Sûreté de Fonctionnement des systèmes informatiques

Walter SCHÖN

Sûreté de Fonctionnement des systèmes informatiques

Méthodes d'analyse prévisionnelles de la sûreté de fonctionnement

(Prévision des fautes)

Méthodes d'analyse prévisionnelle de la SdF

Se répartissent en deux catégories

- Méthodes inductives : montantes (bottom-up) : des causes élémentaires (fautes initiales) vers conséquences
- Méthodes déductives : descendantes (top-down) : des conséquences (particulièrement redoutées) vers causes (fautes ou combinaisons de fautes susceptibles de les provoquer.

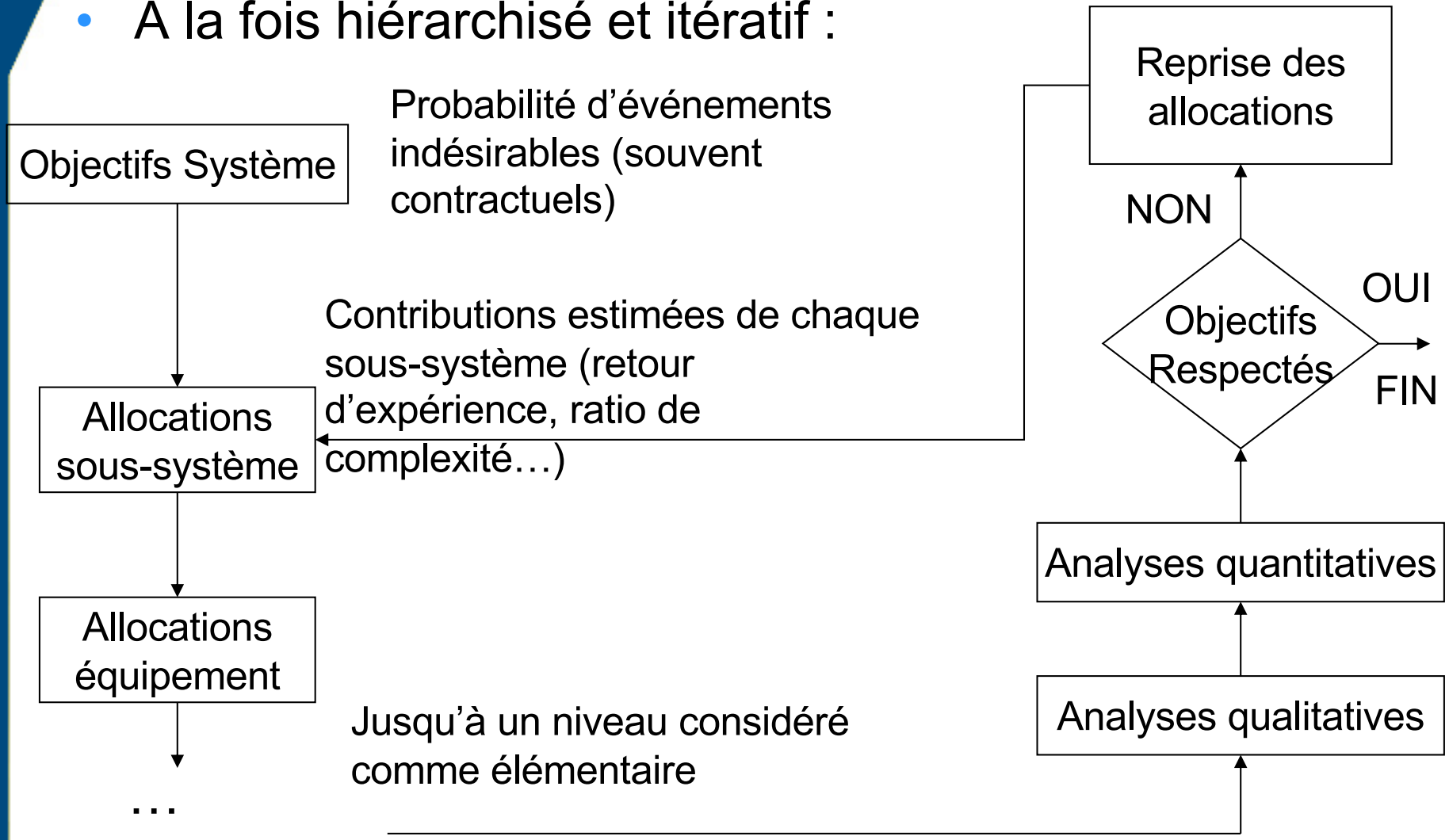
Certaines méthodes sont seulement qualitatives (évaluation ordinale), d'autres également quantitatives (évaluation probabiliste).

Certaines sont plus adaptées à la FDM, d'autres à la Sécurité Innocuité.

Un exemple de démarche inductive…

Le processus de prévision de la SdF

- A la fois hiérarchisé et itératif :



Méthodes d'analyse de la sûreté de fonctionnement : APD et APR

- Acronyme d'Analyse Préliminaire des Dangers (Risques), elles visent à identifier les événements indésirables liés au système, à en identifier la gravité (et à formuler un objectif de probabilité d'occurrence pour une APR)
- Peuvent être inductives (causes vers conséquences) ou déductives (conséquences vers causes).
- Résultat formalisé sous forme de tableaux dont la forme n'est (pour l'instant) pas normalisé, mais dont le contenu typique est donné ci-après
- APD : Preliminary Hazard Analysis : PHA
- APR : Preliminary Risk Analysis : PRA

Contenu typique des différentes colonnes de tableaux APR

- Le système ou la fonction étudiée
- La phase de la mission où le danger peut se manifester
- L'entité dangereuse
- Le ou les événements causant une situation dangereuse
- La situation dangereuse
- Le ou les événements transformant la situation dangereuse en accident potentiel.
- L'accident potentiel
- Les conséquences de cet accident
- Une classification par gravité
- Une estimation préliminaire de probabilité s'il s'agit d'une APR
- Des mesures préventives éventuelles

APD et APR

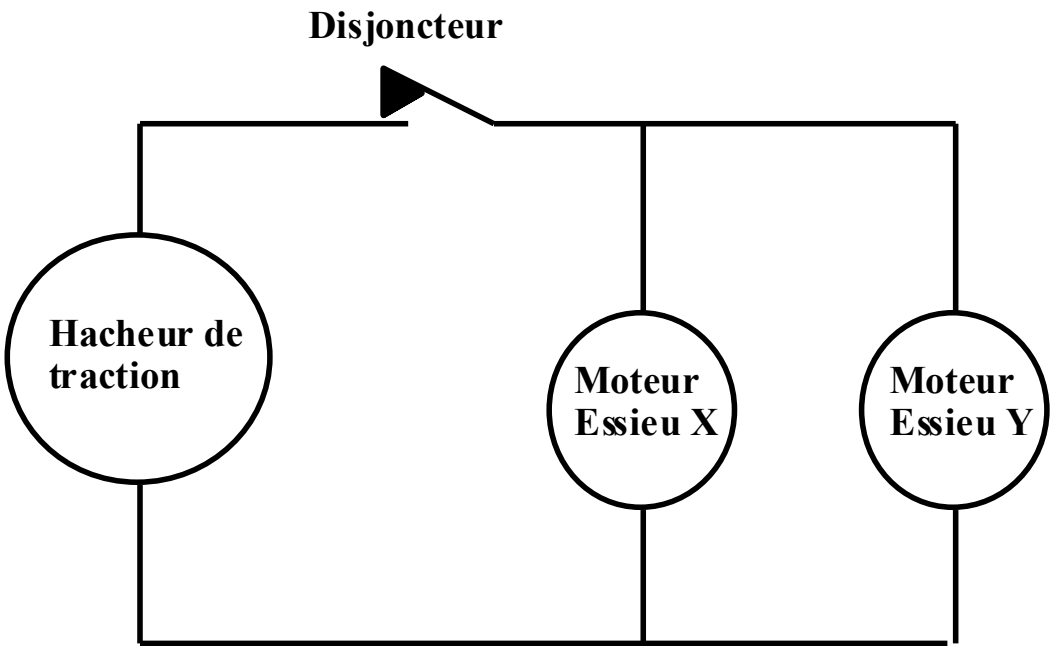
- Une APD ou APR inductive est fréquemment faite à partir d'une arborescence fonctionnelle système.
- Une APD ou APR déductive est fréquemment faite à partir d'une typologie arborescente des dangers système (Exemple : Collision->Par rattrapage->Train aval non détecté…).
- L'APD ou APR est souvent utilisée comme journal des situations dangereuses (indique les moyens de couverture des risques et les documents qui s'y rapportent : analyses détaillées de sécurité, notes de calculs ou d'essais, recommandations d'exploitation…) : Elle est alors le document de plus haut niveau, le plus important d'un dossier de sécurité.
- Dans certains domaines des listes guides d'entités dangereuses / situations dangereuses peuvent être utilisées.

Exemple de liste guide utilisée en aéronautique

Entités dangereuses	Situations dangereuses
Propergols	Accélérations / chocs
Capacités	Corrosion / Oxydation
Batteries	Contamination chimique
Générateurs électriques	Pression / Explosion
Conteneurs sous pression	Exposition à l'humidité
Ressorts tendus	Exposition à l'incendie
Machines tournantes	Exposition aux courants électriques
Dispositifs de chauffage	Chutes / Mouvements
Matériaux combustibles	Endommagement structurel
Mat. favorables à électricité statique	Contraintes
Objets susceptibles de tomber	Fuites

Exemple simplifié d'APR déductive

- Le système suivant (très simplifié) de traction ferroviaire sera utilisé pour illustrer plusieurs méthodes d'analyse :



Exemple simplifié d'APR déductive

Accident potentiel	Causes possibles liées au système	Grav.	Mesures préventives
Collision	Effort de traction intempestif	4	Le système ne doit pas tractionner intempestivement. A défaut toute traction intempestive doit être détectée et provoquer un arrêt d'urgence
Incendie à bord d'un véhicule	Échauffement excessif lié à un court-circuit	3	Tout courant excessif dans le circuit de traction doit être détecté et provoquer une coupure d'alimentation

Extrait d'une APR inductive réelle

Fonction niveau 2	Evénement Indésirable	Situation Dangereuse	Condition qui provoque l'accident	Accident Potentiel		Suivi du risque
				TYPE	GRA	Traitement des risques
Evacuation d'urgence (portes)	Déverrouillage de secours intempestif à l'arrêt	Porte à l'état libre	Absence de quai et déséquilibre d'un passager et ouverture des vantaux	Chute d'un passager sur la voie avec risque de collision avec un autre véhicule la rame étant à l'arrêt	4	Analyse détaillée / Le déverrouillage mécanique ne doit être possible que par une action manuelle volontaire / L'ouverture est asservie à l'information "coté de service" lorsque V < 3km/h / Information actionnement poignée transmise au conducteur

Méthodes d'analyse de la sûreté de fonctionnement : AMDE(C)

- Acronyme d'Analyse des Modes de Défaillance de leurs Effets et de leur Criticité, l'AMDE(C) est une analyse détaillée de toutes les défaillances simples, de leurs conséquences (ainsi qu'un chiffrage préliminaire de probabilité d'occurrence s'il s'agit d'une AMDEC)
- Elle procède de manière inductive en envisageant chaque mode de défaillance de chaque composant.
- Elle permet d'identifier les éléments critiques de sécurité (provoquant des événements critiques ou catastrophiques) ainsi que les fautes dormantes (non détectées immédiatement) bonnes candidates pour participer à des scénarios de fautes multiples.

