SAINT-MALO
11 au 13 octobre 2016

Tutoriel A1 Fondamentaux et méthodes de base de la Sûreté de Fonctionnement

MAÎTRISER LES RISQUES DANS UN MONDE EN MOUVEMENT

Sandrine CHRUN
SETEC
Jean-Marie CLOAREC
SYSTRA

IMdR Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Plan du Tutoriel

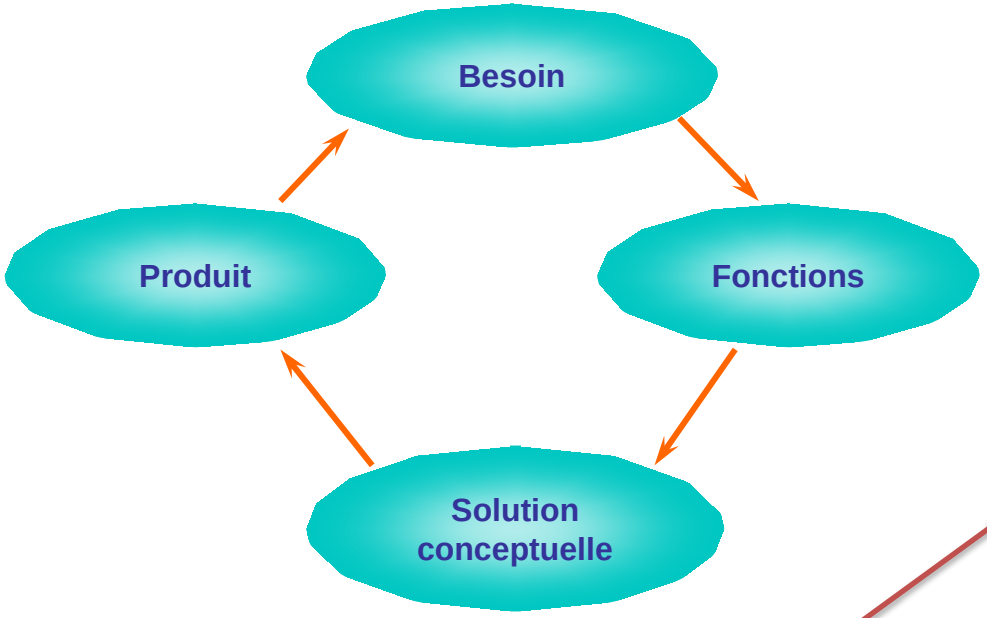
- **Analyse Fonctionnelle :** années 1980
- **Analyse Préliminaire des Risques :** 1960
- **AMDEC :** 1960
- **Analyse de Zone :** 1960
- **Arbre de Défaillances :** 1962
- **Arbre d'Événements :** 1974
- **Réseaux de Petri :** 1962
- **Graphes de Markov :** 1970
- **Conclusions**

ANALYSE FONCTIONNELLE

Analyse Fonctionnelle
Objectifs

- Exprimer le juste besoin de l'utilisateur.
- Décrire la mission du produit.
- Déterminer les fonctions de service à satisfaire.
- Ordonner, caractériser, hiérarchiser les fonctions.
- Identifier les contraintes liées à l'environnement.
- Choisir les solutions techniques qui répondent le mieux au besoin.

AF Externe et AF Interne



2 aspects complémentaires

Analyse fonctionnelle externe :

Expression fonctionnelle du besoin (CdCF)

Analyse fonctionnelle interne :

Validation fonctionnelle d'une solution technique

Les étapes de l'AF

1- Expression du besoin

2- Identification des fonctions de service

3- Identification des fonctions techniques

4- Ordonnancement des fonctions

5- Caractérisation des fonctions

Méthodes

Il n’existe pas UNE mais DES méthodes d’analyse fonctionnelle, qui se différencient par :

- la façon d’appréhender le système étudié,
- leur mode de représentation.

L’utilisation des méthodes dépend :

- de la NATURE du système,
- et du BUT de l’étude.

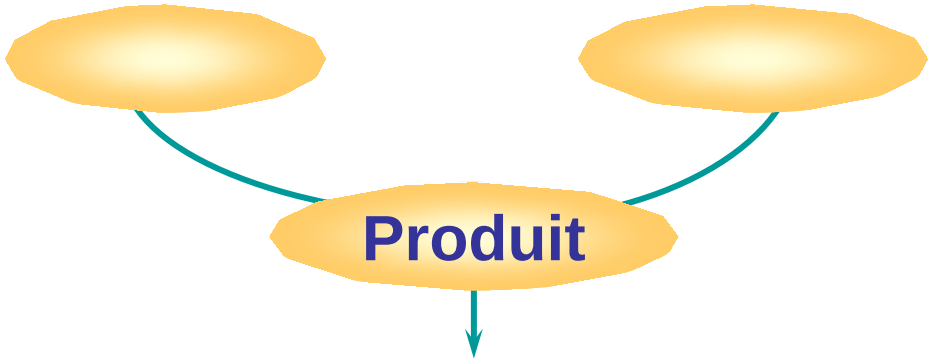
Méthodes

Méthodes d'AF les plus utilisées :

- **MISME** (Méthode d'Inventaire Systématique du Milieu Environnant)
- **APTE**
- **Schémas de Flux**
- **SADT** (Structured Analysis and Design Technic)
- **Arbre fonctionnel** (RELIASEP□)
- **MERISE**

1 – Expression du besoin

À qui rend-il service ?



Sur quoi agit-il ?

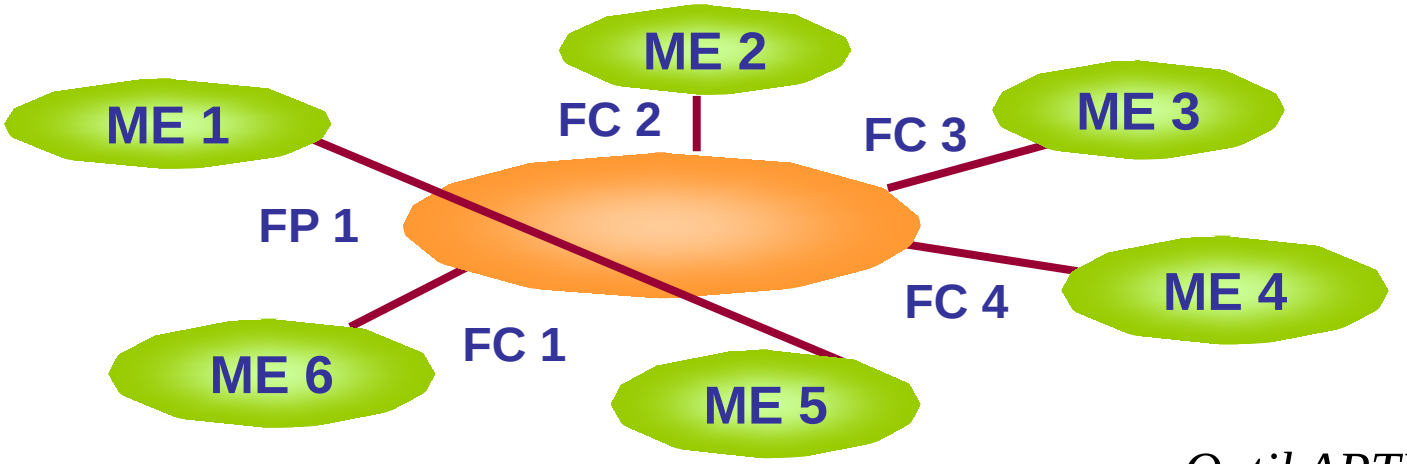
Dans quel but ?

Outil APTE®
"la bête à cornes"

Contrôle de validité :

- Pourquoi ce besoin existe-t-il ?
- Qu'est-ce qui pourrait le faire disparaître ?
- Qu'est-ce qui pourrait le faire évoluer ?

2 – Fonctions de service



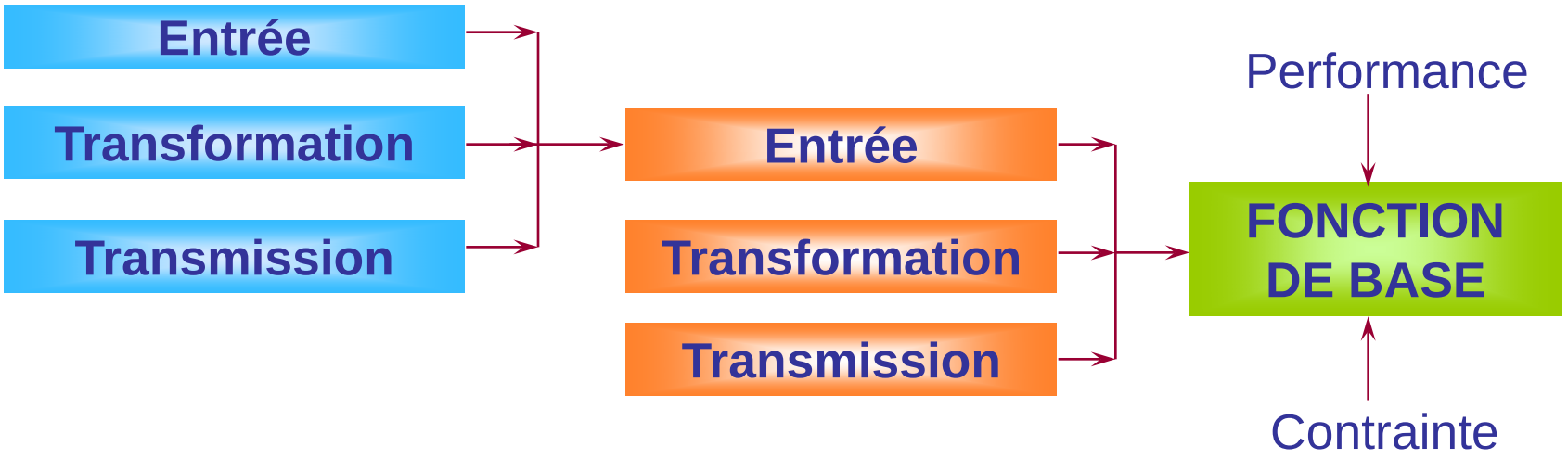
Outil APTE®
"la pieuvre"

ME : Milieux environnants en relation avec le système

FP : Fonctions principales, répondant au besoin

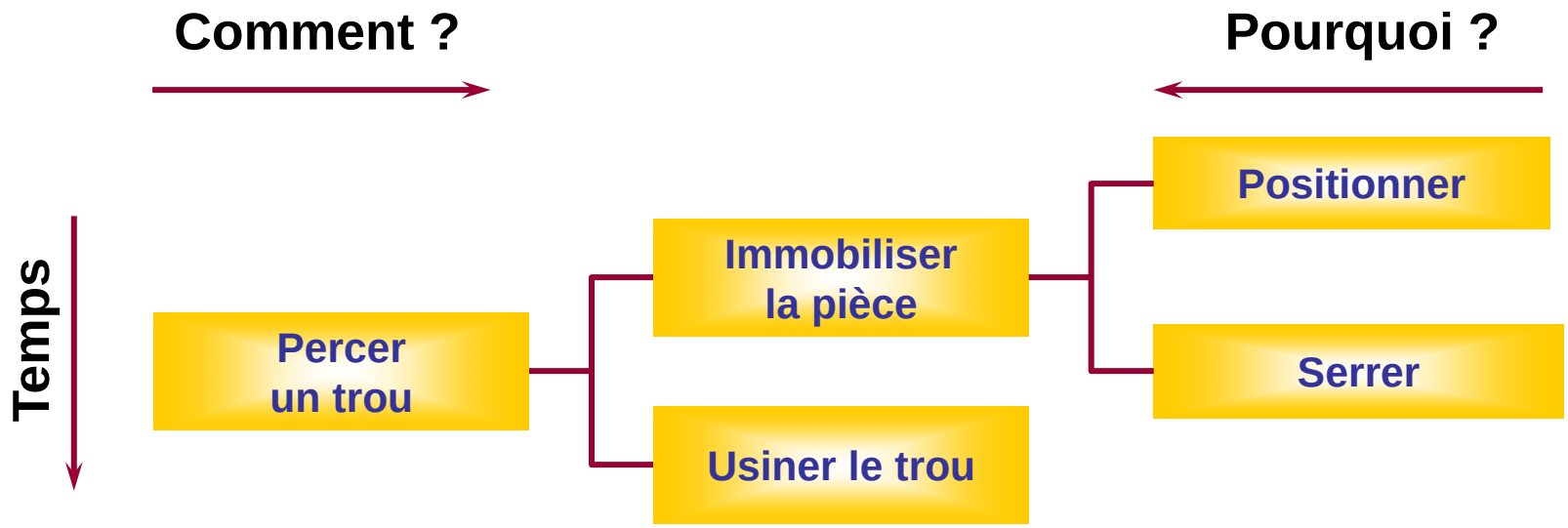
FC : Fonctions de contraintes, nécessaires compte tenu des ME

