UNIVERSITAS INDONESIA ISTIA-UNIVERSITE D'ANGERS

KEHANDALAN SISTEM KONTROL DARI SMART GRID

TESIS

DJOKO SUBAGIO
1006803953

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK

JULI 2012

UNIVERSITAS INDONESIA ISTIA-UNIVERSITE D'ANGERS

KEHANDALAN SISTEM KONTROL DARI SMART GRID

TESIS
Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Teknik

DJOKO SUBAGIO
1006803953

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK

JULI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip
maupun dirujuk telah saya nyatakan dengan benar.

Nama	**: DJOKO SUBAGIO**
NPM	**: 1006803953**
Tanda Tangan	**:** 
Tanggal	**: 13 JULI 2012**

LEMBAR PENGESAHAN

Tesis ini diajukan oleh

Nama : Djoko Subagio

NPM : 1006803953

Program Studi : Teknik Elektro

Judul Tesis : Kehandalan Sistem Kontrol dari Smart Grid

Telah berhasil dipertahankan dihadapan dewan penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Master 2 ISTIA Universite d'Angers (Perancis) dan Magister Teknik Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Prof. Abdessamad KOBI

Penguji I : Prof. Christian ROBLEDO

Penguji II : Prof. Abderafi CHARKI

Penguji III : Prof. Sylvain CLOUPET

Penguji IV : Prof. Abdessamad KOBI

Ditetapkan di : Angers - Prancis

Tanggal : 13 Juli 2012

Ka. Departemen Teknik Elektro
Fakultas Teknik – Universitas Indonesia

Ir. Muhammad Asvial, MSc. PhD.

KATA PENGANTAR

Puji syukur penulis panjatkan Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tesis ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar ganda (Double Degree) Magister Teknik Program Studi Teknik Elektro Fakultas Teknik Universitas Indonesia dan Master 2 ISMP (Ingénierie des Systèmes et Management des Projets) di ISTIA – Universite d'Angers, Perancis.

Tesis ini ditulis dengan bahasa Perancis yang mungkin terdapat beberapa kesalahan grammar dan penggunaan kosa kata yang kurang tepat, oleh sebab itu saya mohon masukan dan kritikan agar supaya tesis ini menjadi lebih sempurna. Kerja keras dari penulis dan dukungan pembimbing dan teman serta keluarga sangat medukung selesainya tesis ini, terimakasih kepada ;

1. Prof. Abdessamad Kobi selaku dosen pembimbing dan Kepala Program Internasional Program studi ISMP ISTIA UNIV-ANGERS, juga selaku Direktur Laboratorium LASQUO tempat penulis magang, yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini.
2. Alm. Bapak Sudarlan Sutrisno, yang selalu mendukung penulis untuk selalu semangat mencapai yang terbaik, sampai akhir hayatnya.
3. Ibu Sutini, Ibu Marliyah, Istri tercinta Chi Hastuti dan keempat putra-putri tercinta (F1-F4), atas dukungannya dan kasih sayangnya yang luar biasa.
4. Teman-teman DDIP 2010 khususnya mbak Dwi, kang Haris, kang Shumaru dan teman-teman Teknik Kontrol Industri khususnya pak Heru dan mas Helly dan atas bantuan dan arahannya.

Semoga tesis ini membawa manfaat bagi pengembangan ilmu di bidang Kontrol Industri, *Reliability Engineering*, dan juga *Power System*.

Angers, 13 Juli 2012

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama : Djoko Subagio

NPM : 1006803953

Program Studi : Teknik Kontrol Industri

Departemen : Teknik Elektro

Fakultas : Teknik

Jenis karya : Tesis

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

KEHANDALAN SISTEM KONTROL DARI SMART GRID

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama

saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Angers, Perancis

Pada tanggal : 13 Juli 2012

Yang menyatakan

(Djoko Subagio)

ABSTRAK

Nama : Djoko Subagio
NPM : 1006803953
Program Studi : Teknik Elektro
Kekhususan : Teknik Kontrol Industri
Judul : Kehandalan Sistem Kontrol dari *Smart Grid*

Smart Grid adalah sistem yang sangat kompleks. Sistem ini menggabungkan teknologi jaringan distribusi energi listrik, teknologi jaringan komputer dan teknologi jaringan telekomunikasi. Oleh karena itu diperlukan desain sistem yang sempurna dan tahan terhadap gangguan yang disebabkan oleh infrastruktur, kerusakan, dan ancaman hacker atau pun teroris. Diperlukan suatu sistem dengan pusat kontrol yang kuat yang mampu mendeteksi, memonitor dan melindungi gangguan yang dapat mengakibatkan pemadaman total atau pencurian energi listrik serta dapat juga mengatur proses jual beli energi dari dan ke pelanggan.