Méthodes d'analyse de la sûreté de fonctionnement : AMDE(C)

- L'AMDE(C) est en général utilisée comme méthode prévisionnelle d'analyse de sécurité innocuité (safety).
- Il est toutefois possible de l'utiliser pour faire de la disponibilité (la notion de gravité étant alors à remplacer par l'impact sur la disponibilité).
- La limitation essentielle de l'AMDE(C) est sa restriction aux fautes simples (scénarios graves souvent à pannes simples sont non détectés) : l'AMDE(C) doit être complétée par une autre méthode.
- Plusieurs normes (dont USA MIL-STD 1629) proposent des formats types de tableaux AMDEC :

Contenu typique des tableaux AMDE(C)

- Composant envisagé
- Fonction du composant
- Mode de défaillance (plusieurs possibles pour un composant)
- Conséquences (éventuellement à plusieurs niveaux : équipement -> sous-système -> système)
- Moyens de détection : identification des fautes dormantes et du temps de latence associé (ex : jusqu'à grande révision)
- Gravité (suivant échelle définie dans le plan sécurité)
- Probabilité dans le cas d'une AMDE(C)
- AMDE(C) : FME(C)A : Failure Mode Effects (and Criticallity Analysis)

Un exemple (simplifié) d'AMDEC

- Considérant à nouveau le système de traction simplifié présenté plus haut :

Composant	Mode de défaillance	Effet système	Détection
Hacheur de traction	Absence de courant de traction	Aucun effort de traction. Blocage en ligne pouvant nécessiter une évacuation	Immédiate (train bloqué)
	Courant de traction intempestif	Effort de traction intempestif pouvant à terme provoquer une collision	Immédiate (mais probablement trop tardive)

Un exemple (simplifié) d'AMDEC

- Le mode de défaillance bloqué ouvert du disjoncteur est un cas typique de faute dormante (ne peut être détecté que par une préconisation de maintenance spécifique)

Composant	Mode de défaillance	Effet système	Détection
Disjoncteur	Ne s'ouvre pas (bloqué fermé)	Absence de protection contre les courts-circuits moteur	Aucune. Un test périodique en maintenance est indispensable
	S'ouvre intempestivement	Coupe tout effort de traction. Blocage en ligne pouvant nécessiter une évacuation	Immédiate (train bloqué

Un exemple (simplifié) d'AMDEC

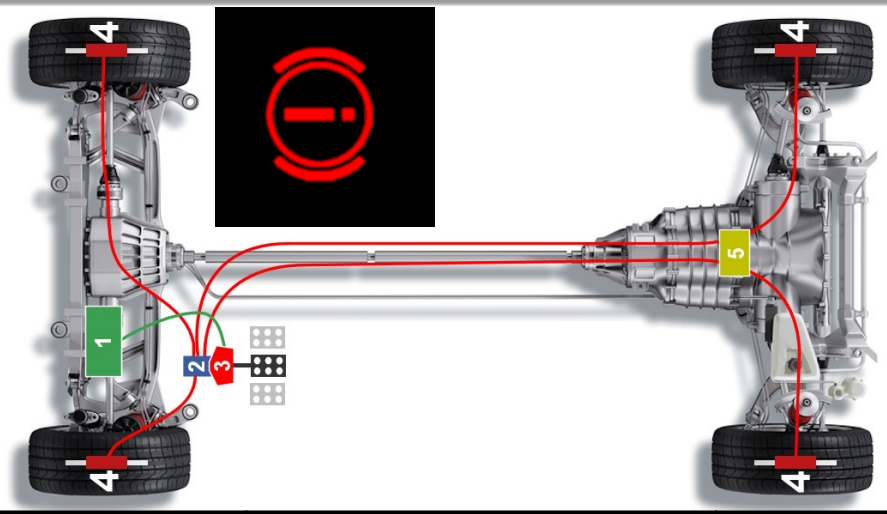
- Le court circuit moteur est envisagé seul (disjoncteur nominal) => L'AMDEC ne décèle aucun effet système de gravité importante (mais décèle une faute dormante qui pourra participer à des scénarios de pannes multiples).

Composant	Mode de défaillance	Effet système	Détection
Moteur X ou Y	Court-circuit	Courant élevé détecté par le disjoncteur => blocage en ligne	Immédiate (train bloqué)
	Circuit ouvert	Perte de la moitié de l'effort total de traction..	Immédiate (performances réduites)

Un exemple de la vie courante…

Composant	Mode de défaillance	Effet système	Gravité	Détection
Lave-Linge	Défaut d'isolement	Fuite électrique provoquant l'ouverture du différentiel	Aucune	Immédiate
Disjoncteur différentiel	Bloqué fermé	Absence de protection contre les défauts d'isolement	Aucune	Une maintenance spécifique doit être prévue

Autre exemple de la vie courante…



Composant	Mode de défaillance	Effet système	Gravité	Détection
Circuit hydraulique frein	Fuite d'huile	Allumage du voyant de défaut, arrêt immédiat	Aucune	Immédiate
Voyant défaut frein	Lampe défectueuse	Absence de surveillance du circuit de frein	Aucune	Pas d'allumage au démarrage

Un exemple (réel) de tableau AMDEC

Désignation	Mode de défaillance	Taux de défaillance	Effets sur la fonction	Effets sur le véhicule	Détection	Gravité
Fusible	Fusible en circuit ouvert	2,00E-09	Isolement batterie permanent, charge / décharge batterie impossible	Perte de l'autonomie BT de 45 minutes sur défaut CVS et de 50 minutes sur défaut HT	Le voyant de signalement batterie en service reste éteint en position normale	2

Analyse des Effets des Erreurs du Logiciel : AEEL : L'AMDEC des logiciels

- L'AEEL est une adaptation de l'AMDEC.
- Le but de cette méthode est de mettre en évidence des points critiques relevés durant les phases de développement d'un logiciel, et de proposer aux personnes chargées des tests de validation, une synthèse de la criticité des modules du logiciel analysé, afin d'affiner leur démarche.

AEEL : Principes

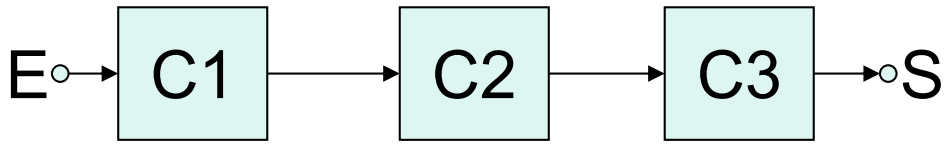
- Le principe de l'AEEL est d'envisager les hypothèses d'erreurs dans des logiciels (à partir de listes d’erreurs types), puis d'examiner les conséquences de ces erreurs :
  - Sur le module ... elles se produisent,
  - Sur les autres modules, en conséquence
  - Sur le système global enfin

Méthodes d'analyse : diagrammes de succès

- Souvent appelés (blocs) diagrammes de fiabilité
- Consistent à visualiser la logique de fonctionnement d'un système avec la règle : le système fonctionne s'il existe un chemin (chemin de succès) entre l'état et la sortie du diagramme qui ne traverse pas un bloc défaillant.
- Permettent une description très naturelle de l'architecture du système (redondances etc.).
- Sont utilisées de manière très efficace comme support des calculs de fiabilité (d'où leur nom).
- Sont par contre peu adaptés à la discrimination fine d'événements plus ou moins graves (donc moins utilisés pour des études de sécurité).
- Diagrammes de fiabilité : Reliability Block Diagrams : RBD

Diagrammes de fiabilité : systèmes série

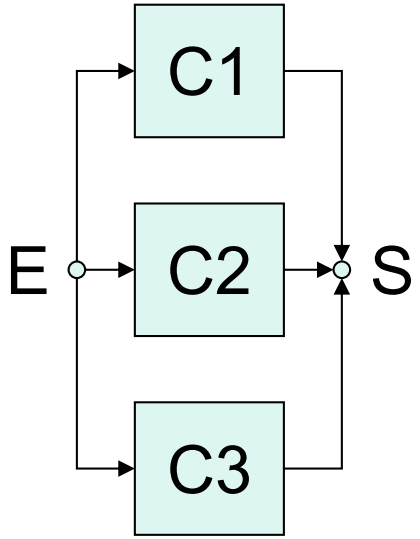
- Un diagramme de fiabilité série représente un système sans redondance : le bon fonctionnement du système nécessite celui de tous ses composants. Toute défaillance de composant entraîne une défaillance système.



Diagrammes de fiabilité : redondance active

- Un diagramme de fiabilité parallèle représente un système redondant : la défaillance du système nécessite celle de tous ses composants. Le bon fonctionnement d'un composant au moins est suffisant pour que le système assure son service.

