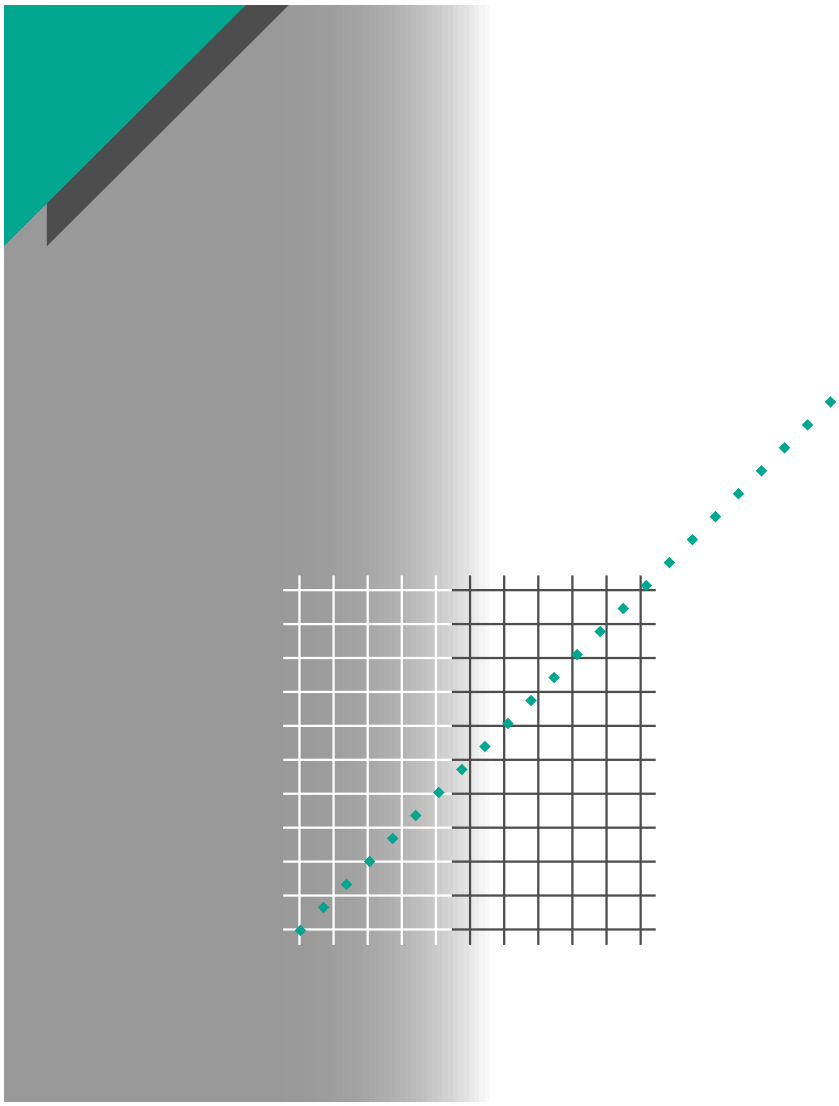
Cahier technique n° 184

Etudes de sûreté des installations électriques



S. Logiaco

GROUPE SCHNEIDER

Merlin Gerin ■ Modicon ■ Square D ■ Telemecanique

Les Cahiers Techniques constituent une collection d'une centaine de titres édités à l'intention des ingénieurs et techniciens qui recherchent une information plus approfondie, complémentaire à celle des guides, catalogues et notices techniques.

Les Cahiers Techniques apportent des connaissances sur les nouvelles techniques et technologies électrotechniques et électroniques. Ils permettent également de mieux comprendre les phénomènes rencontrés dans les installations, les systèmes et les équipements.
Chaque Cahier Technique traite en profondeur un thème précis dans les domaines des réseaux électriques, protections, contrôle-commande et des automatismes industriels.

Les derniers ouvrages parus peuvent être téléchargés sur Internet à partir du site Schneider.
Code : **http://www.schneider-electric.com**
Rubrique : **maîtrise de l'électricité**

Pour obtenir un Cahier Technique ou la liste des titres disponibles contactez votre agent Schneider.

La collection des Cahiers Techniques s'insère dans la « Collection Technique » du groupe Schneider.

n° 184

Etudes de sûreté des installations électriques

Sylvie LOGIACO

Ingénieur ISTG 1987 (Institut Scientifique et Technique de Grenoble) elle s'est d'abord consacrée à l'étude de risques dans l'industrie chimique ; Péchiney, puis Atochem.
Chez Schneider depuis 1991, elle fait partie du pôle de compétence Sûreté de Fonctionnement et à ce titre a effectué de nombreuses études concernant la sûreté de fonctionnement des installations électriques et du contrôle-commande.

CT 184 édition janvier 1999

Lexique

AMDE (Analyse des Modes de Défaillance et de leurs Effets) :
Elle permet d'étudier l'influence des défaillances des composants sur le système.

Analyse dysfonctionnelle :
A partir de l'analyse fonctionnelle, c'est l'analyse des dysfonctionnements d'un système (en pratique, synonyme de « étude de sûreté »).

Disponibilité :
Probabilité pour qu'une entité soit en état d'accomplir une fonction requise dans des conditions données à un instant donné t ; on la note A(t).

Evénement redouté :
Défaillance du système qu'il faut analyser pour prouver que l'utilisateur peut avoir une confiance justifiée du système. Cette défaillance du système est un métrique de la qualité de service.

Fiabilité :
Probabilité qu'une entité puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné $[t_1, t_2]$; que l'on écrit $R(t_1, t_2)$.

Maintenabilité :
Probabilité pour qu'une opération donnée de maintenance puisse être effectuée pendant un intervalle de temps donné $[t_1, t_2]$.

MDT (Mean Down Time) :
Temps moyen pendant lequel le système est indisponible. Il comprend le temps de détection de la panne, le temps de déplacement du service maintenance, le temps d'approvisionnement du matériel en panne, le temps de réparation.

Modèle :
Représentation graphique de la combinaison des défaillances trouvées lors de l'A.M.D.E. et de leur processus de maintenance.

MTBF (Mean Time Between Failure) :
Temps moyen entre deux défaillances d'un système réparable.

MTTF (Mean Time To Failure) :
Temps moyen de bon fonctionnement avant la première défaillance.

MTTR (Mean Time To Repair) :
Durée moyenne de réparation.

MUT (Mean Up Time) :
Temps moyen de bon fonctionnement entre deux défaillances d'un système réparable.

Retour d'expérience :
Données de fiabilité opérationnelle recueillies lors des défaillances du matériel en exploitation.

Sécurité :
Probabilité d'éviter un événement dont les conséquences sont dangereuses.

Sûreté (de fonctionnement) :
La sûreté de fonctionnement est une notion générique qui mesure la qualité de service, délivrée par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée. La confiance justifiée s'obtient à travers les analyses qualitatives et quantitatives des différentes propriétés du service délivré par le système. Ces différentes propriétés sont basées sur les valeurs probabilistes définies ci-après.

Taux de défaillance :
Probabilité pour qu'une entité perde sa capacité à accomplir une fonction pendant l'intervalle [t, t+dt], sachant qu'elle n'a pas été défaillante entre [0, t] ; on le note λ.

Taux de défaillance équivalent :
Probabilité pour qu'un système perde sa capacité à accomplir une fonction pendant l'intervalle [t, t+dt], sachant qu'il n'a pas été en panne entre [0, t] ; on le note λ_{eq}.

Taux de réparation :
Inverse de la durée moyenne de réparation.

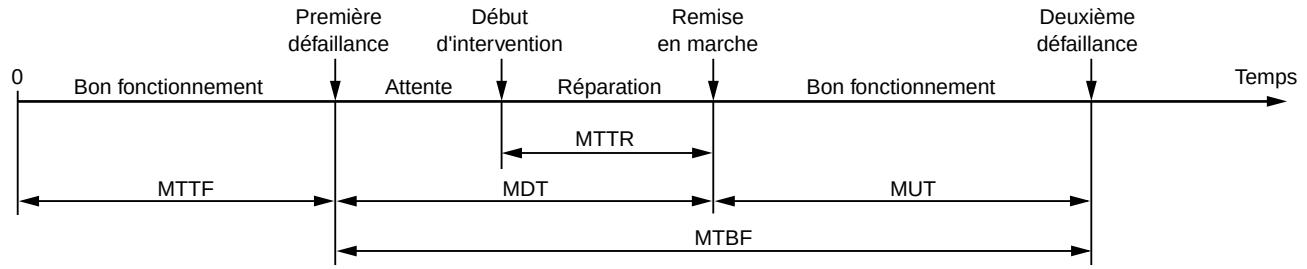


Fig. 1 : relations entre les différentes grandeurs caractérisant la fiabilité, la maintenabilité et la disponibilité d'une machine.

Etudes de sûreté des installations électriques

Dans l'industrie, comme dans le tertiaire la qualité de l'alimentation électrique est de plus en plus importante. La qualité du produit électricité, outre les imperfections telles que variations de tension, distorsion harmonique, se caractérise essentiellement par la disponibilité de l'énergie électrique.
La perte d'alimentation est toujours gênante, mais peut devenir très pénalisante par exemple pour les systèmes de traitement de l'information (informatique - contrôle-commande) ; elle peut même être catastrophique pour certains process et dans certains cas mettre en danger la vie de personnes.

Les études de sûreté de fonctionnement permettent de réaliser l'adéquation entre les besoins en disponibilité électrique et le réseau à mettre en œuvre. Elles permettent également de comparer deux architectures d'installation... La plus coûteuse n'est pas toujours la meilleure...
L'objet de ce Cahier Technique est de montrer comment se fait une étude de sûreté : méthodologie, outils. Deux exemples d'études sont présentés : réseau électrique d'usine et système de contrôle-commande d'un poste haute tension.
Ces études sont de plus en plus facilitées par les « outils » informatiques.

Sommaire

1 Introduction

1.1 Généralités

La tension aux bornes d'un récepteur est affectée par des phénomènes dont l'origine peut être le réseau du distributeur, l'installation électrique d'un abonné raccordé au même réseau de distribution, l'installation électrique de l'utilisateur perturbé.

Les perturbations du produit électricité

■ Les caractéristiques principales de la tension fournie par un réseau public de distribution MT ou BT sont définies par la norme Européenne EN 50160. Elle précise les tolérances qui doivent être garanties pour la tension et la fréquence ainsi que les niveaux des perturbations habituellement rencontrées ; par exemple distorsion harmonique.
Le tableau de la **figure 2** précise les valeurs retenues par la norme.

A tout instant la qualité de l'énergie délivrée aux récepteurs d'une installation peut donc être affectée par diverses perturbations, soit imposées par le réseau externe d'alimentation, soit auto-générées par le réseau interne de distribution.

Le fonctionnement des récepteurs autonomes ou fédérés en systèmes est affecté par ces perturbations.

■ Les dysfonctionnements, la nature et le coût des dommages subis dépendent à la fois de la nature des récepteurs et du niveau de criticité de l'installation. Ainsi la coupure momentanée d'un récepteur critique peut avoir de graves conséquences sur le fonctionnement de l'installation sans que celui-ci soit intrinsèquement affecté.

■ Dans tous les cas, une étude précise des effets des perturbations redoutées doit être effectuée. Des dispositions doivent être prises pour limiter leurs conséquences.

■ Le tableau de la **figure 3** regroupe les perturbations usuellement rencontrées dans les réseaux électriques, leurs causes et les solutions possibles pour réduire leurs effets.

■ La réduction des effets des harmoniques, du Flicker, des déséquilibres de tension, des variations de fréquence et des surtensions est réalisée par la mise en place d'équipements adaptés à chaque cas. Leurs dimensionnements et le choix de leurs points de raccordement font l'objet d'études détaillées qui sortent du cadre de ce document (voir bibliographie).