Para ahli teknik daya telah merancang konsep pusat kontrol yang mendukung kebutuhan itu yaitu dengan WAMS dan WAPS. Hal ini menyebabkan para insinyur keandalan menerapkan beberapa alat manajemen risiko untuk menghitung kehandalan sistem kontrol *smart grid*. Dalam tesis ini akan membahas metode analisa terhadap proses dan *tools* metode yang digunakan.

Kinerja keandalan pusat kontrol smart grid dipengaruhi oleh ukuran sistem bus, kompleksitas, banyaknya faktor penggangu yang disimulasikan dalam studi kasus.

Kata kunci :

Smart grid, kualitas energi listrik, sistem bus, *reliability*, *availability*, SPN, Markov

Abstract

Smart grid is a very complex system. This system combines the distribution power network technology, computer network technology and telecommunications network technology. Therefore required a great system design and resistant to interference caused by the infrastructure, malfunctions, and the threat of hackers and terrorists. Needed a system with a powerful control center that is able to detect, monitor and protect the disruption that can result in a total blackout or electricity theft.

Power engineering experts have designed a concept of central control and its support is WAMS and WAPs. This leads to the reliability engineers apply some risk management tools to calculate reliability of the smart grid control system. In this thesis will discuss methods of analyzing the process and tools used.

Performance reliability of smart grid control center is influenced by the size and complexity of the many confounding factors are simulated in the case study.

Keywords: Dependability, Smart Grid, Control System, WAMS, WAPS

Résumé

Smart grid est un système très complexe. Ce système combine la technologie de réseaux distribution électrique, technologie de réseaux informatique et de la technologie de réseaux télécommunications. Par conséquent besoin d'une grande conception du système et résistant aux brouillages causés par l'infrastructure, des dysfonctionnements, et la menace des pirates et des terroristes. Besoin d'un système avec un puissant centre de contrôle, qui est capable de détecter, surveiller et protéger la perturbation que peut causer une panne totale ou de vol d'électricité.

Experts en ingénierie électrique ont conçu un concept de contrôle central et son support sont WAMS et WAPS. Ceci mène à les ingénieurs de fiabilité s'appliquent certains outils de gestion des risques pour calculer la fiabilité du système de contrôle *smart grid*. Dans cette thèse sera de discuter des méthodes d'analyse du processus et les outils utilisés.

Performances de fiabilité indice du centre de contrôle est influencé par la dimension et la complexité des nombreux facteurs de confusion sont simulées dans l'étude de cas.

Mots-Clés : Sûreté de Fonctionnement, *Smart Grid*, Système Contrôl, WAMS, WAPS

DAFTAR ISI

Daftar Gambar

Daftar Tabel

INTRODUCTION GÉNÉRALE

1. Fond

Le *smart grid* est un réseau de distribution d'électricité qui utilise des technologies informatiques de manière à optimiser la production et la distribution et mieux mettre en relation l'offre et la demande entre les producteurs et les consommateurs d'électricité.

Mise en œuvre de réseau intelligent dans certains pays ont estimé urgent, pour répondre au défi de la demande croissante d'électricité est à craindre doubler d'ici 2030. L'envie d'utiliser les voitures de l'avenir, les voitures électriques et des progrès technologiques qui ont conduit à l'homme ne peut pas vivre sans électricité.

C'est aussi une réponse au besoin de diminuer les émissions de gaz à effet de serre pour lutter contre le dérèglement climatique. Les contraintes industrielles en fiabilité, maintenabilité, disponibilité et sécurité des équipements sont par ailleurs très fortes.

L'apport des technologies informatiques devrait économiser l'énergie, sécuriser le réseau et en réduire les coûts. Pour atteindre cet objectif, la *smart grid* nécessite un système de contrôle fiable et peut fonctionner pendant une grande surface avec la possibilité de son utilisation automatiquement.

Ce rapport fournit une vue d'ensemble systématique de la stabilité et la performance des réseaux électriques y compris le comptage, l'optimisation intelligente et des contrôles. Discussion sur les questions de sécurité et de contrôle liées aux réseaux intelligents y compris électriques vulnérabilités du réseau électrique, cyber-sécurité et les défis de mise en réseau et la génération automatique et contrôle. Contrôle méthodes d'optimisation pour les réseaux intelligents électriques réunit des experts éminents dans les systèmes de puissance, de contrôle et de la communication, et consolide certaines la recherche la plus prometteuse en matière de modélisation récente *smart grid*, le contrôle et l'optimisation dans l'espoir de jeter les bases des progrès futurs dans ce domaine critique de l'étude.

