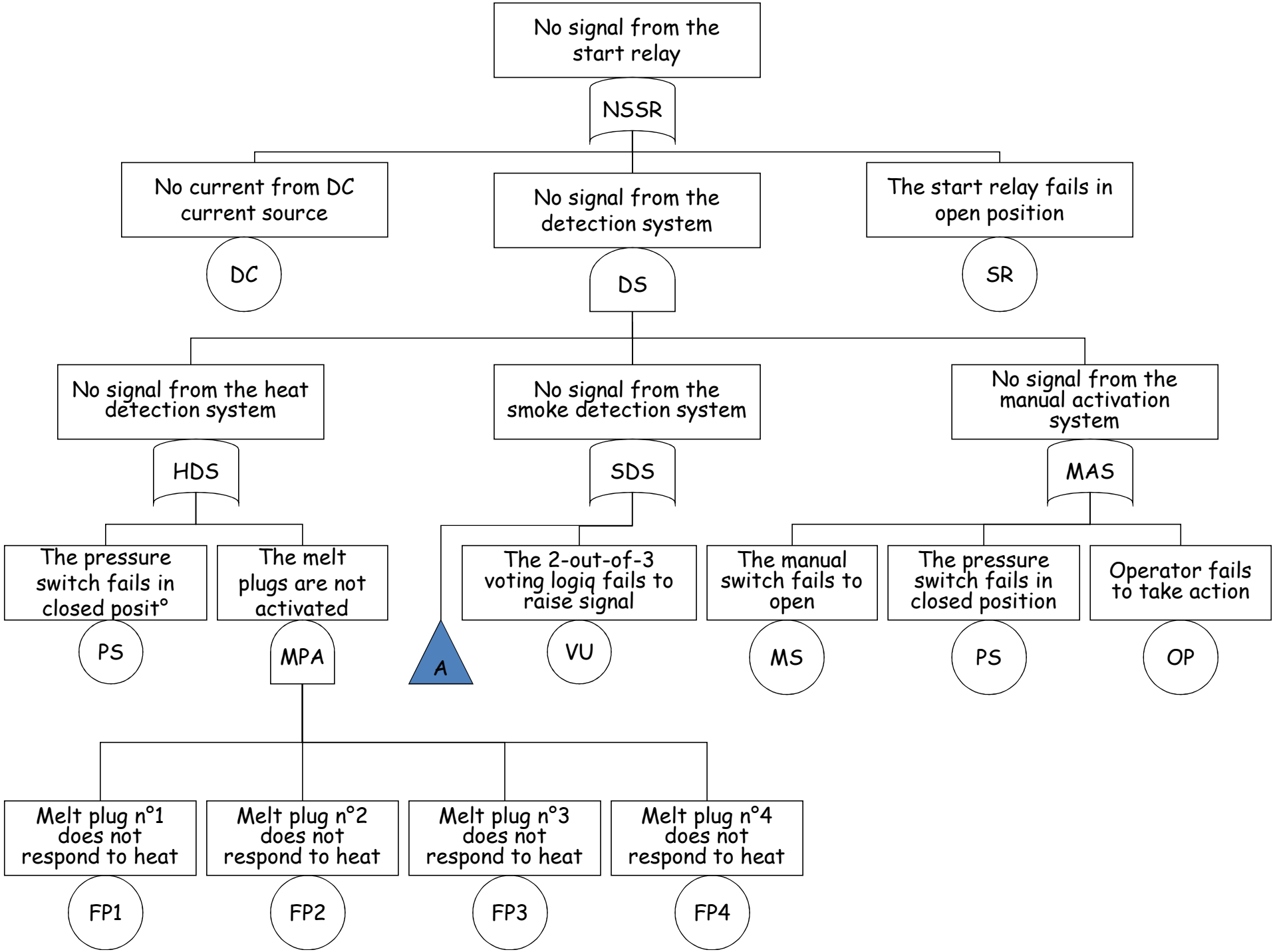
Arrêt du process, activation de l'alarme et des extincteurs

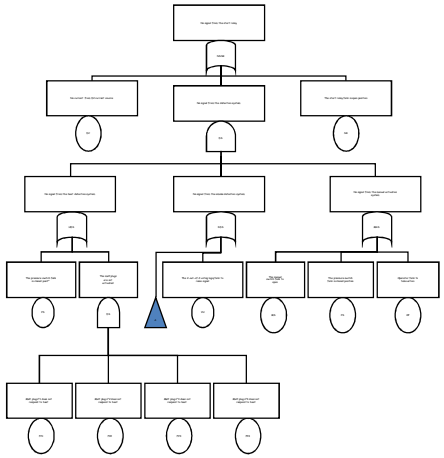
Détection de la fumée

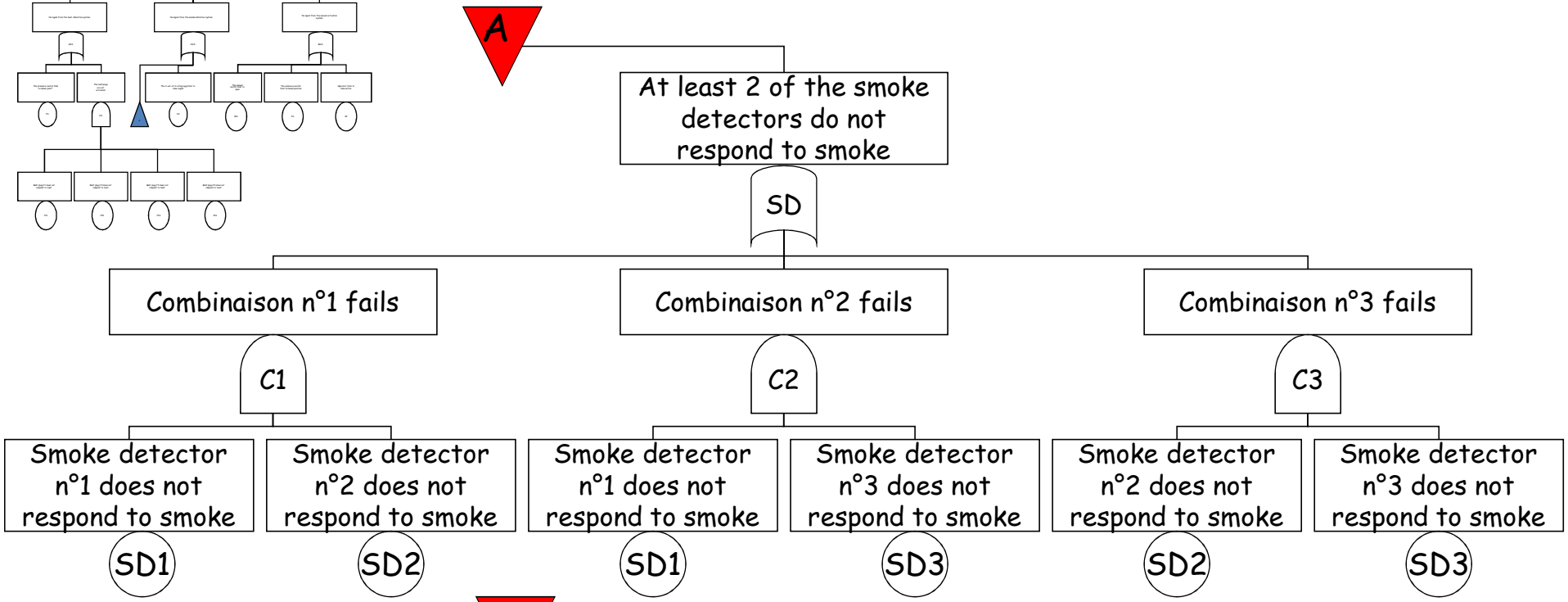


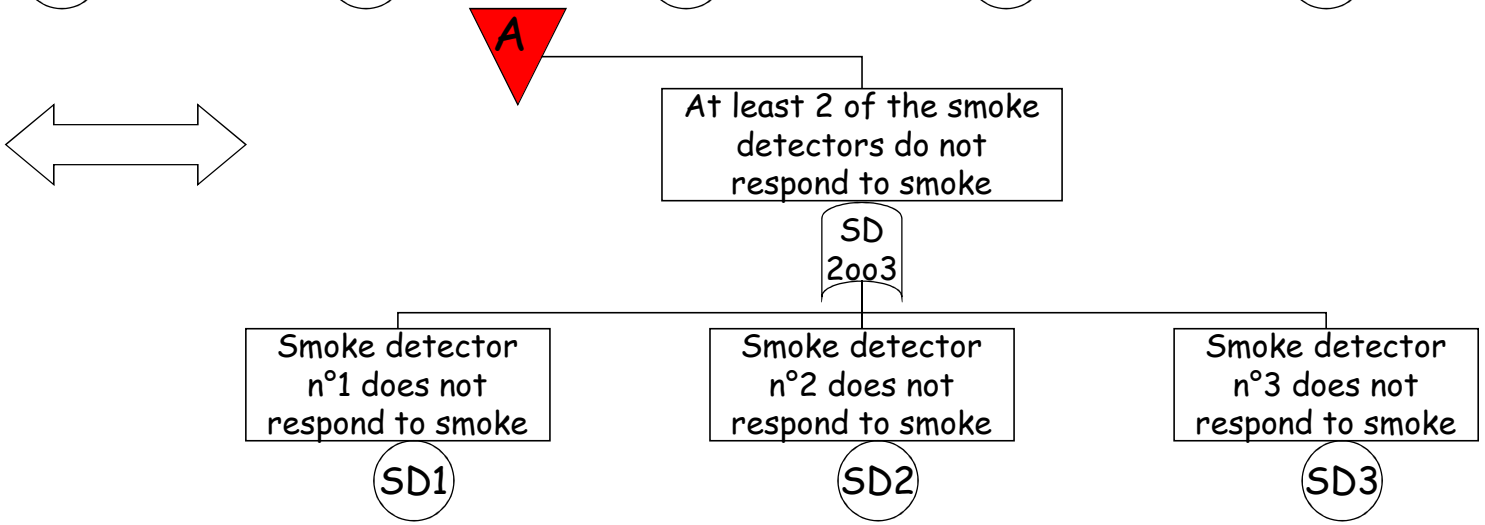


Shutdown of process, alarm, fire extinguishers


No signal from the start relay
NSSR
No current from DC current source
DC
No signal from the detection system
DS
The start relay fails in open position
SR
No signal from the heat detection system
HDS
No signal from the smoke detection system
SDS
No signal from the manual activation system
MAS
The pressure switch fails in closed posit°
PS
The melt plugs are not activated
MPA
A
The 2-out-of-3 voting logiq fails to raise signal
VU
The manual switch fails to open
MS
The pressure switch fails in closed position
PS
Operator fails to take action
OP
Melt plug n°1 does not respond to heat
FP1
Melt plug n°2 does not respond to heat
FP2
Melt plug n°3 does not respond to heat
FP3
Melt plug n°4 does not respond to heat
FP4




A
At least 2 of the smoke detectors do not respond to smoke
SD
Combinaison n°1 fails
Combinaison n°2 fails
Combinaison n°3 fails
C1
C2
C3
Smoke detector n°1 does not respond to smoke
Smoke detector n°2 does not respond to smoke
Smoke detector n°1 does not respond to smoke
Smoke detector n°3 does not respond to smoke
Smoke detector n°2 does not respond to smoke
Smoke detector n°3 does not respond to smoke
SD1
SD2
SD1
SD3
SD2
SD3

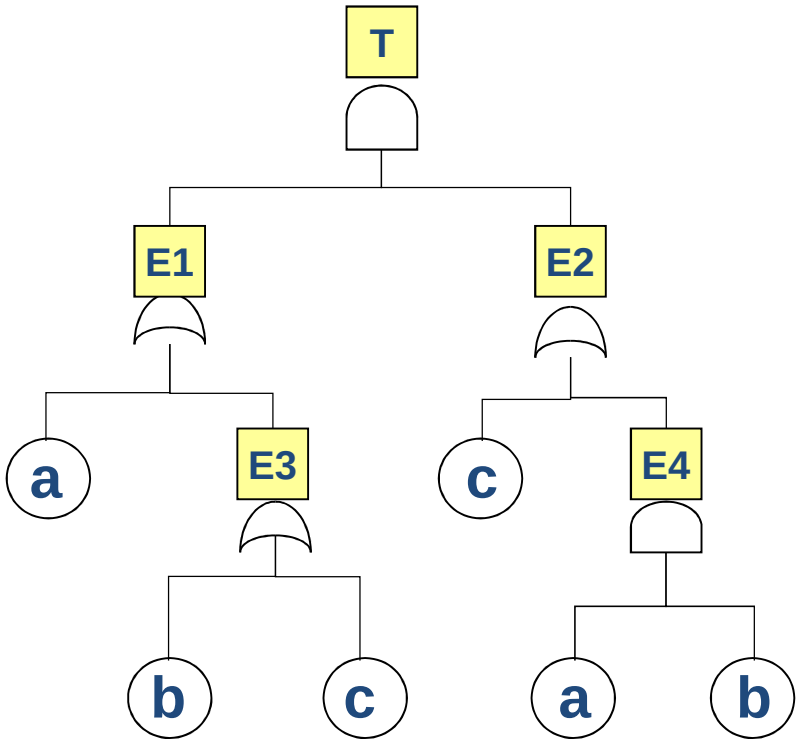

A
At least 2 of the smoke detectors do not respond to smoke
SD 2oo3
Smoke detector n°1 does not respond to smoke
Smoke detector n°2 does not respond to smoke
Smoke detector n°3 does not respond to smoke
SD1
SD2
SD3