Les pertes d'alimentation

Pour les procédés industriels et les systèmes courant faible, elles sont de moins en

Norme EN 50160	Alimentation basse tension
Fréquence	50 Hz ±1 % pendant 95 % d'une semaine 50 Hz +4 %,-6 % pendant 100 % d'une semaine
Amplitude de la tension	Pour chaque période d'une semaine 95 % des valeurs efficaces moyennes sur 10 minutes doivent être dans la plage Un ±10 %
Variations rapides de la tension	De 5 % à 10 % de Un (4 à 6 % en moyenne tension)
Creux de tension	valeurs indicatives : ■ profondeur : entre 10 % et 99 % de Un, majorité des creux de tension < 60 % de Un ■ durée : entre 10 ms et 1 minute, majorité des creux de tension < 1 s ■ nombre : quelques dizaines à 1 millier par an
Coupures brèves	Valeurs indicatives : ■ profondeur : 100 % de Un ■ durée : jusqu'à 3 minutes, 70 % des coupures brèves sont inférieures à 1 s ■ nombre : quelques dizaines à plusieurs centaines par an
Coupures longues	Valeurs indicatives : ■ profondeur : 100 % de Un ■ durée : supérieure à 3 minutes ■ nombre : entre 10 et 50 par an

Fig. 2 : perturbations dans les réseaux ; valeurs retenues par la norme.

moins tolérables, car génératrices de coûts importants.

■ L'immunité aux coupures de l'alimentation fait appel à des équipements spécifiques tels que les alimentations sans interruptions et les groupes autonomes de production d'énergie électrique. Ces équipements ne suffisent généralement pas à résoudre tous les problèmes.

L'architecture du réseau, les automatismes de réalimentation, le niveau de fiabilité des matériels, la sélectivité des protections ainsi que la politique de maintenance jouent un rôle important dans la réduction et l'élimination des temps de coupure. Minimiser les pertes d'alimentation nécessite des études de fiabilité/disponibilité prenant en compte l'ensemble de ces facteurs ainsi que la fréquence et la durée des coupures admises par l'installation.

Ces études permettent de déterminer l'architecture et les équipements les mieux adaptés aux besoins de l'exploitant. Elles nécessitent généralement le classement des récepteurs ou systèmes en fonction de leur niveau de sensibilité et de distinguer :

□ les récepteurs admettant des arrêts prolongés : 1 heure au plus (non prioritaires),

□ les récepteurs admettant des arrêts de quelques minutes (prioritaires),

□ les récepteurs devant être réalimentés après quelques secondes (essentiels),

□ les récepteurs n'acceptant aucune coupure (vitaux).

Perturbations	Causes possibles	Principaux effets	Solutions possibles
Variations de la fréquence	■ Réseau d'alimentation ■ Fonctionnement iloté sur groupes autonomes	■ Variation vitesse des moteurs ■ Dysfonctionnement équipements électroniques	■ Alimentation sans interruption
Variations rapides de la tension	■ Réseau d'alimentation ■ Four à arc ■ Machine à souder ■ A-coups de charge	■ Papillotement de l'éclairage (Flicker) ■ Variation vitesse moteurs	■ Augmentation de la puissance de court-circuit ■ Modification de l'architecture de l'installation
Creux de tension	■ Réseau d'alimentation ■ Appels de charge importants ■ Défauts externes et internes	■ Extinction de lampes à décharge ■ Dysfonctionnement de régulateurs et variateurs ■ Variation de vitesse, arrêt de moteurs ■ Retombée de contacteurs ■ Perturbation de l'électronique numérique ■ Dysfonctionnement électronique de puissance	■ Alimentation sans interruption ■ Augmentation de la puissance de court-circuit ■ Modification de l'architecture de l'installation
Coupures brèves et longues	■ Réseau d'alimentation ■ Ré-enclenchements ■ Défauts internes ■ Permutations de sources	■ Arrêt d'équipement ■ Arrêt d'installation ■ Perte de production ■ Retombée de contacteurs ■ Dysfonctionnements divers	■ Alimentation sans interruption ■ Groupes autonomes ■ Modification architecture du réseau ■ Mises en place politique de maintenance
Déséquilibre de tension	■ Réseau d'alimentation ■ Nombreuses charges monophasées	■ Echauffements des moteurs et des alternateurs	■ Augmentation de la puissance de court-circuit ■ Modification de l'architecture du réseau ■ Equilibrage des charges monophasées ■ Dispositifs de ré-équilibrage
Surtensions	■ Foudre ■ Manœuvre d'appareillage ■ Défaut d'isolement	■ Claquage de matériels	■ Parafoudres ■ Choix du niveau d'isolement ■ Maîtrise des résistances des prises de terre
Harmoniques	■ Réseau d'alimentation ■ Nombreux récepteurs non linéaires	■ Echauffement, endommagement de matériels, moteurs et condensateurs principalement ■ Dysfonctionnement électronique de puissance	■ Augmentation de la puissance de court-circuit ■ Modification de l'architecture de l'installation ■ Filtrage

***Fig. 3** : perturbations dans les réseaux, causes, effets et solutions.*

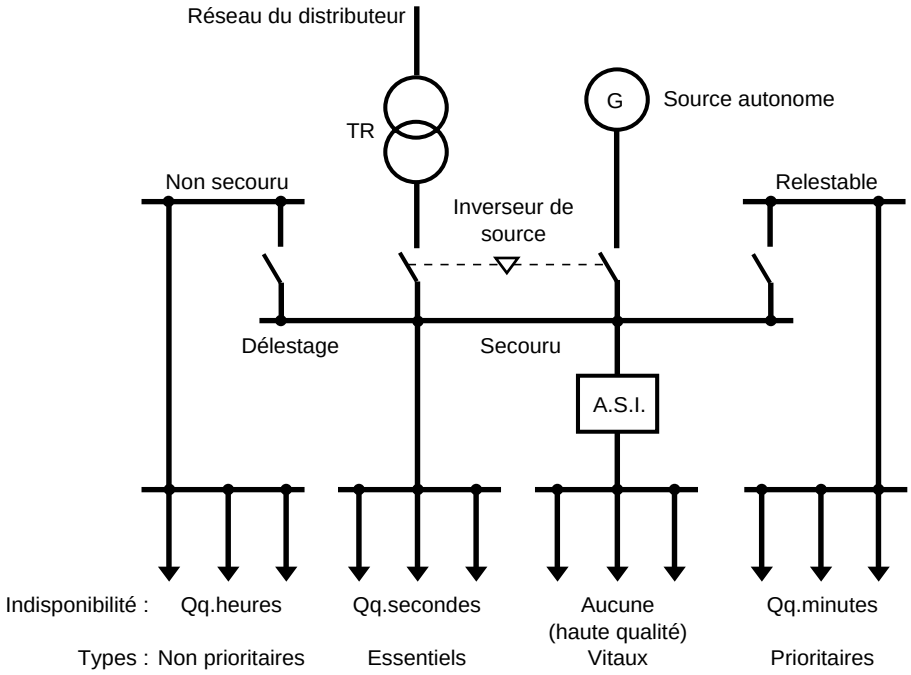


***Fig. 4** : l'électricité fiabilisée. Schéma simplifié d'un réseau.*

A titre d'exemple la **figure 4** reproduit le schéma simplifié d'un réseau pour lequel cette distinction a été faite.

- Les récepteurs **vitaux** ne tolérant aucune coupure, sont alimentés par une alimentation sans interruption.
- Les récepteurs **essentiels** sont réalimentés quelques secondes après la perte du réseau dès que la tension et la fréquence du groupe sont stabilisées.
- Les récepteurs **prioritaires** sont relestés dès la fin du redémarrage des récepteurs essentiels.
- Les récepteurs **non prioritaires** acceptant un long temps de coupure ne sont réalimentés qu'au retour du réseau externe d'alimentation.

Par le choix d'une architecture et d'automatismes de permutation de sources appropriés (cf. Cahier Technique n° 161) on optimise le positionnement et le dimensionnement des sources de secours et de remplacement pour respecter les contraintes d'exploitation.
Il faut rappeler que le choix du régime du neutre est un élément important ; ainsi il est clairement établi que pour des récepteurs demandant un niveau de disponibilité élevé, le choix du neutre isolé est fortement conseillé car il permet la continuité d'alimentation au premier défaut d'isolement (cf. Cahiers Techniques n° 172 et n° 173).

1.2 Les études de sûreté

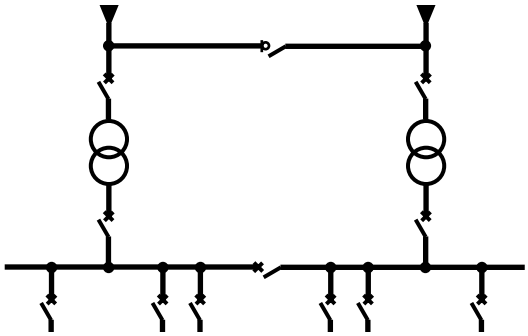
Avant de présenter les études de sûreté des réseaux électriques il est utile de rappeler quelques particularités des définitions de termes utilisés par les fiabilistes. Même si chacun connaît la signification générale des mots : fiable, disponible, maintenance, sécurité, ces termes, lorsqu'ils sont utilisés par les fiabilistes, prennent une signification précise.

Par exemple, le mot « fiabilité » évoque en général l'aptitude d'un système à fonctionner correctement le plus longtemps possible.

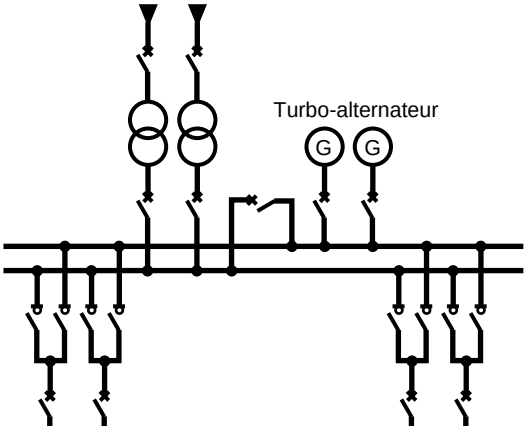
De même, l'expression « maintenabilité » évoque généralement la notion d'aptitude d'un système à être réparé rapidement.

Or, on constate que les définitions du fiabiliste, données dans le lexique en début de ce

a) Double antenne



b) Double jeu de barres



c) Boucle

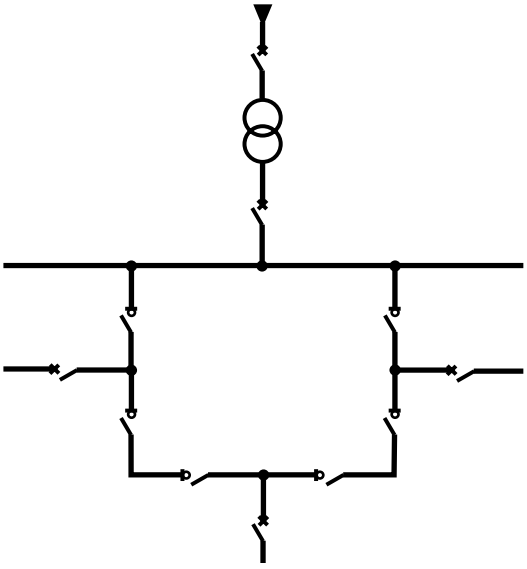


fig. 5 : architectures de réseaux.

document, vont au delà de ces interprétations générales. Elles sont plus précises, en particulier par la spécification d'une notion de durée.
Il est également nécessaire de préciser le domaine d'application et les caractéristiques générales des études.

Domaines d'application

Les études sont réalisées sur tous types de réseaux électriques, de la basse tension à la haute tension et sur leurs systèmes de protection et de contrôle-commande.
Ceci que les réseaux soient :

- en antenne,
- en double antenne (cf. **fig. 5a**),
- en double jeu de barre (cf. **fig. 5b**),
- en boucle (cf. **fig. 5c**),
- et avec ou sans reconfiguration ou délestage.