2. Problème

De la description ci-dessus de fond, les problèmes qui peuvent être prises pour cette thèse sont les suivants:

a. Comment le système de contrôle de la *smart grid*?
b. Comment les caractéristiques du système de contrôle de la *smart grid* (Protection et Contrôle) ?
c. Comment faire l'analyse du SdF au système de contrôle de la *smart grid* ?

3. Objectif

Bien que les avantages à tirer de la réalisation des objectifs de cette thèse est obtenu un aperçu de la performance du système de contrôle de la *smart grid* en termes de fiabilité, de faisabilité et de sécurité afin d'assurer la protection et des performances optimales..

4. Méthodologie

Ce mémoire s'articule autour de quatre chapitres :

Le premiere chapitre : ce chapitre a présenté le *smart grid*, un sens général, les TIC architecture et les systèmes de contrôle**,**

Le deuxième chapitre donne un aperçu des méthodes de recherche de la Sûreté de fonctionnement, systématique et leur utilisation,

Le troisième chapitre étudier et de faire un résumé de quelques revues de recherche le système de contrôle de la *smart grid***,**

Le quatrième (Recommandations/Analyse) fournit une analyse des modèles proposés de plusieurs chercheurs de la revue,

Conclusions.

CHAPITRE I
Réseau intelligent (*Smart Grid*)

1.1 Définition

Les experts de la *Taskforce for smart grid* de la Commission Européenne retiennent la définition suivante : « un réseau électrique intelligent est un réseau qui est capable d'intégrer au meilleur coût les comportements et les actions de tous les utilisateurs qui y sont reliés : producteurs, consommateurs ainsi que ceux qui sont les deux à la fois. L'objectif est d'assurer au système électrique d'être durable et rentable, avec des pertes faibles et avec des niveaux élevés de sécurité, de fiabilité et de qualité de la fourniture».

Smart grid a pour objectif de générer et de distribuer de l'électricité plus efficacement afin de préserver la terre et la réduction des niveaux de CO_2 dans la terre. Visait également à *smart grid* distribue de l'électricité de manière durable afin que le matériel nécessaire et des systèmes qui sont intégrés et bien relié.

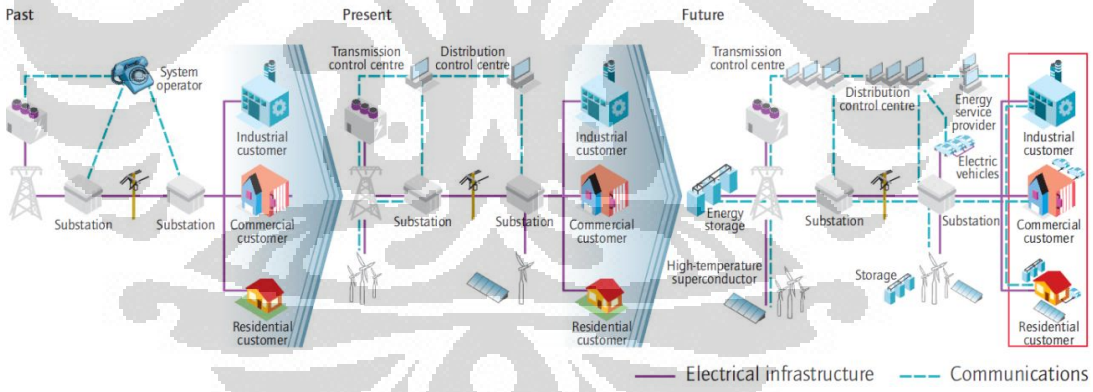


Figure 1.1 L'avenir de la *smart grid*

(Source : IEA, 2012, p 6)

Cette intégration est réalisée grâce à l'utilisation de capteurs et d'équipements numériques de protection, de mesure et de communication, en interface avec les centres de contrôle et de pilotage. Le réseau électrique intelligent offre à tous les consommateurs la possibilité d'obtenir des informations précises sur leurs usages électriques. Cela leur permet de mieux connaître et piloter leur propre

consommation, leur éventuelle autoproduction et d'améliorer leur efficacité énergétique, en liaison avec le réseau et ses opérateurs. Ainsi, on mobilise l'intelligence du réseau au service de la continuité et de la qualité de l'alimentation électrique, dans un contexte de hausse de la demande et de la volatilité de celle-ci, et avec une offre plus décentralisée et plus intermittente, tout en permettant de minimiser (retardement ou suppression) les investissements lourds en matière d'infrastructures de réseaux d'énergie.

