Rapport d'étude



# XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

##### XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

|  |
| --- |
| Étude de sûreté de fonctionnement des alimentations électriques Haute et Basse Tension |
|  |
| Note Technique |

|  |  |  |
| --- | --- | --- |
| Référence : À Completer | Date : 03/11/2021 | Version A |

# Information qualité du document

### Destinataire

|  |  |
| --- | --- |
| Nom | Service |
| à completer | à completer |
|  |  |
|  |  |

### Historique des modifications

|  |  |
| --- | --- |
| Controle finale |  |
| Date | à completer |
| Nom | à completer |
| Signature | à completer |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Rédigé | Controle externe | modifications |
| A | à completer |  |  |  |
| A | à completer |  |  |  |
| A | à completer |  |  |  |

|  |  |
| --- | --- |
| Autres Informations |  |
| Auteur | à completer |
| Confidentialité | Diffusion Restreinte |
| Date de reference | à completer |
| Nom du fichier | à completer |
| Type de document | Note technique |
| Statut document | Final |
| Nombre de pages | à completer |
| Titre du document | Etude de sûreté de fonctionnement des alimentations électriques Haute et Basse Tension |

# Sommaire

Preambule

#### Objectifs

à compléter

### Document et données de référence

## Présentation des études de sûreté de fonctionnement

#### Cadre général du management des risques

##### Contexte

Les systèmes industriels sont conçus afin d’assurer un ensemble de fonctionnalités données dans des conditions définies comme acceptables. Pour un réseau électrique, par exemple, il s’agit généralement de garantir l’alimentation d’un ensemble de points de livraison, en respectant certaines exigences en termes de continuité de fourniture, de qualité de l’onde et de sûreté des biens et des personnes.

Or, ces systèmes peuvent être victimes d’incidents susceptibles d’impacter leurs fonctionnements : il peut s’agir de défaillances matérielles des équipements, d’agressions environnementales (événements climatiques, incendies, pollution…), d’erreurs humaines, de vandalisme, etc

Les manquements à ces fonctionnements attendus constituent, pour les entreprises qui opèrent ces systèmes, des événements redoutés, aussi appelés risques, qui peuvent être plus ou moins critiques en fonction :

* De leur gravité, c’est-à-dire de l’impact qu’ils auraient s’ils se réalisaient.
* De leur vraisemblance, c’est-à-dire de leur probabilité de survenue.

Pour maitriser ces risques, des processus de management dédiés doivent être mis en œuvre dès la conception des systèmes, en vue de les identifier et de s’assurer que leurs niveaux de criticité restent acceptables pour l’entreprise. Cette démarche générale fait l’objet de normes internationales, dont les principales sont l’ISO 31000 « Management du risque – Principes et lignes directrices », et l’ISO Guide 73 « Management du risque – Vocabulaire ».

##### Les analyses de risques

Le management des risques s’appuie sur un processus d’analyse des risques, qui est la démarche formalisée visant à identifier, quantifier et apprécier l’importance relative des différents risques pesant sur un système (existant ou en conception), en vue d’orienter les décisions de l’organisme afin de se prémunir de ceux qu’elle juge inacceptables.

De façon générale, les différentes étapes de cette démarche d’analyse sont illustrées sur la figure ci-après.