Chemin critique / de succès

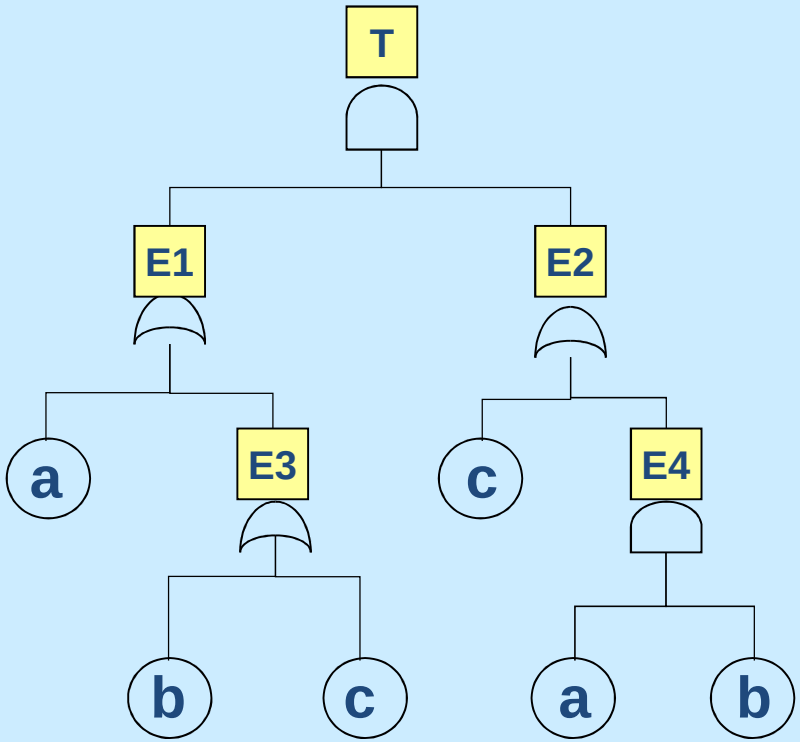
- Chemin critique ou *coupe* :
  - Une *coupe* dans un arbre est un ensemble d'événement de base dont la réalisation simultanée entraine la réalisation de l'événement redouté.
  - Une coupe est dite minimale si l'ensemble ne peut pas être réduit sans perdre son statut de coupe.
  - Le nombre d'événements de base différentes dans une coupe minimale est appelé *l'ordre* de le coupe.
- Chemin de succès :
  - Un *chemin de succès* dans un arbre est un ensemble d'événements de base dont la non-réalisation simultanée entraine la non réalisation de l'événement sommet.
  - Un chemin de succès est dit *minimal* s'il ne peut pas être réduit sans la perte de son statut de chemin de succès.

Méthodologie pour identifier les coupes minimales : **Algèbre de Boole**

Arbre de défaillance



Arbre de défaillance



Expression Booléenne Associée

Evénement intermédiaire

E3 = b + c

E1 = a + (b + c) = a + b + c

E4 = a . b

E2 = c + (a . b)

ABSORPTION

❶ : A ou A = A

❷ : (A et B) ou B = B

Evénement Sommet Redouté

T = E1. E2 = (a + b +c) . (c + (a . b))

T = (a + b + c) . c + (a + b + c) . (a . b)

T = a . c + b . c + c + a . b + a . b + c . a . b

❷ ❶

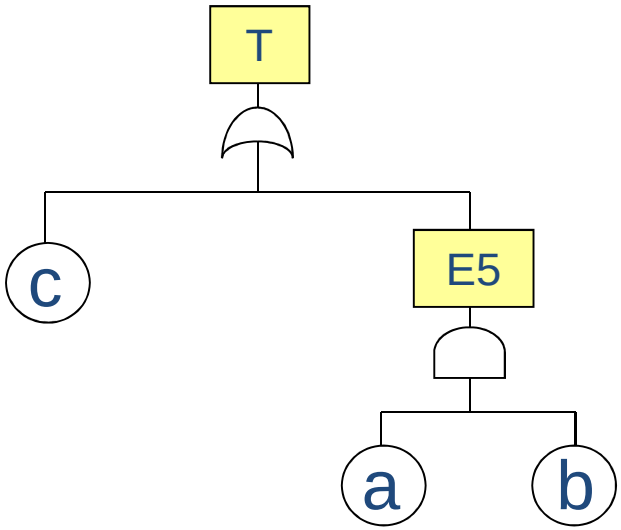
T = a . c + c + a . b + c . a . b

❷ ❷

T = c + a . b

T = c + a . b ⇒ **Arbre réduit**

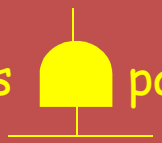
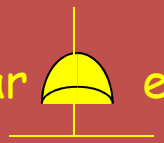
Arbre réduit



Coupe minimale

- L'arbre seulement composé des coupes minimales est appelé **« arbre réduit »**.
- Les coupes minimales sont {c} et {a, b}:
  - {c} (ordre 1)
  - {a, b} (ordre 2)
- a, b et c sont indépendents
- Les coupes minimales représentent les **scénarios de danger critiques.**

Construction de **l'arbre dual**

Remplacer toutes les portes  par  et vice-versa

Identification des chemins de succès minimaux

Analyse par la même approche que les coupes minimales

Analyse qualitative

- Evaluation Qualitative des Risques (QRA) basées sur la criticité des coupes minimales.
- Criticité d'une coupe minimale dépend de :
  - *L'ordre de la coupe*
  - *Le type de la coupe*

Classer les coupes minimales

Rang	Type de l'év. de base
1	Erreur humaines (HE)
2	Défaillance d'un équipement actif (AEF)
3	Défaillance d'un équipement passif (PEF)

Rang	Ev. de base 1	Ev. de base 2
1	HE	HE
2	HE	AEF
3	HE	PEF
4	AEF	AEF
5	AEF	PEF
6	PEF	PEF

Analyse quantitative

Mesure de fiabilité système	Description
$Q_0(t)$	La probabilité que le TOP event se realise à *t*
$R_0(t)$	La probabilité que le TOP event ne se realise pas sur [0,t)
MTTF	Temps moyen avant première défaillance
Freq distr.	Distribution de la fréquence du TOP-event
Freq(TOP)	Fréquence du TOP event
E(#failures)	Nombre espéré de défaillance dans un intervalle de temps
$A_{0,av}(t)$	Disponibilité moyenne du système dans (0,t)

Evaluation quantitative d'un arbre :
Données de fiabilité pour les événements de base

Données d'entrée

Catégorie des données de défaillance	Événement	Paramètre de fiabilité	$q_i(t)$
Fréquence	Événement sans durée	f = fréquence (ou nombre espéré de défaillances par heure)	0
Probabilité sur demande	Composant non activé durant opération normale	q = probabilité que le composant ne soit pas apte à réaliser la fonction sur demande	q
Intervalle de test	Testé périodiquement (remis en fonction si panne détectée)	t^* = période de test, τ = durée moyenne de réparation (en h) λ = taux de défaillance (nombre de déf. par h)	$\frac{\lambda t^*}{2} + \frac{\tau}{t^*}$
Unité réparable	Réparation dès défaillance	τ et λ	$\frac{\lambda\tau}{1+\lambda\tau}\left(1 - e^{-(1+\lambda\tau)t/\tau}\right)$ $\frac{MTTR}{MTTR + MTTF}$
Unité non réparable	Non réparée si défaillance	λ	$1 - e^{-\lambda t}$

Annexe calculatoire

- Pour une unité réparable, on doit déterminer la probabilité que l'unité ne satisfasse pas sa mission à t : $q_i(t)$
- On construit le diagramme de transition à 2 états, la matrice des taux de transition A et on résout le système d'équations de Chapman-Kolmorov :

$$\frac{d}{dt}P(t) = P(t) \cdot A$$

- Où P(t) = [$P_0(t)$, $P_1(t)$] est le vecteur de probabilité d'état avec l'hypothèse qu'à t=0, l'entité fonctionne
- On obtient alors avec λ le taux de défaillance et μ le taux de réparation

$$P_0(t) = \frac{\lambda}{\mu + \lambda}\left(1 - \exp\left(-(\mu + \lambda)t\right)\right) = q_i(t)$$

TOP event calculations

Probability that the TOP event occurs at time t

Properties:

- Uniquely determined by the $q_i(t)$'s
- If all failure data are in the category *on demand probability*, $Q_0(t) = Q_0$
- If at least 1 component in each minimal cut set is in *repairable or non-repairable unit*, $Q_0(t)$ increases in t
- If all failure data are in the category *frequency*, $Q_0(t) = 0$

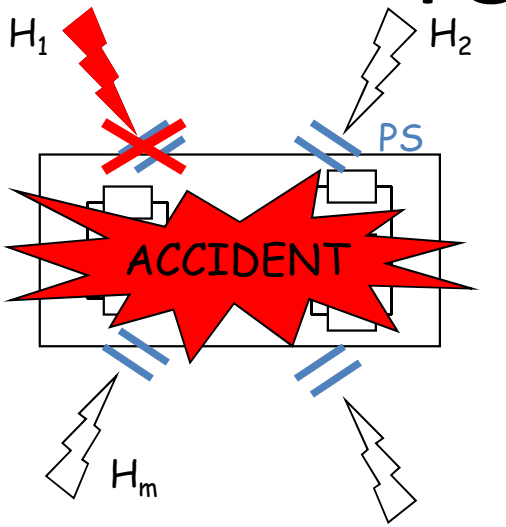
Upper Bound Approximation Method:

No Common Cause Failure

- Determination of all the minimal cut sets K_j
- Evaluation of each $\breve{Q}_j(t) = \prod_{i \in K_j} q_i(t)$ (independence of all input events)
- If ~~all the K_j are disjoint~~, we have $Q_0(t) \cancel{=} 1 - \prod_j (1 - \breve{Q}_j(t))$ → Upper Bound

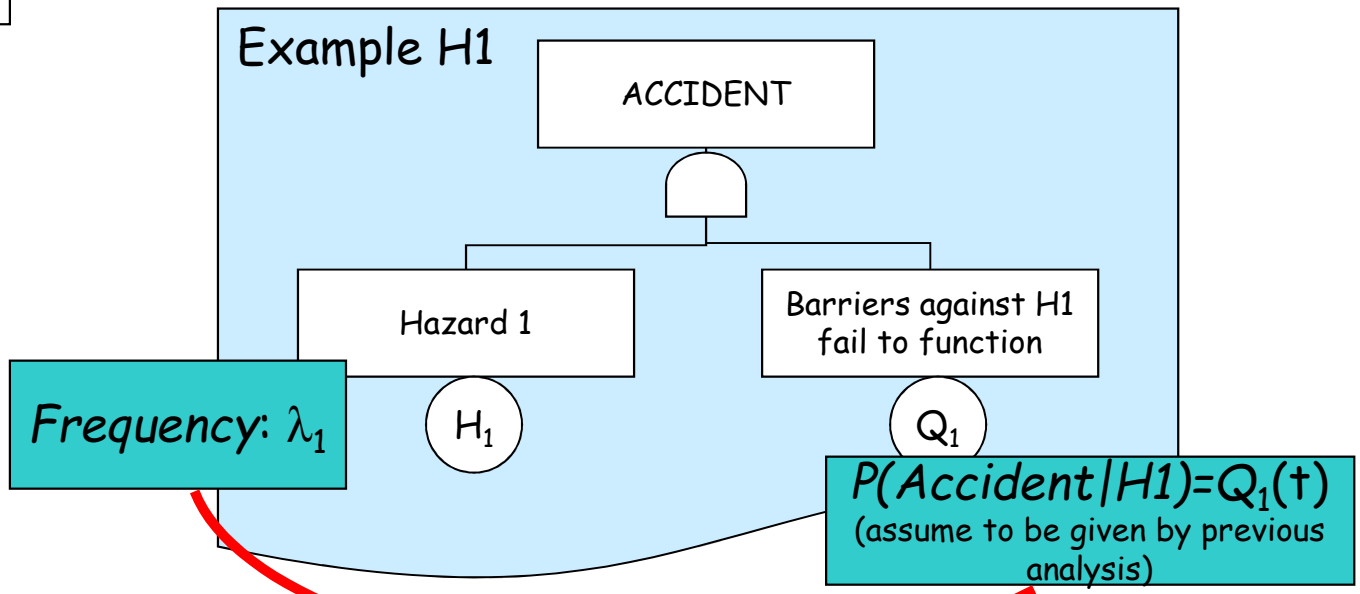
Good approximation if $q_i(t) \approx 0$

TOP Event Frequency



- The system is exposed to a set of Hazards $H_1, H_2, \ldots, H_m$
- The hazards are identified during system design

➔ Barriers and Protective Systems (PS)