Le point crucial du développement de la *smart grid* est totalement sur la capacité du réseau d'alimentation à adopter et à intégrer dans le système et les équipements et technologies de l'information et de communication de manière optimale. Des garanties de sécurité dans ces changements, la maintenance, l'assurance qualité et les exigences de sécurité de réseau qui doivent être remplies.

1.2 Caractérisation d'un *smart grid*

Le *smart grid* modifie le système actuel des réseaux qui repose sur une gestion unidirectionnelle (de l'amont vers l'aval) en introduisant une gestion systématique intégrée à plusieurs niveaux et bidirectionnelle. Le réseau électrique intelligent ainsi, constitué répond aux priorités de la nouvelle économie de l'électricité, que l'on peut synthétiser en trois grandes valeurs d'usage (Source : Gimélec , novembre 2010):

a. Intégration de l'énergie, la demande renouvelables et l'utilisation de l'énergie électrique.
b. Flexibilité de la production, la consommation d'énergie, de réduire le chemin de l'électricité.
c. La gestion des flux d'information, et l'énergie électrique dans bidirectionnelle

La vision du *smart grid* est caractérisé par sa capacité à gérer la centralisation de l'énergie den production décentralisée, y compris la production d'énergie électrique renouvelable à développer l'intégration et un développement optimaux. Il permet aussi le développement et l'intégration de sources d'énergie issues de moyens de stockage, notamment diffus et décentralisés.

Il se caractérise ensuite par le déploiement massif et l'utilisation à tous les niveaux de compteurs intelligents (ou *smart meter*). Ces compteurs sont plus précis, capables de mesurer plusieurs types de flux électriques et surtout, ils sont communicants. Ils permettront de contrôler et de piloter des flux bidirectionnels de courant et d'information, à tous les niveaux du réseau.

Si les grandes caractéristiques d'un réseau électrique intelligent sont similaires partout dans le monde, les objectifs visés diffèrent quelque peu selon le continent où l'on se place : les Etats- Unis mettent en particulier l'accent sur la sécurité du système énergétique et le renouvellement d'un réseau de plus en plus obsolète. La Chine insiste plutôt sur son besoin de répondre à la forte croissance de la demande, quand l'Australie cherche avant tout à lisser sa pointe électrique saisonnière.

Le *smart grid* permet des activités financières, informationnelles et les transactions électriques chez les consommateurs, production l'énergie conventionnel, et autres utilisateurs autorisés. Sa fonctionnalité est définie par les cinq caractéristiques suivantes principaux:

a. Première, il permettra la participation active des consommateurs. Le *smart grid* permettra aux consommateurs d'information, de contrôle, et les options qui leur permettent de s'engager dans des nouvelles marchés de l'électricité. Il va permettre de nouveaux produits, services et marchés. Le *smart grid* permettra de relier les acheteurs et les vendeurs.
b. Deuxième, il pourra accueillir toutes les générations et les options de stockage. Il intégrer de façon transparente tous les types et tailles de génération électrique et des systèmes de stockage en utilisant des procédés d'interconnexion et les normes d'interopérabilité simplifiées universels pour soutenir un "*plug-and-play*" niveau de confort.
c. Troisième, il offrira une qualité de puissance pour l'économie numérique. Il sera suivi, le diagnostic, et de répondre aux problèmes de qualité de puissance résultant en une réduction spectaculaire des pertes d'entreprise actuellement

rencontrées par les consommateurs en raison de la qualité de puissance insuffisante.

d. Quatrième, il permettra d'optimiser l'utilisation des actifs et de fonctionner efficacement. Sur le plan opérationnel, le *smart grid* permettra d'améliorer les facteurs de charge, les pertes du système inférieurs, et d'améliorer considérablement les performances de gestion des pannes.

e. Cinquième, il permet d'anticiper et de répondre aux perturbations du système (*Selt-healing).* Il se guérir en effectuant des auto-évaluations continues pour détecter et analyser les problèmes, prendre des mesures correctives pour les atténuer et, si nécessaire, de restaurer rapidement les composants de grille ou de sections du réseau.