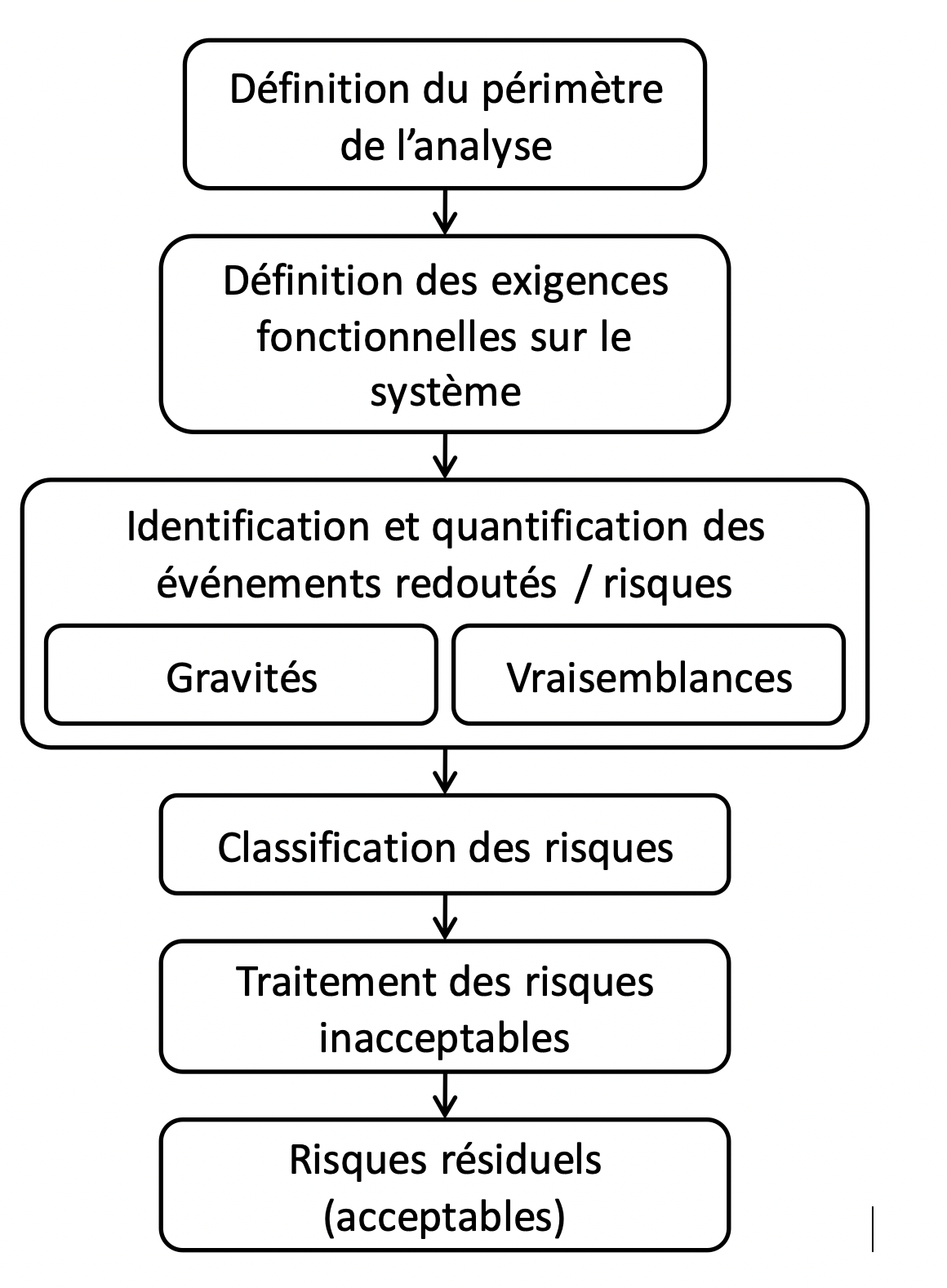


Figure 1 : La démarche d’analyse des risques

Dans un premier temps, le périmètre de l’étude est précisé : il s’agit principalement de définir le système analysé et la nature des incidents susceptibles d’engendrer les événements redoutés pris en compte. Ainsi, par exemple, certaines études peuvent ne s’intéresser qu’aux défaillances matérielles des équipements constitutifs du système, d’autres peuvent se focaliser sur les incidents ayant trait à la sécurité informatique, d’autre encore peuvent considérer à la fois des incidents de nature fortuite et délibérée, etc. Le choix des incidents à considérer est très souvent dicté par les leviers à disposition de l’entité pour traiter les éventuels risques inacceptables par la suite.

Sur ce périmètre défini, les exigences fonctionnelles attendues du système sont précisées. Pour un réseau électrique, par exemple, des besoins ayant trait à la continuité de fourniture peuvent être formulés. Un exemple d’exigence pourrait être « l’alimentation électrique au niveau d’un point d’intérêt donné (par exemple : un tableau basse tension) ne devrait pas être interrompue pendant plus de 5 secondes » (parce que le procédé alimenté en aval dispose d’une inertie lui permettant de supporter une coupure d’une durée inférieure).

Un manquement à une exigence sur une fonction attendue du système constitue un événement redouté (ou risque), pour lequel le niveau de gravité et le niveau de vraisemblance vont être estimés. Généralement, l’appréciation de l’impact d’un risque est un processus relativement maitrisé, dans la mesure où il est intimement lié au métier : une coupure électrique inacceptable sur un processus industriel peut ainsi entrainer une perte de production ou un impact d’image par exemple. En revanche, l’estimation de la probabilité d’occurrence associée est très souvent plus délicate, particulièrement sur les systèmes complexes disposant de redondances et de capacités de reconfigurations visant à palier d’éventuelles défaillances. C’est la raison pour laquelle des outils et méthodes mathématiques spécifiques, qui seront présentées par la suite, sont généralement employées

L’identification et la quantification de l’ensemble des risques pesant sur le système étudié permet la constitution d’une cartographie des risques, classiquement présentée sous la forme d’un tableau à double entrée (gravité, vraisemblance). Un tel tableau permet à la fois de :

* identifier les risques jugés inacceptables, c’est-à-dire ceux pour lesquels le couple (gravité, vraisemblance) est jugé trop important pour l’entreprise.
* Apprécier l’importance relative de ces différents risques les uns par rapport aux autres, et d’identifier ainsi les risques prépondérants pesant sur le système.

Pour traiter les risques inacceptables, l’entreprise va généralement considérer différents leviers, qui peuvent être des solutions techniques ou des mesures organisationnelles. Pour améliorer la continuité de fourniture délivrée par un réseau électrique, il peut s’agir, par exemple, d’améliorer les plans de maintenance des ouvrages, de changer le schéma d’exploitation, de remplacer certains matériels, d’ajouter des redondances, de mettre en œuvre des automatismes de reconfiguration, etc. Ces différentes mesures devant être examinées à travers une approche coûts / bénéfice afin de retenir la meilleure solution technico-économique.

Le traitement des risques inacceptables a pour effet de diminuer leur criticité (en baissant généralement leurs vraisemblances et/ou, plus rarement, leurs gravités). Les risques résiduels ainsi obtenus devraient alors être à des niveaux de criticité tolérables par l’entreprise.

Cette démarche d’analyse de risque, présentée ici de façon générique, fait l’objet de normes pour des domaines métiers spécifiques : la CEI 60812 AMDEC (qui sera évoquée par la suite) pour les études liées aux défaillances matérielles de systèmes industriels, l’ISO 27005 pour la gestion des risques en sécurité de l’information, etc.

Concepts généraux des études de sûreté de fonctionnement

### Definition

Fondamentalement, la sûreté de fonctionnement désigne « l’aptitude à fonctionner quand et tel que requis ». Cette notion très générale couvre donc des notions diverses comme « la disponibilité, la fiabilité, la récupérabilité, la maintenabilité, l’efficacité de la logistique de maintenance et, dans certains cas, d’autres caractéristiques telles que la durabilité, la sûreté et la sécurité ».

Pour les réseaux électriques, les études de sûreté de fonctionnement sont donc des analyses de risques qui s’intéressent à la continuité d’alimentation des installations et aux moyens permettant de l’assurer. Les deux principaux critères considérés pour ces analyses sont donc :

* La fiabilité, c’est-à-dire « l’aptitude d’une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné »..
* La disponibilité, c’est-à-dire « l’aptitude d’une entité à être en état d’accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens nécessaires est assurée ».