Expected Frequency of TOP event

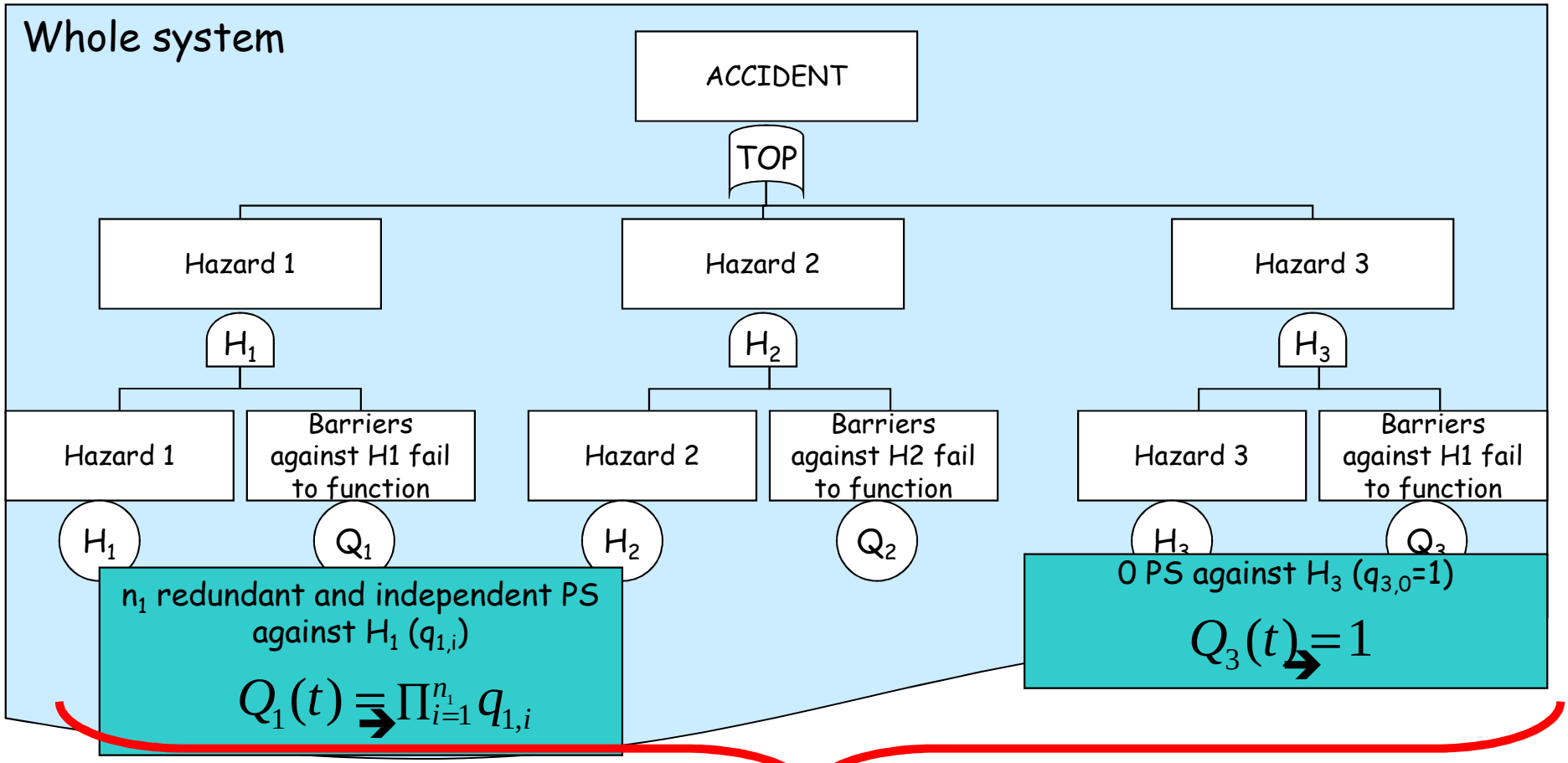
$\lambda_1 Q_1(t)$

Proof

- Let N(t) denote the number of H1 in the time interval (0,t], and NA1(t) denote the number of A1 in the same interval.
- When N(t)=n, NA1(t) will have a binomial distribution, i.e.

$$\Pr\left(NA_1(t) = m \middle| N(t) = n\right) = C_n^m Q_1(t)^m \left(1 - Q1(t)\right)^{n-m}$$

- Hence, the marginal distribution of NA1(t) is a Poisson with intensity (=frequency) λ_1 Q1(t).



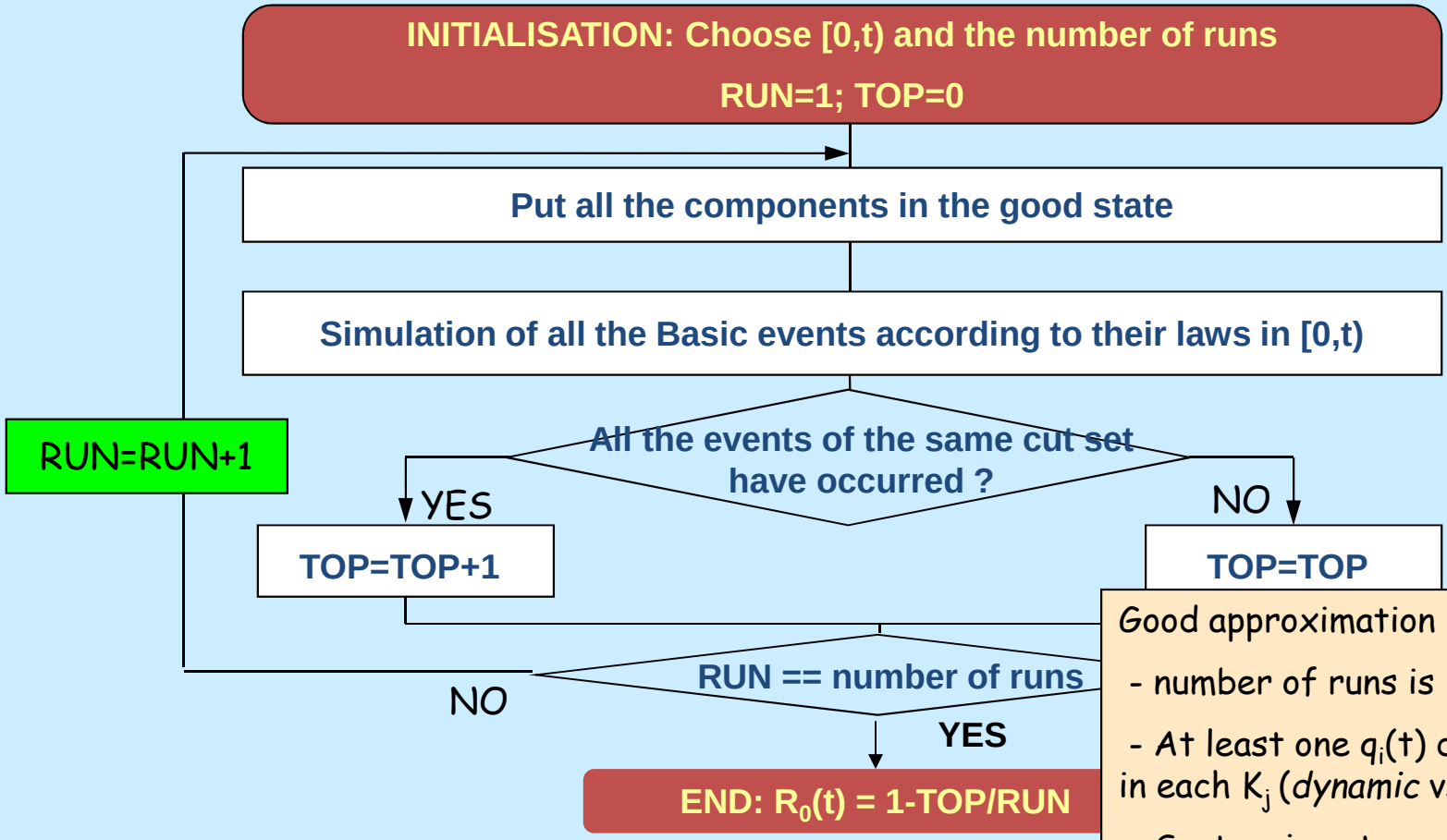
$$\lambda_{TOP} = \sum_{j=1}^{m} \lambda_j Q_j(t)$$

$$Freq(TOP) \approx \sum_{all\ cut\ sets\ K_j} \left\{ \sum_{i \in K_j} \lambda_i \prod_{l \in K_j, l \neq i} q_l(t) \right\}$$

Calculation Using Simulation

The Reliability function $R_0(t)$=P(«TOP event has not occurred in [0,t)») where the system is assumed to be perfect at t=0.

Monte-Carlo Simulation



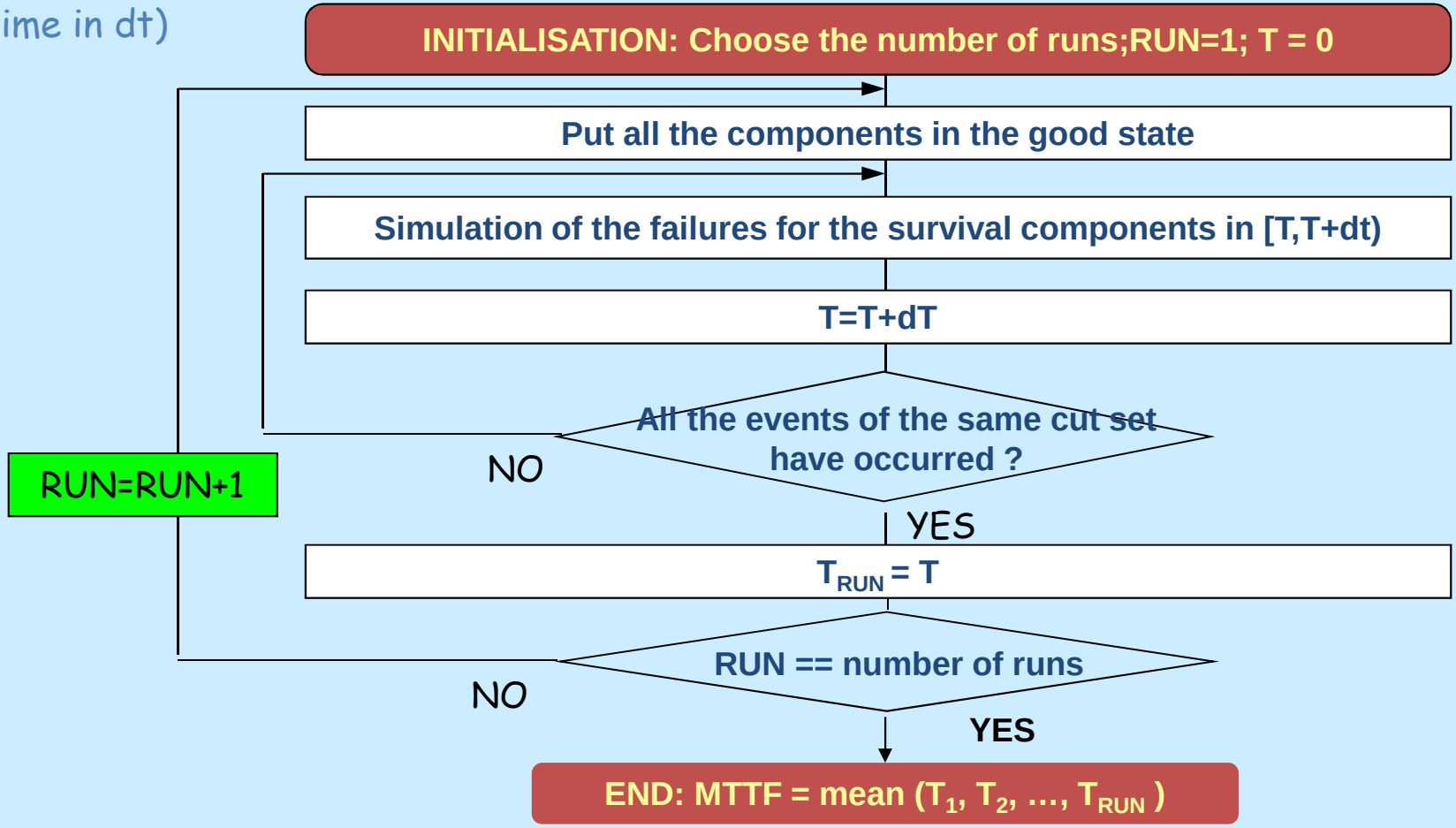
Good approximation if:

- number of runs is large
- At least one $q_i(t)$ depending of t in each K_j (*dynamic* vs *static* tree)
- System is not very reliable

The MTTF is the Mean Time to First Failure, ie. when the time of the failure when the system is assumed to be «as good as new» at t=0.

Monte-Carlo Simulation

(discretization of the time in dt)



Exact calculation

- The Inclusion-Exclusion Principle:

$$P\left(\bigcup_{j=1}^{k} E_j\right) = \sum_{j=1}^{k} P(E_j) - \sum_{i<j} P(E_i \cap E_j) + \ldots + (-1)^{k+1} P\left(\bigcap_{j=1}^{k} E_j\right)$$

  - where Ej = event that the components of Kj are all failed.

- *Structure function* method

- *Pivotal Decomposition, ….*

Measures of Importance

The **reliability importance** of a component generally depends on:

- the *location* of the component in the system,
- the *reliability* of the component.