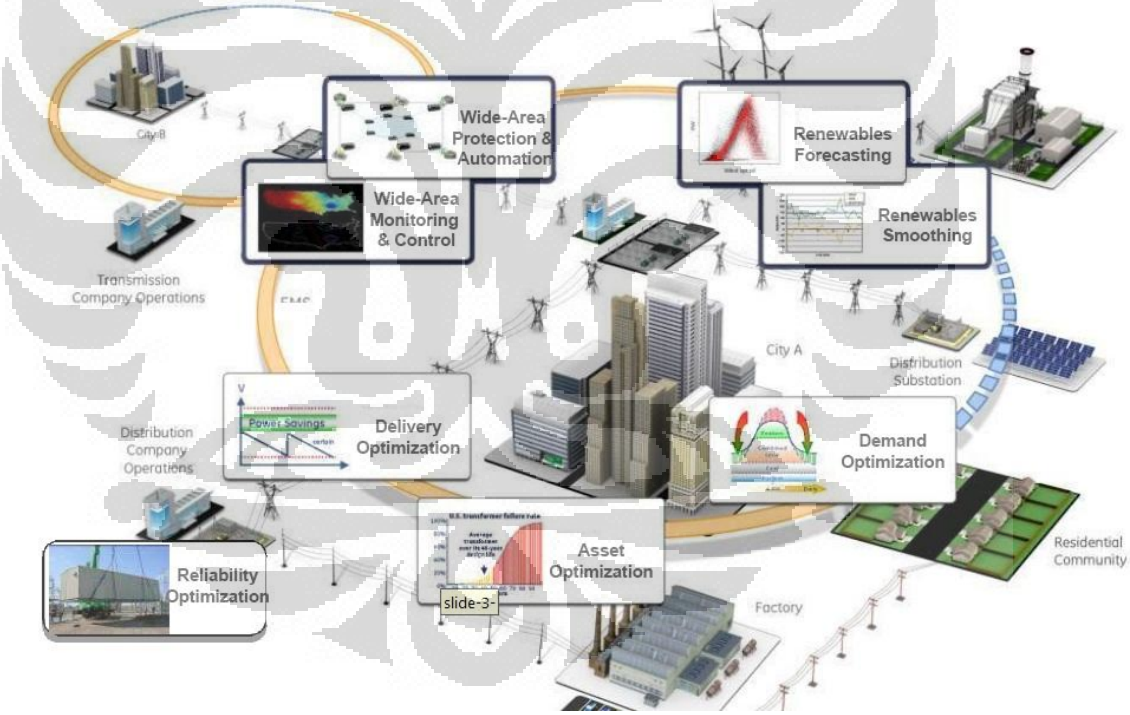


Figure 1.2: *Smart Grid*

(Source: GE, *The Smart Grid and its Benefits*,2008 , p 23)

De la figure 1.2 montre que *smart grid* est un écosystème très complexe impliquant de nombreux acteurs et de l'équipement dans la production et distribution

d'électricité. Les réseaux intelligents peuvent être définis selon quatre caractéristiques :

a. Flexibilité : ils permettent de gérer plus bon l'équilibre entre production et consommation.
b. Fiabilité : ils améliorent l'efficacité et la sécurité des réseaux.
c. Accessibilité : ils favorisent l'intégration des sources d'énergies renouvelables sur l'ensemble du réseau.
d. Economie : ils apportent, grâce à une meilleure gestion du système, des économies d'énergie et une diminution des coûts.

1.3 Fonctionnement technique et les acteurs

Les fonctionnement technique du réseau intelligent associe l'infrastructure électrique aux technologies numériques qui analysent et transmettent l'information reçue. Ces technologies sont utilisées à tous les niveaux du réseau : production, transport, distribution et consommation.

a. **Un contrôle des flux en temps réel** : des capteurs installés sur l'ensemble du réseau indiquent instantanément les flux électriques et les niveaux de consommation. Les opérateurs du réseau peuvent alors réorienter les flux énergétiques en fonction de la demande et envoyer des signaux de prix aux particuliers pour adapter leur consommation (volontairement ou automatiquement).
b. **L'interopérabilité des réseaux** : l'ensemble du réseau électrique comprend le réseau de transport et le réseau de distribution. Le premier relie les sites de production d'électricité aux zones de consommation : ce sont les grands axes qui quadrillent le territoire. Le réseau de distribution s'apparente aux axes secondaires. Il achemine l'électricité jusqu'aux consommateurs finaux. Par l'échange instantané d'informations, les *smart grid* favorise une interopérabilité entre les gestionnaires du réseau de transport et ceux du réseau de distribution.
c. **L'intégration des énergies renouvelables au réseau** : les réseaux intelligents reposent sur un système d'information qui permet de prévoir à

court et à long terme le niveau de production et de consommation. Les énergies renouvelables qui fonctionnent souvent par intermittence et de façon peu prévisible (ex : l'éolien) peuvent ainsi être mieux gérées.

d. **Une gestion plus responsable des consommations individuelle** : les compteurs communicants (ou compteurs évolués, **"Linky"**) sont les premières versions d'application du réseau intelligent. Installés chez les consommateurs, ils fournissent des informations sur les prix, les heures de pointe de consommation, la qualité et le niveau de consommation d'électricité du foyer. Les consommateurs peuvent alors réguler eux-mêmes leur consommation au cours de la journée. De leur côté, les opérateurs du réseau peuvent détecter plus vite les pannes.