Afin de permettre leur caractérisation en termes probabilistes (et donc évaluer les vraisemblances associées), ces deux notions sont précisées en termes mathématiques :

Les termes défiabilité et indisponibilité sont également employés pour désigner la négation de ces deux définitions.

Pour faire le lien avec la démarche d’analyse de risques précédemment exposée, les études de sûreté de fonctionnement vont donc chercher à évaluer si les exigences fonctionnelles formulées sur le système, en termes de fiabilité et de disponibilité, sont respectées ou non. Dans le cas contraire, des préconisations en matière d’exploitation, de maintenance, de logistique de maintenance voir d’architecture du système pourront être étudiées.

### La méthode AMDEC

Si de nombreuses méthodes de sûreté de fonctionnement existent (le guide CEI-ISO 31010 « Gestion des risques – Techniques d’évaluation des risques » en donne un bon panorama), l’une des plus classiques pour les systèmes industriels est la méthode AMDEC (Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticités), qui fait l’objet de la norme CEI 60812.

Elle consiste à identifier les différents modes de défaillance des éléments constitutifs du système étudié, et à préciser leur impact sur son fonctionnement. De la sorte, en connaissant la probabilité de survenue de ces incidents (à partir de données de retour d’expérience par exemple), il est possible d’évaluer la vraisemblance des événements redoutés, et donc leur criticité.

Ainsi, pour l’étude d’un réseau électrique, la méthode consiste à identifier les différents équipements du périmètre (disjoncteurs, transformateurs, jeux de barres…), à préciser leurs sous-composants éventuels (chambre de coupure, cuve…), à identifier les modes de défaillances pouvant les affecter (fuite SF6, défaut masse cuve…) et à indiquer leurs effets sur l’équipement et sur le fonctionnement du système.

Toutefois, comme le précise la norme CEI 60812, « l’AMDE[C] porte généralement sur les modes de défaillance individuels, et les effets de ces modes de défaillance sur le système. […] La procédure n’est donc pas adaptée à la prise en considération de défaillances dépendant ou résultant d’une suite d’événements ». Ainsi, sur des systèmes complexes, comme les réseaux électriques pour lesquels des plans de protection élaborés, des redondances et des systèmes de reprise automatiques existent, la méthode éprouve-t-elle certaines limites.

Par exemple, si un réseau électrique possède une architecture fortement redondée, avec une voie d’alimentation normale, une voie secours et un permutateur automatique de source, une défaillance sur la voie nominale devrait être compensée par permutation sur la voie secours, mais à condition que celle-ci s’effectue correctement et qu’une défaillance ne survienne pas sur l’un des composants de la voie secours pendant la remise en service de la voie normale. La prise en compte de ces différents cas de figure avec la seule méthode AMDEC peut s’avérer laborieuse, et la norme précise ainsi que « d’autres méthodes et techniques, telle que l’Analyse de Markov (CEI 61165) ou l’Analyse par Arbres de Panne (CEI 61025) peuvent être nécessaires pour analyser ces situations ».

C’est la démarche mise en œuvre en pratique pour les études de sûreté de fonctionnement de réseaux électriques à EDF : l’étude AMDEC se limite en fait à une AMDE des composants électriques présents sur le réseau, c’est-à-dire à

l’identification des modes de défaillances pouvant survenir sur ces matériels, avec leurs probabilités d’occurrence associées, et à leurs effets sur les matériels eux-mêmes, puis cette étude est ensuite complétée par une méthode adaptée aux systèmes complexes et dynamiques, qui permet de faire le lien entre ces défaillances de composants unitaires et les événements redoutés sur le système (en termes de fiabilité et disponibilité). A ce titre, les techniques d’analyse de Markov s’avèrent particulièrement adaptées (les arbres de panne permettent de prendre en compte des défaillances multiples, mais pas des phénomènes de reconfiguration / les refus de fonctionnement, qui sont dynamiques, et susceptible de provoquer d’autres événements par la suite).

### La méthode d’analyse de Markov

Depuis plus de dix ans, des études de sûreté de fonctionnement de postes et de réseaux électriques ont été réalisées pour le compte de directions et de filiales du groupe EDF (EDF S.A., ENEDIS, RTE, DALKIA…) ainsi que pour des clients externes, à l’aide de méthodes markoviennes, qui font l’objet de la norme CEI 61165 « Application des techniques de Markov ».

Leur principe repose sur l’identification des différents états dans lesquels peuvent se trouver les systèmes étudiés (états de fonctionnement nominaux, états de fonctionnement dégradés, états de pannes, états de réparation… en fonction des incidents pouvant survenir sur ses matériels constitutifs) afin d’estimer la probabilité de se trouver dans chacun d’entre eux, et donc de permettre ainsi d’évaluer les grandeurs de sûreté de fonctionnement que sont la fiabilité et la disponibilité.

Pour prendre un exemple illustratif simple, supposons que le système étudié est constitué d’un récepteur, ne pouvant pas défaillir, alimenté par une source, ne pouvant également pas tomber en panne, à travers deux voies d’alimentation A et B en redondance (c’est-à-dire qu’une voie suffit à alimenter le récepteur) pouvant chacune tomber en panne. Cette situation est illustrée sur le schéma suivant :