Eléments caractéristiques des études

Les études sont personnalisées en fonction des besoins exprimés.
Ils se traduisent en termes de :

- finesse d'étude,
- type d'analyse,
- types de critères de sûreté de fonctionnement.

■ La finesse de l'étude (cf. **fig. 6**)

□ Etude rapide ou préétude : c'est une étude pessimiste utilisée en général pour faire rapidement des choix techniques.

□ Etude très détaillée qui prend en compte le plus de facteurs possibles.
Prise en compte de tous les modes de fonctionnement, analyse détaillée des défaillances possibles et de leurs conséquences, modélisation la plus proche possible du comportement dysfonctionnel du système.

Caractéristique	Préétude	Etude détaillée
Finesse des hypothèses	1 seul type de défaillance (1 fréquence, 1 durée moyenne)	Défaillances divisées en famille en fonction de leur effet sur le système.
Finesse de la modélisation	Les conséquences des défaillances sont associées en grandes familles	Les conséquences des défaillances sont analysées finement.

Fig. 6 : différences entre une préétude et une étude fine.

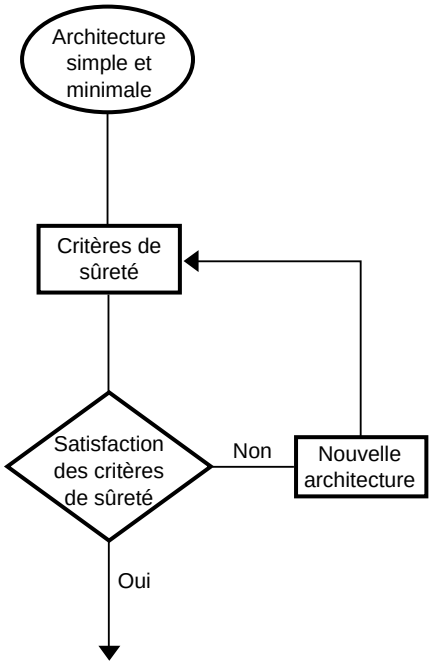


Fig. 7 : aide à la conception.

■ Les types d'analyse

□ Aide à la conception en évaluant des critères de sûreté de fonctionnement (cf. **fig. 7**).

□ Comparaison d'architectures (cf. **fig. 8**).

□ Analyse qualitative d'une architecture.

■ Les types de critères à quantifier (cf. **fig. 9**)

□ Le nombre d'heures moyen pendant lequel le système fonctionne correctement (MUT).

□ Le nombre d'heures moyen pendant lequel le système fonctionne avant que pour la première fois il n'alimente plus certains récepteurs (MTTF).

□ La probabilité de ne plus alimenter certains récepteurs (disponibilité).

□ Le nombre moyen de pannes par an (λ_{eq}).

□ Un temps moyen de réparation ($1/\mu_{eq}$).

□ La fréquence optimale d'une maintenance préventive.

□ Le calcul de lots de rechange.

Ces critères permettent d'évaluer les performances du système et donc de déterminer l'architecture qui répond aux exigences de sûreté sans oublier les contraintes économiques.

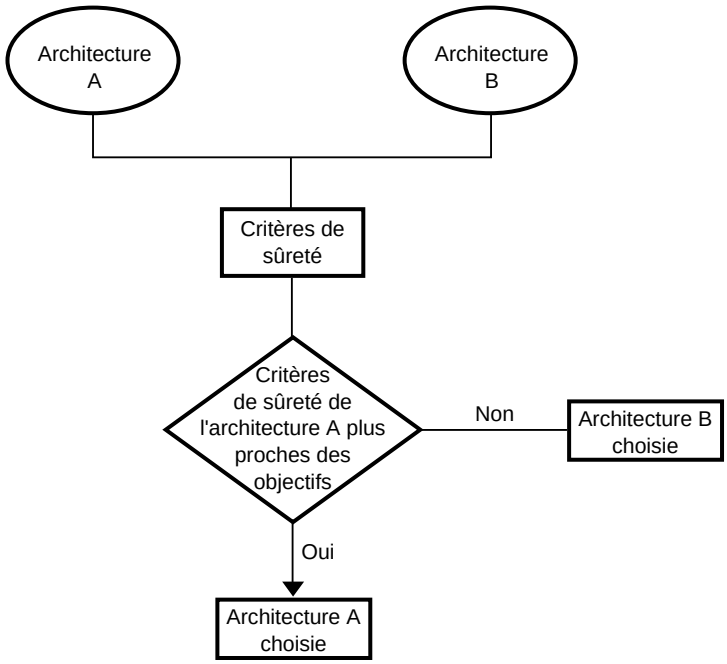
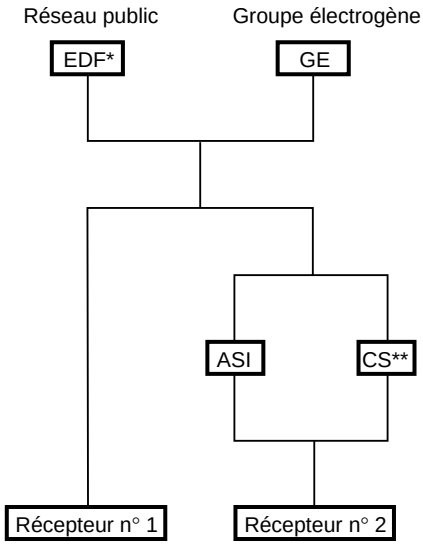


Fig. 8 : comparaison d'architecture.



Il peut être calculé :

- la probabilité que le GE ne démarre pas en cas de perte EDF.
- la fréquence optimale de la maintenance préventive du GE.
- le nombre de minutes par an pendant lequel le récepteur n° 1 n'est pas alimenté.
- le nombre d'heures moyen avant que le récepteur n° 2 ne soit plus alimenté.

* EDF : Electricité de France
** CS : Contacteur Statique

Fig. 9 *: illustration des critères d'évaluation de la sûreté de fonctionnement.*

2 Déroulement des études

2.1 Les phases chronologiques

Quel que soit le besoin exprimé par le concepteur ou l'exploitant d'une installation électrique, le déroulement de l'étude de sûreté comporte les phases (cf. **fig. 10**) :

- expression et analyse du besoin,
- analyse fonctionnelle du système,
- analyse des modes de défaillances,
- modélisation,
- calcul ou évaluation des critères de sûreté.

Dans la plupart des cas cette démarche est à faire plusieurs fois :

- deux fois s'il s'agit de comparer deux schémas,
- n fois s'il s'agit par itérations de déterminer une architecture adaptée au besoin en tenant compte des impératifs technico-économiques.

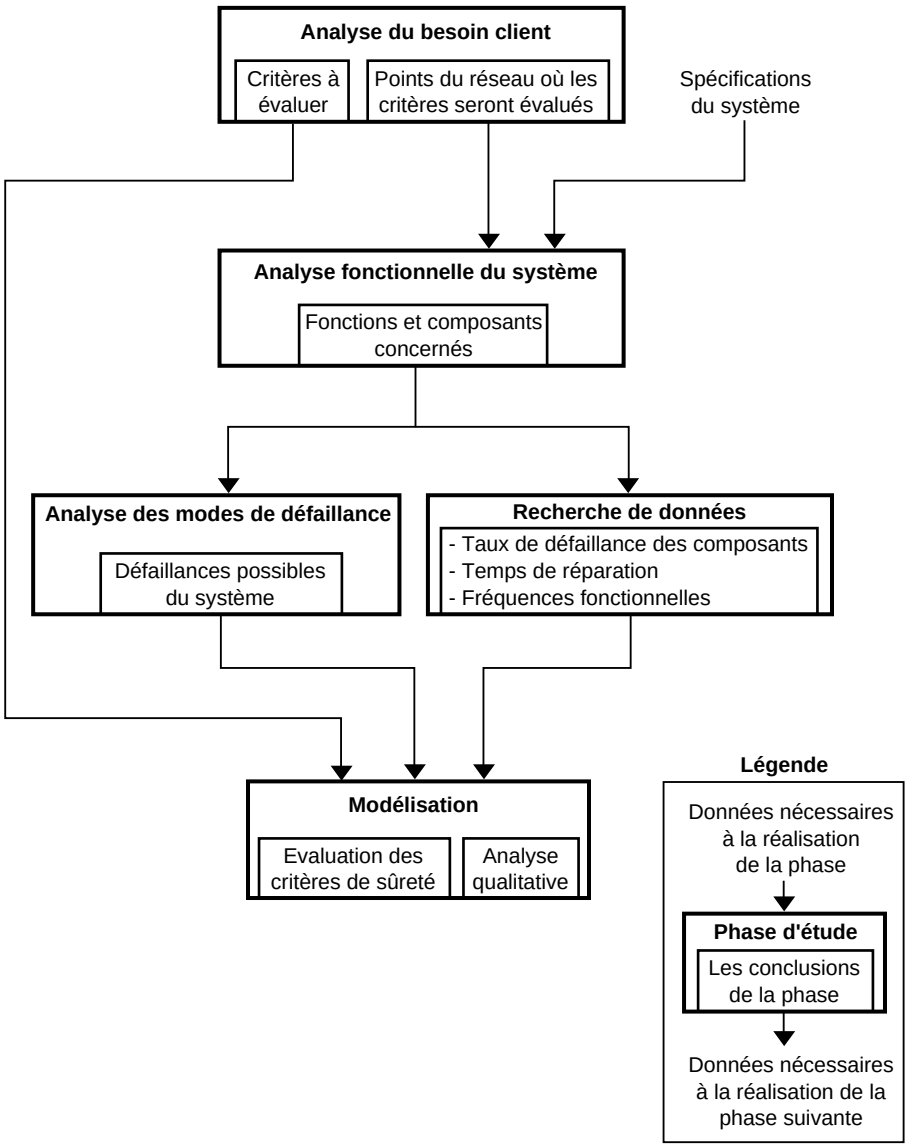


***Fig. 10** : les phases chronologiques de réalisation d'une étude de sûreté de fonctionnement.*

2.2 Expression et analyse du besoin

Comme indiqué à la fin du chapitre précédent le donneur d'ordre doit préciser les points suivants (cf. **fig. 11**).

■ Sur quoi porte l'étude ; par exemple contrôle-commande d'un poste, et fournir les éléments de conception dont il dispose.

■ La nature de la demande (type d'analyse), soit par exemple :

□ démonstration du niveau de confiance que l'on peut accorder à l'alimentation électrique d'un process critique (oriente vers un type d'étude, des types de critères à évaluer),

□ recherche de critères objectifs qui permettent de faire une analyse technico-économique,

□ détermination de l'architecture la plus adaptée aux besoins (oriente vers un type d'analyse),

□ soutien à la conception d'un équipement.

Ces points sont combinables ; ainsi une entreprise peut rechercher l'architecture la mieux adaptée à ses besoins pour alimenter un process critique dans le cadre d'une analyse technico-économique.

Face aux questions : où, pour alimenter quoi, quelle est la criticité et la durée de la perte d'alimentation admissible, le client doit réfléchir par exemple en terme de sécurité, de perte de production ou d'informations.

■ Le risque :
pour une compagnie d'assurance la notion de risque correspond au poids (moral, social, économique) des événements redoutés. En ce qui concerne une perte de production, l'estimation du risque est assez simple : le produit de la probabilité d'occurence par le coût de l'événement redouté donne une idée assez juste. L'évaluation du risque permet de connaître le prix à payer : perte de bénéfice ou assurance ou installation électrique optimisée.

■ Formalisation des besoins (cf. **fig. 12**) :
un moyen d'expression du besoin consiste à classer les divers récepteurs en fonction du temps de coupure qu'ils peuvent supporter (aucun, quelques secondes, quelques minutes, quelques heures).