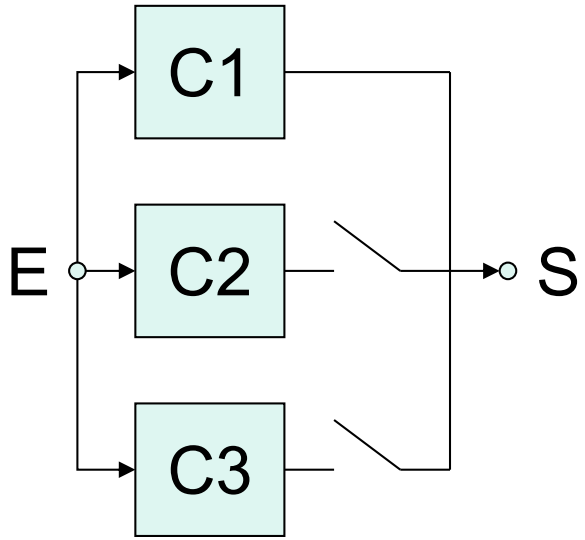
- Ici la redondance est dite active (tous les composants redondants sont actifs), parfois appelée aussi redondance chaude.



Diagrammes de fiabilité : redondance passive

- Une variante très répandue est la redondance à commutation ou redondance passive parfois appelée redondance froide.

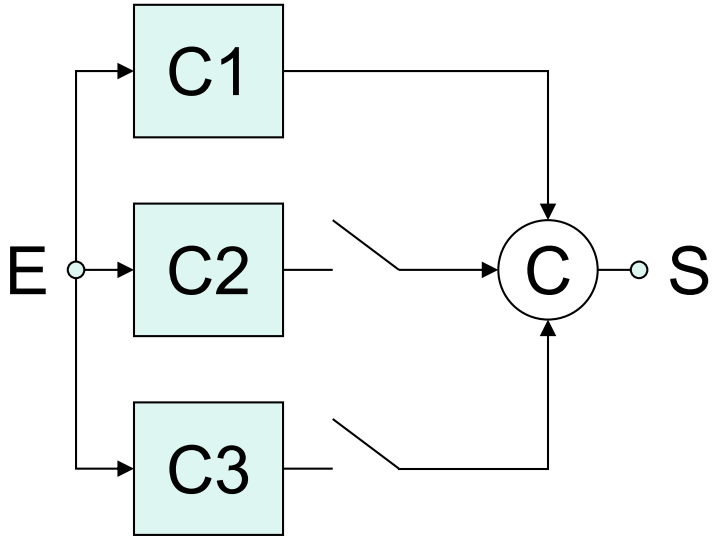
- Les éléments de secours sont en attente et ne sont mis en service que si nécessaire (autres composants défaillants) : Ici défaillance C1 => Commutation sur C2, défaillance C2 => commutation sur C3



- C'est un autre exemple de système à composants dépendants.

Diagrammes de fiabilité : redondance passive

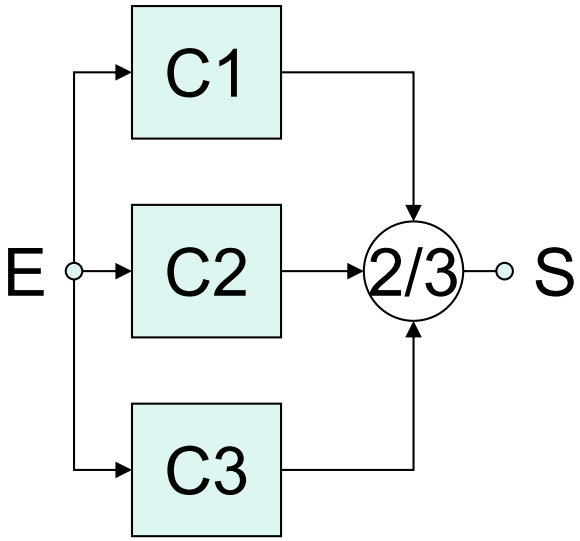
- Ainsi que l'on peut le pressentir qualitativement la fiabilité en redondance passive est meilleure qu'en redondance active (si le taux de défaillance à l'arrêt est plus faible qu'en marche).
- Ceci n'est vrai que dans la mesure où il n'y a pas un organe de détection de défaillance des éléments principaux (et de commutation sur les éléments de secours) : intervenant en série sur le reste du diagramme, ses défaillances peuvent compromettre l'efficacité de la redondance.



Diagrammes de fiabilité : systèmes à vote majoritaire

- Architecture informatique très répandue, le système à vote majoritaire (dit p/n ou poon : p out of n) est constitué de n éléments en partie redondants : le bon fonctionnement du système nécessite le bon fonctionnement de au moins p éléments sur n (ici 2 parmi 3) :

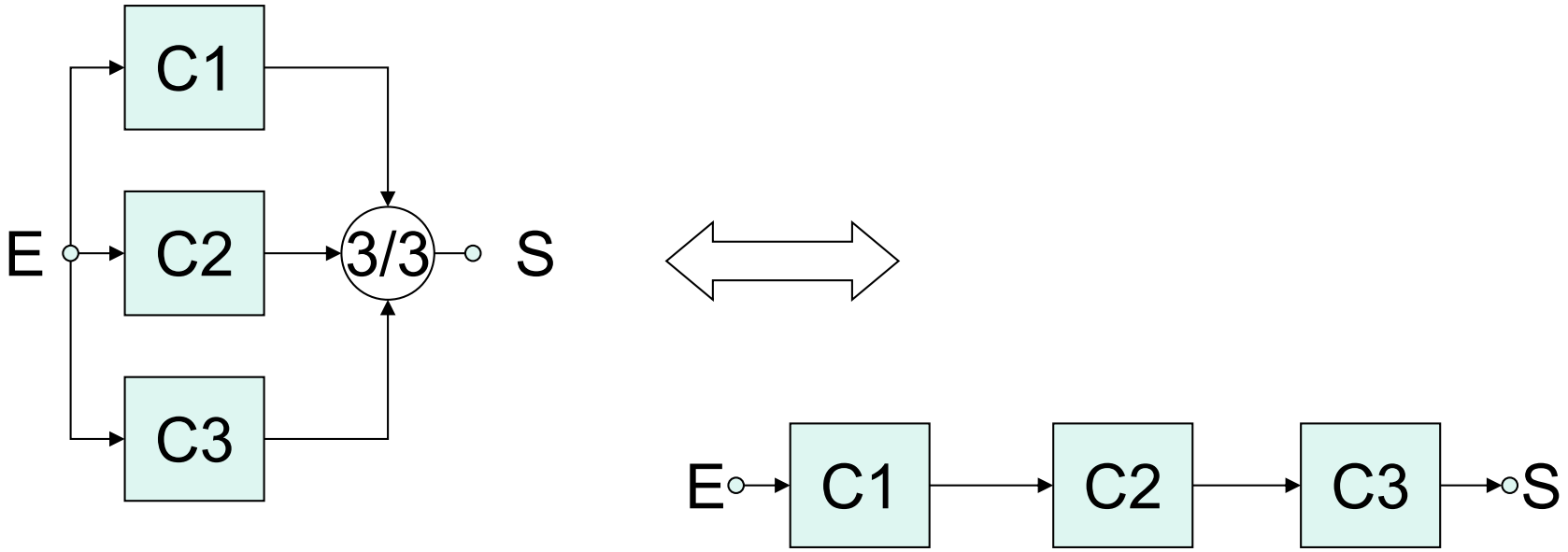
- Ici encore si le p/n est effectué par un véritable organe physique, ses défaillances peuvent mettre à mal la fiabilité de l'architecture (car en série sur le reste).



Systèmes à vote majoritaire

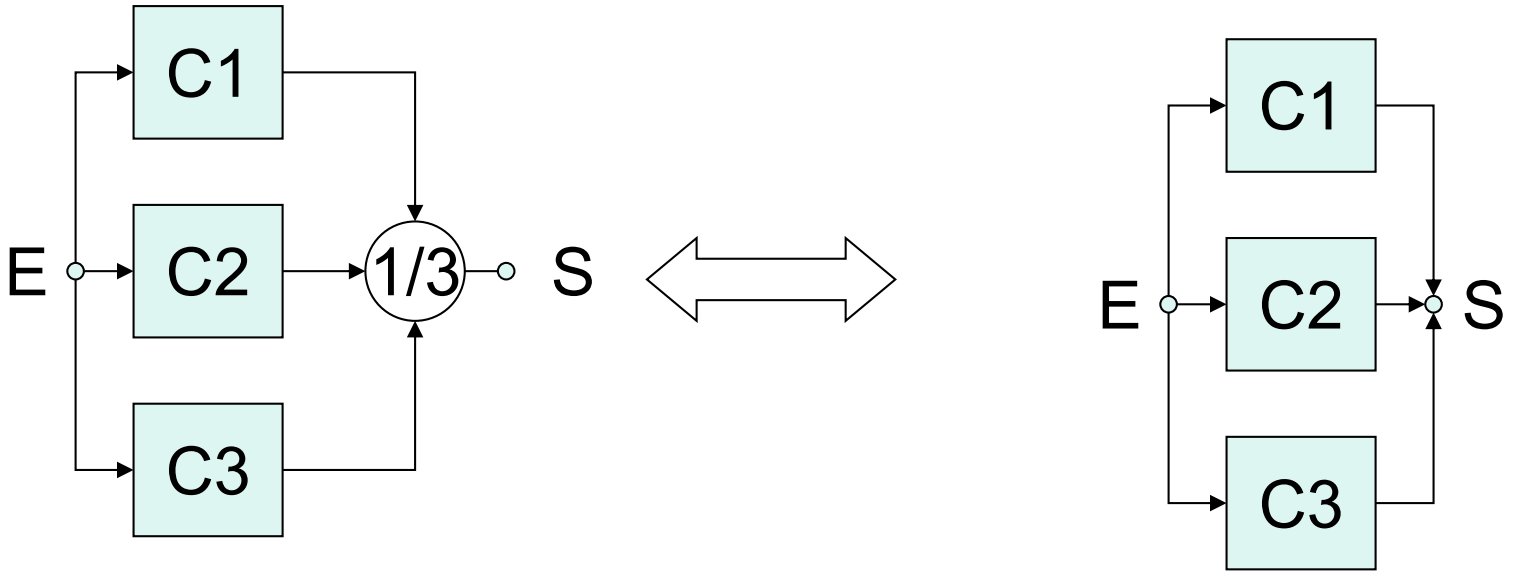
Noter que le système à vote majoritaire généralise les systèmes série et parallèle car :

- Un voteur n/n est un système série :