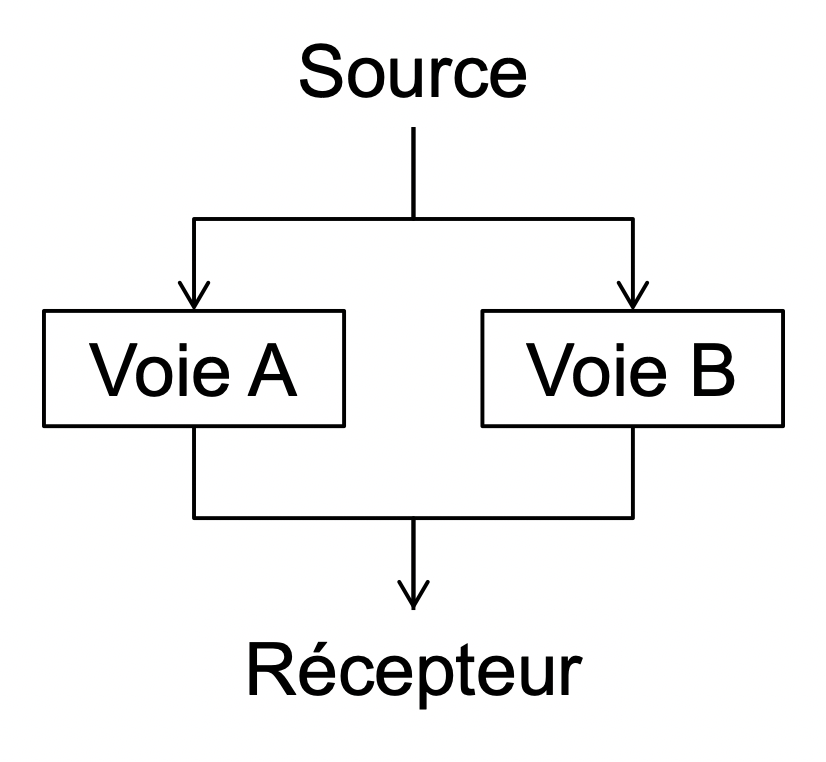


Figure 2 : Système simple à deux voies d’alimentation en redondance

Ce système peut potentiellement se trouver dans quatre états :

* Un état de fonctionnement nominal, dans lequel la voie A et la voie B sont fonctionnelles.
* Deux états de fonctionnement dégradés, dans lesquels la voie A ou la voie B sont défaillantes.
* Un état de panne, dans lequel les deux voies sont défaillantes.

Graphiquement, ces différents états de fonctionnement ou de dysfonctionnement du système, ainsi que les événements permettant de passer de l’un à l’autre, peuvent être représentés de la façon suivante (en considérant, pour cet exemple, que la voie A et la voie B ne peuvent pas tomber en panne simultanément, i.e. qu’il n’existe pas de mode de défaillance commun entre les deux voies) :

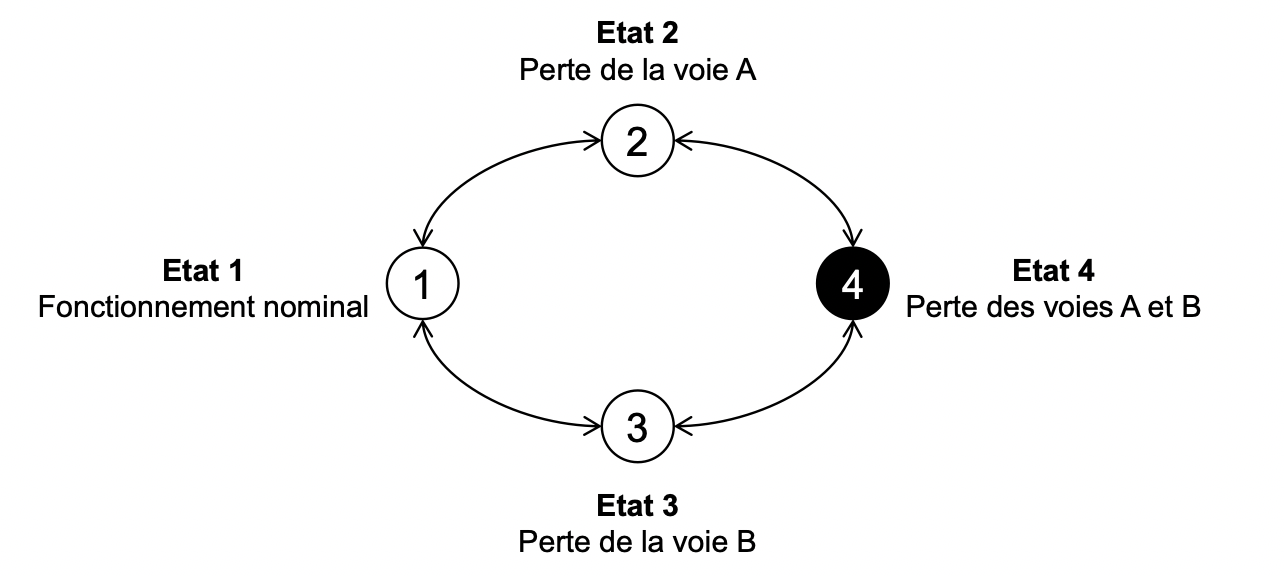


Figure 3 : Graphe des états fonctionnels et dysfonctionnels du système simple

Ce graphique porte le nom de graphe de Markov. Le passage d’un état à l’autre s’effectuant au gré de la survenue des défaillances et des réparations des voies du système. L’état 4, représenté en noir, est un état de panne pour le système. Formellement, les techniques de Markov considèrent que les transitions entre ces états sont régies par des lois de probabilité (et plus particulièrement des lois exponentielles, donc à taux constants), paramétrées par les taux de défaillance et de réparation des différentes pannes pouvant survenir. Ainsi, si le taux de défaillance de la voie A est noté λA (qui peut être exprimé en nombre de pannes par heure), la transition de l’état 1 à l’état 2 sera paramétrée par une loi exponentielle de paramètre λA. L’élaboration de ces taux étant réalisée à l’aide d’un retour d’expérience.

Une fois ce modèle construit, les équations régissant la probabilité d’occupation des différents états sont écrites, et la résolution du système ainsi formé permet l’évaluation de ces probabilités, et, au prix de quelques adaptations, de la fiabilité et de la disponibilité du système.