3 – Fonctions techniques



"ARBRE FONCTIONNEL"
de la méthode RELIASEP®

4 – Ordonnancement



Arborescence fonctionnelle
diagramme FAST

5 – Caractérisation des fonctions

Fonction	Critère d'appréciation	Niveau	Flexibilité
Régler la distance	Distance	10 mm	+/- 1 mm
Connecter au réseau	Norme / tension	NF C15-100 220 v	0 + 20 V

Exemple

Cafetière électrique

Phases d'utilisation :

- **Utilisation normale**
  - Préparation
  - Mise sous tension
  - Réalisation café
  - Maintien à bonne température
  - Service café
  - Mise hors service
- **Rangement**
- **Entretien, nettoyage, détartrage**

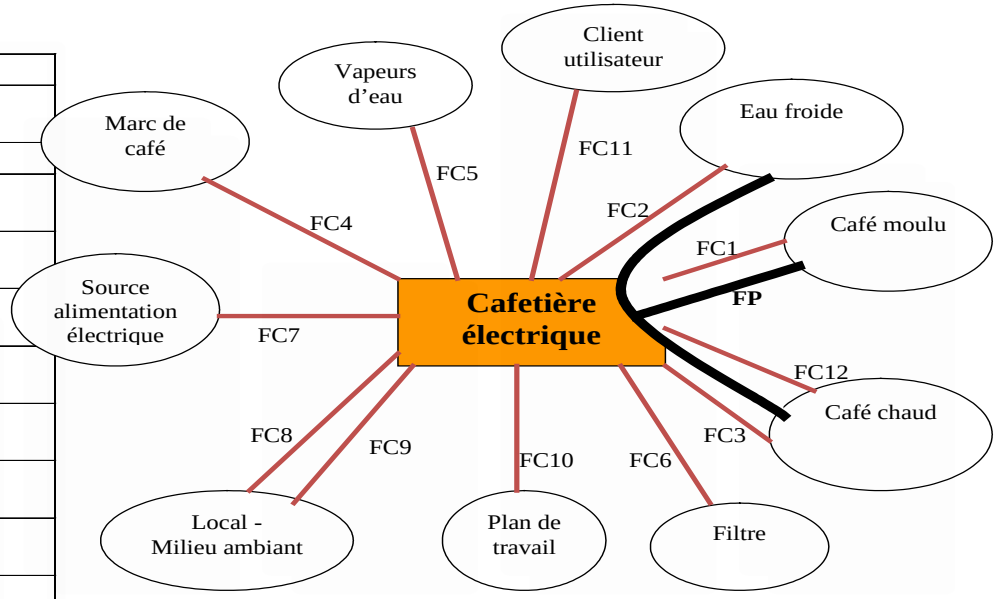
AF Externe

AF externe (CdCF) :

- Identification des milieux extérieurs (sources de défaillances),
- Définition des fonctions de service à assurer et des événements redoutés associés,
- Spécification des objectifs de SdF (F, M, D, S…),
- Définition des contraintes.

Exemple : AF externe

Fonction principale	
FP	Produire du café chaud à partir d'eau et de café moulu Débit, volume, température, qualité gustative …
Fonctions de contraintes	
FC1	Permettre le remplissage de café moulu Facilité, quantité contrôlée …
FC2	Permettre le remplissage de l'eau froide Facilité, quantité contrôlée …
FC3	Permettre le service du café chaud Facilité, sécurité …
FC4	Permettre l'évacuation du marc de café Facilité …
FC5	Réduire l'émanation des vapeurs d'eau Confinement …
FC6	Permettre le changement du filtre Mise en place, retirage, facilité …
FC7	Etre adapté à la source d'énergie électrique Consommation maximum …
FC8	Eviter la pollution du local Etanchéité …
FC9	Résister au milieu ambiant Protection contre les poussières …
FC10	Etre posé sur un plan de travail Stabilité, non agressivité …
FC11	Etre adapté au client utilisateur Facilité d'utilisation, sécurité, entretien, ergonomie, esthétique …
FC12	Maintenir le café chaud Température …



Fonctions de service
en phase d'utilisation normale

AF Interne

AF interne :

- Identification et caractérisation des fonctions techniques,
- Allocation des paramètres de SdF sur les sous-ensembles, fonctions techniques.

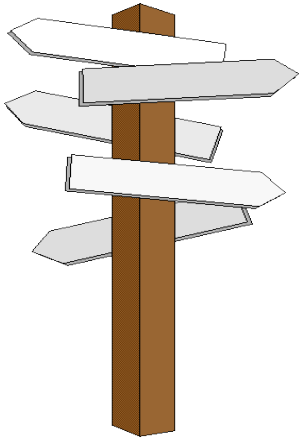
Exemple : AF Interne

Sous-ensembles fonctionnels et fonctions techniques

Sous-ensembles fonctionnels	Fonctions techniques
Structure enveloppe	❑ Support ❑ Liaison
Chauffage eau	❑ Alimentation électrique ❑ Isolation électrique ❑ Production chaleur ❑ Régulation chaleur ❑ Transmission chaleur ❑ Isolation thermique
Transfert eau	❑ Réception eau froide ❑ Stockage eau froide ❑ Circulation eau ❑ Circulation vapeur ❑ Condensation vapeur ❑ Confinement vapeur
Percolation eau-café	❑ Réception filtre et café moulu ❑ Percolation eau-café ❑ Filtrage ❑ Obturation ❑ Evacuation marc de café
Recueil-Service café	❑ Verseuse

AF = Point de départ pour beaucoup de méthodes

- Analyse de la Valeur.
- Analyse des Défaillances.
- Analyse des Risques.
- Étude de Fiabilité, Maintenabilité, Disponibilité, Sécurité.
- ...



ANALYSE PRÉLIMINAIRE DES RISQUES

Analyse préliminaire des Risques

Objectif : mise en évidence et étude des dysfonctionnements susceptibles d'apparaître :

- Identifier les fonctions & éléments potentiellement à risque et les Événements Indésirables (EI) associés
- Caractériser les EI en termes de scénarios d'apparition et de gravité

Principes de mise en œuvre

L'APR peut s'effectuer dès la phase exploratoire :

- dès que l'on connaît les fonctions à remplir par le système,
- dès que l'on connaît les grands choix technologiques.

Elle est effectuée en groupe de travail.

Utilisation de REx sur autres projets (pertinence ?).

Données d’entrée

- Les fonctions à remplir par le système.
- Comment le système va vivre, être utilisé (Profil de mission/vie, exemple : satellite).
- La description et la délimitation du système (Arborescence Technique, Organisation Industrielle, schéma d’architecture et des interfaces).

Gravité

1. Mineure	• Ni dégradation sensible des performances du système • Ni interruption de la mission • Ni blessure de personnes • Ni endommagement notable des biens ou du système
2. Significative	• Dégradation sensible des performances du système pouvant entraîner l'interruption de la mission • Pas de blessure de personnes • Ni endommagement notable des biens ou du système • Pas nécessaire d'entreprendre une action corrective
3. Critique	• Il peut y avoir blessure de personnes et/ou endommagement notable de biens ou du système
4. Catastrophique	• Destruction du système et/ou plusieurs blessés graves et/ou mort de personnes

Fréquence

1. Fréquent ou peu fréquent	Événement dont la probabilité est comprise entre 10^{-5} et 10^{-3} par heure.
2. Rare	Événement dont la probabilité est comprise entre 10^{-7} et 10^{-5} par heure.
3. Extrêmement rare	Événement dont la probabilité est comprise entre 10^{-9} et 10^{-7} par heure.
4. Extrêmement improbable	Événement dont la probabilité est inférieure à 10^{-9} par heure.

Mesures de réduction des risques

Diminution de la PROBABILITÉ d'apparition de l'EI :

- Actions dans le domaine de la PRÉVENTION

Diminution de la GRAVITÉ de l'EI :

- Actions dans le domaine de la PROTECTION

Exemple : Tramway

N°	Repère	Événement Redouté	Situation potentielle dangereuse	G	Causes	Entité dangereu	Exigence de sécurité	Responsable
	1.1	**Collision avec obstacle fixe**						
1	**1.1.1**	Collision avec obstacle fixe	**Engagement du GLO (Gabarit Limite d'Obstacle)**	4	Mauvais dimensionnement des infrastructures	INFRA	Le GLO doit être pris en compte lors de la conception des infrastructures	MOEG
2	1.1.1	Collision avec obstacle fixe	Engagement du GLO (Gabarit Limite d'Obstacle)	4	Mauvais positionnement des équipements	SIGF, VOIE, SLT, ENER	Le positionnement des équipements devra respecter les recommandations du guide STRMTG "Guide d'implantation des obstacles fixes à proximité des intersections tramways /	MOEG
	1.2	**Collision avec obstacle mobile (automobile, piétons, cycliste…)**						
42	**1.2.1**	Collision avec obstacle mobile (automobile, piétons, cycliste…)	**Présence d'un véhicule routier sur la voie (voiture particulière, poids lourds, moto,**	4	Erreur du conducteur de véhicule routier	URB	La conception devra matérialiser le GLO: contraste délimitant le site propre soit par matériaux, soit par finitions différentes	MOEG

Note : dans cet exemple, la probabilité n'a pas été estimée.

Stratégie de traitement de l'EI

Hiérarchiser

- On choisit le juste nécessaire pour traiter les EI en fonction de :
  - l'expérience,
  - le couple (gravité, probabilité).

Stratégie de traitement de l'EI

Définir le type de traitement :

- Comment s'assure-t-on que l'EI est maîtrisé ?
  - apport des connaissances du spécialiste,
  - accord du groupe de travail.
- Confirmation par tests, dire d'experts.

Conseils sur la méthode

- Disposer de données d'entrée justes, complètes et précises.
- Ne pas se laisser influencer (« il y a peu de chances que cela se produise », « cela ne peut pas arriver »).
- Même si P(EI) = ε, l'essentiel est de l'avoir identifié et de le formaliser.
- Bien préciser l'EI, sinon traitement difficile (ex : « mécontentement client »).