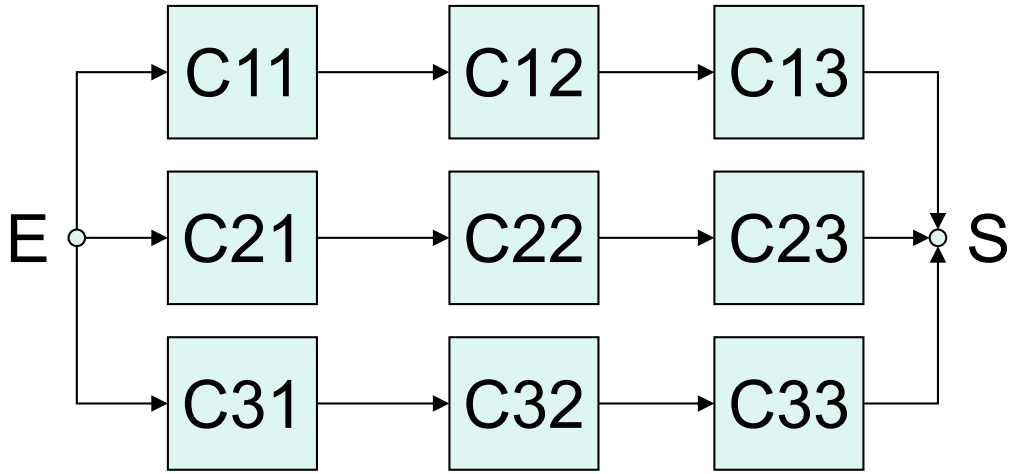
Systèmes à vote majoritaire

- De même un voteur 1/n est un système parallèle.
- On devra donc retrouver les résultats des systèmes série et parallèle comme cas particuliers de voteurs



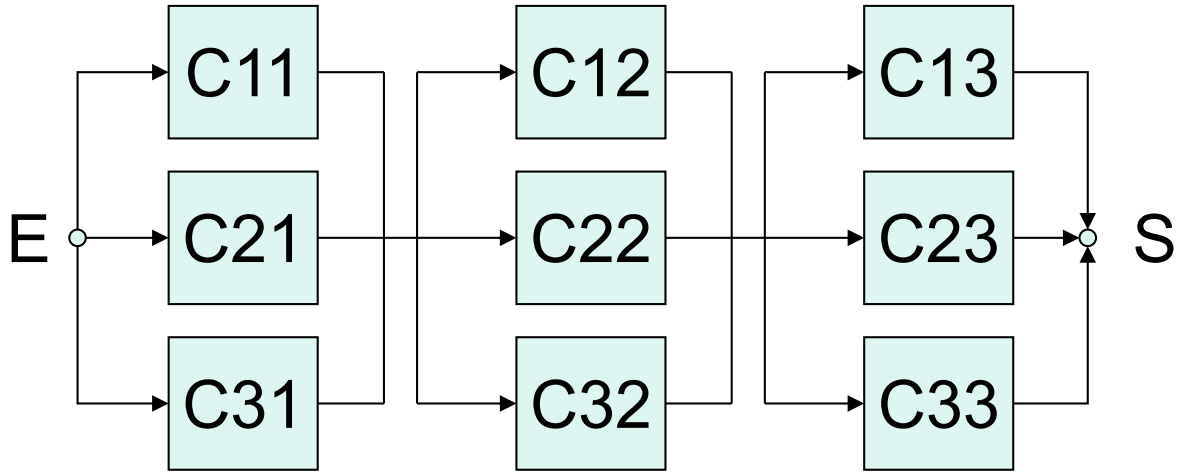
Systèmes série-parallèle

- Il est très fréquent de rencontrer des architectures qui sont des combinaisons de diagrammes parallèle et série, ici le série-parallèle (branches série mises en parallèle).
- Ce sont des fonctions de haut niveau (construites par assemblages série de fonctions élémentaires) qui sont mise en parallèle.



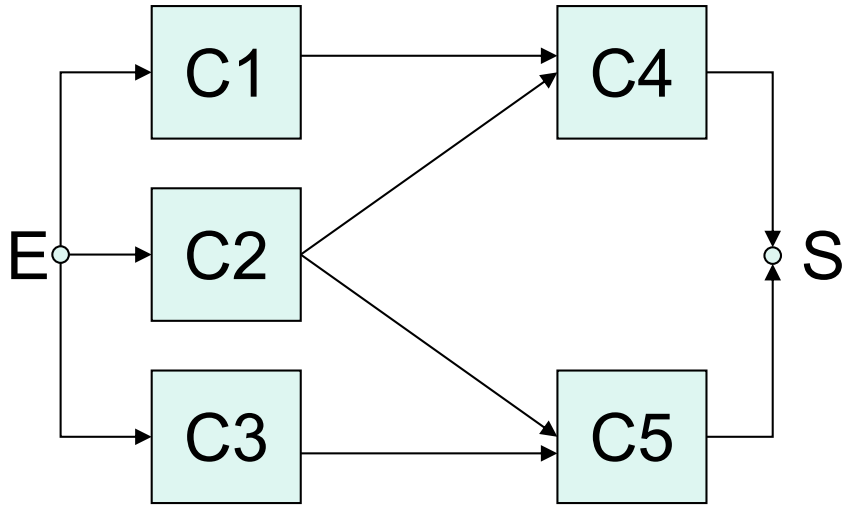
Systèmes parallèle-série

- Autre architecture combinaison de série et de parallèle, le parallèle-série (étages parallèles, mis en série).
- Dans ce cas la redondance est construite au niveau des fonctions élémentaires, et ce sont ces fonctions élémentaires redondantes qui sont mises en série.



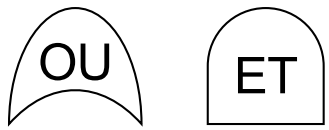
Systèmes complexes

- Les architectures série-parallèle et parallèle-série forment l'essentiel des architectures usuelles. Il existe toutefois des architectures dites « complexes » qui ne peuvent être ramenées à des combinaisons de parallèle et de série :



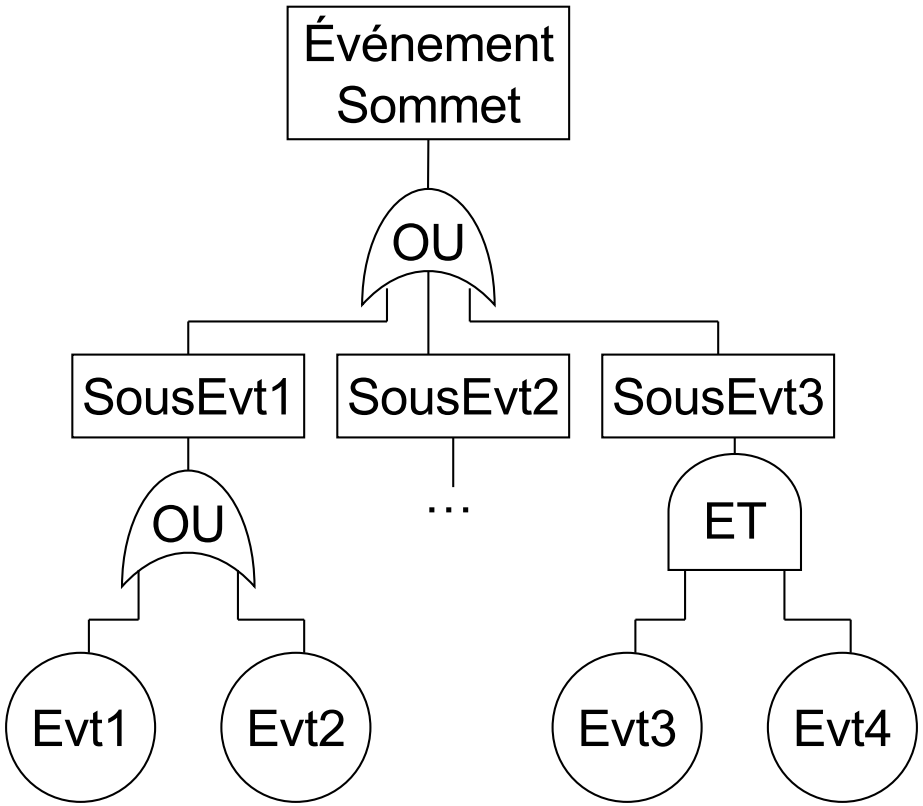
Méthodes d'analyse : Arbres de causes

- Souvent appelés arbres de défaillances ou arbres de fautes (Fault Tree Analysis : FTA). Sont l'indispensable complément de l'AMDEC pour analyse des pannes multiples.
- Ils utilisent les résultats de l'AMDEC en recherchant de manière déductive les combinaisons de défaillances pouvant conduire à une conséquence donnée au niveau du système : Il s'agit donc d'une méthode quasi-incontournable pour les analyses de sécurité.
- Il s'agit d'une représentation graphique et arborescente de relations booléennes avec des conventions graphiques pour les opérateurs inspirées de l'électronique numérique :