Utilisés tels quels, les graphes de Markovs présentent toutefois une limite significative : sur des systèmes réels, le nombre d’états potentiel peut être extrêmement important, aussi la conception du graphe et la résolution des équations sous-jacentes peuvent être très fastidieuses. C’est la raison pour laquelle des outils informatiques, qui permettent la conception automatique de modèles markoviens à partir de formalismes de plus haut niveau, et qui autorisent leur évaluation de façon très optimisée, sont utilisés. A EDF, la R&D a mis au point un ensemble d’outils dédiés à cet effet.

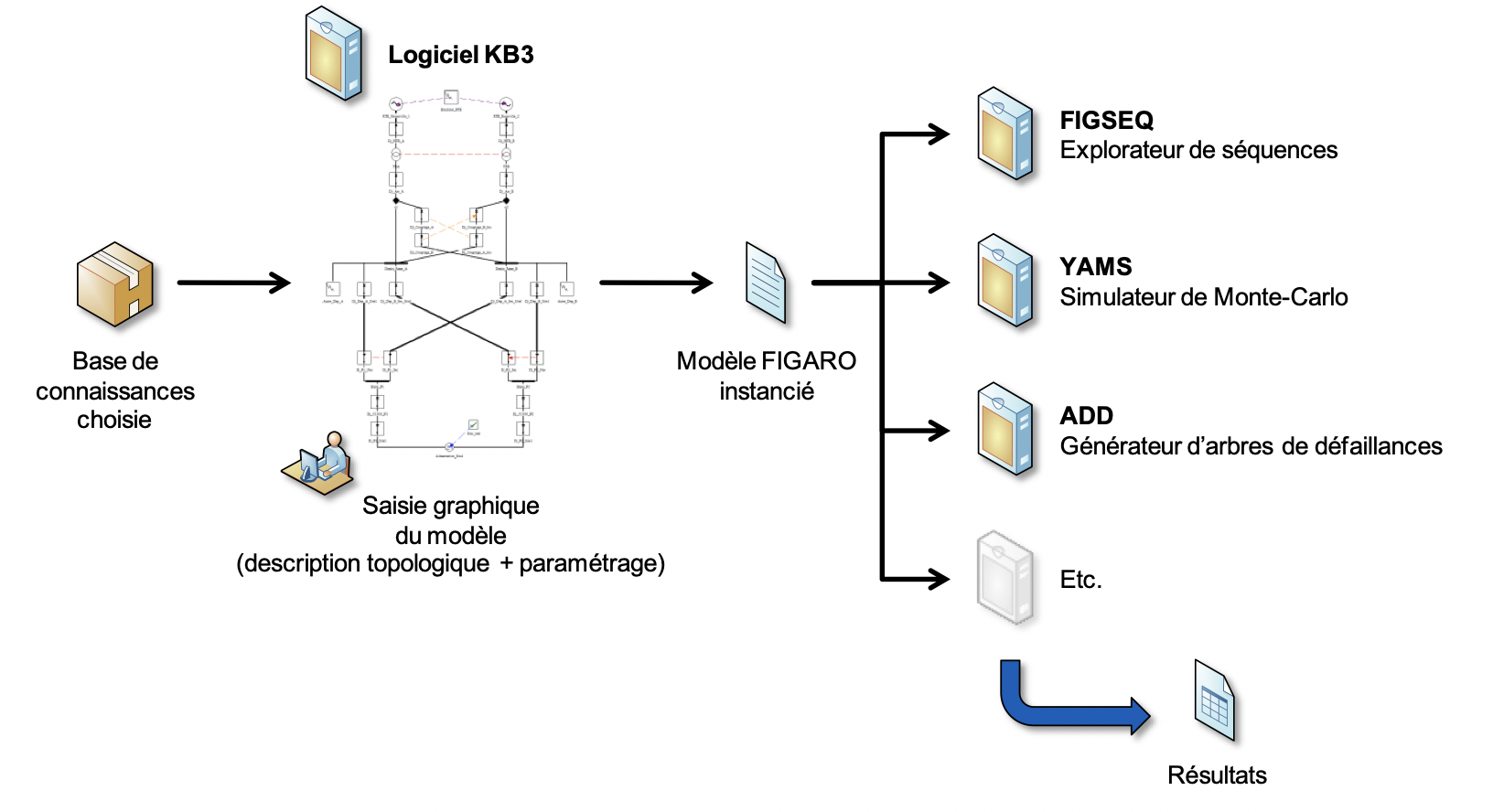
### La plateforme outils FIGARO

Conçue et utilisée par EDF R&D depuis une quinzaine d’années, la plate-forme outils KB3 (également appelée plate-forme outils FIGARO) désigne un ensemble d’outils destinés à automatiser et optimiser les études de sûreté de fonctionnement. Elles permettent notamment la réalisation d’études exploitant les techniques de Markov, en s’affranchissant des problèmes évoqués précédemment, à savoir :

* Les problèmes de combinatoire rencontrés lors de la résolution des modèles grâce à des algorithmes de traitement informatiques très optimisés (outil FigSeq), qui permettent l’exploration locale d’un graphe de Markov, et l’estimation des probabilités d’occupation des états non négligeables, sans avoir à construire le graphe en entier.
* Les difficultés, pour l’analyste, à concevoir le graphe de Markov du système étudié, en permettant l’utilisation de formalismes de représentation . synthétiques de haut niveau, voire des modèles ressemblant fortement à des schémas unifilaires pour les systèmes électriques.

Par ces deux aspects, la réalisation d’études de sûreté de fonctionnement à partir de techniques de Markov, pour des systèmes complexes réels, est rendue possible par la plate-forme. Par ailleurs, outre les indicateurs globaux de fiabilité et de disponibilité évoqués précédemment, l’outil FigSeq permet de déterminer automatiquement les séquences de défaillances menant à l’événement redouté (c’est-à-dire les successions de défaillances pouvant conduire à la perte d’alimentation en un point du système, par exemple)

et d’estimer quantitativement leurs contributions respectives à la défiabilité et à l’indisponibilité globale du système. Ces résultats peuvent ainsi permettre de déterminer les points de faiblesse pour la sûreté de fonctionnement du système, et d’orienter les efforts en termes d’amélioration de la maintenance des composants incriminés, ou de justifier des investissements visant à fiabiliser l’architecture du système, par l’ajout de redondances ou de moyens palliatifs par exemple.