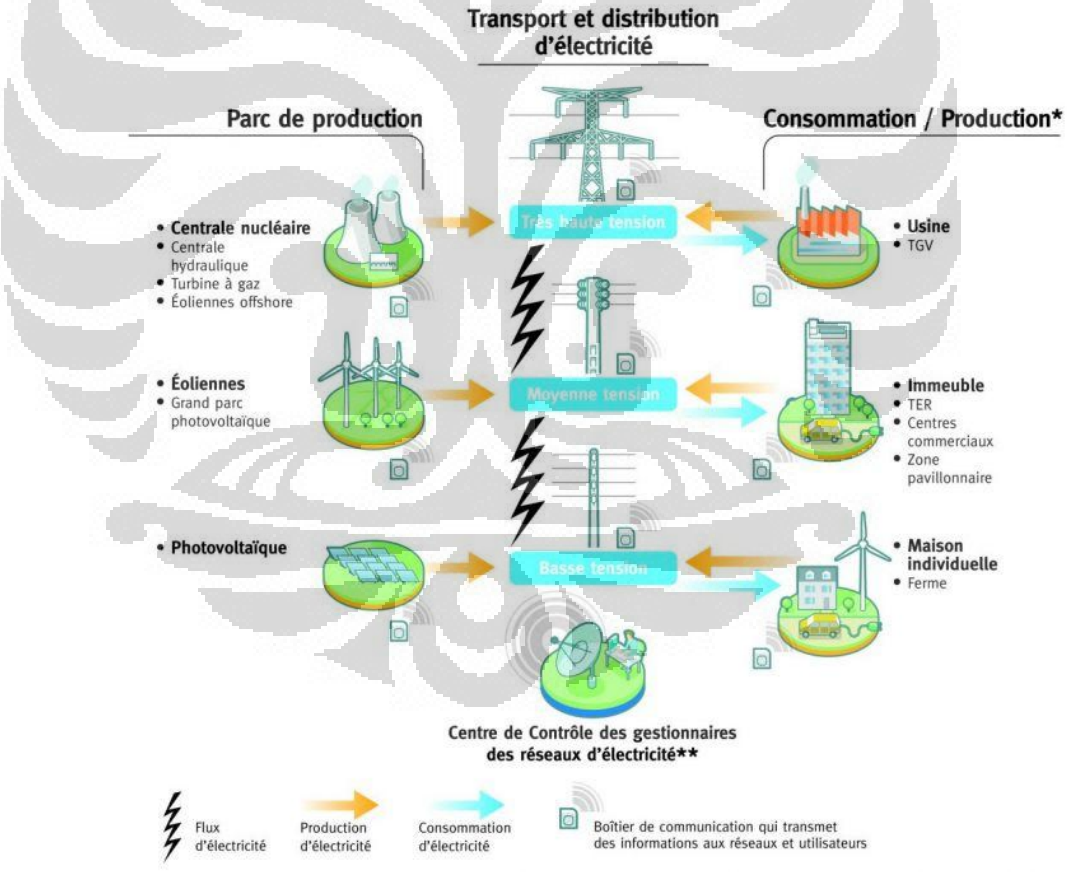


Figure 1.3 Fonctionnement de *smart grid*

(Source : http://www.smartgrids-cre.fr/index.php?p=comprendre-les-smart-grids)

Le développement des réseaux intelligents nécessite le concours de nombreux acteurs majeurs (CDE, 2010):

a. Les consommateurs, en régulant eux-mêmes leur consommation d'électricité, participent à l'efficacité du système.
b. Les producteurs d'électricité comme ENEL ou EDF, alimentent les réseaux de transport d'électricité et doivent être capables de répondre en temps réel à la demande. Le développement des *smart grid* permet également aux producteurs décentralisés de petites capacités d'être raccordés (exemple : les éoliennes ou les panneaux photovoltaïques).
c. Les gestionnaires des réseaux de transport et de distribution, ainsi que les constructeurs de matériel électrique gèrent et installent les équipements de mesure assurant la sécurité et le fonctionnement des réseaux.
d. Les gestionnaires de processeurs et de systèmes informatiques comme Info vista, Intel, Google ou Cisco System, développent les technologies d'information indispensables au fonctionnement des réseaux intelligents.
e. Les pouvoirs publics soutiennent et encadrent le développement des réseaux intelligents notamment par la définition de normes de communication et la protection des systèmes contre les intrusions ou détournements.