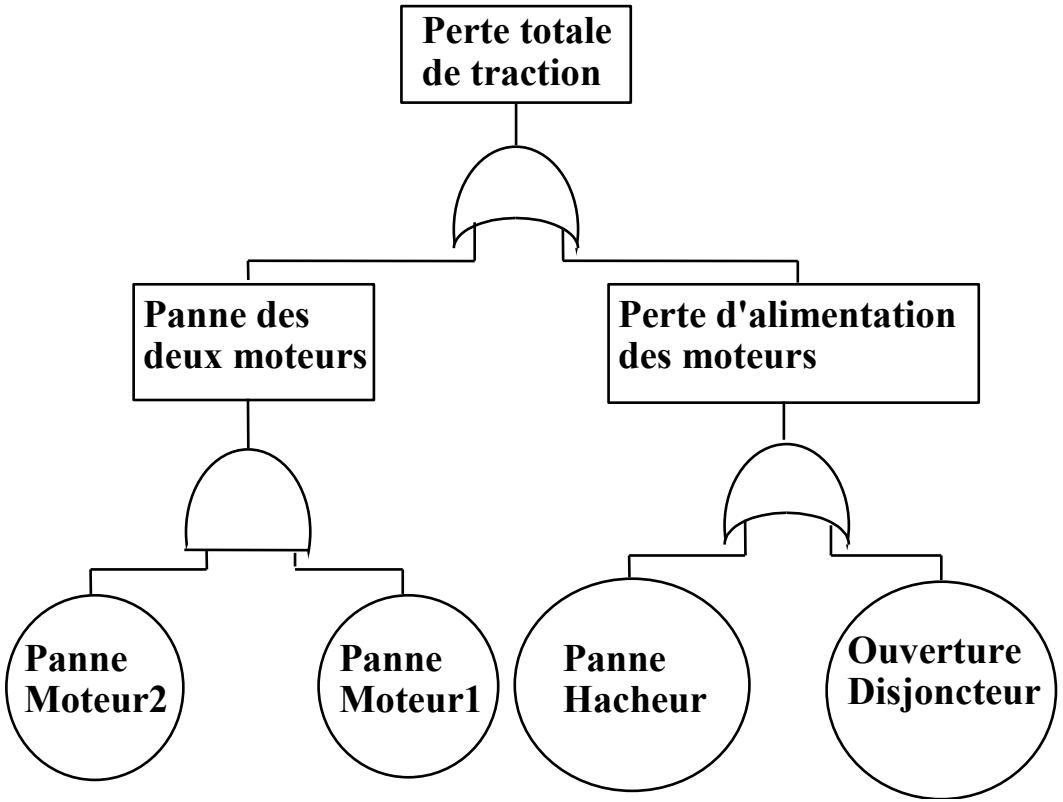


Arbres des causes

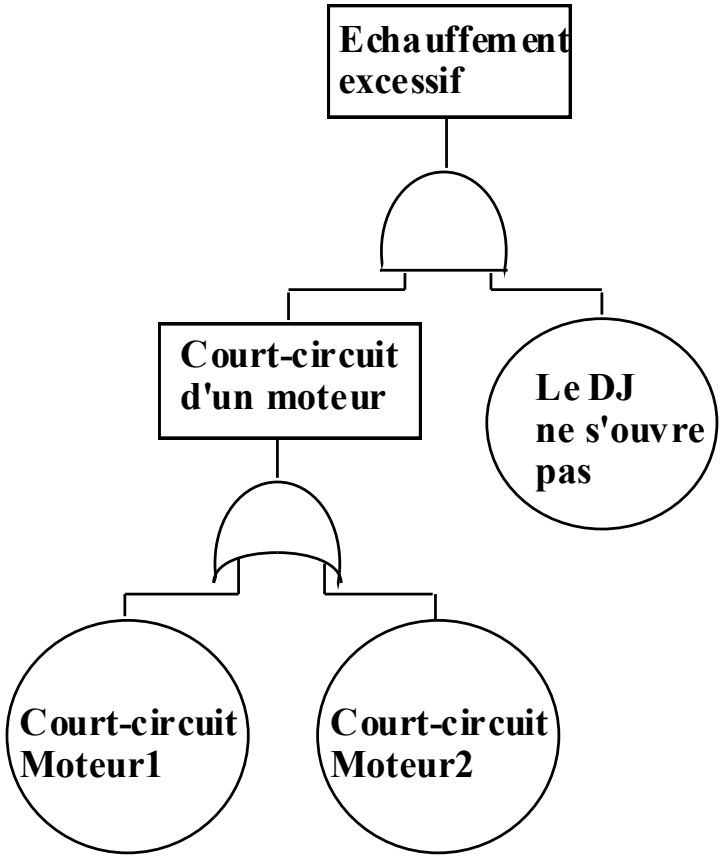
- L'événement sommet est progressivement décomposé en combinaisons d'événements plus simples jusqu'à un niveau d'événements considérés comme élémentaires :



Exemple d'arbre de défaillances



Autre exemple d'arbre de défaillances



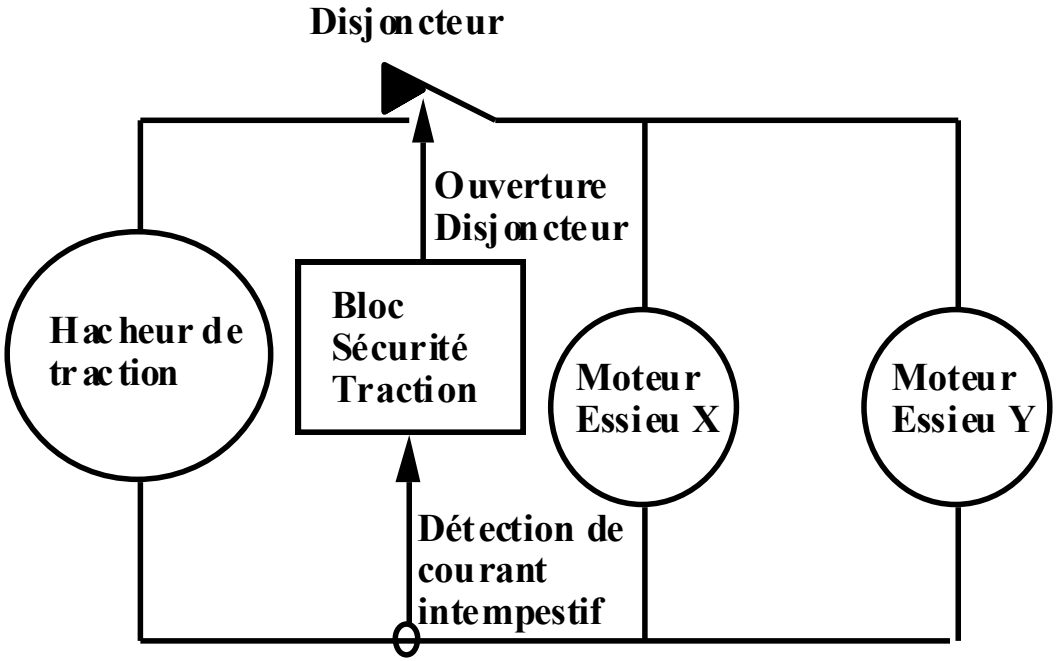
Troisième exemple d'arbre de défaillances

Rappel de l'AMDEC : un scénario catastrophique sur faute simple a été identifié. Ce type de cas (pièces critiques de sécurité) est à limiter au maximum (dans certains cas : pièces mécaniques en particulier, c'est inévitable…)

Composant	Mode de défaillance	Effet système	Détection
Hacheur de traction	Absence de courant de traction	Aucun effort de traction. Blocage en ligne pouvant nécessiter une évacuation	Immédiate (train bloqué)
	Courant de traction intempestif	Effort de traction intempestif pouvant à terme provoquer une collision	Immédiate (mais probablement trop tardive)

Troisième exemple d'arbre de défaillances

- Dans ce cas, il est possible de couvrir le scénario par un dispositif de détection dit bloc sécurité traction :

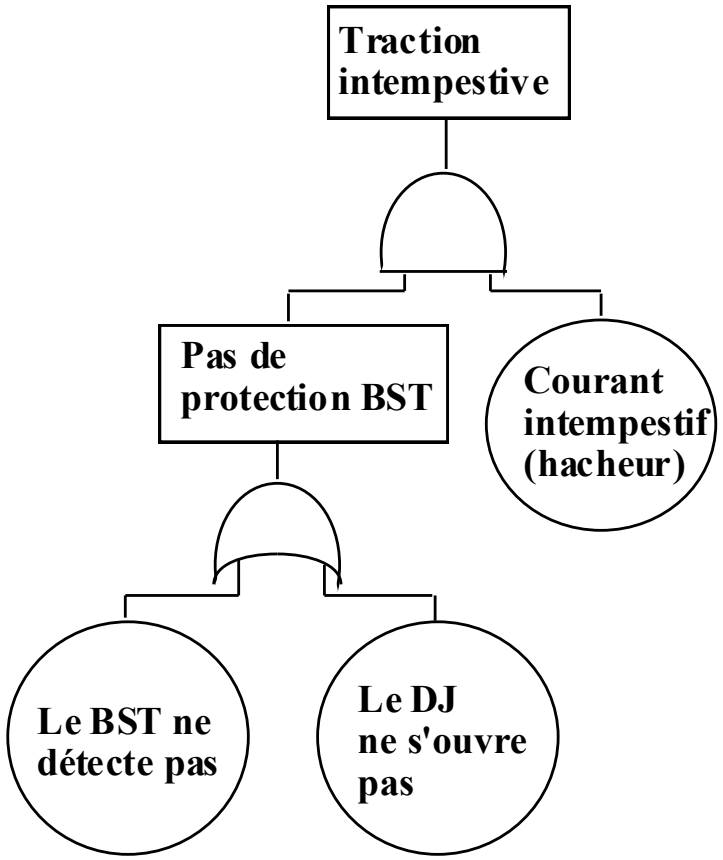


Troisième exemple d'arbre de défaillances

- Dans ce cas l'arbre relatif à l'événement de traction intempestive devient :

Attention toutefois avec ce type de couverture de scénarios : les défaillances des organes de détection sont souvent des fautes dormantes, qui ne sont détectées que lors de maintenances (temps de latence relativement longs)

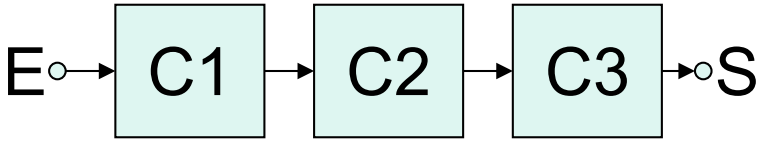
Dans le cas de cet exemple, l'organe de détection est conçu en sécurité intrinsèque : toutes ses défaillances vraisemblables sont des « fausses alarmes » contraires à la disponibilité mais pas à la sécurité.