Many measures which quantify this relation:

- Vesely-Fussell 's Measure of Reliability Importance
- Birnbaum 's Measure of Reliability Importance
- Improvement Potential
- Criticality Importance
- Order of the smallest cut set
- Birnbaum 's Measure of Structural Importance
- Cut set importance

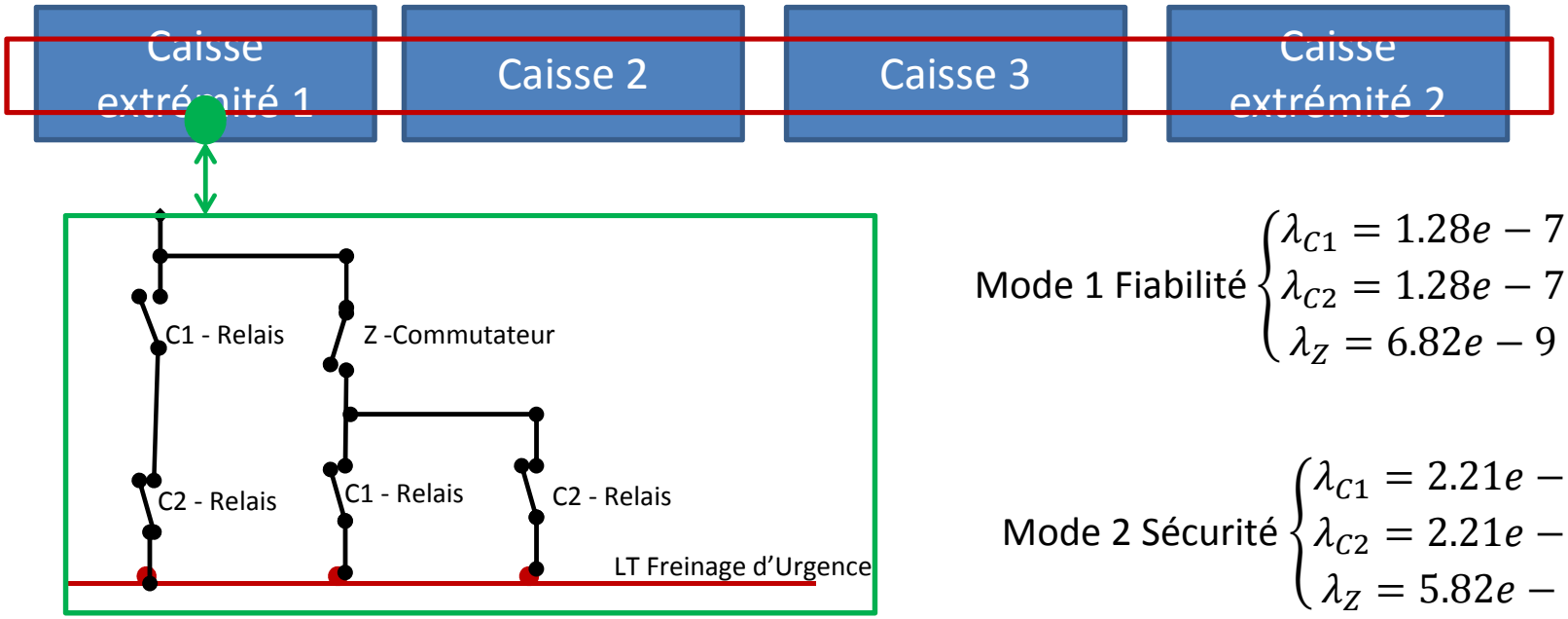
Conclusions

- Advantage
  - Method for quantitative and qualitative analysis
  - Very easy to modelize and to implement
  - Possibility to take into account many types of events
  - Evaluation of the common cause failures
  - Support for the allocation of the objectives (Seveso II)
- Limitations of the method
  - The results obtained with this method can be (completely) inaccurate:
    - for the analyse of a complex systems with interactive elementary components.
    - for the analyse of multiphase systems (the mission of the system can be divided in many consecutive time periods)
    - for the analyse of events that are time-dependent

when the Basic events are non-independent

Application

- Freinage d'urgence de train (FU)
  - Activation si « non alimentation électrique de la ligne FU »



Mode 1 Fiabilité $\begin{cases} \lambda_{C1} = 1.28e-7\ h^{-1} \\ \lambda_{C2} = 1.28e-7\ h^{-1} \\ \lambda_{Z} = 6.82e-9\ h^{-1} \end{cases}$

Mode 2 Sécurité $\begin{cases} \lambda_{C1} = 2.21e-5\ h^{-1} \\ \lambda_{C2} = 2.21e-6\ h^{-1} \\ \lambda_{Z} = 5.82e-7\ h^{-1} \end{cases}$

Analyser le système sous l'angle de la fiabilité et de la sécurité

Éléments de réflexion

- Fiabilité :
  - Définition de l'ERF = « non alimentation de la ligne de train FU »
  - Définition des conditions initiales (relais fermés, commutateur ouvert et courant en entrée)
  - Attention à l'évaluation des quantités fiabilistes dans le cas d'une redondance passive
- Sécurité :
  - Définition de l'ERS = « non coupure de l'alimentation de la ligne de train FU sur demande »
  - Définition des conditions initiales (pas de courant en entrée)
  - Intégration de défaillances de cause commune sur les relais ?
  - Intégration de périodes de tests sur les composants …

Event Tree Analysis

Contents

- Introduction
- ETA in 6 steps
- Case study : Separator Safety System

Introduction

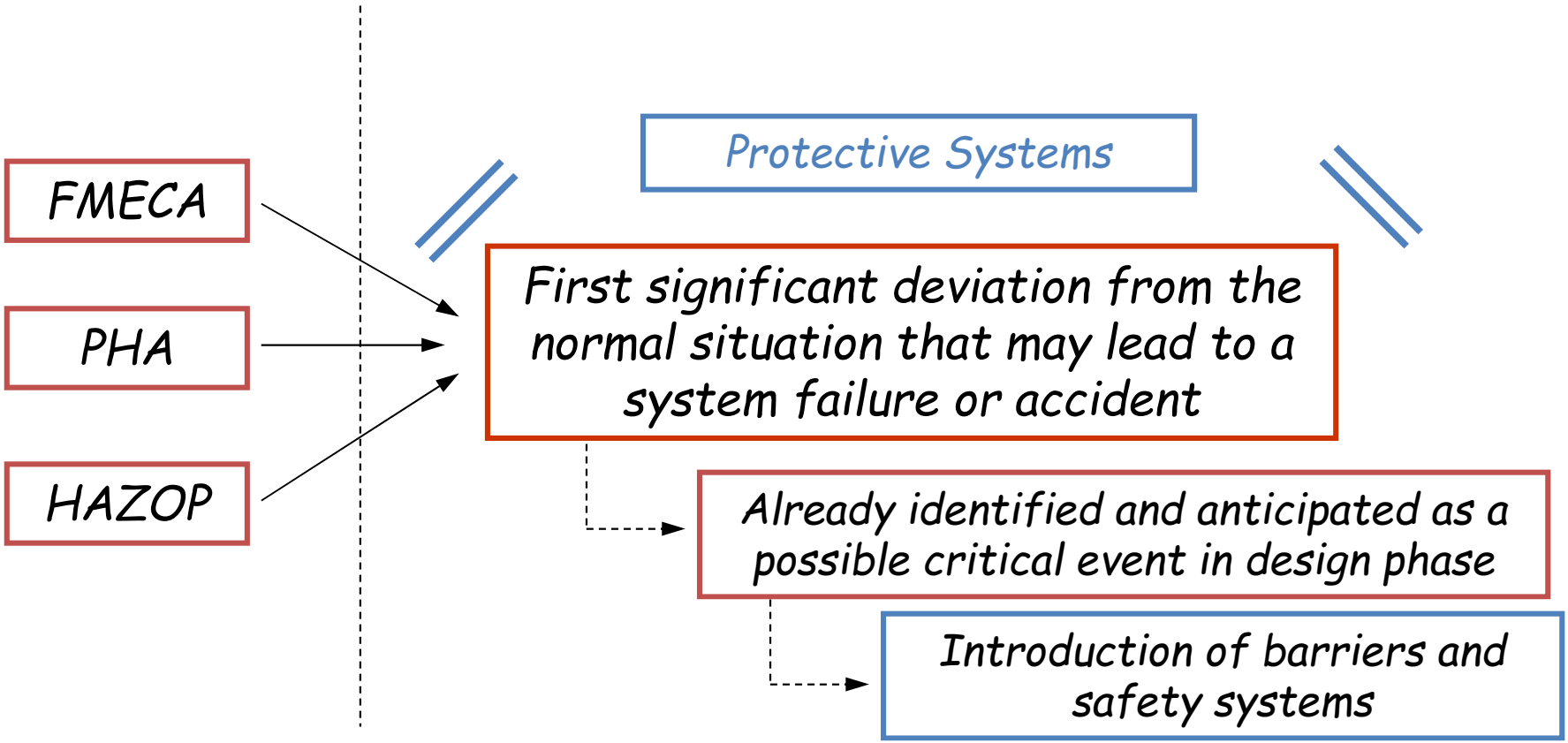
- FTA = Deductive approach
  - Characterization of an critical event by the identification of all its causes
- ETA = Inductive approach
  - Find all outcomes from an initiating event
  - Analyze the accidental progression according to the safety functions

An event tree is a logic tree diagram that starts from a basic initiating event and provides a systematic coverage of the time sequence of event propagation to its potential outcomes or consequences

  - Each event in the tree (success or failure of the safety function) is conditional on the occurrence of the previous event

ETA in 6 steps

1 Identification of a relevant initiating (accidental) event (IE)



ETA in 6 steps

1 Identification of a relevant initiating (accidental) event (IE)

2 Safety Functions

Characterization of the whole system 's defense against the occurrence of the IE

Identification of all the safety functions (barriers, safety systems, procedures, operator actions, …)

Classification (AIChE 1985) :

- Automatic safety systems that respond to the IE (automatic shutdown system)
- Alarms (fire alarm systems)
- Operator procedures following an alarm
- Barriers or containment methods intended to limit the effects of IE

Determination of the sequence of activation of each safety functions

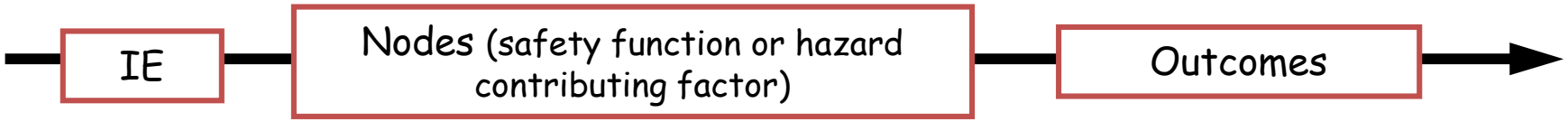
ETA in 6 steps

1 Identification of a relevant initiating (accidental) event (IE)

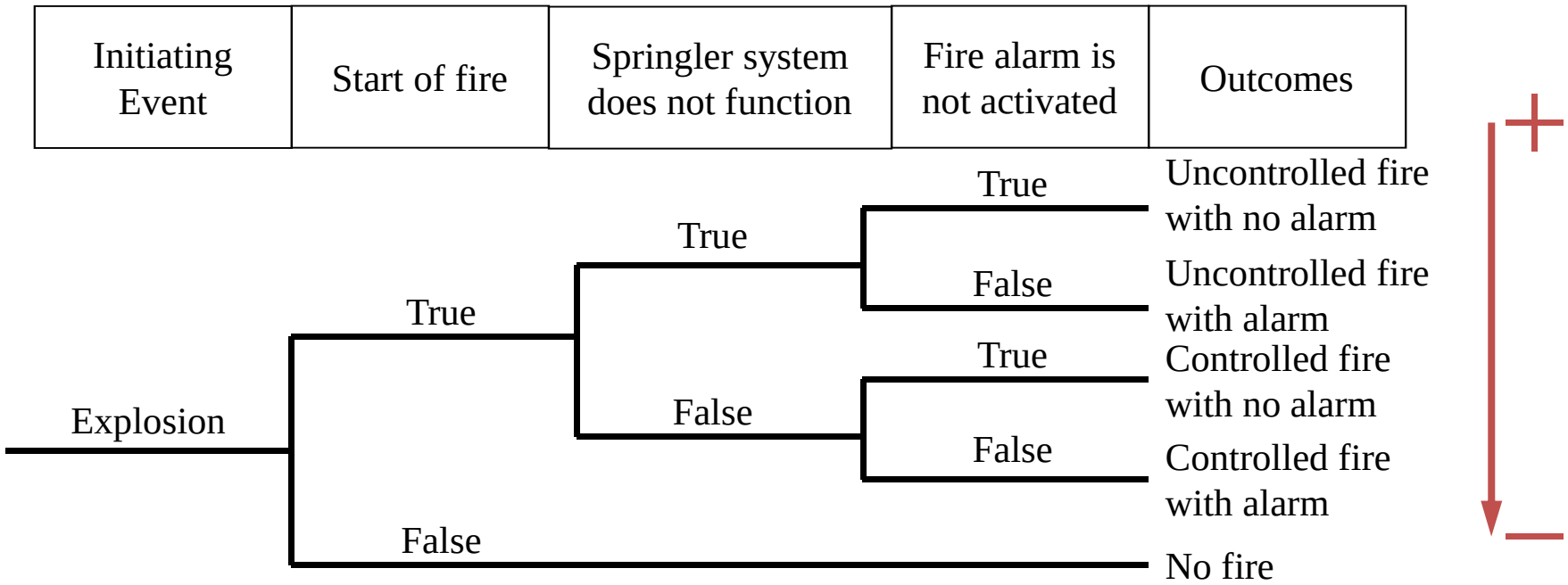
2 Safety Functions

3 Event tree construction

Chronological development of the event chains



Application of the propagation of the accidental situation for a dust explosion



ETA in 6 steps

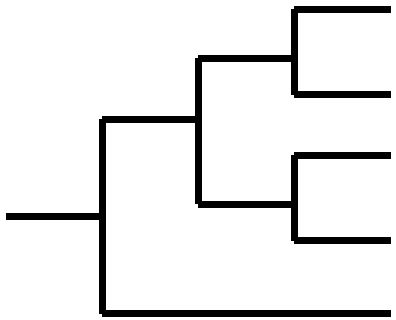
1 Identification of a relevant initiating (accidental) event (IE)