Méthodologie d’étude

# Mise en œuvre de la démarche

### Objectifs généraux

L’étude de sûreté de fonctionnement réalisée vise à quantifier le niveau de fiabilité et de disponibilité des différentes situations considérées, et à identifier les événements les plus fortement impactant sur la sûreté de fonctionnement (à travers les séquences de défaillance produites par les outils de calcul).

### Définition des événements indésirables et des points d’intérêt

La détermination de la fiabilité et de la disponibilité d’une installation revient à quantifier le nombre probable de défaillances pouvant survenir sur le système. Celles-ci sont liées aux modes de pannes des équipements constitutifs du réseau, aux incidents sur l’alimentation électrique fournie au site, à certains effets environnementaux, etc.

La première étape de l’analyse consiste donc à indiquer la nature des événements qui doivent être considérés pour l’étude. En effet, selon les objectifs fixés, il peut être souhaitable ensuite de ne pas prendre en compte les creux de tension, ou d’intégrer certains effets environnementaux spécifiques, par exemple. Pour ce faire, deux notions sont précisées :

* Les événements redoutés (dit aussi indésirables) considérés, c’est-à-dire les événements jugés inacceptables par rapport au fonctionnement attendu du système. Il peut s’agir, par exemple, de « la perte d’alimentation pendant une durée supérieure à 3 secondes » (en raison de l’inertie du procédé alimenté, par exemple). Ces définitions reposent généralement sur des notions temporelles.
* Les points d’intérêt étudiés, c’est-à-dire les points du réseau pour lesquels les événements redoutés vont être examinés. Il peut s’agir d’un départ, d’un jeu de barre d’un poste, d’un tableau Basse Tension, etc.

Chaque couple (événement redouté, point d’intérêt) donne lieu à une étude spécifique.

### Modélisation des cas d’étude sous KB3

A partir des schémas unifilaires du système étudié, et des différents documents descriptifs de la logique de conduite et d’exploitation du réseau, du fonctionnement des automatismes, etc., un modèle topologique, fonctionnel et dysfonctionnel du système est réalisé à l’aide de l’outil KB3 (qui est l’un des logiciels constitutifs de la plateforme outils KB3).

Les données de fiabilité (taux de défaillances, temps de réparation, etc.) des différents ouvrages sont ensuite renseignées, pour permettre la quantification du modèle par les outils de calcul.

# Modes de défaillances

### Défaillances considérées

Pour chacun des composants constitutifs classiques d’un réseau électrique, une AMDE (Analyse des Modes de Défaillances et de leurs Effets) a été réalisée. Ces résultats ont été intégrés aux outils de modélisation de la plateforme KB3, ce qui permet à l’analyste de se concentrer sur les spécificités du réseau qu’il étudie (topologie, logique d’exploitation, automatismes…), en bénéficiant de cette connaissance existante.

A titre d’exemple, les modes de défaillances pris en compte pour le composant « disjoncteur » sont indiqués dans le tableau ci-après :

|  |  |
| --- | --- |
| Défaillance retenue | Description / effet |
| Défaut interne | Met en défaut le disjoncteur et propage un court-circuit. |
| Refus d’ouverture à la sollicitation | Sur court-circuit à isoler, refus d’ouverture de l’organe de coupure entrainant la propagation du court-circuit OU sur reconfiguration du réseau, refus d’ouverture de l’organe de coupure entraînant l’échec de la reconfiguration. |
| Refus de fermeture à la sollicitation | Sur reconfiguration du réseau, refus de fermeture de l’organe de coupure entraînant l’échec de la reconfiguration. |

Pour ces différents événements, des données de fiabilité issues du retour d’expérience d’EDF, ainsi que de traitements effectués par EDF R&D à partir de différents REX internationaux et de données constructeur, sont utilisées pour les calculs. Ces données sont la propriété d’EDF et ne peuvent donc pas être communiquées.

### Défaillances et événements non pris en compte

Parce qu’il n’existe pas de données suffisamment précises (voir pas de données du tout) ou parce que leur prise en compte serait très complexe ou non pertinente pour l’étude réalisée, les événements suivants n’ont pas été considérés pour l’étude :

* Le facteur humain en général, qu’il touche aux erreurs humaines lors de l’exploitation du réseau (fausses manœuvres, négligences), à la réalisation des essais périodiques (non faits ou mal faits) ou à la mise en œuvre des procédures de maintenance (non-respect des doctrines, oublis ou négligences). Ces données sont en effet particulièrement difficiles à élaborer, et très dépendantes de l’organisation mise en œuvre pour l’opération du réseau étudié.
* Les agressions environnementales sur le procédé (pollution, aléas climatiques, etc.). La prise en compte de ces événements nécessite en effet la réalisation d’études spécifiques ciblées, visant à déterminer de façon précise les taux d’occurrence de tels événements, afin d’obtenir des données de fiabilité d’une qualité comparable à celles utilisées pour les ouvrages électriques.
* Les agressions physiques liées à la malveillance sur les ouvrages, les événements liés à la malveillance informatique sur les équipements de contrôle-commande, etc.

En outre, sauf mentions contraires, les opérations de maintenance planifiées ne sont pas considérées.

Toutefois, dans la mesure où l’étude réalisée vise à évaluer la fiabilité et la disponibilité du système étudié, et à comparer des architectures opérées par des équipes identiques, et soumis à des facteurs environnementaux analogues, ces hypothèses permettent aux analyses de se concentrer sur les défaillances et les propriétés intrinsèques du réseau considéré, pour lequel des préconisations en matière d’exploitation et d’évolution d’architecture pourront être formulées.