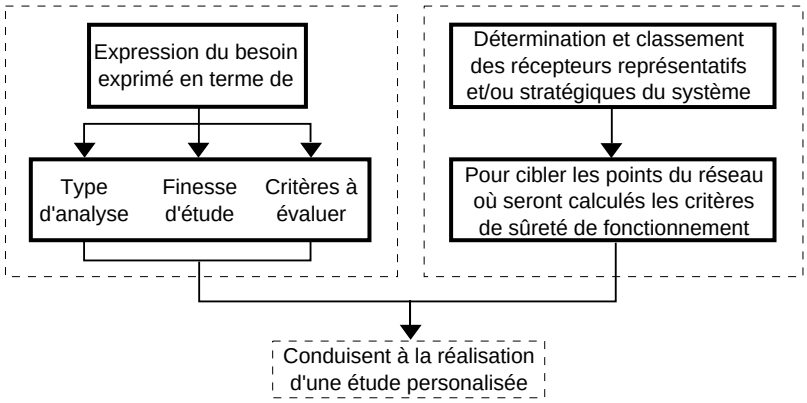


Fig. 11 : informations nécessaires à l'étude.

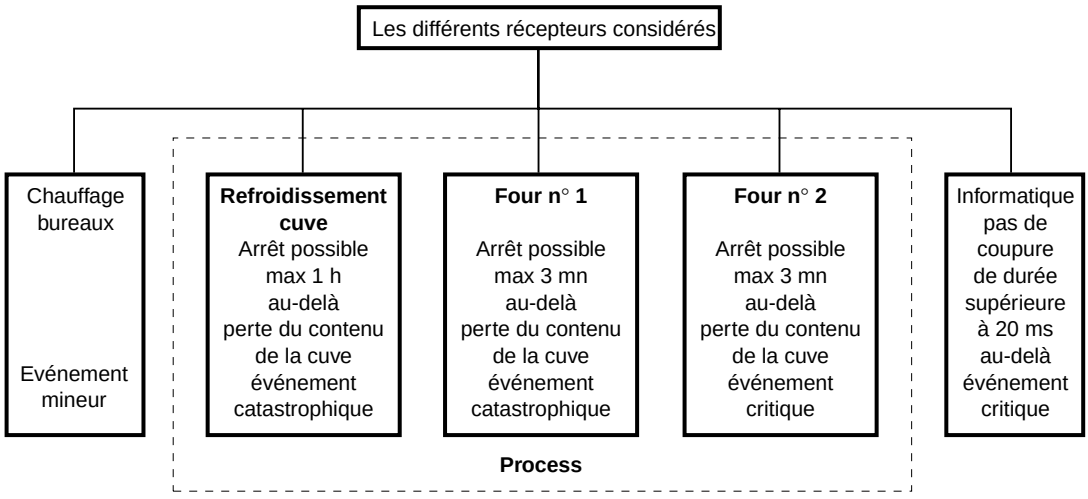


Fig. 12 : les spécifications de disponibilité incombent au client.

2.3 Analyse fonctionnelle du système

L'analyse fonctionnelle décrit sous forme visuelle et textuelle le rôle du réseau et/ou d'éléments constitutifs.

Cette analyse aboutit à deux descriptions complémentaires du réseau :

- une description, formalisée par des blocs diagrammes fonctionnels (cf. **fig. 13**), dont le but est de présenter l'architecture du système et les liens fonctionnels entre les différents éléments du système,
- une description comportementale (cf. **fig. 14**) dont le but est de décrire l'enchaînement des différents états possibles. L'accent est principalement mis sur l'identification des événements qui induisent des évolutions du système. Le modèle développé lors de cette analyse met l'accent notamment sur les différents points de reconfiguration de l'architecture.

Cette deuxième analyse permet de prendre en compte l'aspect fonctionnel quand il interagit avec l'aspect dysfonctionnel.

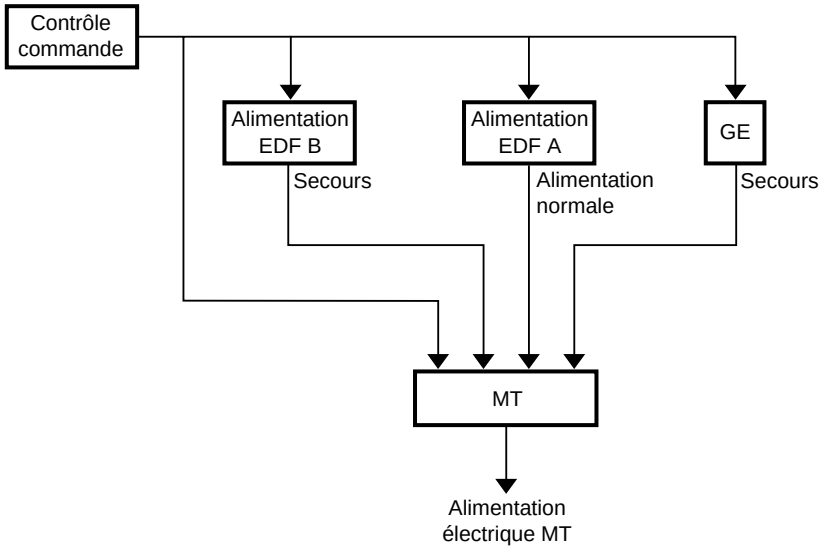
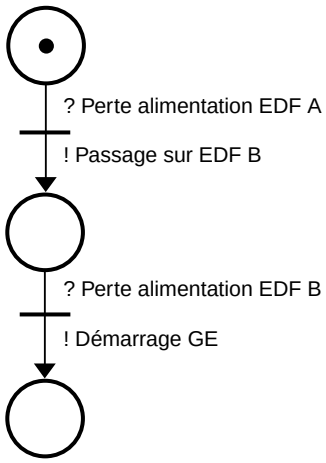


Fig. 13 : blocs diagrammes fonctionnels.



Ce réseau de Pétri exprime le fait qu'en cas de perte de EDF A il y a passage sur EDF B.
Si EDF B est défaillant il y a alors démarrage des GE.

Fig. 14 : description comportementale sous forme de réseau de Pétri.

2.4 Analyse des modes de défaillances

Cette analyse a pour objet de fournir :

- la liste des modes de défaillances possibles pour chacun des éléments identifiés dans l'analyse fonctionnelle,
- leurs causes d'occurrence (une seule cause suffit),
- les conséquences de ces défaillances sur le système (appelées aussi événements simples),
- le taux de défaillance associé à chaque mode de défaillance dans le cadre d'une étude quantitative.

Les résultats sont présentés sous forme de tableaux (cf. **fig. 15**).
Cette analyse peut être considérée comme la première étape de modélisation.

Fonctions	Modes de défaillances	Causes	Effets sur le système
Arrivée EDF	Perte du mode normal	■ Panne EDF ■ Panne transformateur ■ Disjoncteur intempestivement ouvert	Basculement sur le secours
Secours	Perte du mode secours en fonctionnement	■ Défaillance en fonctionnement du GE ■ Disjoncteur intempestivement ouvert ■ Panne transformateur	Perte de l'alimentation électrique
	Panne mode normal et mode secours non disponible	■ Non démarrage GE ■ Disjoncteur bloqué ouvert	

***Fig. 15** : analyse des modes de défaillances.*

2.5 Données de fiabilité

Dans le cadre d'évaluation quantitative il est nécessaire d'avoir les données probabilistes des défaillances des équipements du système.
Les caractéristiques probabilistes sont à associer aux modes de défaillances. Ce sont :

- le taux de défaillance et sa décomposition en fonction des modes de défaillances,
- le temps moyen de réparation associé et la fréquence de la maintenance préventive (cf. **fig. 16**).

Les taux de défaillances

Rappelons qu'il s'agit de quantifier la probabilité qu'il y ait une défaillance entre [t, t+dt], sachant qu'il n' y a pas eu de défaillance avant t.

Schneider Electric dispose d'une base de données alimentée par plusieurs sources :

- études internes et analyse des matériels en retour après défaillance,
- statistiques de défaillances observées par les distributeurs d'énergie et autres constructeurs,
- recueils de fiabilité notamment américains,
- □ pour les composants non électroniques :

- l'IEEE 500 (retours d'expérience de centrales nucléaires des USA),
- la NPRD 91 (retours d'expérience de systèmes militaires et non militaires des USA),

Equipements	Modes de défaillances	Taux de défaillance	Temps de réparation, fréquence de maintenance préventive
Disjoncteur	■ Bloqué fermé ■ Intempestivement ouvert	λ_1 λ_2	μ_1, —
Groupe électrogène	■ Défaillance en fonctionnement ■ Défaillance au démarrage	λ_4 λ_5	μ_2, 6 mois
Transformateur	■ Défaillance en fonctionnement	λ_6	μ_3, X mois

***Fig. 16** : extrait fictif de données de fiabilité nécessaires à une étude.*

□ pour les matériels électroniques, les données sont généralement obtenues par calcul à partir du Military Handbook 217 (F) ou du recueil de fiabilité du Centre National d'Etudes des Télécommunications.

Certains composants pendant une période de leur vie ont un taux de défaillance (λ) qui est constant en fonction du temps. C'est à dire que leur capacité à être en panne est indépendante du temps ; c'est le cas des composants électroniques (loi exponentielle).
Les composants électrotechniques vieillissent, autrement dit leur taux de défaillance n'est pas constant avec le temps. Les données le plus souvent disponibles supposent des taux constants.
L'utilisation de données non spécifiques au système étudié, de taux de défaillance constants alors que certains constituants vieillissent, est malgré tout fort intéressante car cela permet d'établir des comparaisons valables entre systèmes.
Le fait de trouver une architecture 10 fois plus fiable qu'une autre, 10 fois plus disponible... veut dire que cette architecture est dix fois meilleure pour le critère considéré ; la valeur relative est souvent plus importante que la valeur absolue.

La base de données de fiabilité de Schneider Electric a pour but de rassembler le plus de données possibles. Des critères de validité ont été mis en place pour garantir la qualité des données intégrées. On s'assure :

■ de la façon dont le retour d'expérience a été effectué, sur quelles données il est basé,

■ de la méthode de calcul prévisionnel utilisée, des conditions d'utilisation, de température, d'environnement...

A terme, ce travail permet de disposer de données de fiabilité pour l'étude d'une installation quelconque ou d'être capable de les obtenir par extrapolation.

Les temps moyens de réparation
sont directement fonction de la politique de maintenance de l'entreprise. Les choix décisifs portent notamment sur les possibilités de stock, les heures de présence des dépanneurs, les fréquences de maintenance préventive, le type de contrat de maintenance avec les fournisseurs...
L'impact de la variation des paramètres de politique de maintenance sur les performances du système peut faire l'objet d'une analyse spécifique.

Les reconfigurations fonctionnelles
Dans le cas de reconfigurations fonctionnelles, lorsque le fonctionnel interagit avec le dysfonctionnel (par exemple dans le cas de délestage tarifaire) la fréquence de ces reconfigurations intervient dans la modélisation.

2.6 Modélisation

Les dysfonctionnements du réseau sont représentés par un modèle. Le modèle est une représentation graphique des combinaisons des événements déterminés par l'analyse des modes de défaillances qui contribuent par exemple à la perte de l'alimentation électrique de certains récepteurs et de leur processus de réparation.
Ce modèle permet :

■ de dialoguer avec le client pour valider notre compréhension des dysfonctionnements du réseau,

■ d'analyser qualitativement les performances du réseau, par la recherche des modes communs, des combinaisons les plus simples qui contribuent à l'événement redouté,

■ d'évaluer les performances du réseau par le calcul des critères de sûreté de fonctionnement.

Différentes techniques sont disponibles selon l'architecture du système étudié, les événements indésirables concernés, les critères à évaluer et les hypothèses prises en compte dans le(s) modèle(s).