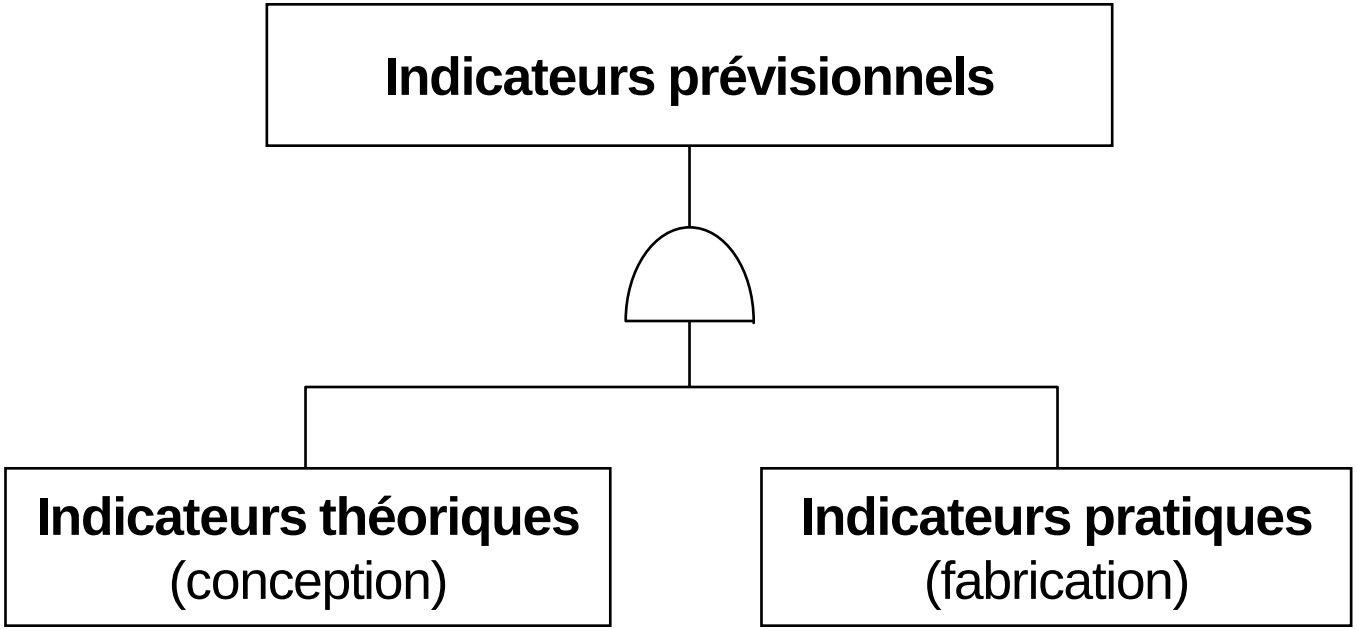
Cotation en gravité des EI :

- Doit être issue d'un consensus et de l'expérience.
- Revoir/revalider la cotation en fin d'APR.
- Éviter de corréler gravité et probabilité (« ce n'est pas grave car c'est peu probable »).
- Pas de conclusions hâtives (« cela ne peut pas être grave car le système n'est pas un organe de sécurité »).

Difficultés

- Une APR peut être plus ou moins approfondie :
  - selon le niveau de décomposition,
  - selon que l'analyse porte sur tout ou partie des éléments du système.
- *Ne pas se "noyer" dans les détails (difficulté pour remonter au niveau de l'effet système et donc à identifier l'EI).*
- *Ne pas hésiter à faire appel aux spécialistes (technologies ou matériaux peu ou non connus par le métier ou dans le domaine étudié).*

Les Indicateurs : pourquoi ?



Les Indicateurs

- **Fiabilité** : MTBF, MTTF, MUT, λ, ...
- **Maintenabilité** : MTTR, MDT, ...
- **Disponibilité** : D(t), D, ...
- **Sécurité** : P(x), ...

La donnée de base de tous ces indicateurs est le «λ».

Sur quoi agissent-ils ?
- produit,
- sous-système.

À qui servent-ils ?
- concepteur,
- décideur,
- chef projet.

Indicateurs de S.d.F.

Estimer :
- la fiabilité,
- la maintenabilité,
- la disponibilité,
- le niveau de sécurité du produit

Fournir des objectifs aux concepteurs, aux sous-traitants, ...

Comparer les résultats aux objectifs

Dans quel but ?

PAS DE MATHS !!!!

AMDEC

AMDEC — Définition

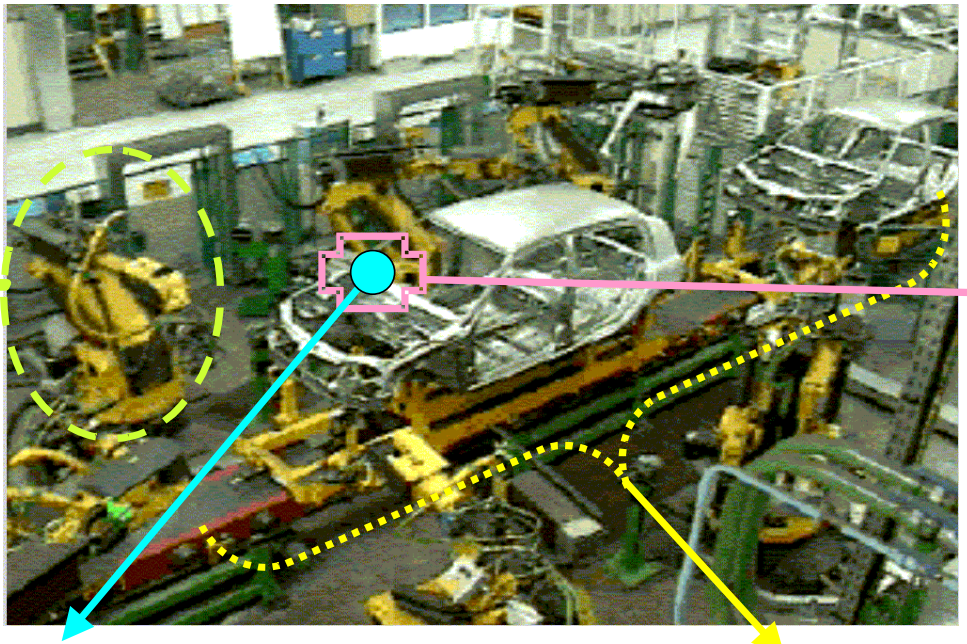
- Technique d’analyse inductive et systématique des défaillances des systèmes industriels, permettant leur hiérarchisation et la recherche d’améliorations adaptées.

- Méthode faisant appel aux compétences pluridisciplinaires d’un groupe de travail.

AMDEC et Cycle de Vie

Développement, amélioration d'un produit

Conception du produit → Industrialisation du produit → Conception du moyen de production



AMDEC Moyens

AMDEC Système/ Interface

AMDEC Produit

AMDEC Processus

Démarche AMDEC

- **Phase 1 :** Analyse qualitative des dysfonctionnements.
- *Identifier les mécanismes de défaillance de manière exhaustive pour chaque élément (ou fonction technique) du système.*
  - Modes de défaillance potentiels ou réels
  - Causes possibles
  - Effets sur le système et sur l'utilisateur
  - Moyens de détection

- **Phase 2 :** Évaluation de la criticité.
- *Affecter un niveau de criticité à chaque défaillance.*
- *Déterminer les défaillances critiques (par rapport à un seuil prédéfini).*
- 2 ou 3 critères :
  - F : Fréquence d'apparition de la défaillance
  - G : Gravité des effets de la défaillance
  - D : Probabilité de non-détection de la défaillance (apport de l'automobile)

Défaillance

IEC 61508-4 :

- **Défaillance systématique :**
  reliée de manière déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception, du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs.
- **Défaillance aléatoire :**
  survenant de manière aléatoire et résultant de divers mécanismes de dégradation au sein du matériel. Les taux de défaillance aléatoire peuvent être quantifiés.

Évaluation des Défaillances

Fréquence

Exemple 1

1. Un incident maximum toléré durant toute la vie du système.
2. Quelques incidents durant la vie du système.
3. Quelques incidents par an.
4. Quelques incidents par mois.
5. Quelques incidents par semaine.

Exemple 2

1. Il n'est pas raisonnable de prévoir une défaillance.
2. Défaillances occasionnelles observées en proportions réduites.
3. Défaillance notoire.
4. Quasi certitude.

Évaluation des Défaillances

Gravité

Exemple 1

1. Aucune incidence sur le produit.
2. Produit récupérable moyennant une légère reprise.
3. Opérations importantes de récupération du produit.
4. Perte de produit irrécupérable.
5. Perte importante de produit irrécupérable.

Exemple 2

1. Le client n'est pas en mesure de déceler le défaut.
2. Légère gêne, baisse des performances du produit.
3. Insatisfaction, dégradation des performances.
4. Mécontentement, produit hors d'état de marche.
5. Problèmes potentiels de sécurité.

Évaluation des Défaillances

Non-détection

Exemple 1	Exemple 2
1. Incident signalé en clair.	1. Le défaut affecte une caractéristique évidente à déceler.
2. Localisation de l'incident signalé en clair.	2. Le défaut affecte une caractéristique facile à identifier.
3. Opérateur à proximité.	3. Le défaut affecte une caractéristique délicate à identifier.
4. Aucun moyen de détection.	4. Le défaut n'est pas apparent ou indécelable.

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secours	* Coupure * Blocage en position	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué e, position normal pour des raisons de puissance nécessaire et disponible			Modification à prévoir au niveau de l'installation

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inver e source	Basculement automatique rs	* Coupure * Blocage en position	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué e, position normal pour des raisons de puissance nécessaire et disponible			Modification à prévoir au niveau de l'installation

Composant : Groupe électrogène

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secou	Coupure ocage ition	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué e, position normal pour des raisons de puissance nécessaire et disponible			Modification à prévoir au niveau de l'installation

Fonction : alimentation du site de la société en cas de panne du réseau EdF

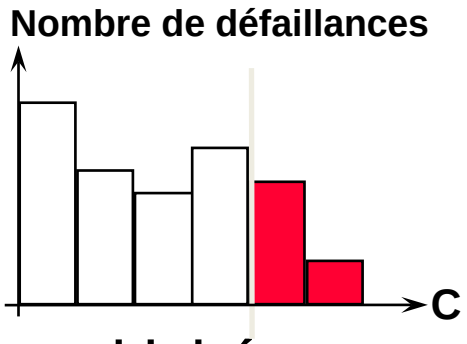
Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Mode	cause		urs en cas éseau. ment lant 10 min nomie de	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secours	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service		rseur de oqué e, al pour e puissance disponible			Modification à prévoir au niveau de l'installation

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur			ières s de liers
Tableau inverseur de source	Basculement automatique normal - secours	* Coupure * Blocage en position	Non basculement Incident dans le tableau					évoir

- **Phase 3 :** Proposition d'actions correctives
- *Diminuer la criticité des défaillances en proposant des actions adaptées de conception, fabrication, exploitation…*
- Recherche des actions à engager :
  - prévention de la défaillance
  - détection de la cause
  - réduction des effets



- Évaluation prévisionnelle de la nouvelle criticité.