# Sources de données utilisées

Les taux de défaillances et les temps de réparation des matériels électriques utilisés pour paramétrer les études sont issus des sources suivantes :

### Pour les matériels Haute Tension et Basse Tension

* Rapports du NORDEL sur le retour d’expérience des réseaux HTA et HTB du Danemark, de la Finlande, de l’Islande, de la Suède et de la Norvège (2000-2007) ;
* Base ZEDB, Analysis for 2004, « Centralized Reliability and Events Database, Reliability Data for Nuclear Power Plant Components » ;
* T-Book, 6th edition, « Reliability Data of Components in Nordic Nuclear Power Plants », 2005 ;
* Base NRC (US Nuclear Regulatory Commission) : « Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants », 2007 ;
* EDF-DER-97-NB-00059, « The European industry reliability data bank (EIREDA) », 1998 ;
* Documentation SOCOMEC NOT-10-53918 : « Availability Comparisons », 2010 ;
* Documentation MGE UPS System « UPS Reliability and System Configurations » ;
* Documentation Piller Power Systems « UNIBLOCK-T : ASI DYNAMIQUE avec batteries ou accumulateur cinétique, de 420 kVA à 2500kVA en BT et HTA » et « UNIBLOCK UBTD Alimentation dynamique Diesel No-Break », 2013 ;
* REX interne EDF S.A. (bases de données TOPASE et DEFIA)

Dans la mesure où la plupart des données listées ne sont pas publiques et/ou nécessitent d’être achetées, les valeurs correspondantes ne sont pas reproduites dans ce document.

Indicateurs d’intérêt produits et interprétation

# Indicateurs liés à la fiabilité du système

Pour chaque étude, les indicateurs de sûreté de fonctionnement ci-dessous sont évalués. Cette section vise à préciser leur signification et à en donner des exemples d’interprétation.

### Défiabilité

Notion complémentaire à la fiabilité, c'est-à-dire la probabilité qu'une entité ne puisse pas accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné. La défiabilité s'interprète donc comme la probabilité que l'évènement redouté défini soit observé sur le point d'intérêt, sur un intervalle de temps donné.

Par exemple, pour un point d’intérêt et un événement redouté donné, si la dé-fiabilité du système est de 1e-2 sur l'intervalle sur un an, la probabilité d'observer sur une année est de 1 %.

Pour en permettre une interprétation plus intuitive, deux indicateurs liés seront également calculés : le taux de défaillance équivalent et le MTTF.

### Taux de défaillance équivalent

Il s'agit du taux de panne équivalent du point d'intérêt, pour l’événement redouté spécifié, dans l’hypothèse où les défaillances du système sont régies par des lois exponentielles. Le lambda équivalent permet généralement d’interpréter de façon plus intuitive la défiabilité du système. Par exemple, pour un point d’intérêt et un événement redouté donné, si cette valeur est de 1,87E-06 pannes par heures, soit 1,64E-02 pannes par an, celui-ci subit donc, en moyenne, 1,64E-02 interruptions par an.

### MTTF (Mean Time To Failure)

Désigne le « Mean Time To Failure », autrement dit le temps moyen avant l’observation de l’événement redouté au point d’intérêt considéré, dans l’hypothèse où les défaillances du système sont régies par des lois exponentielles. Le MTTF permet également d’interpréter de façon plus intuitive la défiabilité du système.

Par exemple, pour un point d’intérêt et un événement redouté donné, le temps moyen avant défaillance peut valoir 5,35E+05 heures, soit environs 61 ans (cette durée importante peut s’expliquer par la présence de redondances sur le système).

Indicateurs liés à la disponibilité du système

### Disponibilité (asymptotique)

Probabilité qu’une entité soit en état d’accomplir une fonction requise dans des conditions données à un instant donné, en supposant que la fourniture des moyens extérieurs nécessaires est assurée. La disponibilité peut donc s'interpréter comme la proportion de temps où le système est disponible, au sens de l'événement et du point d'intérêt défini pour l'étude.

Cette valeur asymptotique correspond à un système dont le temps de fonctionnement tend vers l'infini, afin que les probabilités d'occuper un état de fonctionnement ou de non fonctionnement se soient stabilisées (en effet, au lancement de l'étude, le système est considéré comme fonctionnel, sans défaillance présente : la probabilité d'occuper un état de fonctionnement est donc plus importante au début qu'après un certain temps de fonctionnement (où des défaillances et des réparations ont eu lieu).

Par exemple, pour un point d’intérêt et un événement redouté donné, si cette valeur est de 1E-2, le système est indisponible pendant 1 % de son temps.

Pour en permettre une interprétation plus intuitive, un indicateur lié sera également calculé : la durée d’indisponibilité annuelle moyenne équivalente.

### Durée d’indisponibilité annuelle moyenne

Durée annuelle équivalente d’indisponibilité du système. L’indisponibilité annuelle moyenne permet généralement d’interpréter de façon plus intuitive l’indisponibilité.

Par exemple, pour un point d’intérêt et un événement redouté donné, si l’indisponibilité est de 1E-4, le système est indisponible environ 53 minutes par an.

# Remarque sur certains indicateurs

Si les indices de défiabilité et de d’indisponibilité sont par définition probabilistes, les indicateurs associés que sont le lambda équivalent, le MTTF et la durée d’indisponibilité annuelle moyenne doivent également être considérés sous l’angle probabiliste (et statistique) associé. Ainsi, par exemple, la durée moyenne d’indisponibilité annuelle n’a pas nécessairement de sens absolu : un système peut être disponible à 100 %, ou presque, pendant plusieurs années, et rencontrer une défaillance impactant significativement sa disponibilité sur une certaine période (avec une durée bien supérieure à l’indisponibilité moyenne annuelle). Il faut donc garder à l’esprit que cet indicateur correspond à une moyenne, comme le sont le lambda équivalent et le MTTR.

Le principal intérêt de ces métriques est de fournir des valeurs qui pourront être comparées les unes aux autres, entre différentes architectures.