Les principales techniques de modélisation

■ Combinatoire : combinaison d'événements simples, c'est le cas des arbres de défaillance (cf. **fig. 17**).
Un arbre de défaillance est une décomposition d'événements en événements simples.
Ainsi les causes immédiates de la perte de l'alimentation électrique sont recherchées, ce sont des événements intermédiaires. Les causes de ces événements intermédiaires sont recherchées à leur tour. La décomposition se poursuit jusqu'a ce qu'elle soit devenue impossible ou inutile. Les événements terminaux sont appelés événement de base. La décomposition d'un événement en événements-causes s'effectue par l'intermédiaire d'opérateurs logiques appelés portes (porte ET, porte OU).
L'arbre de défaillance de la **figure 17** exprime que dans le réseau pris en exemple il y aura perte totale de l'alimentation électrique s'il y a perte de « l'alimentation EDF » et perte des « groupes électrogènes ». Dans ce type de modélisation il n'est pas tenu compte du fait que la défaillance des groupes électrogène n'a un sens que s'il y a eu perte de « l'alimentation EDF » dans un premier temps.
Les réseaux avec reconfiguration et stratégies de maintenance complexes sont difficilement modélisables par un arbre de défaillance.

■ Combinatoire et séquentielle : combinaison d'événements simples en tenant compte du moment où les événements se produisent.

□ De type markovien (cf. **fig. 18**).
Pour formaliser ce type de modèle il est d'usage d'utiliser un graphe qui représente les différents

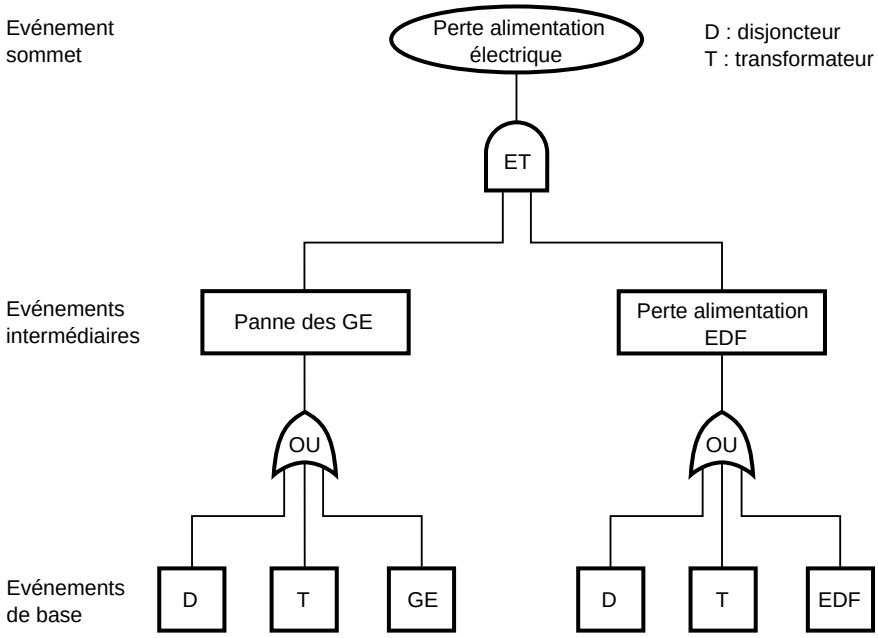


***Fig. 17** : modélisation par arbre de défaillance. Le fait que la défaillance des GE n'a un sens que si il y a eu perte EDF dans un premier temps n'apparait pas.*

λ_a : fréquence à laquelle il y a perte de l'alimentation EDF
λ_b : fréquence de panne des GE
μ : fréquence de réparation

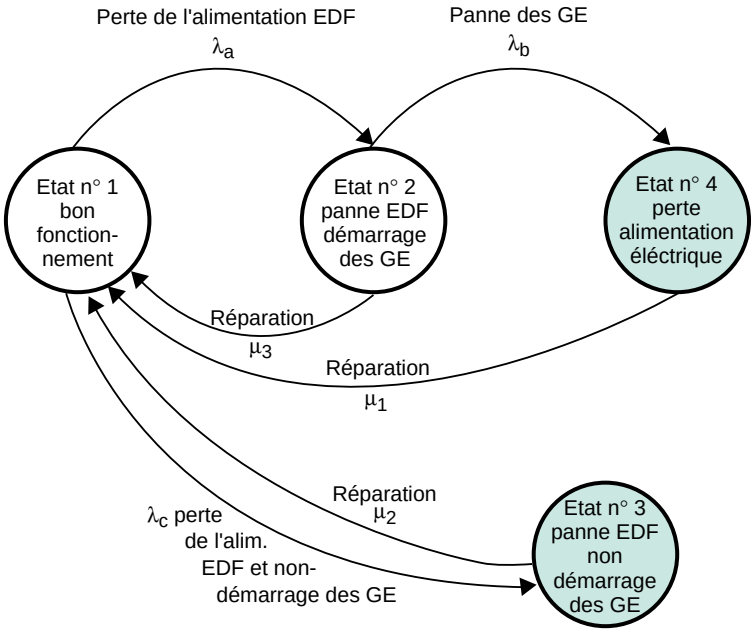


***Fig. 18** : modélisation dysfonctionnelle sous forme de graphe de Markov. λa, λb, μ sont par principe constants.*

états possibles du système. Les arcs qui permettent de relier les états du système sont caractérisés par des taux, qui peuvent être des taux de défaillances, des taux de réparations, des fréquences représentatives du mode d'exploitation. Ces taux représentent la probabilité que le système change d'état entre t et t+dt.

Le graphe de la **figure 18** exprime que le système peut avoir 4 états de fonctionnement :

- l'état n° 1 est l'état de bon fonctionnement,
- l'état n° 2 est l'état où « l'alimentation EDF » est défaillante et où les groupes électrogènes ont démarré,
- l'état n° 3 est l'état où « l'alimentation EDF » est défaillante et où les groupes électrogènes n'ont pas démarré,
- l'état n° 4 est l'état où les groupes électrogènes ont eu une défaillance en fonctionnement sachant que « l'alimentation EDF » est défaillante.

Une modélisation markovienne sous-entend que les fréquences (ou taux) qui permettent de passer d'un état du système à un autre sont des constantes. Les algorithmes de calcul associés à cette technique de modélisation ne peuvent être appliqués que dans ces conditions. Cette limite amène à faire des estimations qui peuvent être plus ou moins proches de la réalité.

□ De type quelconque

Le formalisme employé est généralement celui des réseaux de Pétri. Le réseau est représenté par des places, des transitions et des jetons. Le franchissement d'une transition par un jeton correspond à un événement fonctionnel ou dysfonctionnel possible du système. Ces transitions peuvent être associées à n'importe quel type de loi probabiliste. Seule la simulation permet de résoudre de tels calculs.

Le réseau de Pétri de la **figure 19** représente les différentes défaillances que le système peut subir :

- à la transition n° 1 est associée la probabilité de défaillance de «l'alimentation EDF»,
- à la transition n° 2 sont associées les probabilités de démarrage et de non démarrage des groupes électrogènes,
- à la transition n° 3 est associée la probabilité de défaillance en fonctionnement des groupes électrogènes.

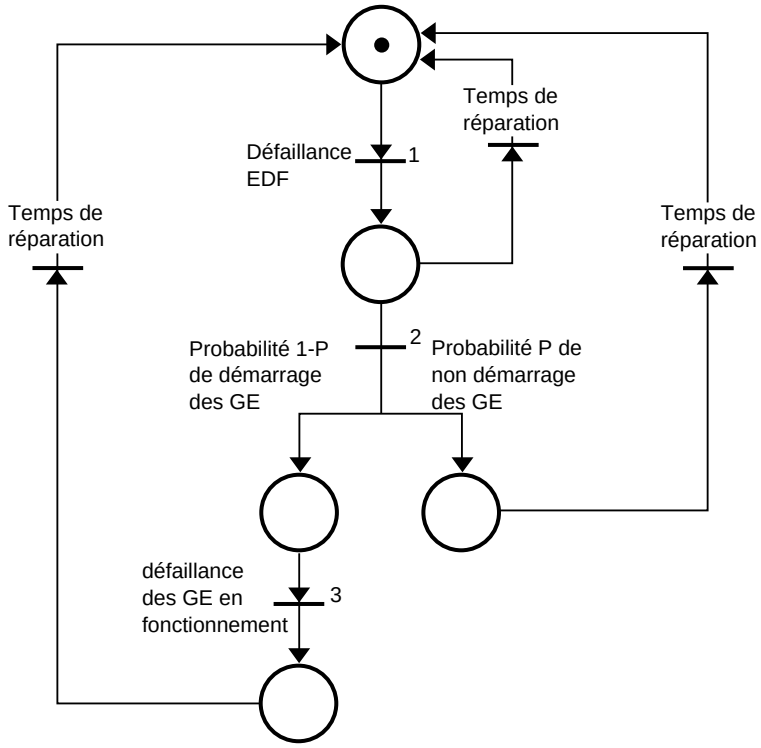


***Fig. 19** : modélisation sous forme de réseau de Pétri.*

Critères pour choisir un type de modélisation :

La **figure 20** présente ces critères sous forme de tableau.

Critères de choix	Arbre de défaillance	Graphe de Markov	Réseau de Pétri
Interaction du mode d'exploitation dans la modélisation	Résolution impossible ou fausse suivant les algorithmes	Sous certaines conditions la résolution peut être impossible ou fausse suivant les algorithmes utilisés	Adapté
Dispersion numérique des données (facteur 1000)	Résolution impossible ou fausse suivant les algorithmes utilisés ; sans problème si simulation	Sous certaines conditions la résolution peut être impossible ou fausse suivant les algorithmes utilisés	Adapté
L'aspect temporel des pannes est important	Non	Adapté	Adapté
Estimation liée à des événements rares	Temps de simulation qui peut être prohibitif, en cas de résolution analytique pas de problème	Adapté	Temps de simulation qui peut être prohibitif
Estimation de :			
■ MUT	-	Adapté	Adapté
■ MTTF	Adapté	Adapté	Adapté
■ D(t)	-	Adapté	-
■ D(∞)	Adapté (calcul analytique)	Adapté	Adapté
■ D moyen à t	Adapté (simulation)	-	Adapté
■ MTTR	-	Adapté	Adapté
■ λ_{eq}	-	Adapté	Adapté

***Fig. 20** : critères pour choisir un type de modélisation.*

2.7 Calculs d'évaluation des critères de sûreté

Deux techniques différentes peuvent être utilisées.

■ Résolution analytique :

□ pour les graphes d'états,

□ pour les arbres de défaillances.

Quand les systèmes sont grands ou complexes la résolution analytique peut être impossible.

■ Simulation du comportement des composants (fonctionnement ou panne) d'un système :

□ pour les réseaux de Pétri,

□ pour les arbres de défaillances.

Pour être précis il faut réaliser un grand nombre de simulations et le temps de calcul peut être prohibitif si l'estimation des mesures est liée à des événements rares.

La modélisation d'un système par réseau de Pétri est la modélisation la plus proche du fonctionnement réel du système étudié. Mais compte tenu des limites liées à la simulation cette technique n'est pas utilisée systématiquement.

3 Exemples d'études

3.1 Comparaison d'architecture entre deux réseaux électriques d'usine

■ Présentation de l'usine

Une usine de production d'eau potable fournit 100 000 m^3/jour, à faible puissance, 300 jours/an et 200 000 m^3/jour à forte puissance 65 jours/an.

La production d'eau est assurée par 4 tranches de production, chacune capable de fournir 100 000 m^3/jour.

A chaque tranche, sont associés six types de récepteurs R_1, R_2, R_3, R_4, R_5, R_6 (des pompes, des désinfecteurs…) qui doivent fonctionner simultanément pour assurer la production (cf. **fig. 21**).

Les récepteurs assurant le fonctionnement de chaque tranche peuvent être repérés de la façon suivante :

R_{1a},…, R_{6a} tranche n° 1
R_{1b},…, R_{6b} tranche n° 2
R_{1c},…, R_{6c} tranche n° 3
R_{1d},…, R_{6d} tranche n° 4

Pour assurer le fonctionnement à faible puissance, une seule tranche est nécessaire ; à forte puissance, deux tranches sont nécessaires.