2 Safety Functions

3 Event tree construction

4 Description of the resulting event sequences

Qualitative classification of the scenarios according to their criticality



Outcome Descr.	Frequency	Loss of live					Material damage				Environmental damage			
		0	1-2	3-5	6-20	>20	N	L	M	H	N	L	M	H

ETA in 6 steps

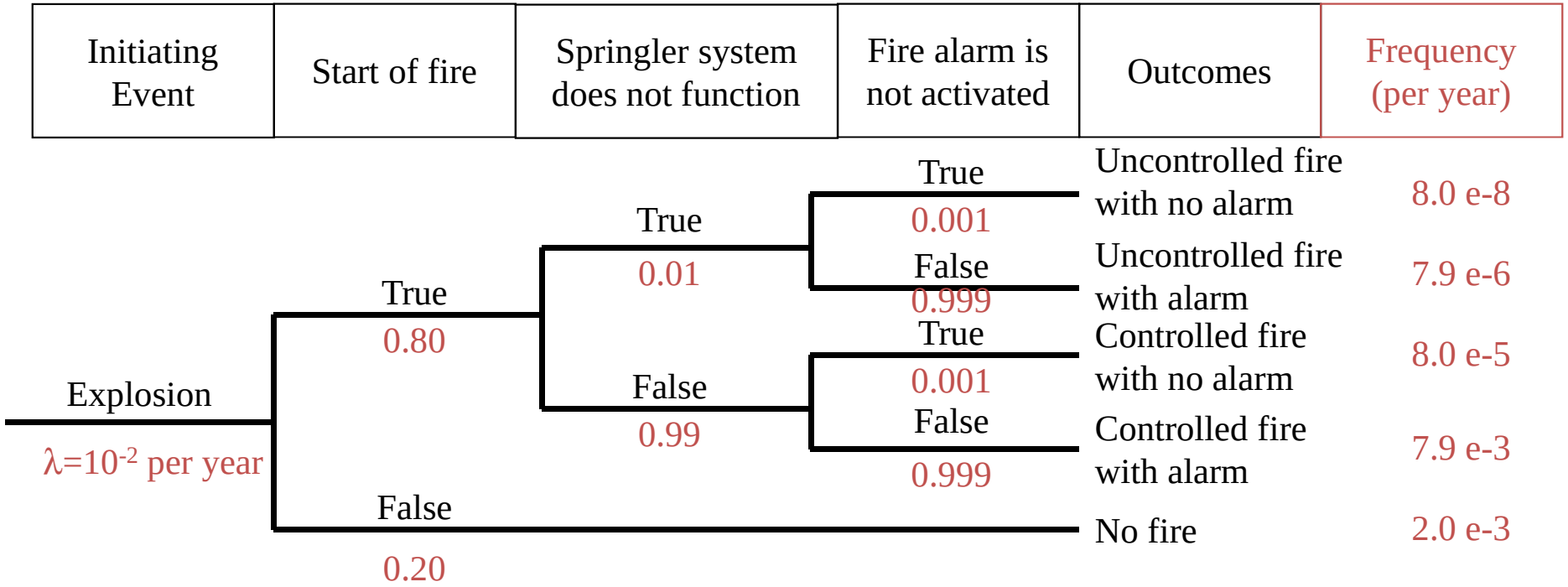
1 Identification of a relevant initiating (accidental) event (IE)

2 Safety Functions

3 Event tree construction

4 Description of the resulting event sequences

5 Quantitative assessment



ETA in 6 steps

1 Identification of a relevant initiating (accidental) event (IE)

2 Safety Functions

3 Event tree construction

4 Description of the resulting event sequences

5 Quantitative assessment

6 Compilation and presentation of the results from the analysis

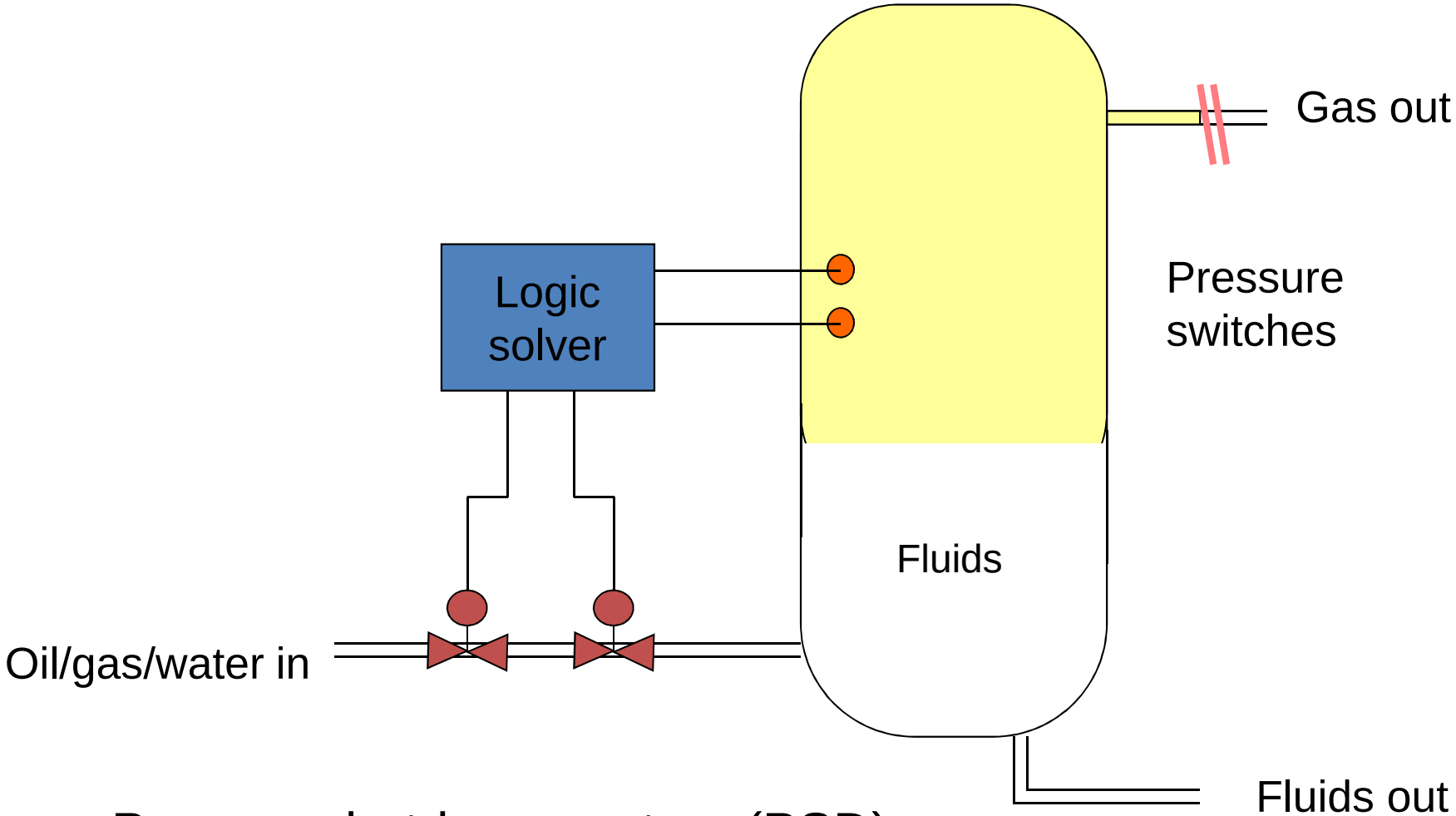
- Discussion of the different assumptions
- Outline the critical weakness of the system
- Proposition of corrective actions (possibility to evaluate the impact of the introduction of a new protective system against the IE)

Pros and Cons

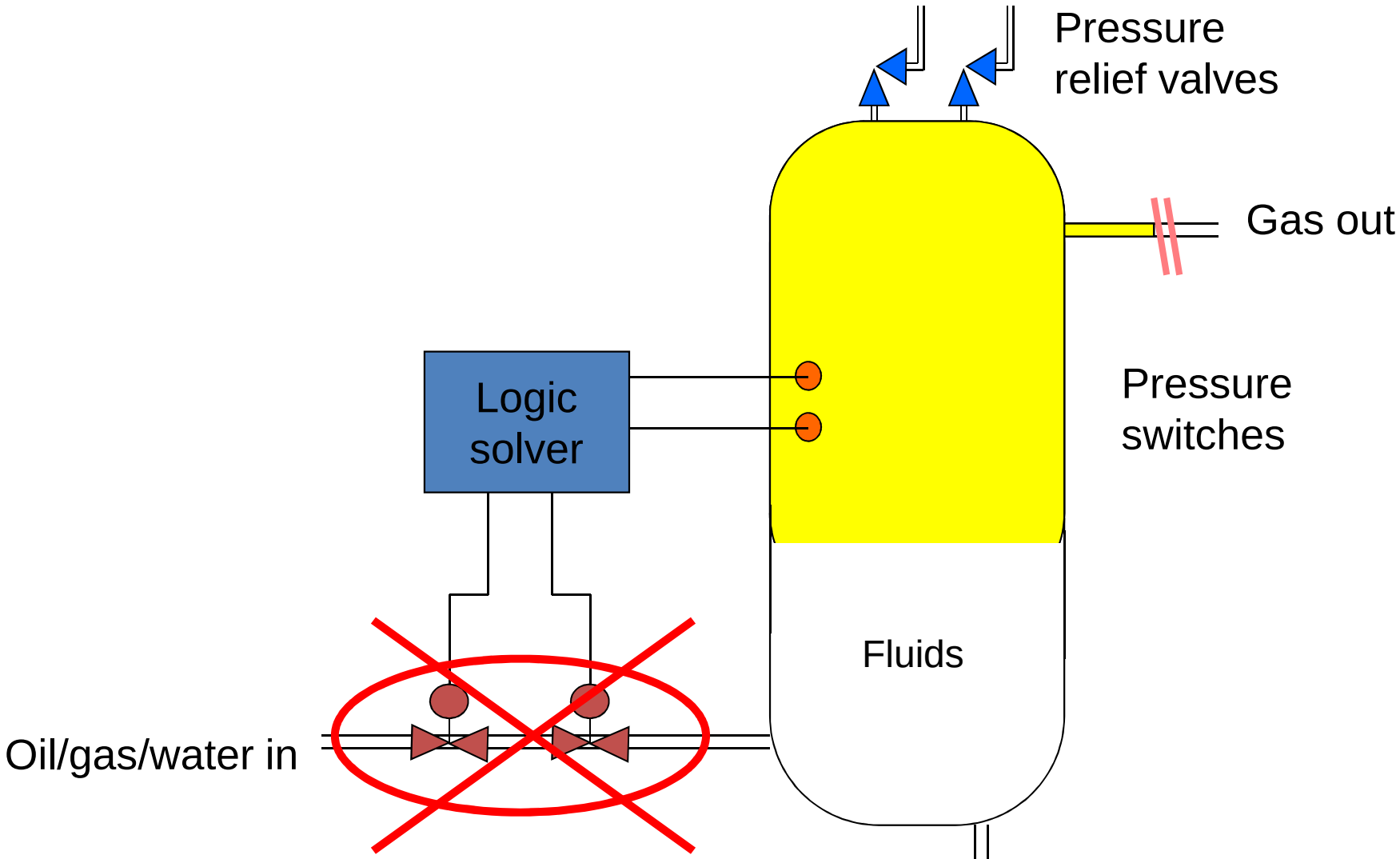
- Positive
  - Visualize event chains following an accidental event
  - Visualize barriers and sequence of activation
  - Good basis for evaluating the need for new / improved procedures and safety functions
- Negative
  - No standard for the graphical representation of the event tree
  - Only one initiating event can be studied in each analysis
  - Easy to overlook subtle system dependencies
  - Not well suited for handling common cause failures in the quantitative analyses
  - The event tree does not show acts of omission