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secours	* Coupure * Blocage en position	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué e, position normal pour des raisons de puissance nécessaire et disponible			cation à prévoir eau de lation

Détection : Alarmes locale et centralisée

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secours	* Coupure * Blocage en position	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué e, position normal pour des raisons de puissance nécessaire et disponible			voir

Compensation : Informatique sur onduleurs (autonomie de 10 minutes)

Exemple

Composant ou sous-ensemble	Fonction	Défaillance		Effet		Détection	Compensation	Observations
		Mode	cause	Local	Système			
Groupe électrogène	Alimentation en cas de panne du réseau	Non démarrage ou arrêt intempestif	* Pas d'alimentation fioul * Démarreur hors service * Armoire hors service	GE hors service	* Pas de secours en cas de perte du réseau. * Fonctionnement possible pendant 10 min grâce à l'autonomie de l'onduleur	Alarme locale et centralisée	Onduleur : autonomie 10 min	* Operations de maintenance et d'entretien régulières * Prévoir des tests de démarrages réguliers
Tableau inverseur de source	Basculement automatique normal - secours	* Coupure * Blocage en position	Non basculement Incident dans le tableau	Perte basculement normal - secours	Aucun : l'inverseur de source est bloqué position normal p des raisons de pu nécessaire et dis			Modification à prévoir eau de llation

Observations : Opérations de maintenance et d'entretien régulières prévues

- **Phase 4 :** Synthèse de l'étude/décisions
- *Effectuer un bilan, décider et lancer les actions à effectuer.*
  - Hiérarchisation des défaillances
  - Liste des points critiques
  - Choix des actions à engager
  - Délais
  - Responsables

De l'AMDEC subie à l'AMDEC maîtrisée

C'est trop long !

- Réaliser une AMDEC efficace demande du temps.
- Nécessité de préparer les réunions.

Jusqu'à quel niveau de détail descendre ?

- À définir selon l'objectif.
- Déterminer les sous-ensembles critiques par l'APR.
- S'appuyer sur l'analyse fonctionnelle.

De l’AMDEC subie à l’AMDEC maîtrisée

Comment identifier et quantifier les défaillances potentielles ?

- Exploiter les études antérieures, les bases de données, les informations du SAV.

Autres applications

Risques projets.

Maintenance :

- OMF : Optimisation de la Maintenance par la Fiabilité
- RCM : Reliability Centered Maintenance

Sécurité.

Organisations.

Procédures : ADP :
Analyse des procédures (RATP), …

AMDEC – Conclusion

AMDEC = Support à la réflexion, à l'analyse

- Support de capitalisation,
- Aide à la décision,
- Outil de progrès permanent,
- Vecteur de communication.

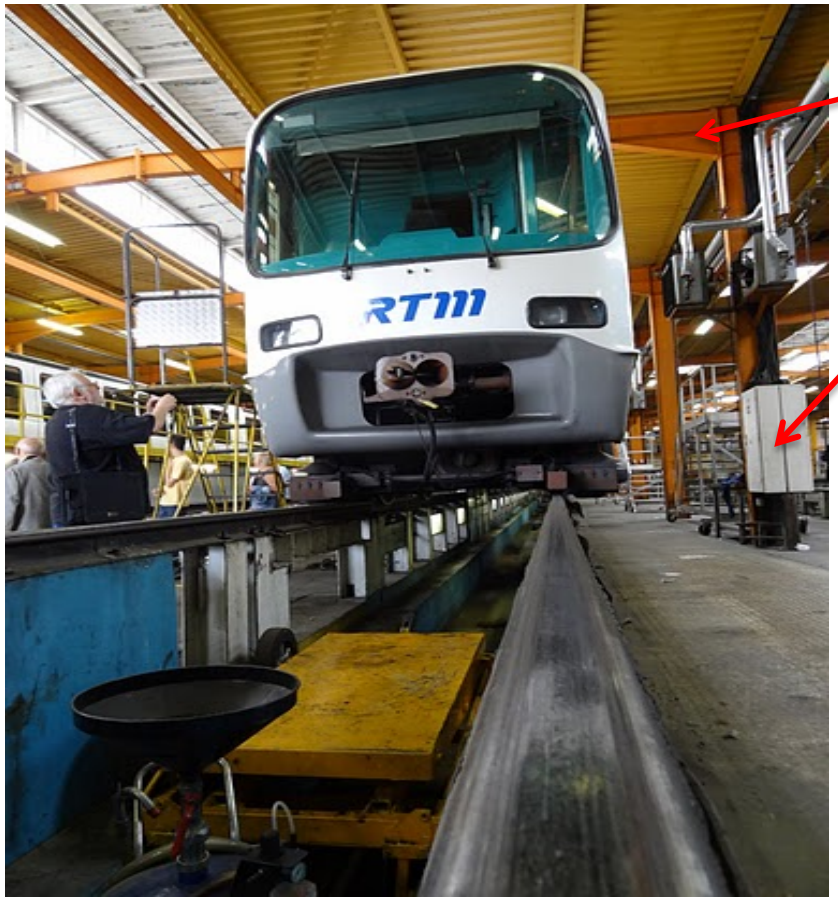
- C'est une méthode qui, au fur et à mesure qu'on la pratique, s'avère un outil extrêmement puissant, à condition de ne pas sortir des limites dans lesquelles elle doit être menée.

ANALYSE DE ZONE

Analyse de Zone

Analyser les risques liés :

- à la disposition géographique des matériels,
- aux conditions d'accès,
- au repérage des éléments,
- aux interactions physiques (émissions thermiques, bruit acoustique, nœuds de vibration, EMC, ...),
- aux fausses redondances (DC10),
- aux incompatibilités (couplage électrochimique, stray current).



Pont roulant

Électricité

Résultats

- Effets des flux perturbateurs sur les différentes zones du produit ou sur le milieu extérieur.
- Défaillances de causes communes.
- Actions correctives ou essais à entreprendre.
- Préparation d'études spécifiques
  (ex : analyses de risques particuliers :
  feu, explosions, contamination, …).

Pros & Cons

Avantages

- Mise en évidence de problèmes non détectables par les analyses papier.

Inconvénients

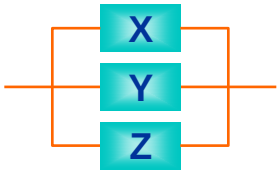
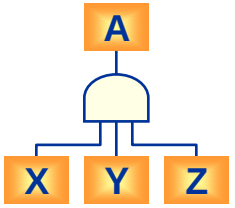
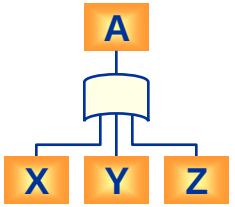
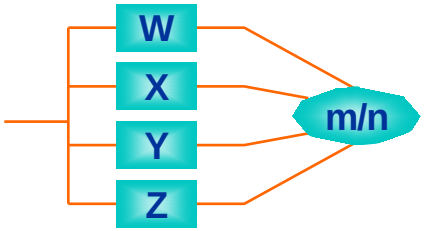
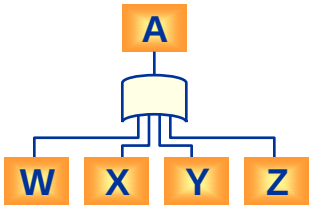
- Nécessité de disposer de maquettes de plus en plus représentatives des exemplaires définitifs.
- Aller voir sur le terrain !!!

ARBRE DE DÉFAILLANCES

Arbres de Défaillances
Élaboration

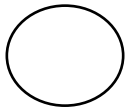
- Définition de l'EI (APR, AMDEC, ...)
- Démarche déductive
  - décomposition successive aux niveaux inférieurs
- Représentation par :
  - opérateurs logiques
  - événements
  - symboles de transfert

Opérateurs Logiques

Opérateur	Représentation fonctionnelle	Symbole
ET : *		
OU : +		
COMBINAISON (m, n)		

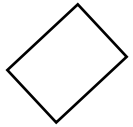
Événements

Combinaison d'événements



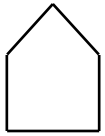
Élémentaire :

- généralement une défaillance (rupture)
- phénomène assez connu pour ne pas le développer plus

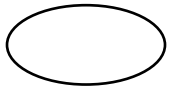


Non élémentaire non développé :

- événement ayant une cause externe (séisme)



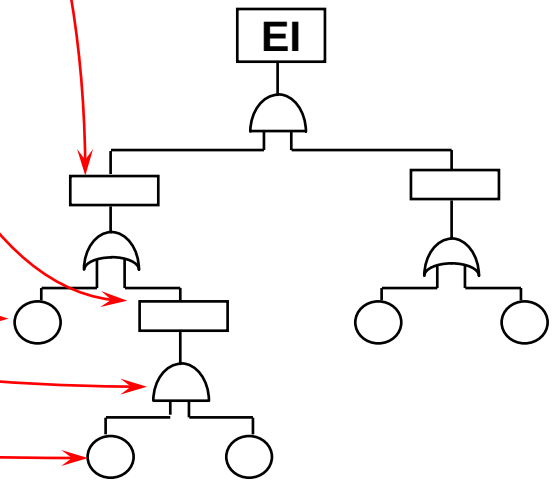
Événement élémentaire normal



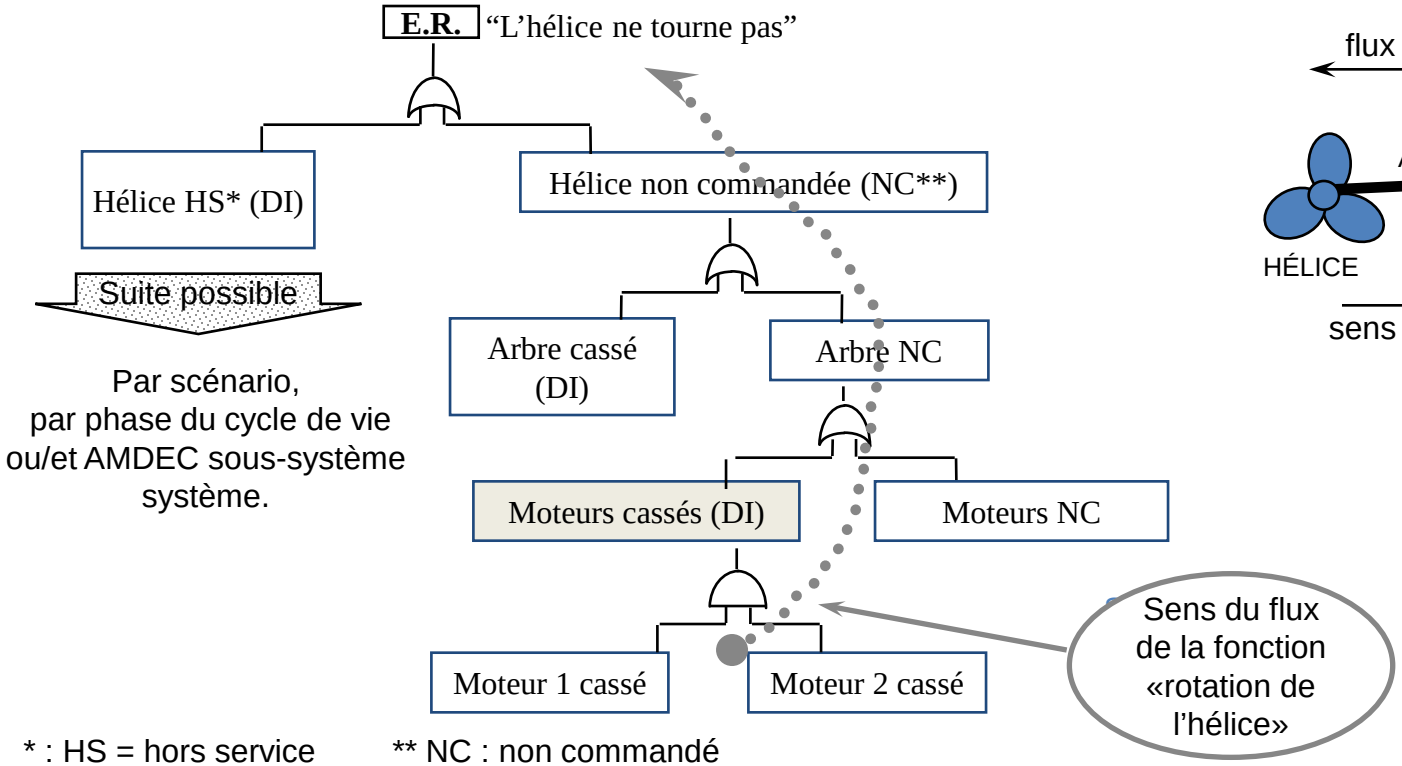
Construction

- Décomposition d'un événement intermédiaire :
  - En événement(s) de base ou en événement(s) intermédiaire(s),
  - Puis réitération de la démarche.