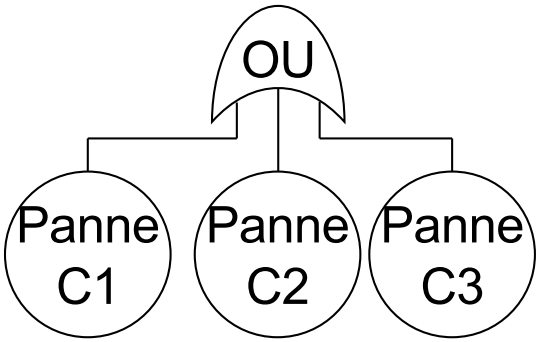


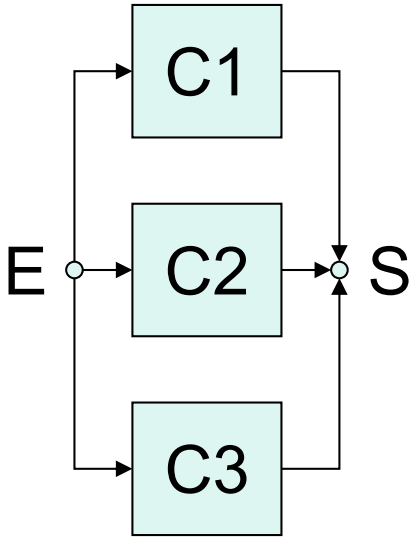
Arbres de causes et diagrammes de succès

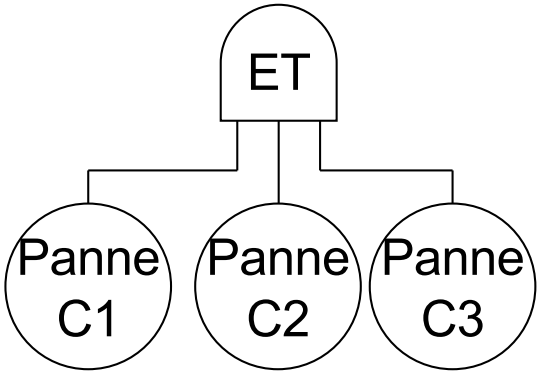
- Diagrammes de succès : ne cherchent pas à discriminer des défaillances systèmes plus ou moins graves: orientés fiabilité.
- Arbres de causes : recherche de causes conduisant à une défaillance système particulière : orientés sécurité.
- Il est possible toutefois d'établir un parallèle entre diagrammes de succès et arbres de causes dont l'événement sommet est relativement général (défaillance système sans autre précision).
- Porte OU : défaillance conséquence si l'une au moins des défaillances causes est présente : diagramme série.
- Porte ET : défaillance conséquence si toutes les défaillances causes sont présentes : diagramme parallèle.

Arbres de causes et diagrammes de succès

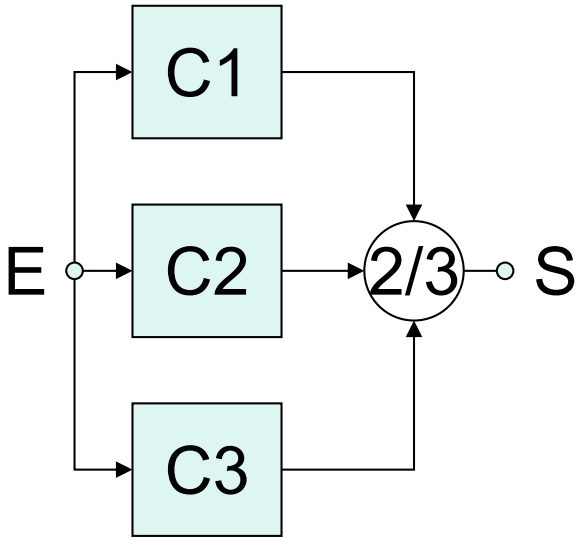


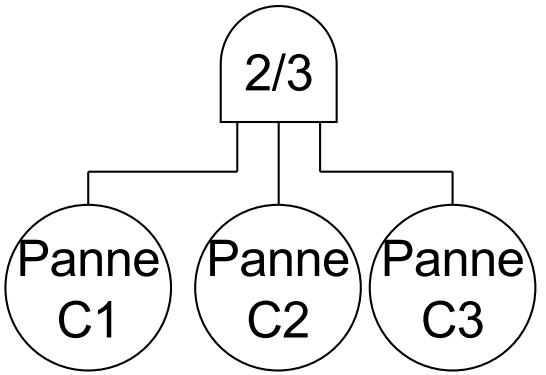






Arbres de causes et diagrammes de succès





Plus généralement :

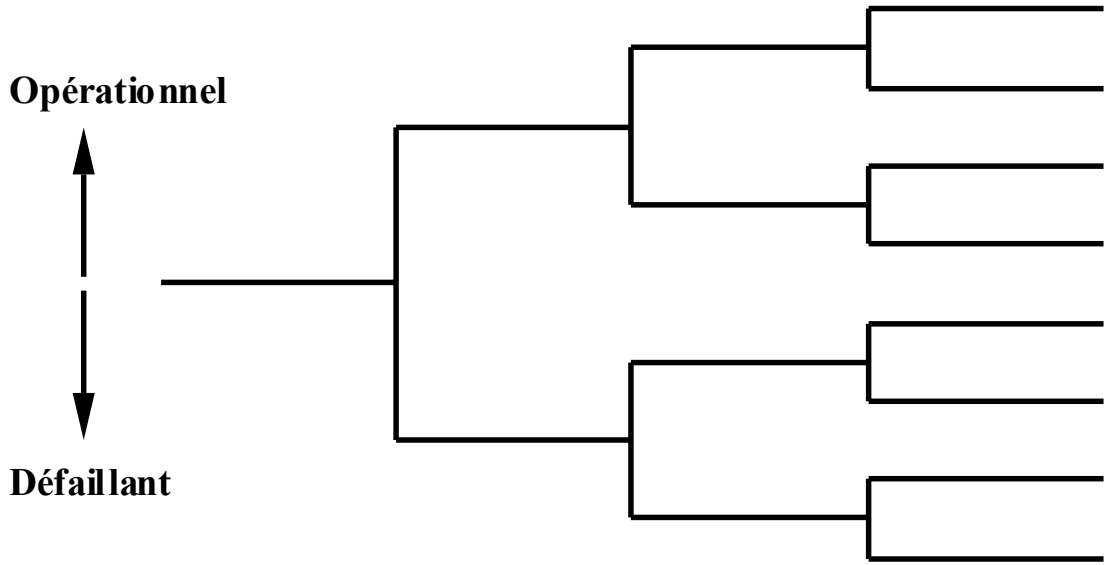
Voteur p/n : fonctionnement système si au moins p parmi n fonctionnent (au plus n-p sont en panne)

Voteur (n-p+1)/n : panne système si au moins n-p+1 parmi n sont en panne (au plus p-1 fonctionnent)

Diagrammes de conséquences

- Méthode inductive apparue dans les années 1970 pour l'étude des séquences critiques des centrales nucléaires : Étude des différentes conséquences possibles d'un même événement initiateur en fonction de l'état de systèmes élémentaires censés jouer le rôle de barrière

Evénement initiateur	Système élémentaire 1	Système élémentaire 2	Système élémentaire 3	Conséquences



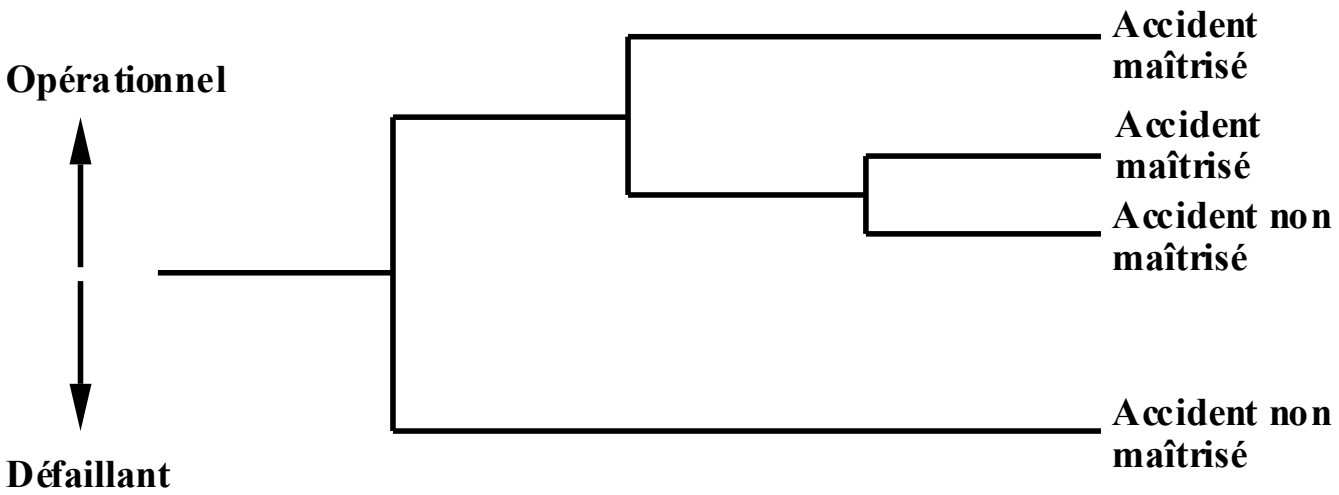
Diagrammes de conséquences

- Peuvent devenir rapidement volumineux (potentiellement 2^n branches pour n systèmes élémentaires)
- Peuvent toutefois être simplifiés en tenant compte :
  - Des aspects temporels : les barrières intervenant en premier doivent être envisagées en premier
  - Des aspects fonctionnels : les systèmes élémentaires conditionnant le fonctionnement d'autres systèmes élémentaires doivent être envisagés en premier
- La sélection des systèmes élémentaires pertinents et leur classement dans un ordre pertinent permet souvent de simplifier l'arbre en « coupant » des branches inutiles.