Case Study

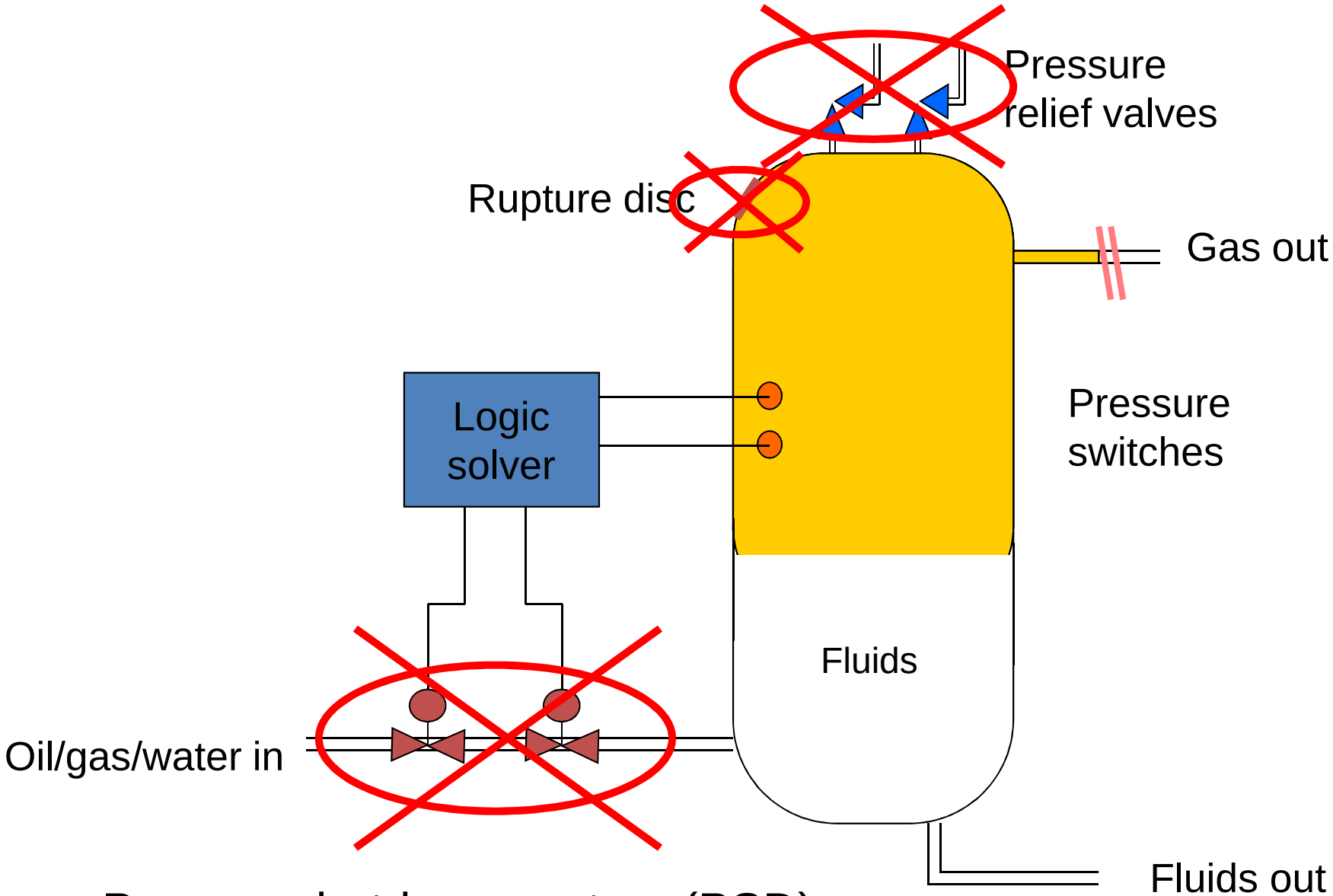
- Analyse the reliability of the first stage separator system with
  - Fault Tree approach
  - Event Tree approach
  - Design the Reliability Block Diagram of the system



Process shutdown system (PSD)



Process shutdown system (PSD)



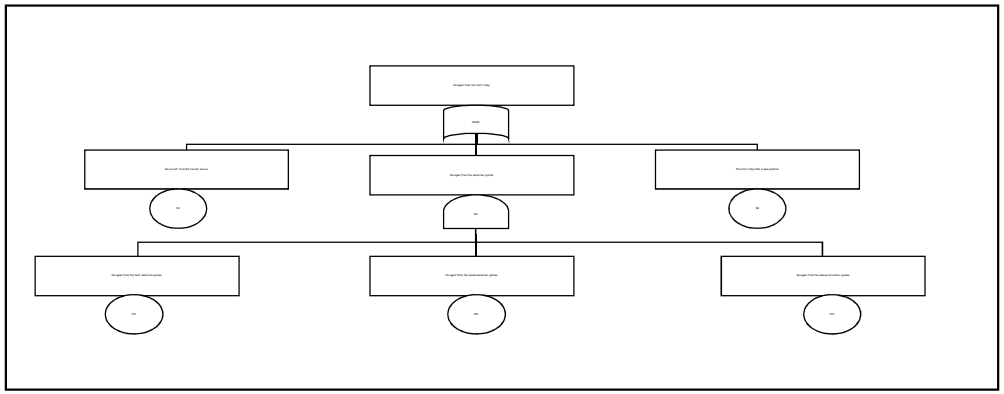
Process shutdown system (PSD)

Piper Alpha accident in 1986 – 167 fatalities

Fault Tree

Relevant top event: « Critical overpressure in the first stage operator »

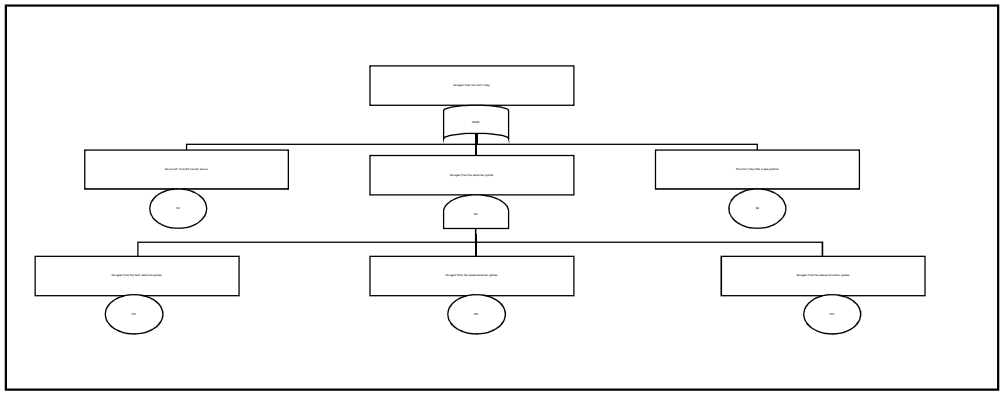
- critical situation occurs during normal production
- the fluid level in the separator is normal



Fault Tree

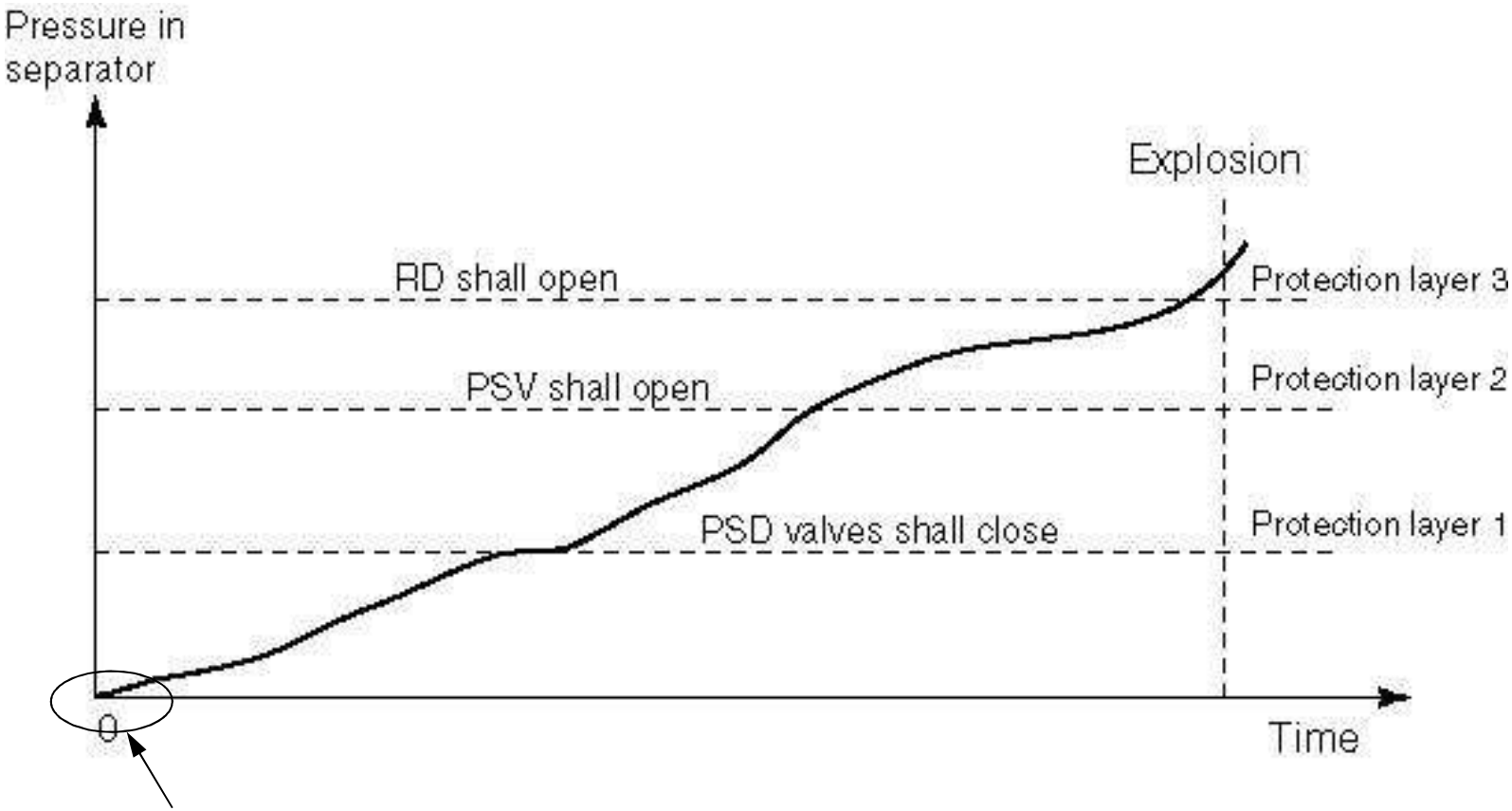
Relevant top event: « Critical overpressure in the first stage operator »

- critical situation occurs during normal production
- the fluid level in the separator is normal