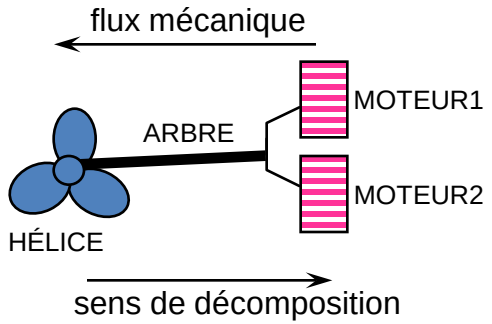
- Recherche des causes des événements intermédiaires jusqu'à l'obtention d'événements de base.



Exemple



Par scénario,
par phase du cycle de vie
ou/et AMDEC sous-système
système.



* : HS = hors service

** NC : non commandé

Traitement qualitatif

Coupes minimales ou chemins critiques :

- Plus petite combinaison d'événement entraînant l'EI,
- Peuvent être d'ordres différents :
  - ordre 1 : simple défaillance entraînant l'EI,
  - ordre 2 : paire de défaillances qui, se produisant en même temps, entraînent l'EI,
  - ...

Traitement qualitatif indispensable :

- Pour l'exploitation des informations contenues dans l'arbre,
- Pour réaliser ensuite le traitement quantitatif.

Traitement quantitatif

Probabilité de chaque événement de base :

- Sources de données :
  - REx ,
  - Bases de données générales : IEC 62380, MIL HDBK, Fides, Eireda, IEE Std 500, NPRD 2016, China 299B, ...
  - Données constructeurs, industriels, ...

Traitement quantitatif

Probabilité de chaque coupe minimale.

Probabilité de chaque événement indésirable.

Étude de sensibilité.

Limites

Pas de quantification des dépendances temporelles (avant, après).

Dans le cas de système complexe :

- étude qualitative trop complexe,
- étude quantitative trop approximative.

Construction de plusieurs arbres de défaillances lorsque le système est complexe.

Conseils

Tous les domaines techniques.

Arbres de défaillances utilisés pour :

- quantifier fiabilité, disponibilité et sécurité,
- répartir, allouer des E.I. et des objectifs aux différents acteurs de l'organisation industrielle,
- aider au diagnostic,
- aider aux analyses suite à incident.

ARBRES D'ÉVÉNEMENTS

Arbres d'Événements Principe

Méthode d'analyse prenant en compte l'ordre d'apparition des événements et permettant d'identifier, à partir d'un événement initiateur, les chemins d'aggravation conduisant à un événement indésirable.

Construction - 1

Identification d’un événement initiateur.

- détermination des conséquences immédiates sur le système de cet évènement initiateur en fonction :
  - du succès ou de l’échec des fonctions de sécurité directement concernées par l’événement initiateur,
  - de l’existence ou non de facteurs d’aggravation.

Vient de l’AMDEC, de l’APR, de l’AdD

Construction - 2

Poursuivre la démarche jusqu'à :

- avoir successivement mis en œuvre toutes les fonctions de sécurité,
- n'avoir plus de facteur d'aggravation,
- aboutir à un événement indésirable.

Éliminer les branches inutiles ou impossibles.

Traitement Qualitatif

Identification des conséquences d'une séquence d'événements.

Permet d'éliminer des séquences d'événements aux conséquences inacceptables :

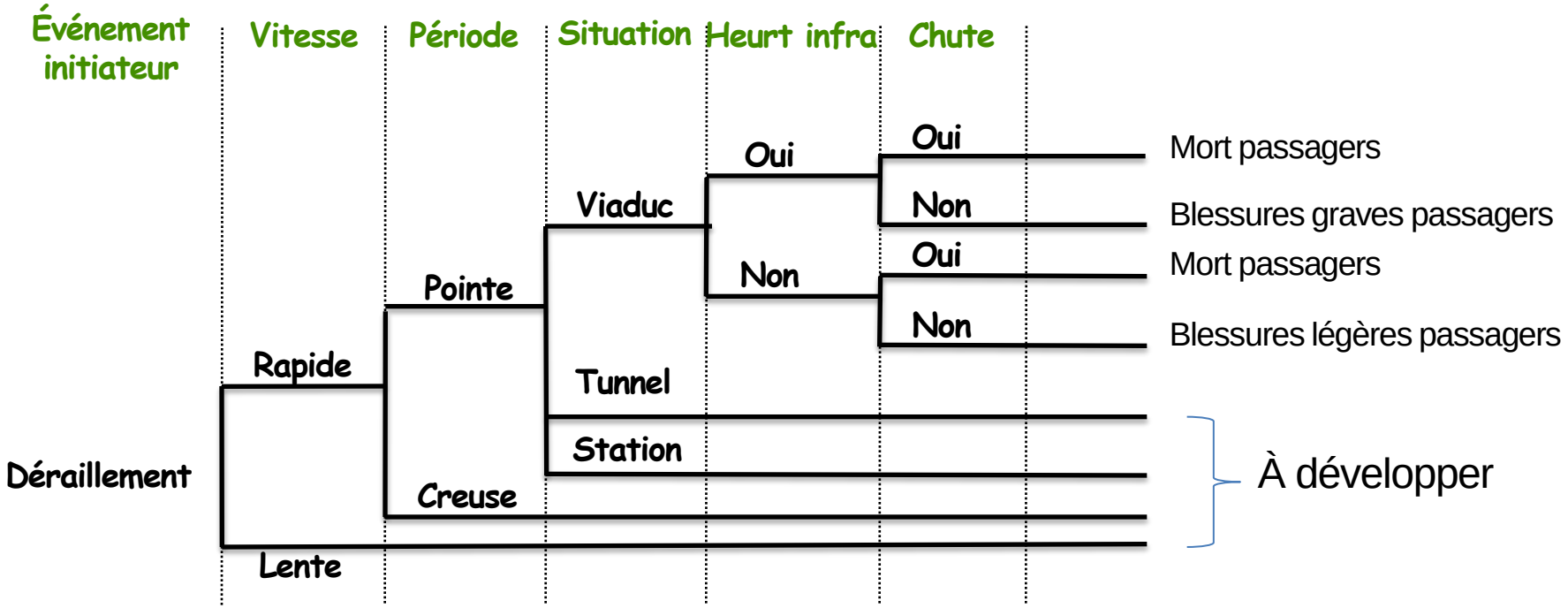
- en agissant sur la conception,
- en prenant des dispositions adaptées de mise en œuvre.

Traitement Quantitatif

Obtenir la probabilité d'occurrence de l'événement indésirable après affectation de probabilité d'occurrence aux différents événements impliqués dans la séquence :

- événement initiateur
- défaillance des fonctions de sécurité
- occurrence de facteurs d'aggravation

Exemple : Déraillement



Données d’entrée

- Architecture du système.
- Description de l’environnement.
- Événements initiateurs.
- Probabilités d’occurrence des événements initiateurs, des fonctions de sécurité, des facteurs d’aggravation.

Données de sortie

- Identification des séquences d'événements pouvant conduire à un événement indésirable.
- Mise en évidence des chemins d'aggravation.
- Identification des points faibles de la conception (analyse qualitative).
- Probabilités d'occurrence d'événements indésirables (analyse quantitative).

Limites

- Le système est considéré irréparable,
  ou non prise en compte des réparations,

- Les événements initiateurs et les événements intermédiaires sont supposés indépendants les uns des autres.

Intérêt

- Adaptée aux systèmes présentant un aspect séquentiel très marqué.
- Prise en compte de l'ordre d'apparition des événements intermédiaires.
- Permet de traiter les différents états que prend le système.
- Adaptée à l'étude de systèmes décrits de manière linéaire.

RÉSEAU DE PETRI

Réseau de Petri
Introduction

Les réseaux de PETRI permettent de rendre compte :

- de parallélisme dans le temps,
- de synchronisation,
- de partage de ressource(s).

Ils donnent un grand nombre d'informations quantitatives.

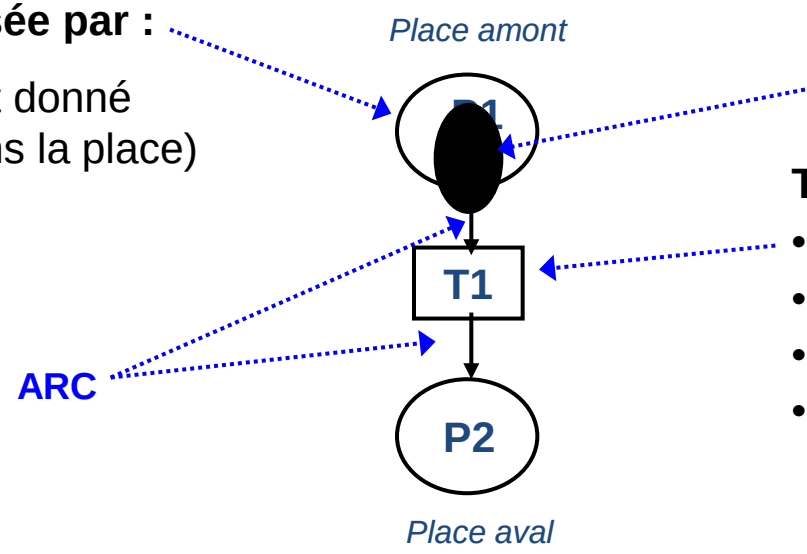
Un RdP est utilisé pour décrire un système (dynamique, à événements discrets) et l'étudier.

Principes

Graphe orienté marqué :

PLACE (P) caractérisée par :

Marquage à un instant donné
(nombre de jetons dans la place)



TRANSITION (T) décrite par :

- Place amont
- Place aval
- Conditions logique de tirage
- Lois temporelles de tirage :
  - déterministes (Δt)
  - aléatoires (lois de probabilité)

Démarche

- Décomposition en sous-système (recensement des états possibles du sous-système)
- Élaborer les liens entre sous-systèmes (dépendances)
- Réseaux de Petri des sous-système
- Réseaux de Petri des liens

} = Modèle

- Modèle + Simulation de Monte-Carlo = Résultats (fiabilité, disponibilité, temps moyen dans un état redoute, …)

Exemple : atelier industriel

Soit un atelier avec 3 machines.

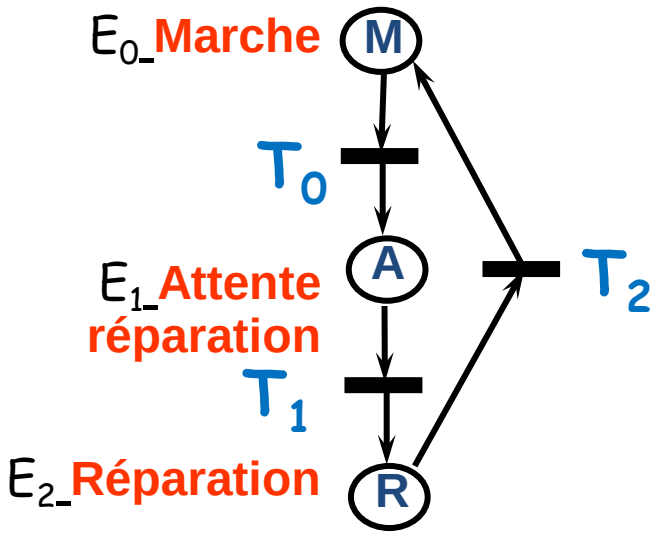
2 équipes de réparateurs sont disponibles (dépendance).