Diagrammes de conséquences

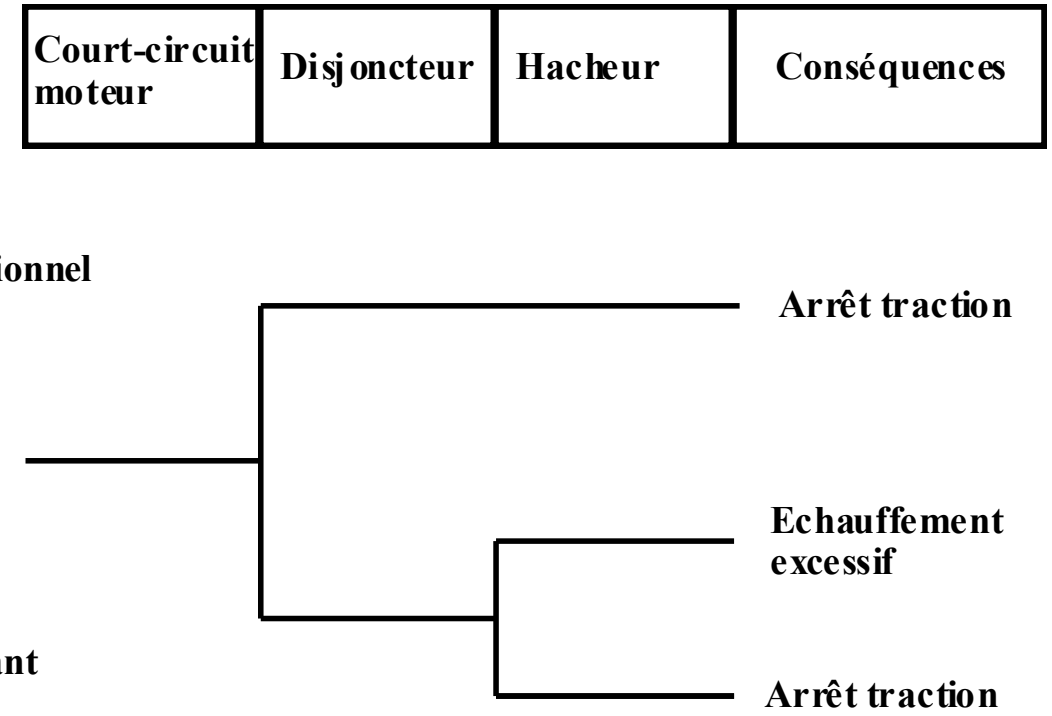
- Exemple : deux systèmes de secours dépendent fonctionnellement d'une alimentation commune

Panne du système principal	Alim. des systèmes de secours	Système de secours 1	Système de secours 2	Conséquences



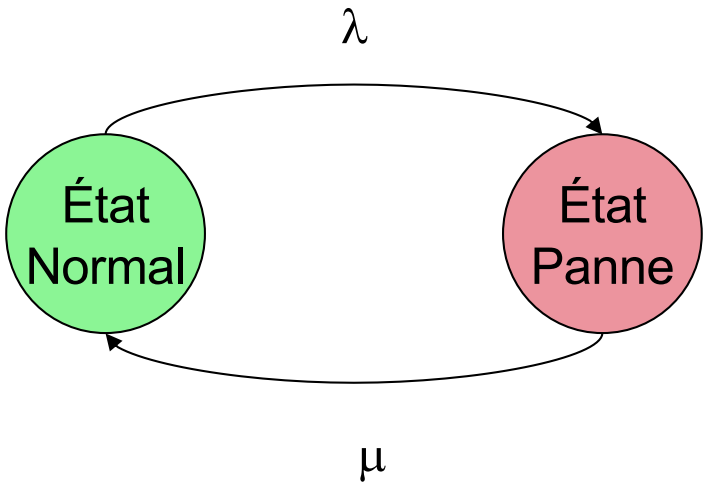
Diagrammes de conséquences : exemple simplifié

- Donne une analyse assez pertinente du scénario d'incendie auquel peut conduire notre système de traction simplifié :



Graphes d'états

- Consistent à visualiser la logique du système sous forme de graphes états transitions.
- Le graphe est dit Markovien si les taux de transition (probabilité de transition par unité de temps) sont constants
- Exemple d'un composant unique à deux états (un état normal et un état dit « panne » à λ et μ constants :



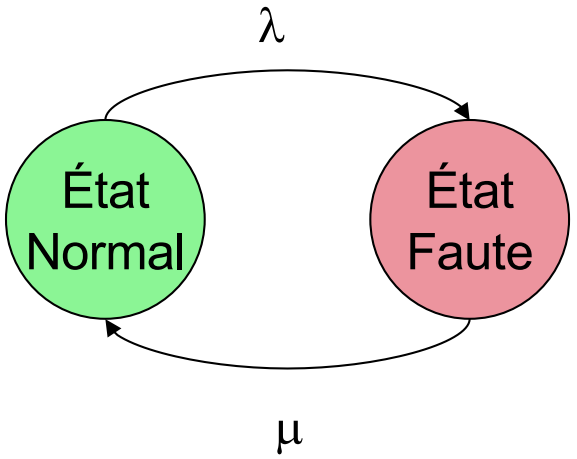
Graphes de Markov

- Très utilisés en SdF des systèmes informatiques (pour prévision de disponibilité en particulier).
- Modélisation très facile de systèmes à composants dépendants
- S'expriment et se résolvent assez facilement sous forme de systèmes d'équations différentielles linéaires à coefficients constants dans le cas Markovien) : A=P(Normal)

$$dA/dt = -\lambda A + \mu (1-A)$$

Terme de transition sortante

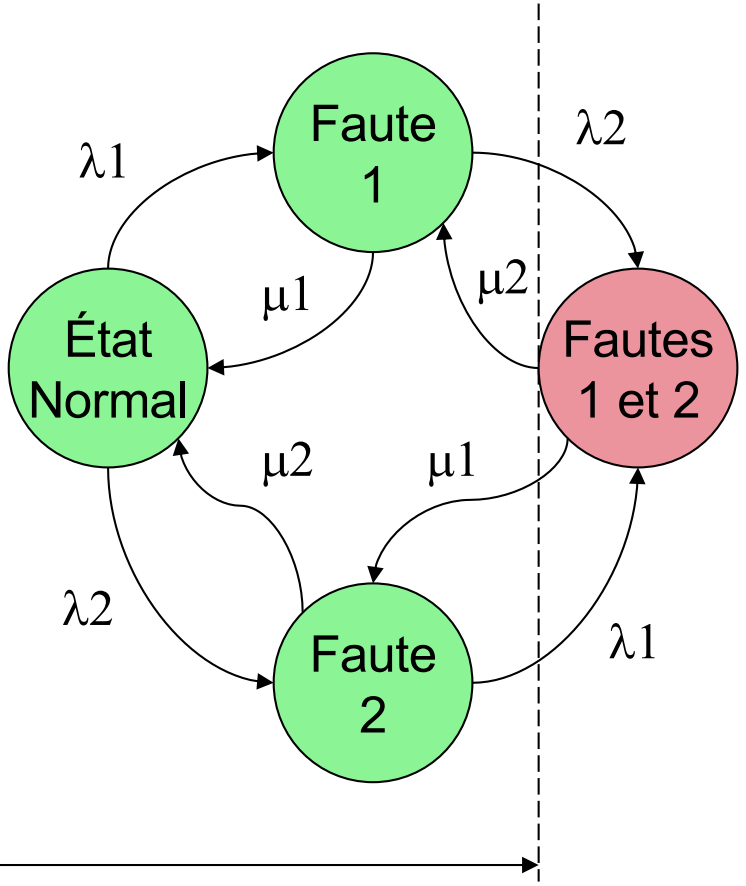
Terme de transition entrante



Graphes de Markov : Système parallèle

- Outil très puissant mais rapidement complexe (explosion combinatoire, 2^n états pour n composants) : exemple de deux composants

➢Ci-contre : cas d'un système redondant (parallèle) : le système tolère une faute : la défaillance système ne se produit qu'en cas de double faute.

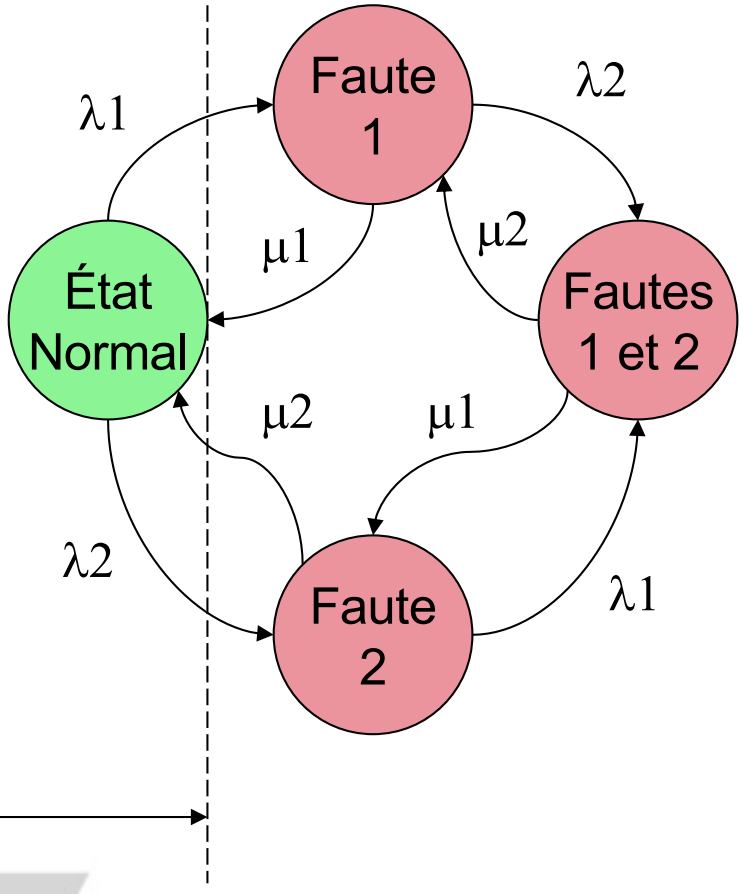


➢La « frontière » entre états défaillants et non défaillants système se situe ici :

Graphes de Markov : Système série

Le même graphe avec donc les même équations sous-jacentes (donc les même probabilités d'occupation des états en fonction du temps) permet de traduire le système « série » (non redondant)

- La « règle du jeu » de sommation de ces probabilités pour obtenir la disponibilité est simplement modifiée. Le système est défaillant dès qu'une faute est présente.
- La frontière entre états défaillants ou non se situe dans ce cas ici :



Graphes de Markov : Traitement quantitatif

- Lorsque les taux de transition sont constants (graphe dit Markovien) les probabilités d'occupation des états obéissent à un système d'équations différentielles linéaires du premier ordre à coefficients constants.
- Système facilement obtenu par « bilan des transitions » entrantes et sortantes depuis et vers chaque état.
- N états => N-1 équations (somme des probabilités =1).
- Résolution manuelle (transformation de Laplace) possible pour graphes à quelques états.
- De nombreux excellents logiciels traitent des graphes de Markov jusqu'à environ quelques centaines d'états.