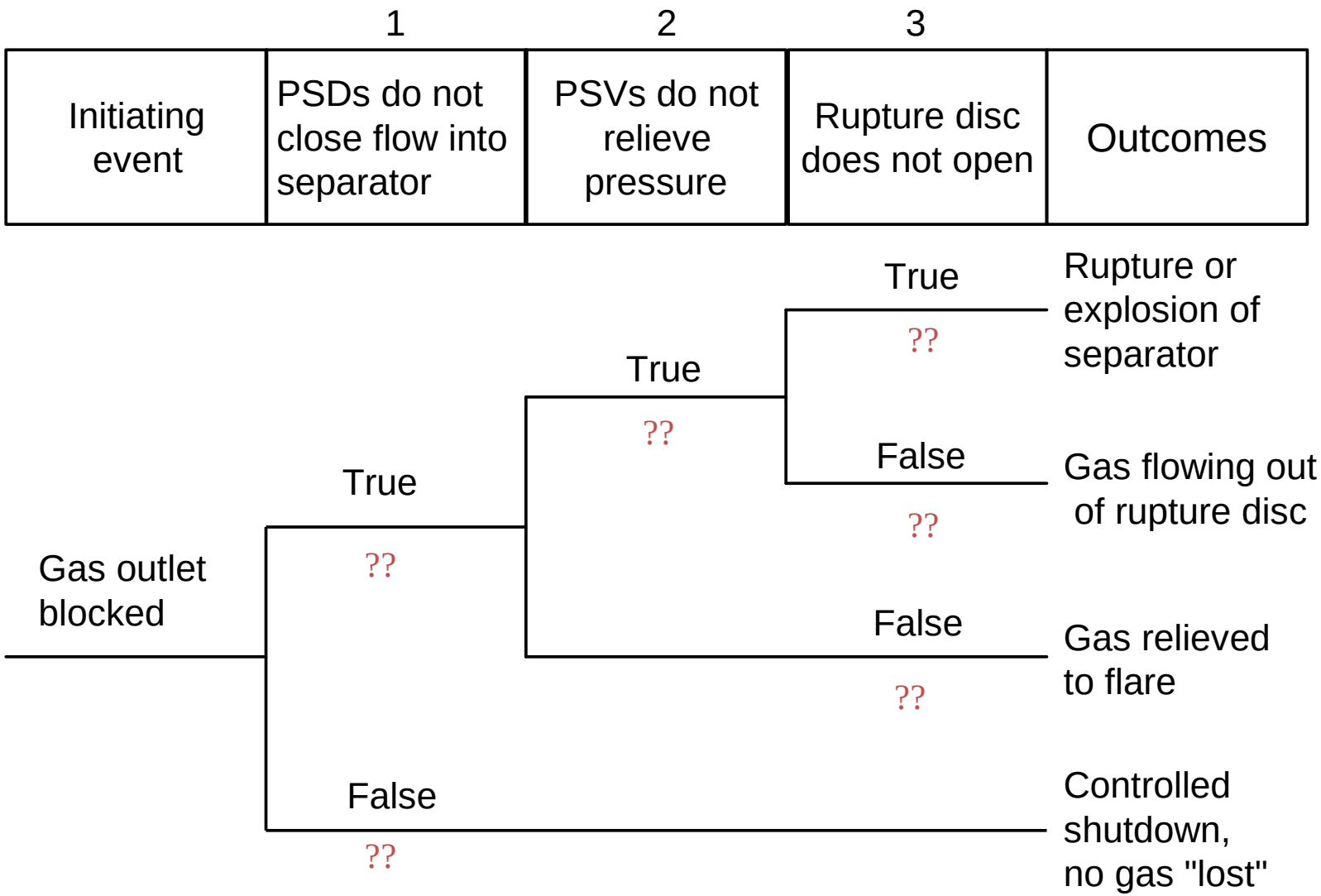


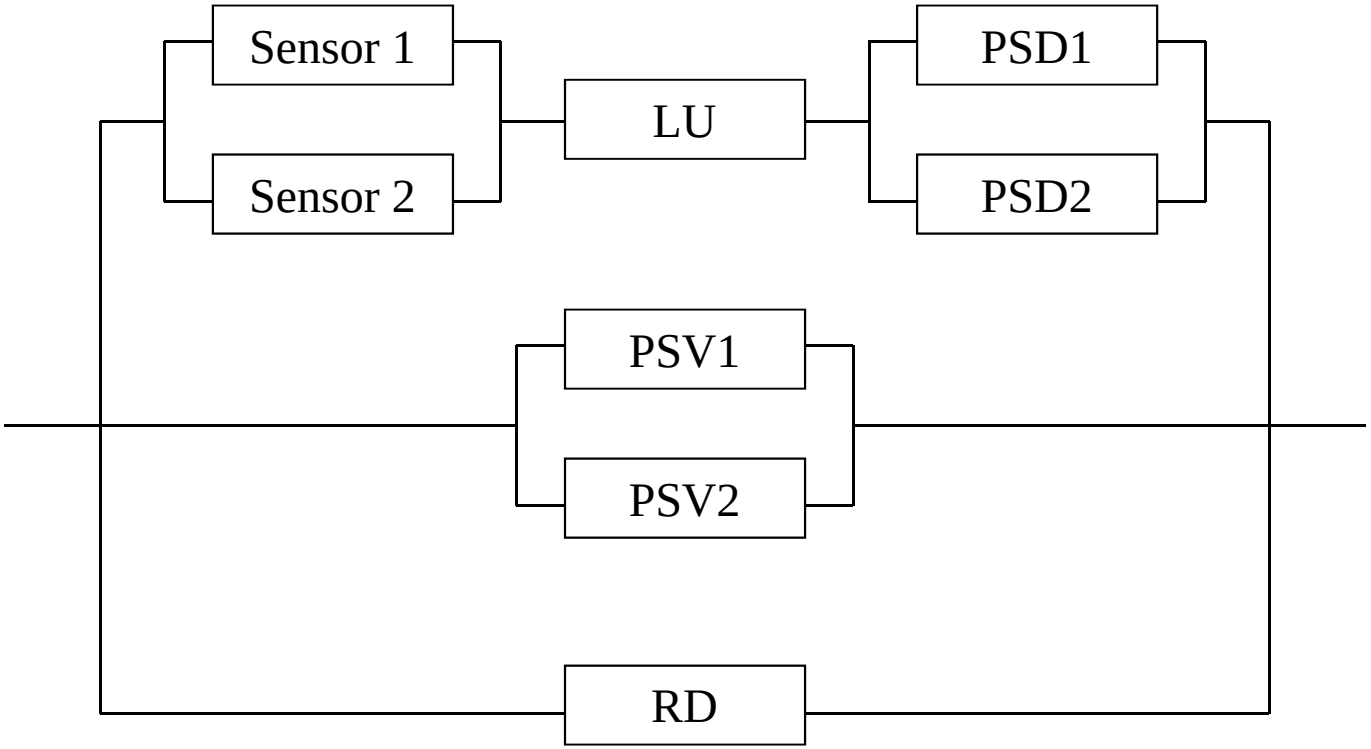
Note

- the lowest level of resolution = failure mode of a technical item
- might be of interest to break down some of the rather complex items into subitems (e.g. valves)
- failure of the pressure switches should be split in
  - individual failures (independent)
  - common cause failures (simulataneously) eg: miscalibration



Gas outlet blocked = IE


1
2
3
Initiating event
PSDs do not close flow into separator
PSVs do not relieve pressure
Rupture disc does not open
Outcomes
Gas outlet blocked
True
??
False
??
True
??
False
??
True
??
Rupture or explosion of separator
Gas flowing out of rupture disc
Gas relieved to flare
Controlled shutdown, no gas "lost"


Sensor 1
Sensor 2
LU
PSD1
PSD2
PSV1
PSV2
RD

LES FACTEURS D’IMPORTANCE

Objectifs

- Déterminer l'importance d'un composant dans une structure complexe en fonction du critère associé (fiabilité, structure, …)
- Utilisé pour :
  - Orienter les efforts d'amélioration des systèmes complexes en phase de conception (accroitre la fiabilité intrinsèque des composants les plus critiques, définir des redondances, réduire les effets de stress environnementaux, améliorer la maintenabilité du composant) et analyser les performances globales du système en termes de sensibilité (par exemple, par rapport à l'incertitude sur l'estimation des paramètres).
  - Dans la phase d'exploitation, orienter les efforts de maintenance et de surveillance/inspection des composants les plus critiques

Les mesures les plus connues

- Les mesures probabilistes
  - **Le facteur de Birnbaum**
  - **Le facteur d'amélioration**
  - **Le « Risk Achievement Worth »**
  - **Le « Risk Reduction Worth »**
  - **Le facteur d'Importance critique**
  - **Le facteur de Vesely-Fussel**

- Les mesures structurelles
  - **Indicateur structurel de Birnbaum**
  - Indicateur de Barlow et Proschan
  - Indicateur de Butler

Indicateur de Birnbaum

Définition : $I^B(i|t) = \frac{\partial h(\boldsymbol{p}(t))}{\partial p_i(t)}$ $pour\ i = 1, \dots, n$ avec $h\big(\boldsymbol{p}(t)\big)$ la fiabilité du système et $p_i(t)$ la fiabilité du composant *i.*

Si $I^B(i|t)$ est grand, de faibles variations de la fiabilité du composant *i* entraineront de grandes variations de la fiabilité du système.

Autre formulation de la mesure d'importance de Birbaum :

- $I^B(i|t) = h(1_i, \boldsymbol{p}(t)) - h(0_i, \boldsymbol{p}(t))$ où $h(1_i, \boldsymbol{p}(t))$ est la probabilité conditionnelle de fonctionnement sachant que le composant *i* fonctionne
- $I^B(i|t)$ est la probabilité que le système soit dans un état pour lequel le composant *i* est critique pour le système (dans le sens où ce composant est inclus soit dans une coupe minimale d'ordre 1, soit l'ensemble des autres composants d'une même coupe minimale soient défaillants à *t*).

Exemple : Soit un système formé de 2 composants indépendants ayant des fiabilités $p_1$et p_2 avec $p_1 > p_2$. Classer l'importance des composants :

- Si la structure est en série
- Si la structure est en parallèle

Facteur d'amélioration

Définition : $I^{IP}(i|t) = h(1_i, \boldsymbol{p}(t)) - h\big(\boldsymbol{p}(t)\big)\ pour\ i = 1, \dots, n$ avec $h\big(\boldsymbol{p}(t)\big)$ la fiabilité du système.

En pratique, on ne peut pas garantir une fiabilité d'un composant = 1. On introduit alors le facteur d'amélioration crédible $I^{CIP}(i|t) = h\big({p_i}^{(n)}(t), \boldsymbol{p}(t)\big) - h\big(\boldsymbol{p}(t)\big)$ où ${p_i}^{(n)}(t)$ peut représenter une probabilité associée à un état de l'art pour ce type de composant.

Lien entre facteur d'amélioration crédible et mesure d'importance de Birnbaum

- $I^{CIP}(i|t) = I^{B}(i|t)\big({p_i}^{(n)}(t) - p_i(t)\big)$

Exemple : Soit un système formé de 2 composants indépendants ayant des fiabilités $p_1$et p_2 avec $p_1 > p_2$. Classer l'importance des composants en fonction du facteur d'amélioration :

- Si la structure est en série
- Si la structure est en parallèle

Risk Achievement Worth

Définition : $I^{RAW}(i|t) = \frac{(1-h(0_i,\boldsymbol{p}(t)))-(1-h(1_i,\boldsymbol{p}(t)))}{1-h(\boldsymbol{p}(t))} = \frac{(1-h(0_i,\boldsymbol{p}(t)))}{1-h(\boldsymbol{p}(t))} - 1 \; pour \; i = 1, \dots, n$

Remarque 1 :
On omet généralement le « moins 1 ».
Pour tout système cohérent, on a alors $I^{RAW}(i|t) \geq 1$ et quand $I^{RAW}(i|t) = 1$, le composant *i* n'a aucun effet.

Remarque 2 :
Le RAW est utile pour estimer l'importance du risque des composants qui sont retirés du système.

Exemple : Soit un système formé de 2 composants indépendants ayant des fiabilités p_1 et p_2 avec $p_1 > p_2$. Classer l'importance des composants en fonction du RAW :

- Si la structure est en série
- Si la structure est en parallèle

Risk Reduction Worth

Définition : $I^{RRW}(i|t) = \frac{1-h(\boldsymbol{p}(t))}{(1-h(1_i,\boldsymbol{p}(t)))}$ $pour\ i = 1, \dots, n$

Remarque 1 :
Le risque est ici réduit par rapport à la meilleure situation vis-à-vis du composant *i.*

Lien entre le RRW et d'autres facteurs d'importance :

- $I^{RRW}(i|t) = \left(1 - \frac{I^{IP}(i|t)}{\left(1-h(\boldsymbol{p}(t))\right)}\right)^{-1} = \left(1 - \frac{I^{B}(i|t)\left(1-p_i(t)\right)}{\left(1-h(\boldsymbol{p}(t))\right)}\right)^{-1}$

Remarque 2 :
Le RRW est utile pour borner les gains en termes de risque en fonction des améliorations.

Exemple : Soit un système formé de 2 composants indépendants ayant des fiabilités $p_1$et p_2 avec $p_1 > p_2$. Classer l'importance des composants en fonction du RRW :

- Si la structure est en série
- Si la structure est en parallèle

Criticality Importance

Définition : $I^{CI}(i|t) = \frac{I^{B}(i|t)\left(1-p_i(t)\right)}{\left(1-h(\boldsymbol{p}(t))\right)} pour\ i = 1, \dots, n$

En d'autres mots, le $I^{CI}(i|t)$ est la probabilité que le composant *i* soit la cause de la défaillance du système, sachant celui est défaillant à l'instant *t.*

Lien entre le CI et d'autres facteurs d'importance :

- $I^{CI}(i|t) = 1 - \frac{1}{I^{RRW}(i|t)}$

Remarque 2 :
Le composant *i* est critique. Quand le composant est réparé, le système fonctionne à nouveau. C'est la raison pour laquelle le CI peut être utilisé pour prioriser les actions de maintenance dans un système complexe.

Exemple : Soit un système formé de 2 composants indépendants ayant des fiabilités $p_1$et p_2 avec $p_1 > p_2$. Classer l'importance des composants en fonction du RRW :

- Si la structure est en série
- Si la structure est en parallèle

La mesure de Vesely-Fussel

Définition : $I^{FV}(i|t)$ est la probabilité qu'au moins une des coupes minimales contenant *i* est défaillante à *t*, sachant le système défaillant à *t*.

$$I^{FV}(i|t) \approx \frac{1 - \prod_{j=1}^{m_i}\left(1 - \breve{Q}^{i}{}_{j}(t)\right)}{Q_0(t)} \approx \frac{\sum_{j=1}^{m_i} \breve{Q}^{i}{}_{j}(t)}{Q_0(t)}$$

Avec $\breve{Q}^{i}{}_{j}(t)$ la probabilité que la coupe minimale *j* parmi celle contenant *i* soit défaillante à *t*.

Lien entre le FV et d'autres facteurs d'importance :

- Le FV donne les mêmes résultats que le CI.

Le calcul de $I^{FV}(i|t)$ peut se calculer facilement « à la main ».

Exemple : Considérons une structure de type pont formée de 5 composants indépendants avec des fiabilités p_i. Déterminez $I^{FV}(3)$.