Elles peuvent tomber en panne.

En cas de panne :

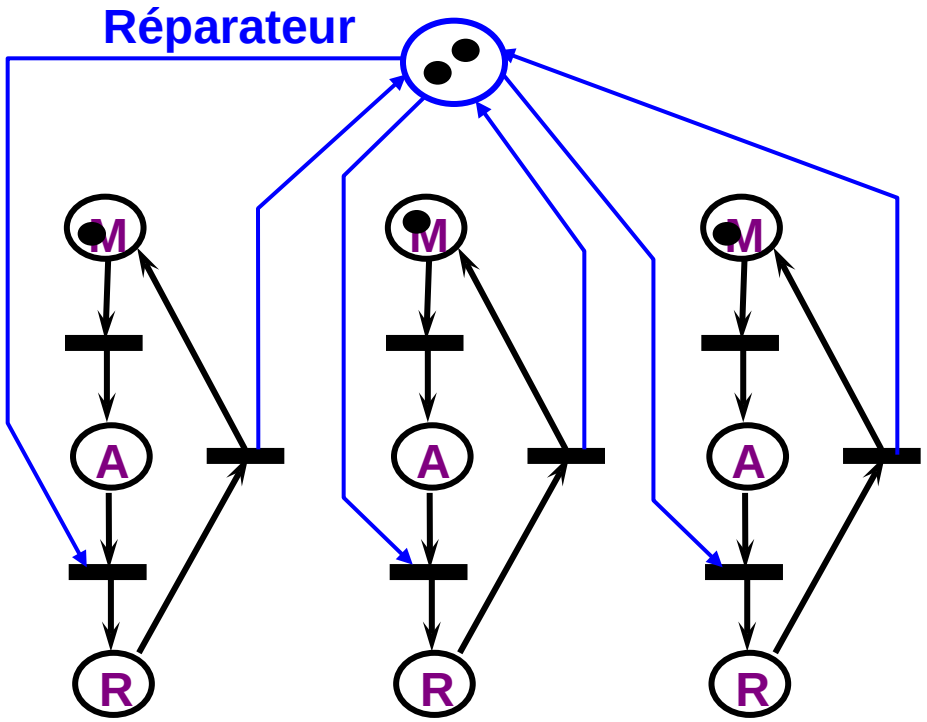
- la première panne d'une machine va occuper l'équipe de réparateur R1,
- la deuxième panne d'une machine va occuper l'équipe de réparateur R2,
- la troisième panne d'une machine devra attendre que l'une des deux premières libère l'équipe qui la répare.

Recensement des États

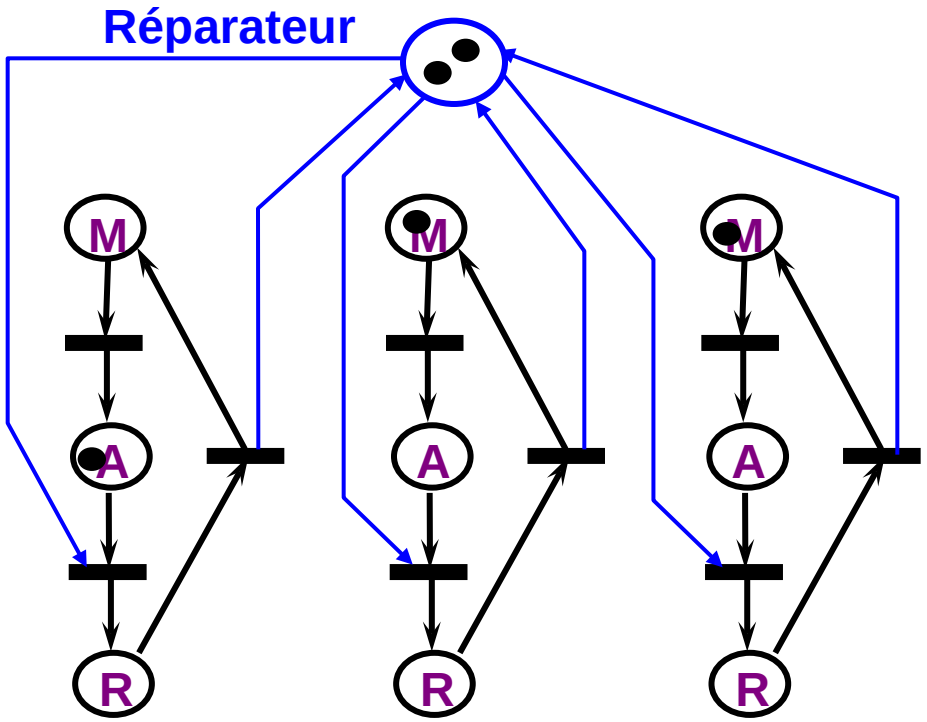


- E0 = machine en marche
- E1 = en attente de réparation
- E2 = en cours de réparation
- T0 = défaillance de la machine
- T1 = Équipe de réparateur disponible/ début de réparation
- T2 = Fin de réparation