Étude de sûreté de fonctionnement réalisée

# Présentation générale de l’étude de Sûreté de Fonctionnement

### Objectifs généraux de l’étude

L’étude de sûreté de fonctionnement réalisée sur le réseau électrique interne du site Client se fixe un double objectif :

* Compléter l’analyse d’incident réalisée sur le réseau électrique cible dont le déploiement est prévu en 2019-20 en apportant des éléments quantitatifs permettant d’apprécier la sûreté de fonctionnement des installations.
* Estimer l’impact de propositions d’évolutions du réseau électrique cible sur sa sûreté de fonctionnement.

### Points d’intérêt et événements redoutés définis

Pour répondre à cet objectif, l’étude de sûreté de fonctionnement a été réalisée en des points d’intérêts du site, pour lesquels des événements redoutés pertinents ont été définis. Ces éléments ont été choisis de façon à fournir des indicateurs de sûreté de fonctionnement qui soient représentatifs des différentes situations rencontrées sur les installations du site.

Ainsi, au niveau du réseau Basse Tension, dix points d’intérêt ont été définis :

* Point 1 : Le tableau DE685502 situé en aval du point d’alimentation n°1 « Alimentation des baies informatiques»,
* Point 2 : Le départ depuis le TGBT du poste dénommé « Alimentation machine Faisceau d’électrons »,
* Point 2bis : Le départ depuis le TGBT du point d’alimentation n°2 dénommé « Alimentation Groupes Froids Faisceau d’électrons »,
* Point 3 : Le tableau DF56E05 situé en aval du TGBT du point d’alimentation n°3 « Alimentation PC74 »,
* Point 3bis : Le tableau DF56E08 situé en aval du TGBT du point d’alimentation n°3 « Alimentation PC78 »,
* Point 4 : Le tableau DF56D01 situé en aval du TGBT du point d’alimentation n°3 « Alimentation PC125A »,
* Point 4bis : Le tableau DF56D03 situé en aval du TGBT du point d’alimentation n°3 « Alimentation PC84 »,
* Point 5 : Le départ depuis le TGBT du point d’alimentation n°3 dénommé « Alimentation du Four »,
* Point 6 : Le tableau DF56DE01 situé en aval du TGBT du point d’alimentation n°3 « Alimentation TT30 ».
* Point 7 : Le tableau DF26H01 situé en aval du TGBT du point d’alimentation n°4 « Alimentation Zone Y1Q »

Pour les points d’intérêts 1, 2, 2bis, 5, 6 et 7, il a été considéré que les procédés alimentés en aval sont sensibles à la moindre coupure ou creux de tension. En conséquence, l’événement redouté défini pour ces tableaux est « la perte d’alimentation électrique pendant une durée supérieure à 0 seconde ». Enfin, pour les points d’intérêts 3, 3bis, 4 et 4bis, l’alimentation électrique des tableaux les alimentant est secourue par des Groupes Electrogènes Haute Tension dont le temps de démarrage, de montée en charge et de permutation de source s’établit à quelques dizaines de secondes.

L’évènement redouté choisi est « la perte d’alimentation électrique pendant une durée supérieure à 30 secondes ».

Il a en effet été considéré que les procédés directement alimentés par ces sous stations sont en capacité de supporter des creux de tension issus du Réseau Public de Transport (RPT) ou une coupure correspondant à la durée de fonctionnement d’un automate de reprise.

### Hypothèses générales considérées

Cette section expose les hypothèses de modélisation retenues pour l’ensemble des études réalisées (réseau cible et propositions d’évolutions). Les résultats d’études présentés ci-après devront être considérés en gardant à l’esprit les hypothèses suivantes et le fait que les données de fiabilité utilisées ne cadrent pas nécessairement exactement avec la fiabilité des équipements réellement présents, qui dépend fortement de la façon dont ils sont exploités et maintenus.

### Autonomie des sources internes de secours

Le site dispose d’une centrale de production électrique interne de secours destinées à pallier les incidents et les pertes d’alimentation électrique au niveau du RPT ou celles résultant de défaillances internes au site situé principalement au niveau des postes RR (travées A et B) ou en amont de ces derniers. Les hypothèses suivantes ont été considérées quant à l’autonomie d’alimentation conférée par ces dispositifs .

* Groupes Electrogènes : il a été considéré que l’autonomie de ces dispositifs permet d’assurer l’alimentation électrique pendant des durées longues, couvrant le temps de réparation des ouvrages dont la défaillance est à l’origine de leur mise en fonctionnement. Cette hypothèse suppose que leur alimentation en carburant est garantie. Bien sûr, en pratique, une telle autonomie sur des durées longues peut représenter un coût important.

### Temps d’intervention des exploitants sur site suite à incident

Le « temps d’intervention des exploitants sur le réseau électrique interne du site suite à incident » couvre les phases de déplacement, de diagnostic, de décision et d’action visant à isoler la partie du réseau en défaut et à remettre en service les parties de l’installation pouvant être réalimentées, avant de procéder à la réparation du matériel défaillant (pour lequel le temps de réparation varie en fonction dudit matériel).

Pour cette étude, l’hypothèse d’un temps d’intervention égal à 1 heure a été retenue en accord avec l’exploitant.

### REX des incidents du Réseau Public de Transport ayant impacté le site

En se basant sur l’historique des coupures d’alimentation du site observées sur la période du 14/06/2018 au 29/08/2018, il a été défini les paramètres de fiabilité de l’alimentation électrique du site par le Réseau Public de Transport pour les coupures très brèves par an.

• 9,6 coupures très brèves par an en moyenne

Concernant les coupures longues, les informations issues du « Contrat de Service Publique entre l’État et EDF » ont été utilisées pour paramétrer la fiabilité de l’alimentation électrique du site. L’hypothèse du nombre de coupures retenue pour l’étude est donc :

• 1,5 coupure longue par an en moyenne