Classification des facteurs d'importance probabilistes

- Facteurs d'importance pour la détection d'événements *significatifs pour la sûreté (=fiabilité)* :
  - Birnbaum, RAW et CI
- Facteurs d'importance pour la détection d'événements *significatifs pour le risque (=sûreté)* :
  - RRW et VF
- Aide au diagnostic de panne
  - RRW et VF
- Aide à la maintenance
  - CI

La mesure de Birnbaum de l'importance structurelle

Définition : $B_\phi(i) = \frac{\eta_\phi(i)}{2^{n-1}}$ où $\eta_\phi(i)$ est le nombre de chemins critiques pour le composant *i.*

Définition : Un chemin critique pour *i* est un vecteur d'état $(1_i, \boldsymbol{x})$ tel que $\phi(1_i, \boldsymbol{x}) = 1$.
Le nombre de chemin critique est donné par $\eta_\phi(i) = \sum_{(\cdot,\boldsymbol{x})}[\phi(1_i, \boldsymbol{x}) - \phi(0_i, \boldsymbol{x})]$

Exemple : Considérons une structure de type 2-sur-3. Pour le composant 1, on a :

$(\cdot, x_2, x_3)$	$\phi(1, x_2, x_3) - \phi(0, x_2, x_3)$	$C(1, x_2, x_3)$
(.00)	0	
(.01)	1	{1,3}
(.10)	1	{1,2}
(.11)	0	

$$\eta_\phi(1) = 2; B_\phi(1) = \frac{2}{4} = \frac{1}{2}$$

Pour des raisons de symétrie, on a $B_\phi(1) = B_\phi(2) = B_\phi(3)$

Conclusion : modes d'application

- Possibles règles d'application des FI pour :
  - La maintenance :
    - Si CI très élevé, amélioration de la maintenance préventive
    - Si FAR très élevé, privilégier la surveillance à la maintenance préventive
    - Si CI et FAR sont faibles, maintenance corrective uniquement
  - L'aide à la conception
    - Définition des « barrières de sûreté » : efficaces, minimales et indépendantes.
- Quelques limites :
  - Indicateurs relatifs à une valeur de risque de référence
  - Importance d'un composant relative aux valeurs des autres
  - Validité des indicateurs liée à la taille des études (limite physique des ordinateurs)

Modèle d’analyse dynamique de la fiabilité des systèmes complexes

Processus de Markov

Exemple d'un système parallèle

- Pour 2 composants à 2 états, nombre d'états du système = 2^2 = 4 états

Etat système	Composant 1	Composant 2
0	Fonction	Fonction
1	Fonction	Défaillant
2	Défaillant	Fonction
3	Défaillant	Défaillant

- La question est alors
$P(t) = (P_0(t), P_1(t), P_2(t), P_3(t))$

Éléments de base

- $X(t)$: l'état du système à l'instant t
- $E = \{0,1,2,3\}$: espace des états du système
- $P_i(t) = \Pr(X(t) = i)$
- $P(t) = (P_0(t), P_1(t), P_2(t), P_3(t))$: distribution de probabilité d'état

Propriété de Markov

- Supposons le processus dans l'état *i* à l'instant s, $X(s) = i$.
- La probabilité conditionnelle d'être en *j* à $t + s$ est
  $P(X(t+s) = j | X(s) = i, X(u) = x(u), 0 \leq u, < s)$
  avec $\{x(u), 0 \leq u, < s\}$ l'histoire du processus

Définition : Le processus est dit avoir la ***propriété markovienne*** si
$P(X(t+s) = j | X(s) = i, X(u) = x(u), 0 \leq u, < s) = P(X(t+s) = j | X(s) = i)$

Propriétés :

- $P(X(t+s) = j | X(s) = i) = P(X(t) = j | X(0) = i) = p_{i,j}(t)$
- $\boldsymbol{P}(t) = \begin{bmatrix} P_{00}(t) & \cdots & P_{0r}(t) \\ \vdots & \ddots & \vdots \\ P_{r0}(t) & \cdots & P_{rr}(t) \end{bmatrix} = \left[p_{i,j}(t)\right]_{1 \leq i,j \leq r}$: matrice de probabilité de transition
- $\sum_{j=1}^{r} p_{i,j}(t) = 1$
- Soit $\widetilde{T_i}$ le temps de séjour dans l'état *i*, la loi de $\widetilde{T_i}$ est une loi exponentielle.
- Les temps de séjour $\widetilde{T_1}, \widetilde{T_2}, \ldots$ sont indépendants et suivent des lois exponentielles de paramètres $\alpha_i, E\left(\widetilde{T_i}\right) = \frac{1}{\alpha_i}$

Taux de transition

Définition : On définit le taux de transition de l'état *i* vers l'état *j* par

$$a_{ij} = \alpha_i P_{ij} \; pour \; tout \; j \neq i$$

où α_i est le taux de sortie de *i* et P_{ij} la probabilité de passer « instantanément » de *i* en *j*.

Remarques :

- Comme $\sum_{j \neq i} p_{ij} = 1$, $\alpha_i = \sum_{j \neq i} a_{ij}$
- De plus, pour Δt petit, on a $P_{ij}(\Delta t) = \Pr(\widetilde{T}_i < \Delta t) = 1 - e^{-a_{ij}\Delta t} \approx a_{ij}\Delta t$

Illustration

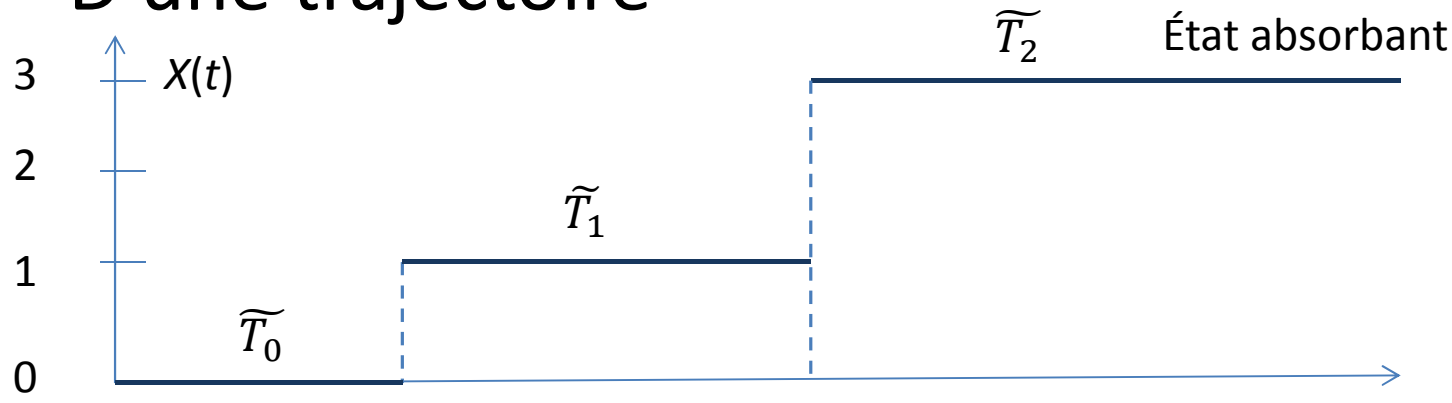
- Par analogie, que vaut a_{01} dans l'exemple d'introduction dans le cas non réparable?
- Construire la matrice associée des taux de transition $\boldsymbol{A}$

Conclusion : Un processus de Markov est défini par :

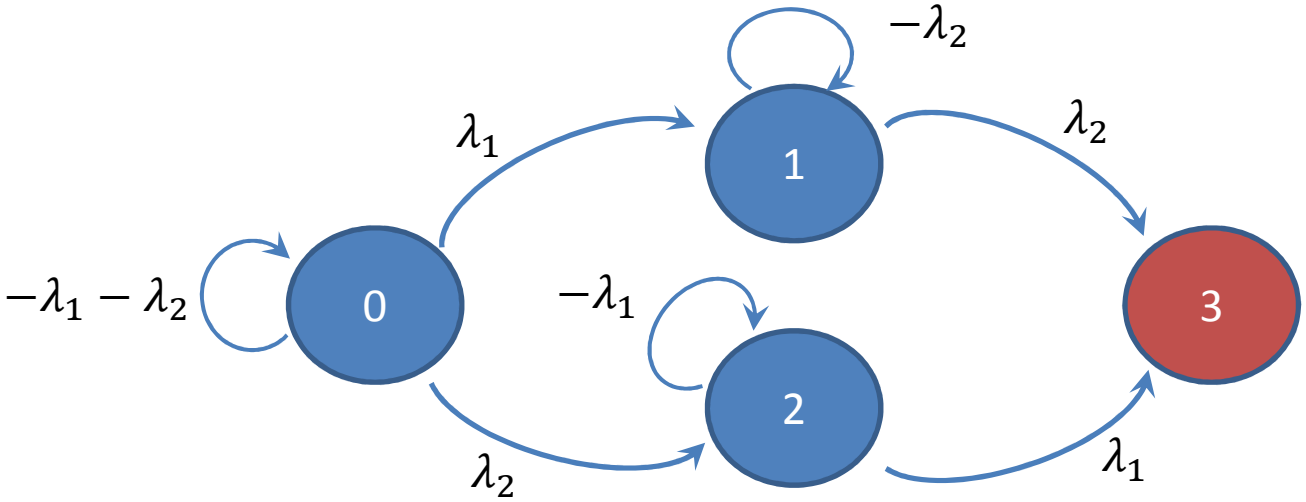
- Son espace d'état
- La matrice associée des taux de transition $\boldsymbol{A}$
- L'état du système à l'état initial, $t = 0$

Représentation graphique

- D'une trajectoire



- De transition d'états (ou graphe de Markov)



Détermination des probabilités d'état

1. Ecrire les équations d'états du processus de Markov (ou équations différentielles de Kolmogorov)
2. Résoudre les équations d'états
   1. Soit par la résolution d'équations différentielles
   2. Soit par l'évaluation de la loi stationnaire

Construction des équations d'états

- Equations différentielles de Kolmogorov

$$P_{ij}(t+\Delta t) = \sum_{k=0}^{r} P_{ik}(\Delta t) P_{kj}(t)$$

- On peut alors montrer que

$$\frac{d}{dt} P_{ij}(t) = \sum_{k=0}^{r} a_{ik} P_{kj}(t)$$

Qui s'écrit sous forme matricielle

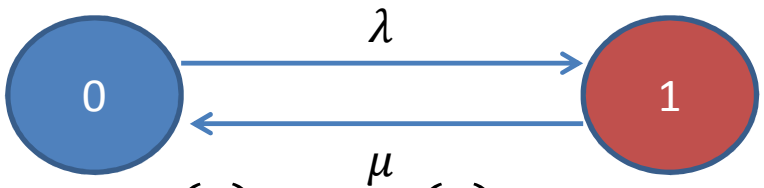
$$\dot{\boldsymbol{P}}(t) = \boldsymbol{A} \cdot \boldsymbol{P}(t)$$

On peut également montrer

$$\dot{\boldsymbol{P}}(t) = \boldsymbol{P}(t) \cdot \boldsymbol{A}$$

Exemple -1

- Contexte :
  - 1 système réparable avec un seul mode de défaillance (λ, μ) en état de marche à t =0



  - Déterminer $P_0(t)$ et $P_1(t)$
  - Construction de la matrice de taux de transition

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

  - Equations d'états

$$\left[\dot{P}_0(t), \dot{P}_1(t)\right] = [P_0(t), P_1(t)] \cdot \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

$$\Rightarrow \dot{P}_0(t) = -\lambda P_0(t) + \mu P_1(t)$$

Exemple -2

– On combine avec $P_0(t) + P_1(t) = 1$

– La solution est alors

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

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

– Remarques :

- $P_1(t)$ représente la disponibilité du système (état de marcher)
- $\lim_{t \to \infty} P_1(t) = \frac{\mu}{\lambda+\mu} = \frac{MTTF}{MTTF+MDT}$

Exemple - 3

- Evaluation par la loi stationnaire
  - La loi stationnaire $\lim_{t\to\infty} P_j\,(t) = P_j, \forall j$, existe (chaine de Markov irréductible)
  - Si $\lim_{t\to\infty} P_j\,(t) = P_j = cste, \lim_{t\to\infty} \dot{P}_j\,(t) = 0, \forall j$

  Alors $\boldsymbol{P} \cdot \boldsymbol{A} = \boldsymbol{0}$ (1)
  - Si on combine (1) avec $P_0 + P_1 = 1$, on tombe sur un système linéaire « facile » à résoudre

Méthode générale

1. **S’assurer que l’hypothèse Markovienne tienne …**
2. Identification des états de fonctionnement et de défaillance
3. Construire le graphe d’états
4. Définir les taux de transition et estimer les quantités associées (taux de défaillance et taux de réparation)
5. Définir la matrice des taux de transition
6. Ecrire les équations d’états
7. Construire le système d’équations
    1. Différentielles en associant la loi de probabilité totale
    2. Stationnaires en associant la loi de probabilité totale
8. Résolution du système

Remarque

Aujourd’hui, des progiciels permettent de résoudre directement les équations d’états à partir des graphes d’états.

La compétence reste alors la compréhension et la modélisation de la dynamique du système.

Performance du système (en régime stationnaire)

- Fréquence de visite de l'état *j* :

$$\nu_i = P_j \alpha_j = \sum_{k \neq j} P_k a_{kj}$$

Et le temps entre les visites à l'état *j* est $^1/_{\nu_j}$

- Disponibilité du système

$$A_s = \sum_{j \in B} P_j$$

Où *B* est l'ensemble des états de bon fonctionnement (*F* celui des états de défaillance)

- Fréquence des défaillances du système

$$\omega_F = \sum_{j \in B} \sum_{k \in F} P_j a_{jk}$$

- Durée moyenne de défaillance du système : $\theta_F = (1 - A_s)/\omega_F$
- Temps moyen entre défaillances du système : $MTBF_S = 1/\omega_F$

Exercices d'application

- Déterminer les probabilités d'état à un instant *t* donné des systèmes formés de 2 composants pour les configurations suivantes :
  - Système série
  - Système en parallèle avec 2 réparateurs
    - Redondance active
    - Redondance passive
- Quelle est la disponibilité d'un système en parallèle avec 1 seul réparateur (redondance active) ?
- Quelle est la disponibilité d'un système parallèle formé de deux composants présentant un mode commun de défaillance avec un seul réparateur ?

« Rappels » Transformée de Laplace

- Définition de la transformée

$$\mathcal{L}[f(t)] = f^*(s) = \int_0^\infty e^{-st} f(t)dt = E(e^{-sT})$$

- Définition de la transformée inverse

$$f(t) = \mathcal{L}^{-1}[f^*(s)]$$

- Propriétés importantes
  - $\mathcal{L}[\alpha f(t)] = \alpha \mathcal{L}[f(t)]$
  - $\mathcal{L}[f'(t)] = s\mathcal{L}[f(t)] - f(0)$
- Quelques transformées classiques
  - $f(t) = \mathcal{L}^{-1}[f^*(s)] = 1 \Leftrightarrow f^*(s) = \mathcal{L}[f(t)] = \frac{1}{s}$
  - $f(t) = \mathcal{L}^{-1}[f^*(s)] = e^{\alpha t} \Leftrightarrow f^*(s) = \mathcal{L}[f(t)] = \frac{1}{\alpha + s}$