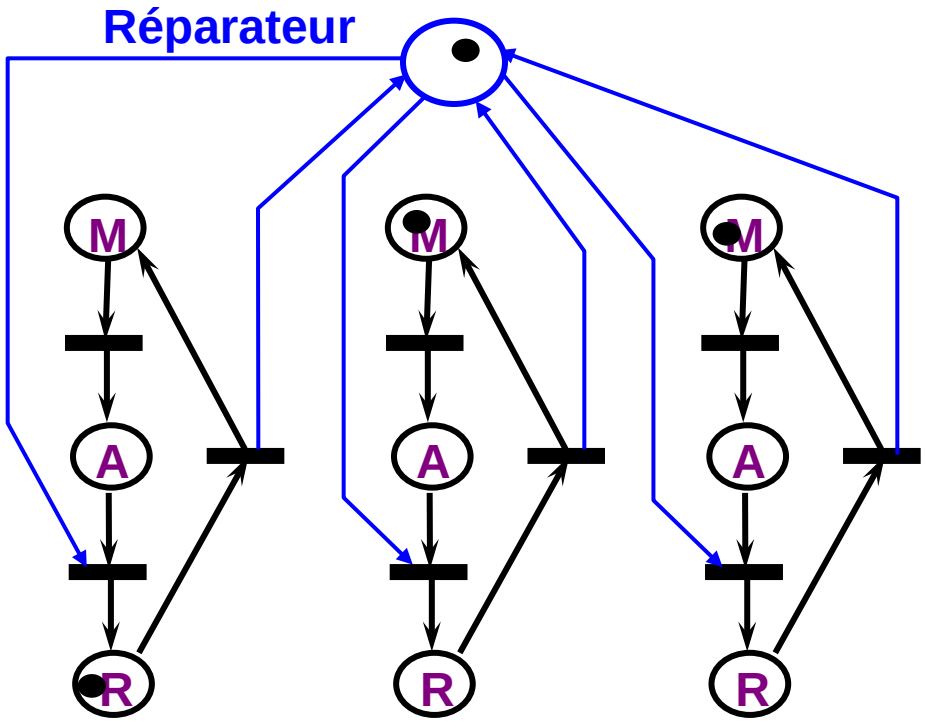
Démarrage : tout est OK



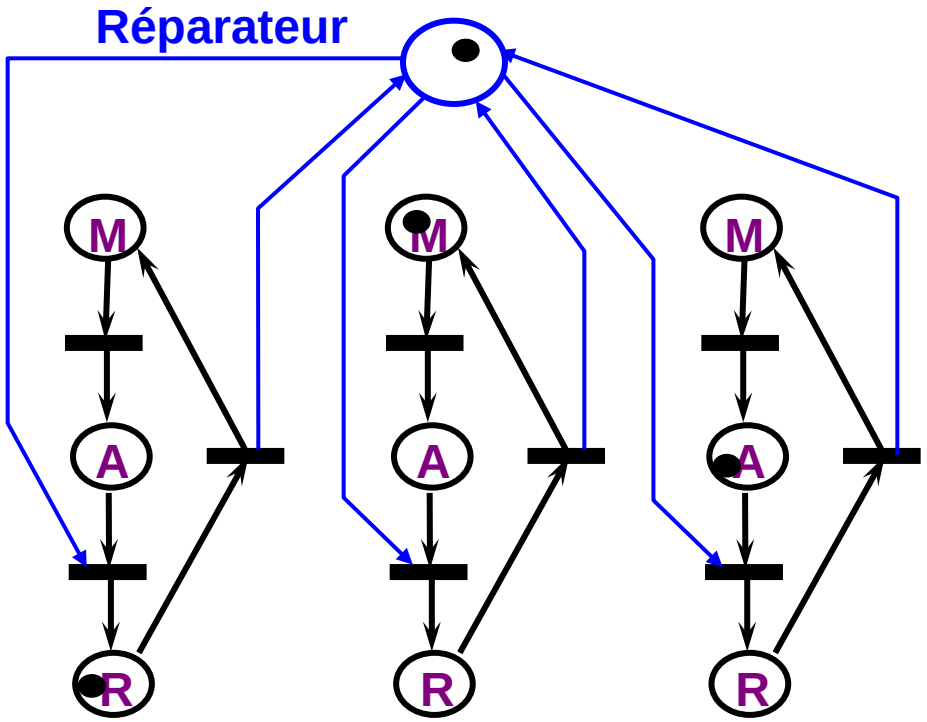
Machine 1 en panne



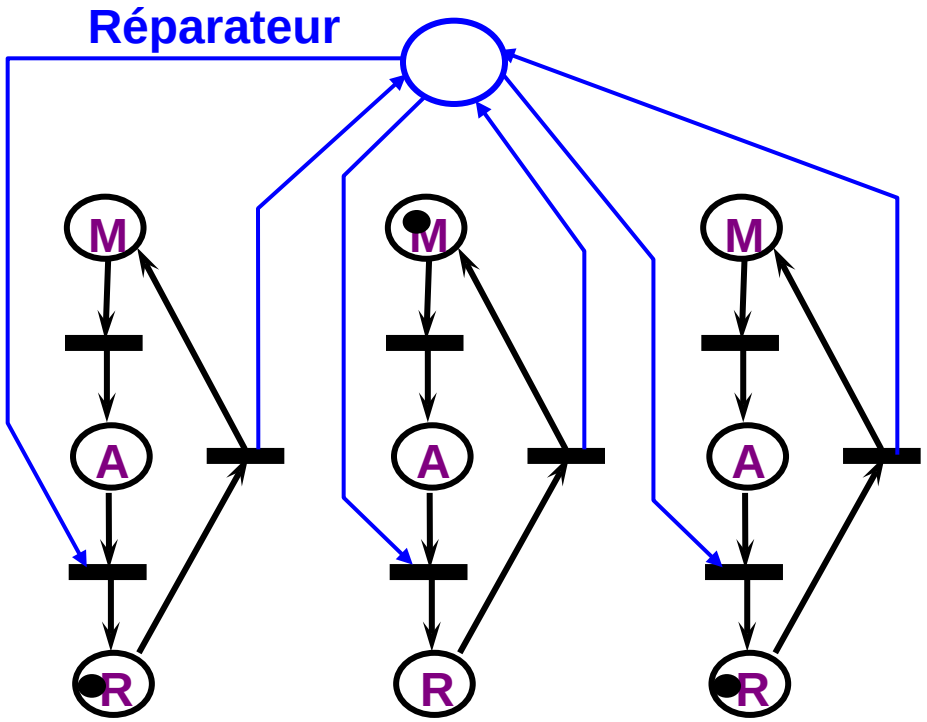
Une des 2 équipes répare la machine 1



Machine 3 en panne

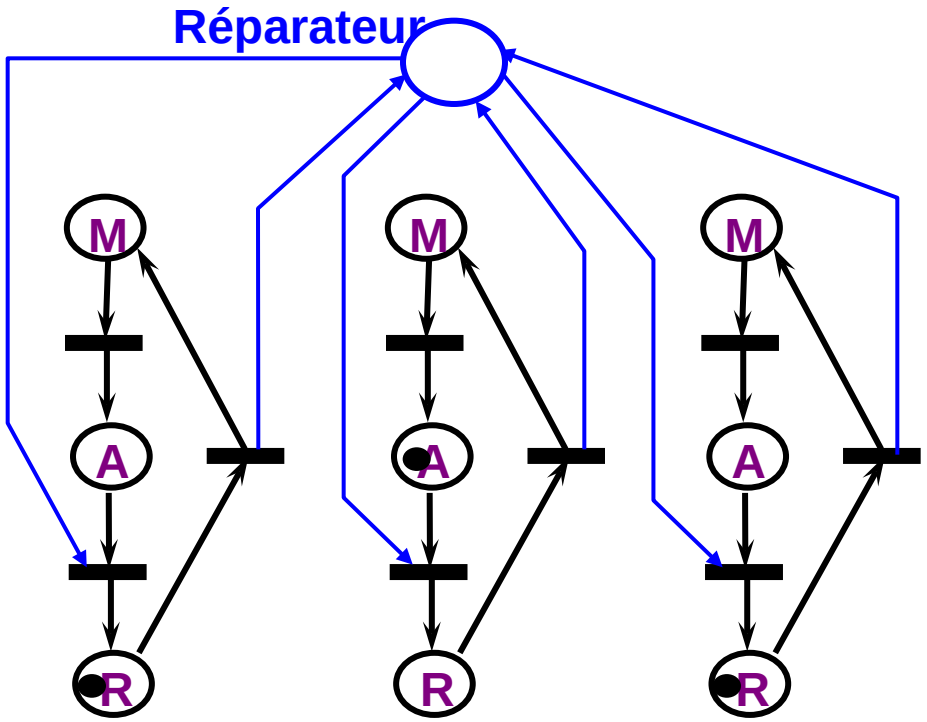


La 2e équipe répare la machine 3



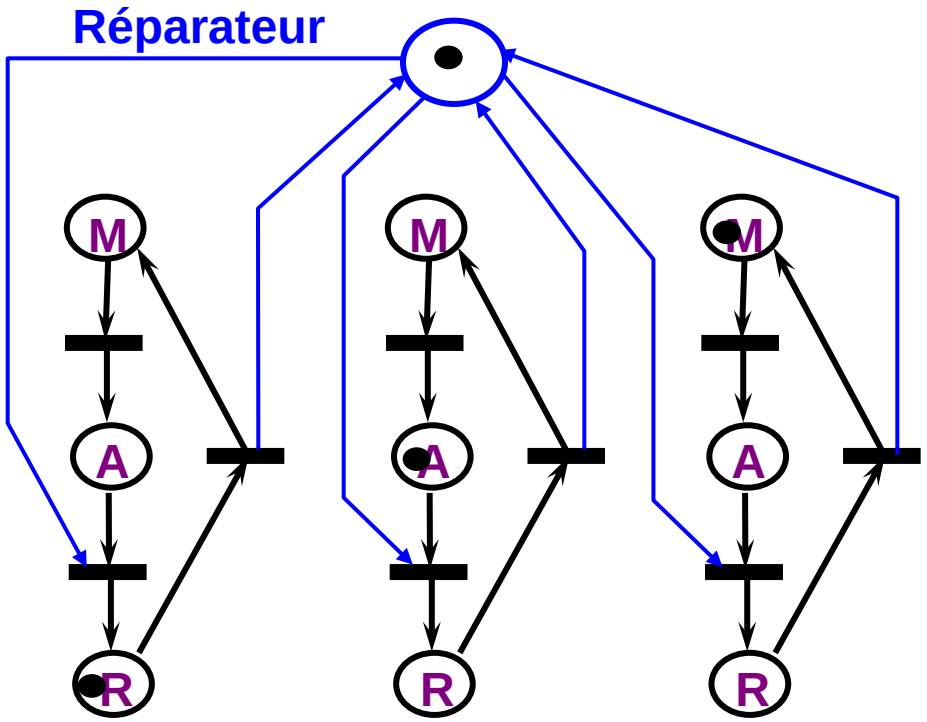
Plus d'équipe de réparateur disponible

Machine 2 en panne



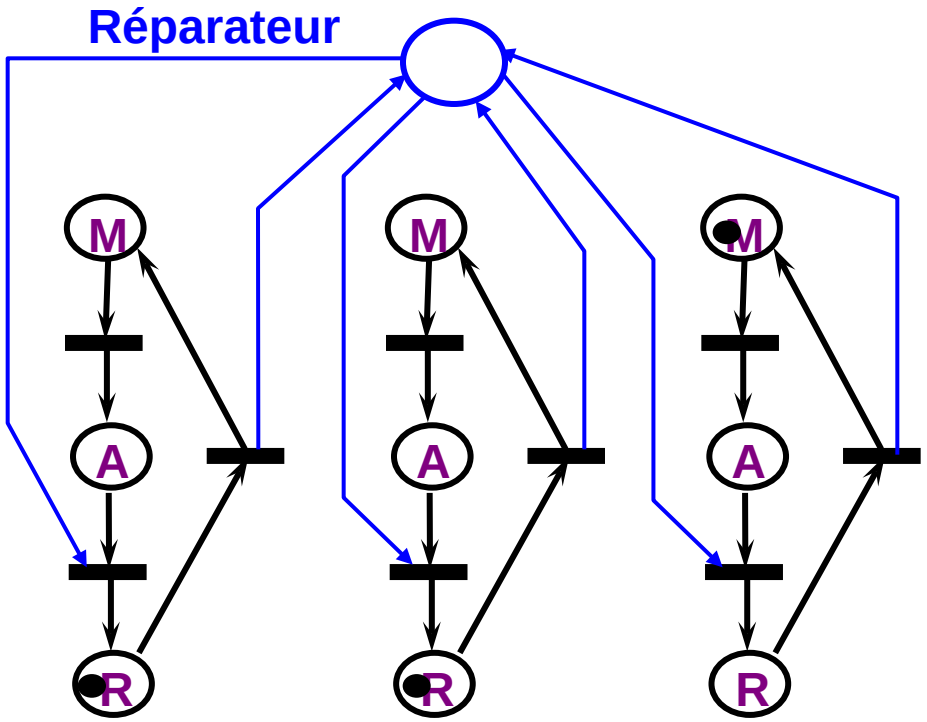
Elle attend la disponibilité de l'une des équipes de réparateurs

Machine 3 réparée

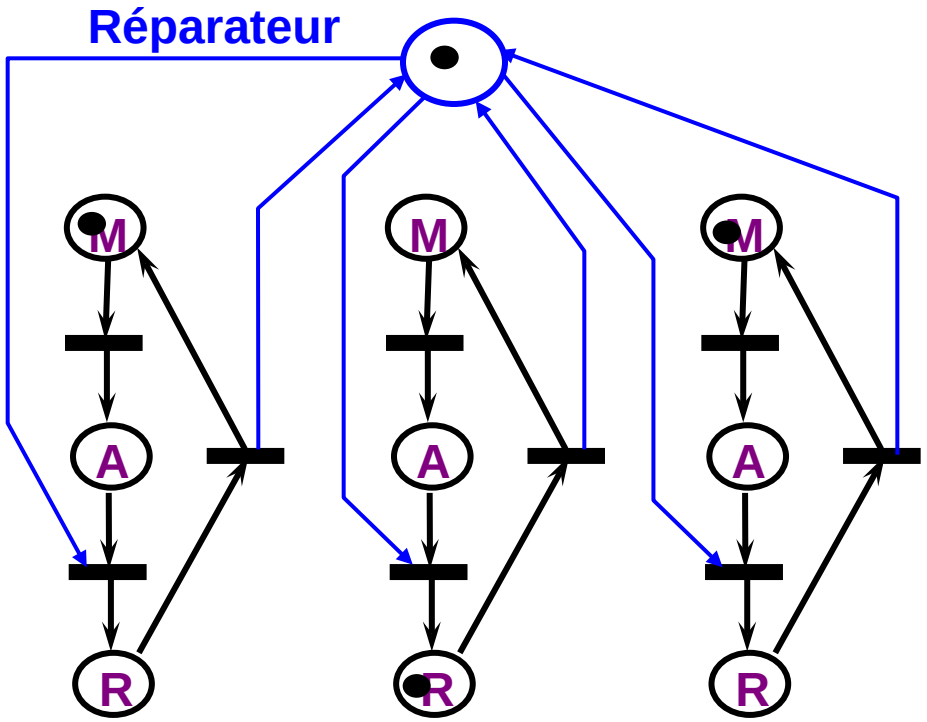


Une équipe de réparateurs est disponible

Machine 2 en réparation



Machine 1 réparée



Une équipe de réparateurs redevient disponible
Etc.

Conseils

- Les Réseaux de Petri permettent une modélisation globale des systèmes complexes.
- Les Réseaux de Petri permettent de prendre en compte toutes sortes de dépendance (équipes de réparateurs, stocks de pièces, …).

Conseils

- Les Réseaux de Petri permettent d'obtenir un grand nombre de résultats (fiabilité, disponibilité, nombre moyen de pièces produites, nombre moyen de réparations & gains et coûts associés, …)
- Possibilité de paramétrer le modèle afin de déterminer un optimum (nombre d'équipes de réparation, taille des stocks de pièces de rechange, …)

Limites

- Nécessite la connaissance de beaucoup d'information sur le système (stratégie de maintenance, logistique, …).
- Nécessite une très bonne connaissance de la modélisation par Réseau de Petri (assez similaire à un langage informatique bien que très graphique).
- Un RdP trop grand reste difficile à maîtriser. Il faut toujours le décomposer en un certain nombre de sous-systèmes/sous-réseaux.