1.4 *Smat grid* en France

En France de nombreux acteurs de l'énergie se sont néan moins déjà positionnes sur la première brique de la mise en place du *smart grid* : le *smart metering* ou comptage intelligent, les géants de l'informatique et des télécoms américains se battant déjà pour être aux premières loges de cette évolution. Le *smart metering* est une chaine technologique de comptage (mesure, acquisition, rapatriement et traitement de données de comptage).

S'appuyant sur des technologies communicantes, il vis à rapatrier de manière automatisée, les mesures de consommations ou de capteurs ou d'appareils de mesure

disséminés dans la ville ou dans l'habitat, vers des utilisateurs qu'ils soient gestionnaires de réseaux, fournisseurs ou clients consommateurs. Des acteurs reconnus sur la chaine de valeur (fabricants, operateurs télécom, gestionnaires de réseaux eau, gaz, électricité,….) et des groupes (Legrand, EDF, GDF SUEZ, ALSTOM, AREVA et France TELECOM,….) et des PME.

Certains de l'industrie nationale, ils ont l'initiative de développer un réseau intelligent en France, entre autres:

1. Projet de mise en place de compteurs intelligents (LINKY) d'ERF.
2. Réponses de la part d'énergéticiens à l'appel à manifestation d'intérêt démonstrateurs de l'AMDEC sur les réseaux et systèmes électriques intelligents intégrant les énergies renouvelables.
3. Coordination de la France via GDFSUEZ du projet européen EU-DEEP de 2004 à 2009 ayant conduit à de nombreuses recommandations pour l'ensemble des acteurs et à l'élaboration de buisines modelés.

1.5 Protection, Automatisation et Contrôle du *Smart Grid*

Les réseaux électriques permettent un aiguillage des flux électriques entre la production en amont et la consommation en aval. Leur grande diffusion et leurs caractéristiques critiques de disponibilité nécessitent la mise en œuvre d'équipements de protection extrêmement rapides permettant d'une part d'isoler les sections de réseau en défaut et d'autre part de piloter à distance la reconfiguration de certaines branches de réseau selon les incidents encourus ou les campagnes de mise en retrait de certains équipements (Gimélec, 2011).

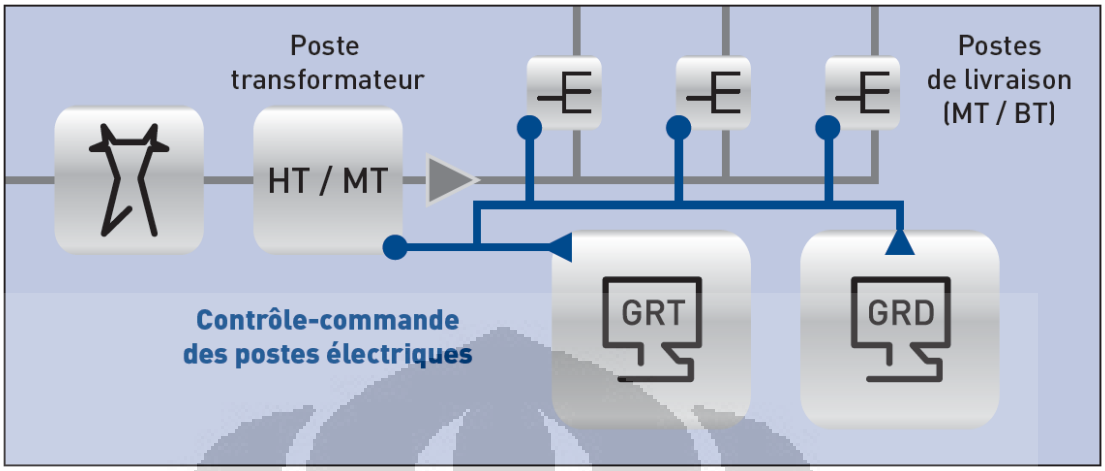


Figure 1.4 Les gestionnaires de réseaux doivent pouvoir piloter à distance les divers postes électriques
(Source : Groupement des industries de l'équipement électrique, 2011, p 15)

Ceci nécessite la mise en œuvre d'équipements de protection, de contrôle et d'automatisme dans chacun des postes électriques des réseaux de transport et de distribution. Alors que ces technologies ont progressivement migré vers les technologies numériques dans les postes de transport critiques des réseaux, une part importante d'automatisation reste à réaliser au niveau des réseaux de distribution pour permettre une interaction bidirectionnelle avec les nouveaux consommateurs énergétiques incorporant de plus en plus de points de micro production. Ceci requiert le déploiement de technologies ouvertes vers les technologies de contrôle commande employées au niveau des ressources de production et de consommation (Figure 1.4).