■ Analyse de la demande, des besoins

Après deux entretiens avec le client, les spécialistes ont déterminé :

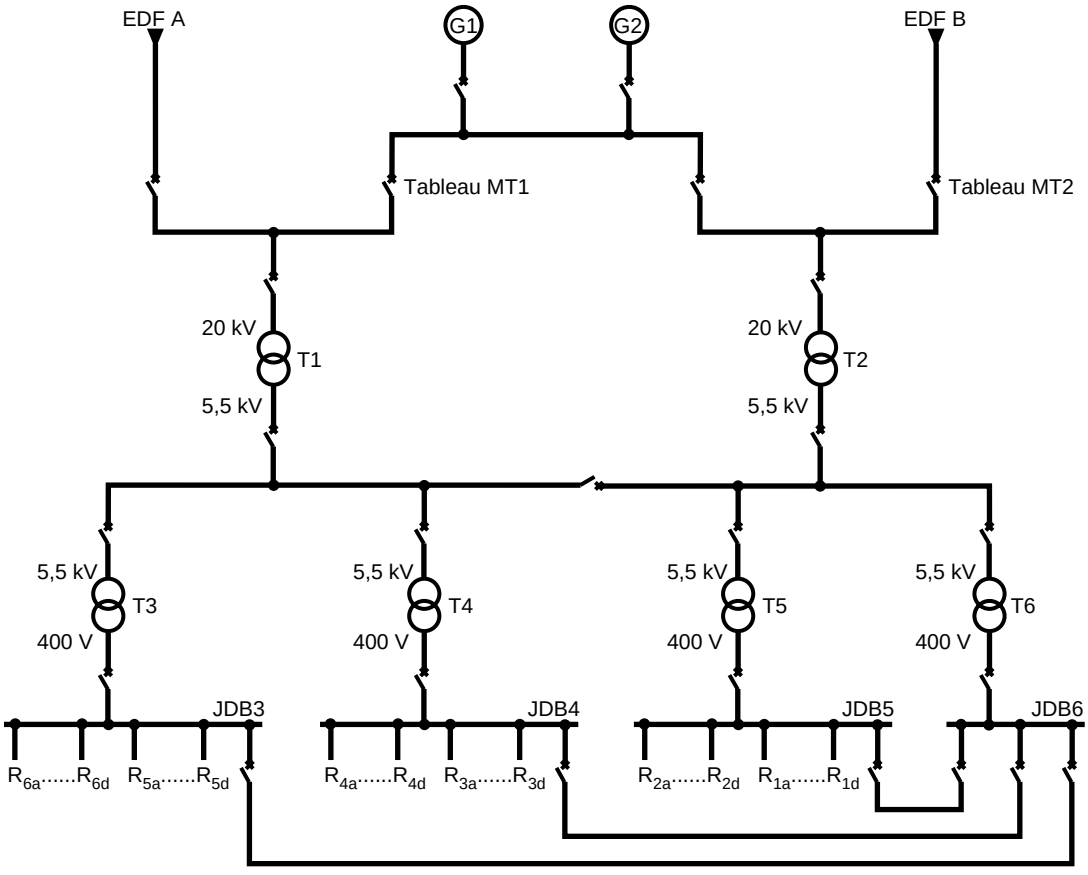


Fig. 21 : schéma de principe simplifié de l'installation d'origine. Certains modes communs pénalisants ne figurent pas.

□ qu'il fallait :

- proposer une nouvelle architecture pour le réseau électrique BT, l'architecture au niveau MT (5,5 kV) devait peu évoluer,
- prouver que le schéma proposé était au moins aussi bon que l'ancien pour certains critères de sûreté de fonctionnement.

□ que les critères de sûreté de fonctionnement à évaluer étaient :

- la probabilité de perdre simultanément l'alimentation électrique des récepteurs n° 1 et des récepteurs n° 6,
- la probabilité de perdre l'alimentation électrique des récepteurs n° 3.

■ Analyse fonctionnelle : considérations générales sur le fonctionnement du réseau

□ Le site est alimenté par deux arrivées EDF indépendantes. Deux groupes électrogènes sont là pour palier aux défaillances des arrivées EDF.

□ En fonctionnement normal le site est alimenté par l'arrivée EDF A. Si cette arrivée est défaillante l'arrivée EDF B prend le relais. Si les deux arrivées EDF sont défaillantes les groupes électrogènes démarrent.

□ Il existe deux niveaux de production, la marche faible et la marche forte. En cas de marche forte la puissance des groupes électrogènes n'est pas suffisante pour assurer la production.

□ La répartition de l'alimentation des récepteurs est telle que la disponibilité n'est pas très bonne. Ainsi par exemple un défaut sur le jeu de barres JDB3 met hors service tous les récepteurs de type R_5 et R_6. La production est arrêtée, plus aucune tranche ne pouvant fonctionner.

□ Le réseau électrique existant était tel qu'il y avait des jeux de barres en mode commun. Un court circuit sur ces jeux de barres rendait inopérantes les reconfigurations.
La probabilité de court circuit d'un jeu de barres est faible mais le système étant fortement reconfigurable cette défaillance devient prépondérante. Les modes communs se situaient au niveau du couplage, lors des reconfigurations intéressant le transformateur T4.

□ Pour le nouveau réseau les récepteurs ont été séparés de manière à ce qu'il soit possible d'assurer la marche faible avec les récepteurs associés à un seul transformateur et la marche forte avec les récepteurs associés à deux transformateurs.
La **figure 22** présente le schéma du réseau proposé.

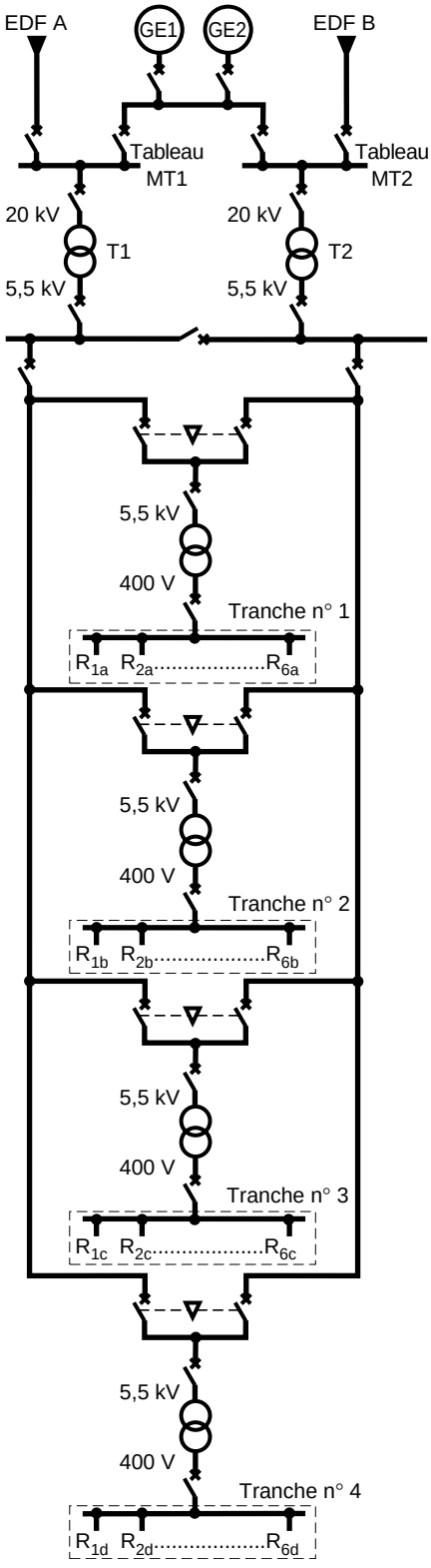


Fig. 22 : schéma de principe de la nouvelle architecture.

La **figure 23** présente son analyse fonctionnelle.

■ Analyse des résultats

L'amélioration des résultats par le réseau proposé est mise en valeur en donnant les rapports d'amélioration, le réseau existant servant de référence.

Outre les probabilités de perte simultanée des récepteurs 1 et 6, et la probabilité de perte des récepteurs 3, nous avons évalué leur fréquence de perte. Ont ausi été calculées la fréquence de mainenance optimale pour les groupes et la contribution aux événements redoutés du réseau MT et BT.

Voici les améliorations obtenues :

□ sur la probabilité relative de perdre simultanément l'alimentation des récepteurs n° 1 et 6 :

- marche faible 110
- marche forte 55
- au global 105

□ sur la probabilité relative de perdre l'alimentation des récepteurs n° 3 :

- marche faible 99
- marche forte 54
- au global 97

Globalement il est 100 fois plus probable de perdre l'alimentation électrique des récepteurs n° 1 et 6 avec l'ancien réseau qu'avec le réseau proposé. En effet dans l'ancien réseau, il y a des

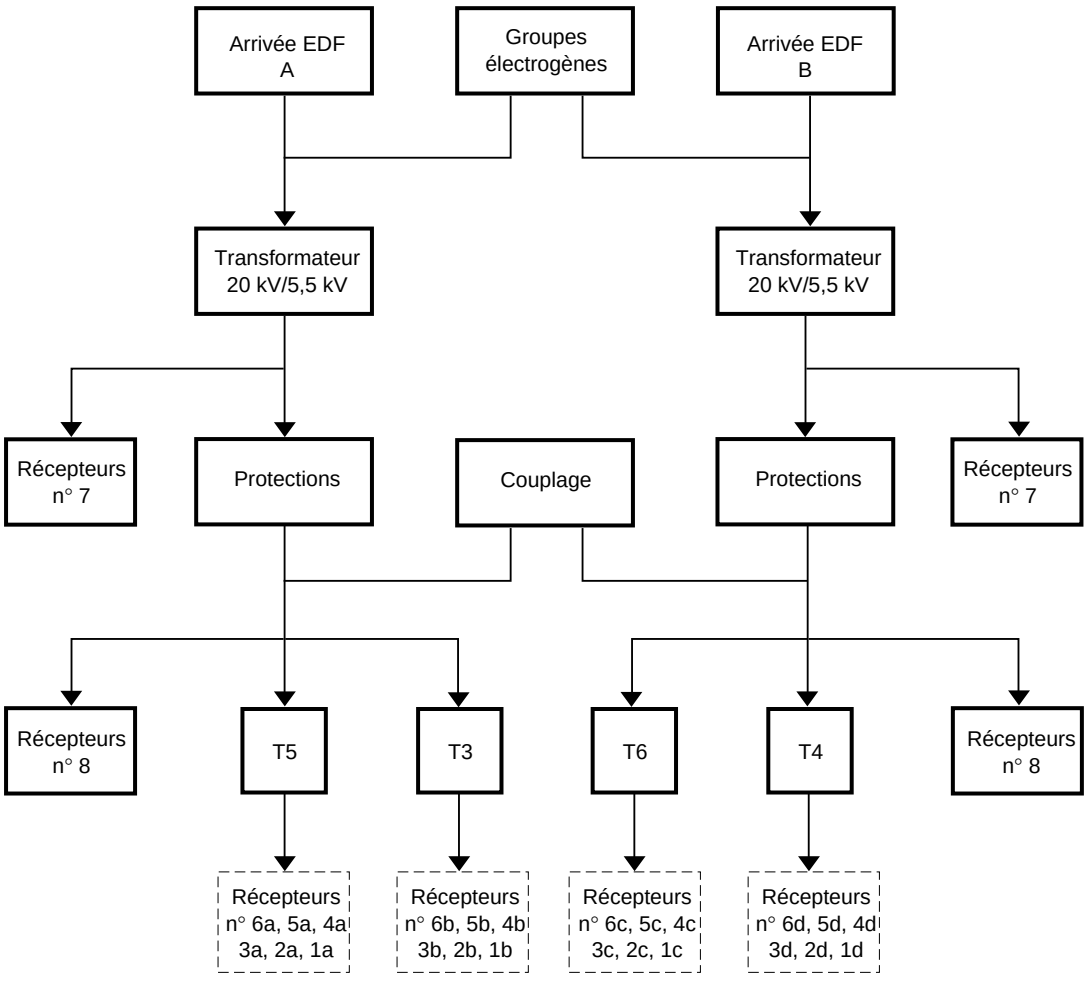


***Fig. 23** : analyse fonctionnelle de la nouvelle architecture.*

défaillances qui contribuent directement à la perte de la fourniture d'énergie électrique.