Graphes de Markov : Systèmes à composants dépendants

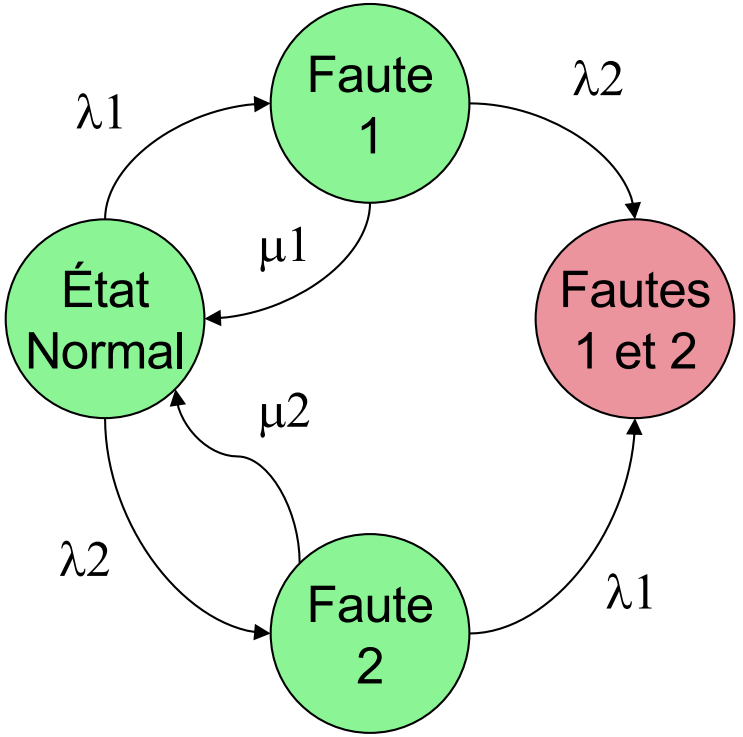
- Un des domaines privilégiés des graphes de Markov est la modélisation de systèmes composants dépendants. Exemple :
- Système composé de deux calculateurs redondants.
- La défaillance d'un calculateur est immédiatement signalée et peut être réparée sans interruption de service.
- Quelle est la probabilité pour que sur une durée donnée, le système devienne défaillant (la deuxième défaillance calculateur survenant avant d'être parvenu à réparer la première) ?
- Problème de fiabilité de système réparable.
- Composants dépendants car la défaillance d'un calculateur n'a pas les mêmes conséquences suivant l'état de l'autre.

Graphes de Markov : Fiabilité de systèmes réparables

- Modélisation simple et élégante en graphe de Markov :
- L'état de défaillance système est rendu absorbant par suppression des transitions de retour.

➢Le système d'équation différentielles s'en déduit immédiatement (plus simple que celui utilisé pour la disponibilité).

➢D'où la fiabilité recherchée (probabilité d'être à l'instant t dans l'état de défaillance système).

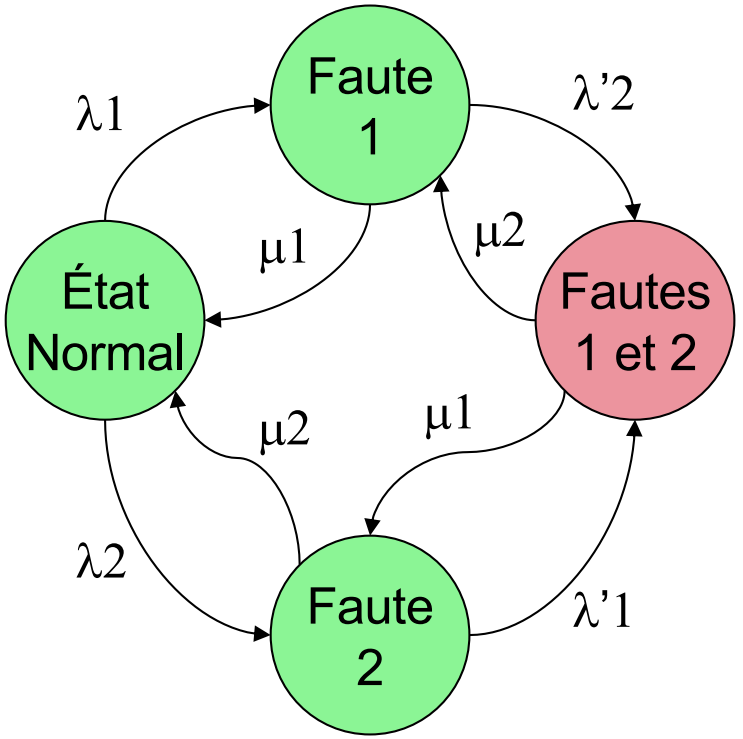


Graphes de Markov : Taux de défaillance dépendant de l'état d'un autre composant

- Autre exemple : on revient à un problème de disponibilité d'un système à deux composants redondants :

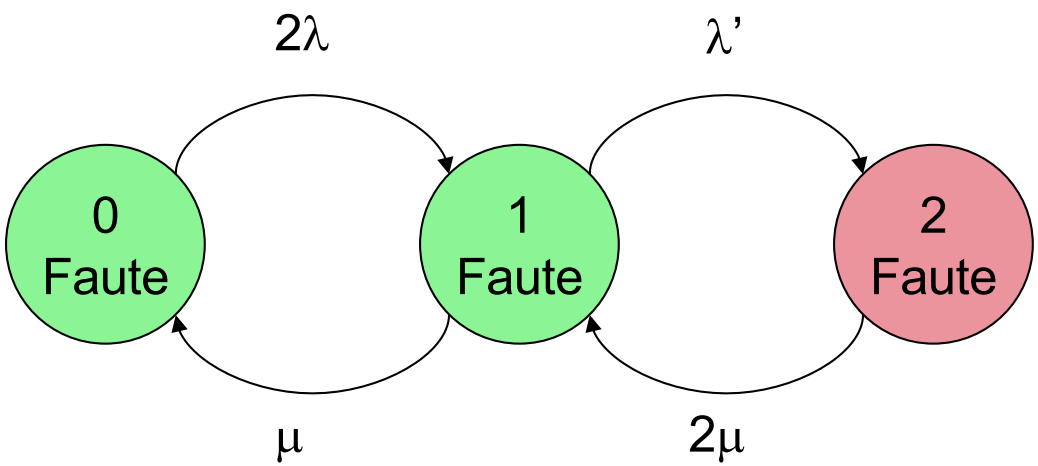
➢Lorsque les deux composants sont opérationnels leurs taux de défaillance sont λ1 et λ2

➢En cas de défaillance de l'un d'entre eux, le survivant est davantage sollicité (taux de défaillance λ'1 et λ'2)



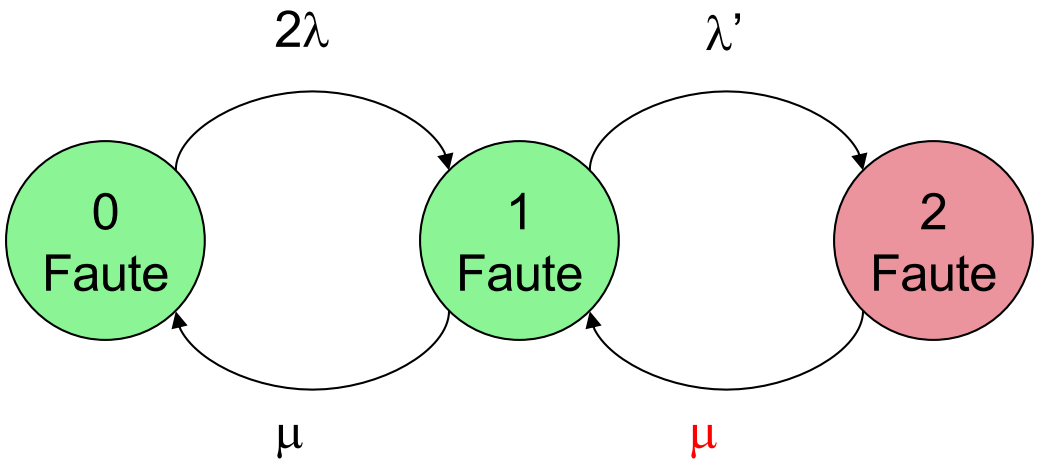
Graphes de Markov : Simplifications lorsque les composants sont identiques

- Lorsque les deux composants sont identiques, il est possible de simplifier le diagramme précédent en fusionnant les deux état à une faute :



Graphes de Markov : Cas d'un réparateur unique

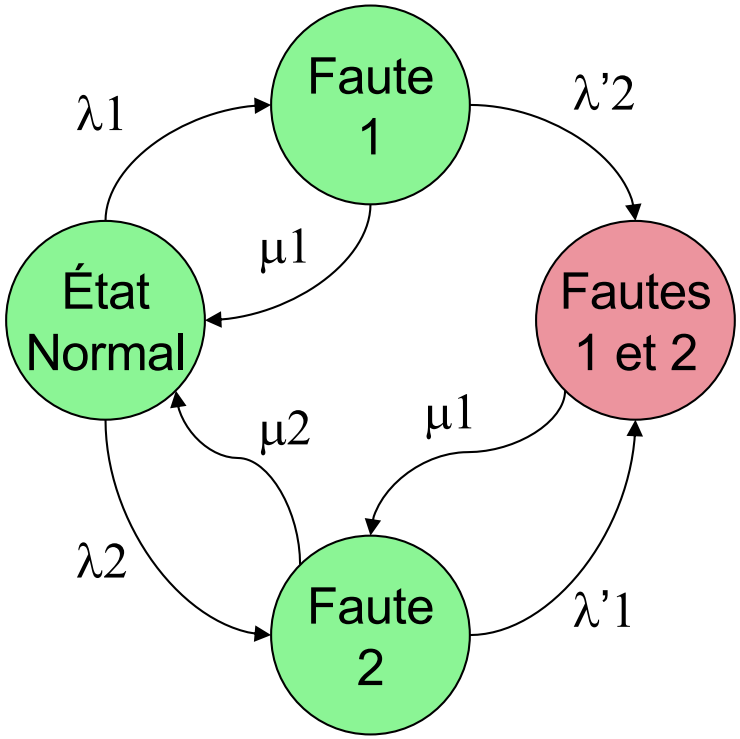
- On voit clairement l'hypothèse sous-jacente au graphe précédent : les réparations des deux composants sont indépendantes (il y a donc 2 réparateurs : 1 par composant).
- Lever cette hypothèse ne modifie que très peu le graphe de Markov (et donc son traitement quantitatif) :



Graphes de Markov : Politique de maintenance

- Si les composants ne sont pas identiques, il est nécessaire de préciser la politique de maintenance : quel composant réparer en premier si les deux sont défaillants ?

➢ La première politique possible (privilégier 1 par exemple) a pour inconvénient que l'on abandonne la réparation (commencée) de 2 si c'est celui qui est devenu défaillant en premier.



Graphes de Markov : Politique de maintenance

- Une politique plus usuelle (premier en panne premier réparé) nécessite de complexifier un peu le graphe :