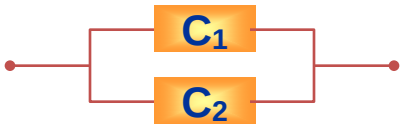
GRAPHE DE MARKOV

Graphe de Markov

- recensement des états possibles du système ; pour un système à n composants à deux états possibles (en et hors service) : p = 2n états possibles
- classification en états : panne, dégradé, bon fonctionnement
- définition des transitions possibles entre états (défaillance ou réparation)
- chaque état du système est un sommet du graphe

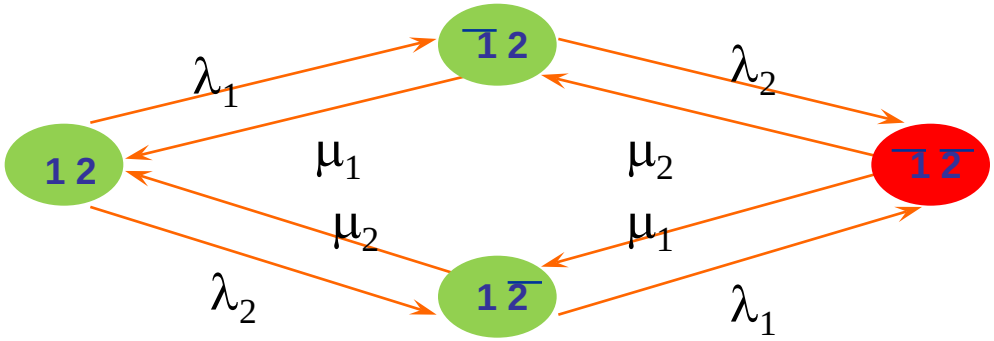
- chaque transition est symbolisée par une flèche orientée
- à chaque état Ei est associée une probabilité qui dépend du temps : Pi(t) = P[E(t) = Ei]
- à chaque transition est associé un taux de transition qui peut dépendre du temps

Exemple : parallèle



État de panne système

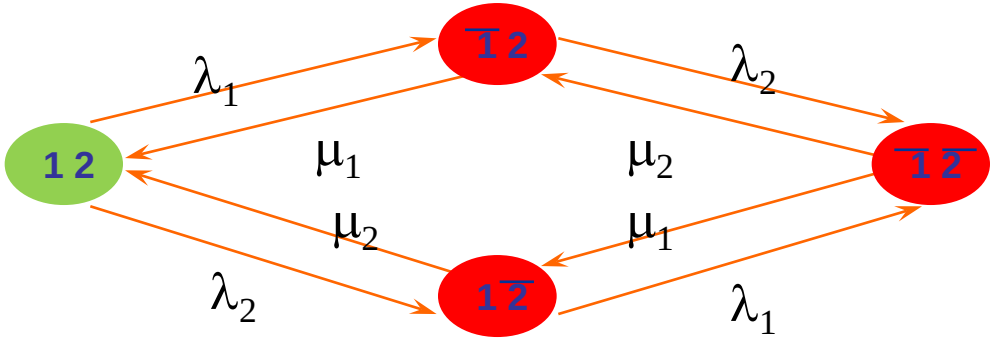
État de marche système



Série

État de panne système

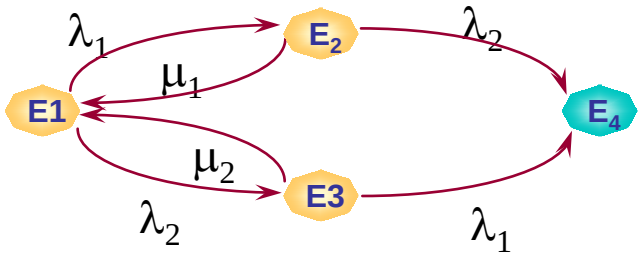
État de marche système



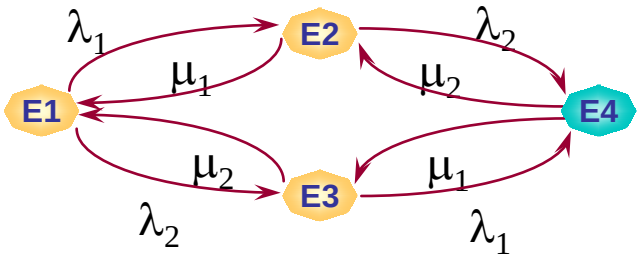
Disponibilité/Fiabilité

Cas où les deux composants sont montés en parallèles

Calcul de fiabilité



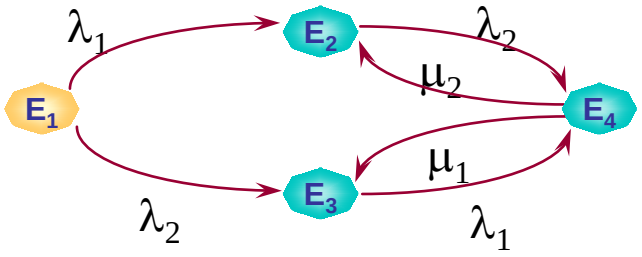
Calcul de disponibilité



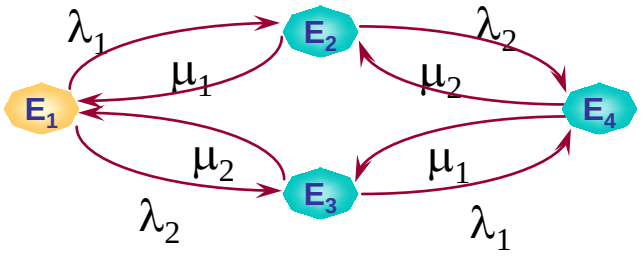
Disponibilité/Fiabilité

Cas où les deux composants sont montés en série

Calcul de fiabilité



Calcul de disponibilité



Conseils - 1

- prise en compte quantitative des dépendances fonctionnelles
- évaluation de la fiabilité et de la disponibilité d’une majorité de systèmes réparables ou non
- possibilité de couplage avec la techniques des arbres de défaillances

Conseils - 2

- s’applique à des systèmes, des procédés, des processus
- permet l’élaboration d’un modèle éventuellement analytique
- possibilité de calculer facilement des ordres de grandeurs par application d’approximations
- s’appuie sur une théorie mathématique très développée

Limites

- limité au cas des l et m constants
  (extension possible par la méthode des états fictifs)
- risque d’explosion combinatoire
- non prise en compte de deux changements d’états simultanés
- processus sans mémoire

CONCLUSIONS

Difficultés

- Ces analyses nécessitent une formation initiale.
- Elles demandent rigueur et objectivité.
- Il faut bien définir le niveau de détail de l'analyse pour éviter un excès de lourdeur.
- Il faut adapter les analyses aux moyens de l'entreprise et aux exigences des clients.
- Il faut le soutien de la direction et la motivation des participants.

Intérêts - 1

- Ces méthodes permettent de garantir le bon fonctionnement des systèmes industriels et de maîtriser les risques,
- Elles apportent une réponse argumentée aux exigences contractuelles et réglementaires,
- Elles favorisent la participation et la communication entre les équipes et les partenaires,

Intérêts - 2

- Elles apportent un outil de capitalisation des bonnes pratiques,
- Elles sont un préliminaire indispensable aux études de sécurité, soutien logistique, coût global de possession…
- Elles permettent de donner confiance et satisfaction au client.

Bibliographie - 1

- Fiches Méthodes IMdR (http://www.imdr.fr/)
- Guide d'utilisation de l'analyse fonctionnelle en matière de Sûreté de Fonctionnement. - I.S.d.F. Projet 1/91
- AMDEC - Guide pédagogique ISdF - MFQ, 1991
- Sûreté de fonctionnement et maîtrise des risques : La maintenabilité, Guide CETIM-ISdF, 1999

Bibliographie - 2

- Maîtriser la disponibilité : Un enjeu économique, Guide CETIM, 2002
- La management de la fiabilité dans les projets : Un enjeu stratégique, Guide CETIM-IMdR, 2005
- Gestion des risques des dispositifs médicaux : Guide pratique, Guide CETIM-SNITEM, 2007
- L'Analyse préliminaire des Risques: Desroches, Baudrin, Dadoun - Lavoisier

Bibliographie - 3

- Norme NF EN 60812 : Techniques d’analyse de la fiabilité du système - Procédure d’analyse des modes de défaillance et de leurs effets (AMDE), août 2006

- Maîtrise des risques et sûreté de fonctionnement (repères historiques et méthodologiques), Lannoy - Lavoisier

Bibliographie - 4

- Pratique de l'analyse fonctionnelle, Tassinari - Dunod
- Management des grands Contrats, Ligeron - Lavoisier
- Sûreté de fonctionnement des systèmes industriels – Fiabilité – Facteurs humains – Informatisation, Villemeur - Eyrolles
- Fiabilité des Systèmes, Pagès, Gondran - Eyrolles

Bibliographie - 5

- DEF-STAN 0040 – Reliability & Maintainability
- MIL-STD (338, 785, 882, 1629A, …)
  et MIL-HDBK (217, 470, 471, 472, …)
- MODSafe Modular Urban Transport Safety and Security Analysis
- Railway applications - The specification and demonstration of RAM

Bibliographie - 6

- IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”
- Reliability Toolkit – RAC
- Maintainability Toolkit – RAC
- Fiches START du RAC
- EN 50126

Bibliographie - 7

- IEC 61882: Hazard and Operability studies (HAZOP) – Application Guide
- IEC 62740: Root Cause Analysis (RCA)
- IEC 62505: Analysis Techniques for Dependability – Event Tree Analysis”
- IEC 61025: Fault Tree Analysis
- IEC 61165: Application of Markov Techniques

Bibliographie - 8

- IEC 62551: Analysis Techniques for Dependability – Petri-net Modelling

Glossaire

AMDEC : Analyse des Modes de Défaillance, de leurs Effets et Criticité (FMECA)

AdD : Arbre de Défaillances (FTA)

AdE : Arbre d'Événements (ETA)

CdCF : Cahier des Charges Fonctionnelles

AF : Analyse Fonctionnelle

SdF : Sûreté de Fonctionnement

FMDS : Fiabilité, Maintenabilité, Disponibilité, Sécurité

RAMS : Reliability, Availability, Maintainability and Safety

EI : Événement Indésirable

APR : Analyse Préliminaire des Risques (PHA)

REx : Retour d'Expérience

MTBF : Mean Time Between Failure

MTTF : Mean Time To Failure

MUT : Mean Up Time

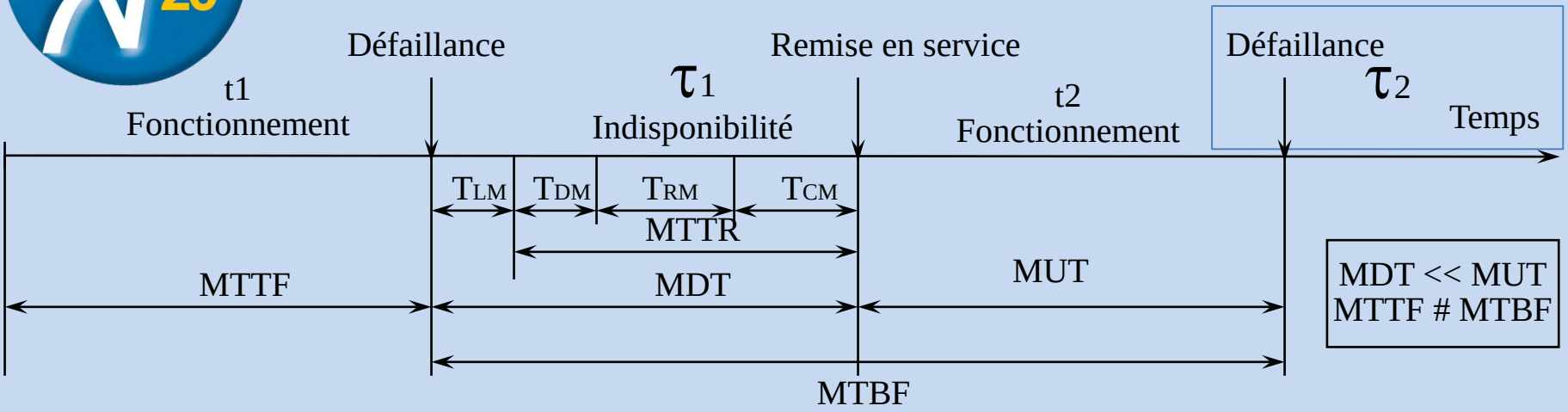
MDT : Mean Down Time

OMF : Optimisation de la Maintenance par la Fiabilité

RCM : Reliability Centered Maintenance

EMC : Electro Magnetic Compatibility

RdP : Réseau de Petri



MTTF : Durée Moyenne de fonctionnement d'un système avant la 1ère défaillance

MTBF : Durée Moyenne entre deux défaillances consécutives d'un système réparé

MDT : Durée Moyenne d'indisponibilité

MUT : Durée Moyenne de fonctionnement

MTTR : Durée Moyenne de réparation

TLM : Temps Logistiques Moyen
(détection de la défaillance + arrivée des moyens humains et matériels)

TDM : Temps de Diagnostique Moyen

TRM : Temps Moyen de Réparation proprement dite

TCM : Temps Moyen de Contrôle après réparation