Si le système fonctionnait uniquement en marche faible ce rapport serait quasiment le même car le système fonctionne surtout en marche faible, d'ou sa prépondérance sur le résultat global.

Si le système fonctionne uniquement en marche forte il est environ 50 fois plus probable de perdre l'alimentation électrique des récepteurs 1 et 6 avec l'ancien réseau.

Dans le cas de la marche forte ce sont les pannes liées à la MT qui sont prépondérantes et cette partie du réseau est peu modifiable.

□ sur la fréquence de perte d'alimentation des récepteurs n° 1 et des récepteurs n° 6 :

- marche faible 22
- marche forte 21
- au global 21

□ sur la fréquence de perte d'alimentation des récepteurs n° 3 :

- marche faible 18
- marche forte 21
- au global 20

Les performances du nouveau réseau sont moins nettes en ce qui concerne les fréquences de pannes.

Les paramètres de calcul d'une probabilité d'indisponibilité sont les fréquences de pannes et les temps de réparation. Les défaillances qui contribuent directement à la perte d'énergie influencent d'autant plus la probabilité d'indisponibilité que leur temps de réparation est grand.

Le nouveau réseau rend possible la maintenance préventive en temps masqué, c'est à dire sans interrompre la production normale de l'usine.

■ Evaluations supplémentaires

Il a paru intéressant d'évaluer des critères supplémentaires de comparaison entre les deux architectectures.

□ Probabilité relative de perdre la marche forte

En cas de marche forte les enjeux économiques sont très importants. Les critères qui avaient été calculés ne mesuraient pas ce risque. Il est tout à fait possible de perdre la marche forte alors que les récepteurs n° 1, 6, et 3 sont alimentés en électricité.

Il est 4 fois moins probable avec le nouveau réseau de perdre la marche maximale.

L'amélioration est moins marquée que pour les autres critères calculés, les pannes principales se situant au niveau MT qui n'est pas modifié.

□ Fréquence optimale de maintenance préventive

La courbe résultant des calculs (cf. **fig. 24**) montre l'impact de la fréquence de maintenance préventive des groupes électrogènes sur la probabilité qu'ils soient disponibles au moment d'une sollicitation.

Pour une fréquence de maintenance de 6 mois la courbe montre qu'il existe un seuil bas pour la probabilité d'indisponibilité à l'arrêt.

□ Contribution aux événements redoutés de la partie MT et de la partie BT pour le réseau proposé.

La partie MT a une contribution beaucoup plus forte que la partie BT (d'environ 99,9 % contre 0,1 %).

Puisque le réseau MT n'a pas été modifié, sa maintenance préventive devra être optimisée ; par ailleurs il sera hautement souhaitable d'avoir recours à un contrôle-commande de qualité sur le réseau MT.

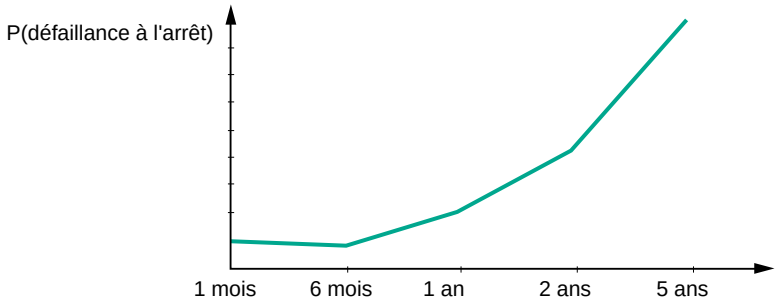


***Fig. 24** : indisponibilité à l'arrêt d'un groupe électrogène en fonction de la périodicité de la maintenance.*

3.2 Intérêt d'un poste de contrôle-commande délocalisé pour un poste THT

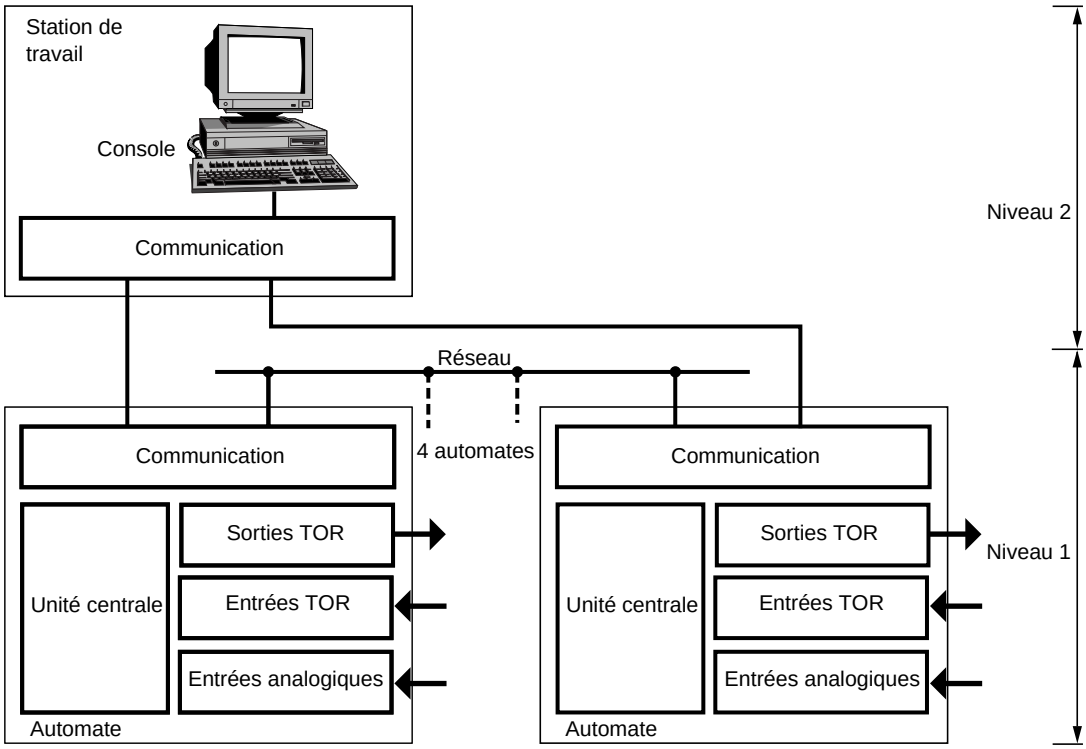


Fig. 25 : architecture de base du contrôle-commande d'un poste THT.

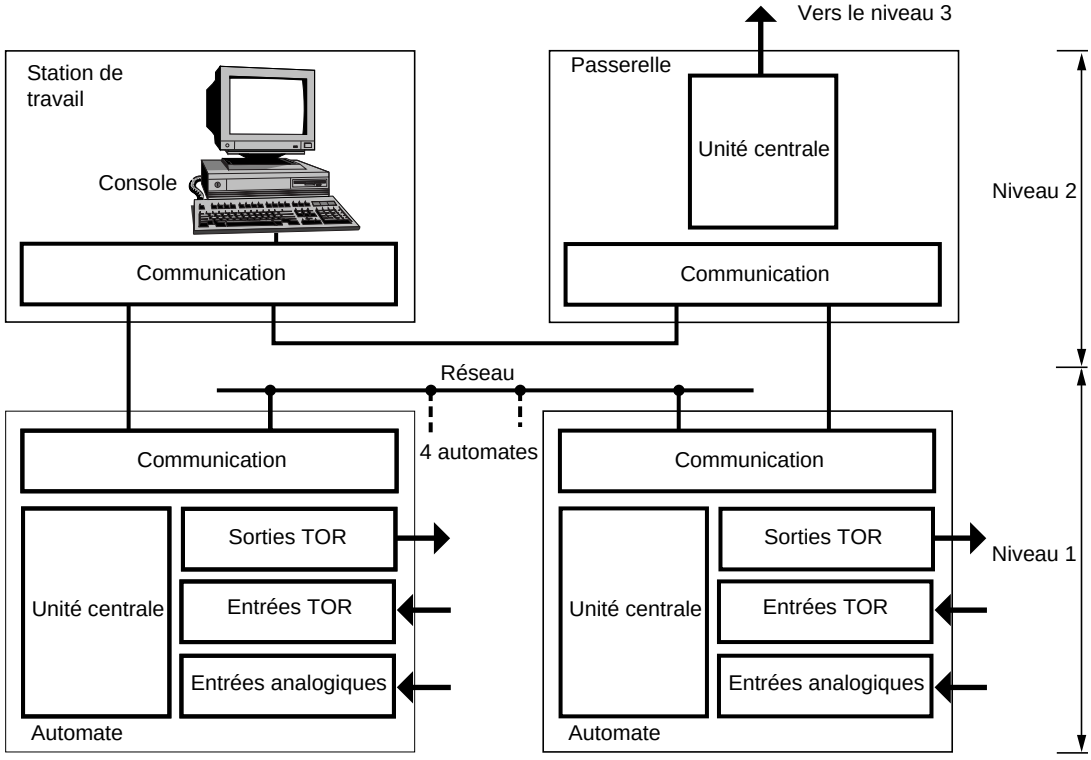


Fig. 26 : architecture de contrôle-commande du poste THT avec passerelle et station de travail.

■ Analyse de la demande, des besoins

Dans le cadre d'offres de contrôle-commande de poste THT à l'étranger Schneider réalise des préétudes de sûreté. La préétude suivante devait déterminer quelle était l'architecture qui permettrait d'atteindre les objectifs de sûreté fixés par le client vis à vis de la perte du contrôle-commande.

Il fallait rechercher s'il était nécessaire de réaliser une station de travail redondante et délocalisée.

■ Analyse fonctionnelle

Le contrôle-commande du poste THT concerné comprend :

- quatre automates qui réalisent l'acquisition des états des équipements électrotechniques du poste, la restitution des commandes (niveau 1),
- une station de travail qui permet de visualiser l'état du poste, de transmettre les commandes (niveau 2),
- et éventuellement une station de travail délocalisée. La station de travail délocalisée est alors redondante avec la station de travail du poste.

La **figure 25** présente la solution de base qui correspond à une seule station de travail au niveau 2.

La **figure 26** présente la solution avec passerelle vers une station délocalisée.

■ Analyse des résultats

Le contrôle-commande choisi doit avoir une probabilité d'indisponibilité inférieure à 10^{-4} à t = 1200 heures. Soit un temps de non fonctionnement du système inférieur à 7 minutes après 1200 heures de fonctionnement (50 jours). L'événement redouté comme la perte du contrôle-commande a été affiné en trois événements redoutés correspondant aux calculs de :

- la probabilité de perdre totalement le contrôle-commande (mode commun),
- la probabilité de perdre au moins une information TOR,
- la probabilité de perdre au moins une information ANA,

soit trois calculs par architecture.

Le matériel est divisé en deux classes :

- le matériel dont on dispose de lots de rechange (n),
- le matériel dont on ne dispose pas de lots de rechange (s).

Deux calculs sont réalisés par événement redouté, pour montrer l'impact sur le résultat final du choix des temps moyens de réparation (cf. **fig. 27**).

L'hypothèse 2 est la plus réaliste ; ce sont ces temps qui seront pris en compte pour choisir entre les deux solutions.

	MDT matériel de type n	MDT matériel de type s
Hypothèse 1	1 heure	3 heures
Hypothèse 2	4 heures	12 heures

Fig. 27 : deux hypothèses de temps moyens de réparation.

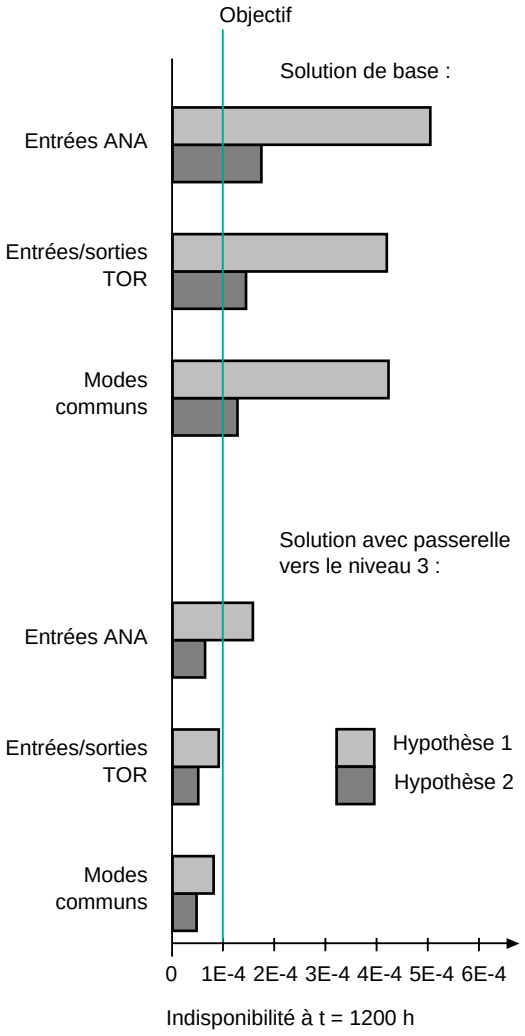


Fig. 28 : histogramme des indisponibilités pour les deux solutions (le repère orange correspond à l'objectif à atteindre, il est atteint si l'histogramme reste à gauche du repère).

Comme le montre la **figure 28** :

- la solution sans station délocalisée ne permet pas d'obtenir la disponibilité souhaitée,
- la solution avec contrôle-commande déporté permet d'atteindre l'objectif pour les entrées TOR et les modes communs ; mais la probabilité de perdre au moins une entrée ANA reste supérieure à l'objectif fixé.

4 Les outils de la sûreté de fonctionnement

4.1 Outils d'aide à l'analyse dysfonctionnelle

Certains outils génèrent automatiquement une analyse dysfonctionnelle à partir de l'analyse fonctionnelle du système et des modes de défaillances des composants. Il y a génération d'un modèle, qui permet l'évaluation des critères de sûreté de fonctionnement.

Ces outils sont utiles pour des systèmes complexes et/ou répétitifs.
Ils permettent de créer une base de données sur les modes de défaillance des composants, sur les conséquences de ces défaillances lorsque ceci est possible (cf. **fig. 29**).

Nom de l'outil	Technique de modélisation	Technique de résolution de calcul	Caractéristiques principales
Adélia	Arbre de défaillance	■ Analytique ■ Simulation	Outil développé par Schneider Electric pour modéliser les dysfonctionnements des composants des réseaux électriques. Il intègre une base de données sur les dysfonctionnements des réseaux électriques. La description du réseau et de l'événement redouté entraîne la création automatique de l'arbre de défaillance correspondant.
Sofia	Arbre de défaillance	■ Analytique (polynome logique)	Outil développé par SGTE Sofreten. Génération automatique d'un arbre de défaillance et de l'AMDE associée, par la description fonctionnelle du système et la création d'une base de données dysfonctionnelle associée.

Fig. 29 : deux types d'outils d'aide à l'analyse dysfonctionnelle utilisés habituellement par Schneider.

4.2 Outils de modélisation

Deux types d'outils (cf. **fig. 30**) :

- les outils de simulation,
- les outils de calcul analytique.

Remarque : un graphe de Markov peut être très facilement transformé en réseau de Pétri et faire l'objet d'une simulation. Inversement à tout réseau de Pétri un graphe peut être associé mais il faut alors « markoviniser » les transitions : dans un graphe de Markov les fréquences de passage des transitions sont forcément constantes.

Type de modélisation	Outil de simulation	Outil de calcul analytique
Graphe de Markov		**Supercab** développé par ELF AQUITAINE
Réseau de Pétri	**MOCA-RP** développé par Microcab	

Fig. 30 : les outils de modélisation.

Schneider dispose actuellement sur PC d'une interface graphique intitulée PCDM qui génère automatiquement le fichier de définition du graphe de Markov ou du réseau de Pétri dessiné (cf. **fig. 31**).
Ceci apporte un gain de temps et une fiabilisation de la saisie des données.
L'utilisation des « réseaux de Pétri » est la technique de modélisation actuellement la plus proche du comportement réel d'un système.

L'accélération de la simulation de réseaux de Pétri notamment grâce au logiciel MOCA-RP fait l'objet d'une thèse dont les premiers résultats ont été présentés au congrés ESREL 96 (European Safety Reliability).
Dans un avenir proche l'utilisation des réseaux de Pétri ne sera plus limitée par le temps de simulation.

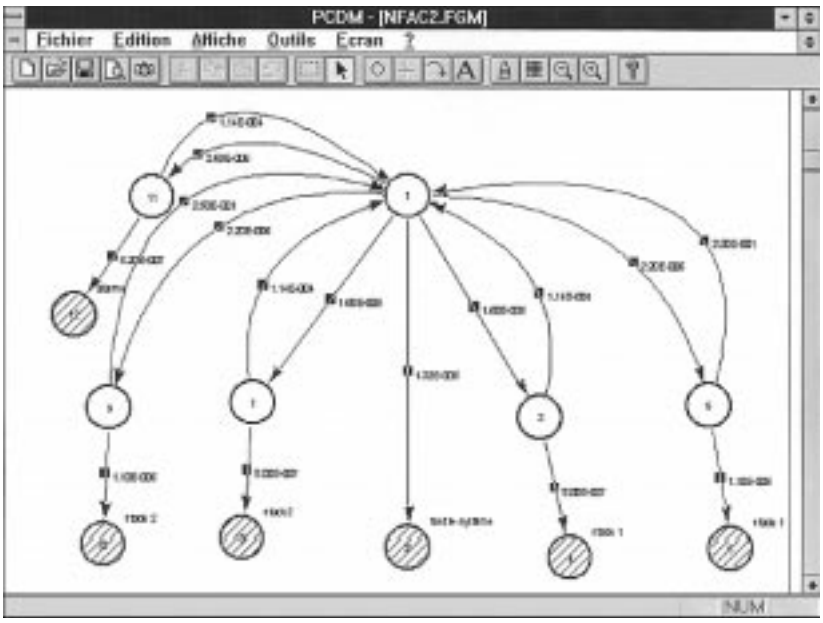


***Fig. 31** : interface graphique PCDM - graphe de Markov.*

5 Conclusion

La sûreté se décline en :

- sécurité,
- fiabilité,
- disponibilité,
- maintenabilité.

Les impératifs de sécurité ont d'abord imposé les études de sûreté sur les applications à risques : les transports ferroviaires et aériens, les centrales nucléaires. Si on y ajoute les impératifs de fiabilité, disponibilité et maintenabilité, bien d'autres domaines sont concernés.

Les exigences ont progressé vis à vis de la qualité de l'électricité. Compte tenu de l'amélioration considérable des méthodes et des matériels, les utilisateurs sont en droit aujourd'hui d'exiger un haut niveau de disponibilité. Pour atteindre cet objectif avec une confiance justifiée, les études de sûreté sont nécessaires.

Elles permettent d'optimiser :

- l'architecture du réseau électrique,
- le système de contrôle-commande,
- la politique de maintenance.

Elles permettent de choisir les solutions adaptées pour atteindre le seuil de disponibilité désiré, au meilleur coût. Souvent, l'étude peut se limiter à un point clé de l'installation, sur lequel repose la plus lourde part de l'indisponibilité globale.

Dans de nombreux cas, il est intéressant de faire appel à un spécialiste. Un conseil de sa part peut être déterminant.

6 Bibliographie

Normes

- CEI 50 : Vocabulaire electrotechnique international, chapitre 191: Sûreté de fonctionnement et qualité de service.
- CEI 271/UTE C20310 : Liste des termes de base, définitions et mathématiques applicables à la fiabilité.
- CEI 300 : Gestion de la sûreté de fonctionnement - 3ème partie : Guide d'application - Section 1 : Techniques d'analyse de la sûreté de fonction-nement - Guide méthodologique.
- CEI 305/UTE C20321 à 20327 : Essai de fiabilité des équipements.
- CEI 362/UTE C20313 : Guide pour l'acquisition des données de fiabilité, de disponibilité et de maintenabilité à partir des résultats d'exploitation des dispositifs électroniques.
- CEI 671 : Essais périodiques et surveillance du système de protection des réacteurs nucléaires.
- CEI 706/X 60310 ET 60312 : Guide maintenabilité de matériel
- CEI 812/X 60510 : Techniques d'analyse de la fiabilité des systèmes. Procédure d'Analyse des Modes de Défaillance et de leurs Effets (AMDE).
- CEI 863/X 60520 : Prévision des caractéristiques de fiabilité, maintenabilité et disponibilité.
- CEI 880 : Logiciels pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires.
- CEI 987 : Calculateurs programmés importants pour la sûreté des centrales nucléaires.
- CEI 1165 : Application des techniques de Markov.
- CEI 1226 : Centrale nucléaire - Système d'instrumentation et de contrôle-commande important pour la sûreté - classification.
- NF C 71-011 : Sûreté de fonctionnement des logiciels - Généralité.
- NF C 71-012 : Sûreté de fonctionnement des logiciels - Contraintes sur le logiciel.
- NF C 71-013 : Sûreté de fonctionnement des logiciels - Méthodes appropriées aux analyses de sécurité.

Publications diverses

[1] « Fiabilité des systèmes »
A. PAGES et M. GONDRAN
Eyrolles 1983

[2] « Sûreté de fonctionnement des systèmes industriels »
A. VILLEMEUR
Eyrolles 1988

[3] Recueils de données de fiabilité :
- Military Handbook 217 F
Department of Defense (US)
- Recueil de données de fiabilité du CNET(Centre National d'Etudes des Télécommunications)
1993
- IEEE 493 et 500 (Institute of Electrical and Electronics Engineers)
1980 et 1984
- IEEE Guide to the collection and presentation of electronic sensing component, and mechanical equipment reliability data for nuclear-power generating stations
- Document NPRD91 (Nonelectronics Parts Reliability Data) du Reliability Analysis Center (Department of Defense US)
1991

[4] Recommandations
- MIL-STD 882 B
- MIL-STD 1623

Cahiers Techniques Schneider

- Introduction à la conception de la sûreté
Cahier Technique n° 144
P. BONNEFOI
- Distibution électique à haute disponibilité
Cahier Technique n° 148
G. GATINE 1989
- Sûreté de fonctionnement et tableaux électriques BT
Cahier Technique n° 156
Ph. ROMANET-PERROUX
- Permutation automatique des alimentations dans les réseaux HT et BT
Cahier Technique n° 161
G. THOMASSET
- La sélectivité énergétique en BT
Cahier Technique n° 167
R. MOREL, M. SERPINET
- Sûreté des protections en MT et HT
Cahier Technique n° 175
M. LEMAIRE

Participation Schneider à différents groupes de travail

- Groupe statistiques du comité 56 (normes de fiabilité) de la CEI,
- Sûreté du logiciel au groupe Européen EWICS - TC7 : computer and critical applications,
- Groupe de travail de l'AFCET sur la sûreté de fonctionnement des systèmes informatiques,
- Participation à la mise à jour du recueil de fiabilité du CNET,
- Groupe de travail IFIP 10.4
Dependable computing.

Schneider

Direction Scientifique et Technique,
Service Communication Technique
F-38050 Grenoble cedex 9
Télécopie : (33) 04 76 57 98 60

Réalisation : Sodipe - Valence
Edition : Schneider.
Impression : Clerc - Fontaine - 2000.
- 100 FF-