La surveillance de la zone terme large a été introduit pour faciliter le suivi dynamique d'un vaste espace d'un système d'alimentation avec les applications spécifiques de la protection du système. La première installation WAMS & WAPS (WAMPS) sur l'interconnexion de l'Est était sur le système NYPA (1993) dans le but de la surveillance des perturbations dynamiques et les perturbations géomagnétiques dans les harmoniques. Les systèmes occidentaux installations WAMPS ont été consacrés à la surveillance des événements et l'analyse des perturbations. Le suivi à long terme implique qu'il s'agit d'un système d'acquisition de données et une

infrastructure de communication qui apporte les données dans un emplacement central. Depuis l'application envisagée est la protection du système, la collecte de données à un emplacement central devrait être assez rapide pour faciliter la protection du système. Cela implique que les latences de temps doit être à la sous-région cycle. Traditionnellement systèmes WAMPS utilisé des concentrateurs de données rapides et de liens de communication dédiés à atteindre les performances requises (Figure 1.5).

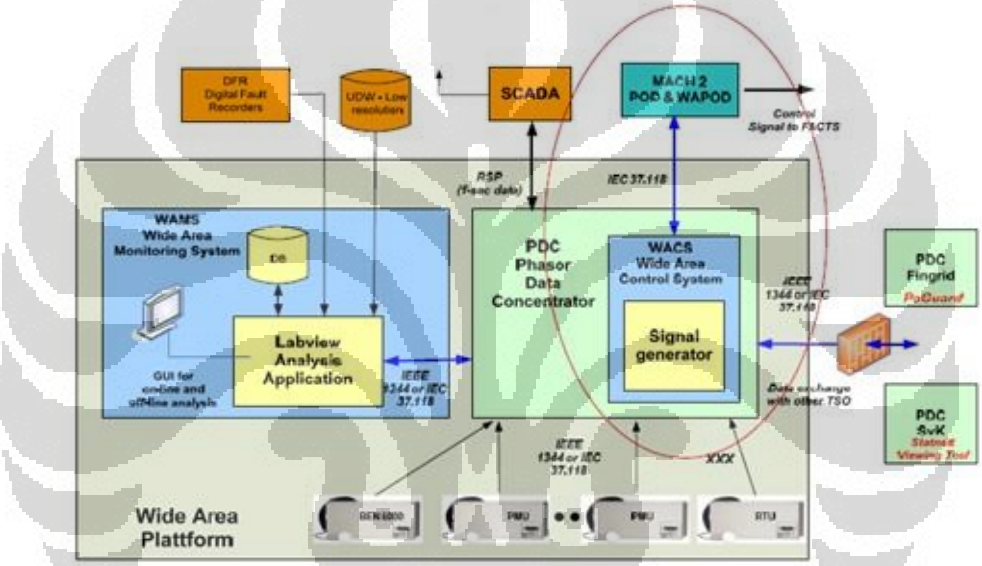


Figure 1.5 WAMS de *Smart Grid*

(Source: KTH - Royal Institute of Technology, 24th of May 2011, p36)

Il est reconnu que WAMPS ont des applications autres que la protection du système et de contrôle. Une application cible important est suivi de la stabilité du système. Un autre est la conscience situationnelle. Comme une question de fait, l'un des meilleurs pilotes de la modernisation du réseau est l'amélioration des capacités connaissance de la situation de la gestion du système d'alimentation en vrac de transmission. Larges région dans le domaine temporel des systèmes GPS d'échantillonnage synchronisées, sont reconnues par de nombreux services publics d'électricité, le gouvernement et les entités de recherche comme une technologie clé

pour la conscience situationnelle et de la *smart grid*. Il a le potentiel de fournir des informations système rapide et fiable sous forme de phaseur qui constitue la pierre angulaire pour le contrôle et la protection du système d'alimentation électrique (courte durée), de gérer le système et de faciliter les marchés (plus de temps). Par conséquent tout système étendu de surveillance peuvent servir de nombreux clients avec des exigences différentes en termes de temps de latence de fréquence et de temps dans les données (Vanfretti, 2011).

Il est reconnu que les systèmes GPS synchronisés d'acquisition de données sont la technologie clé pour atteindre les objectifs de la surveillance de zone large. Avec l'introduction des mesures GPS synchronisés, la technologie WAMPS a fait quelques étapes de l'évolution. Ces technologies fournissent l'infrastructure pour exécuter des fonctions de contrôle de la grille avec une précision et d'accélérer pas possible avec d'autres technologies. Une liste des applications de contrôle et les fonctions possibles est la suivante:

a. Système de protection
b. Estimation d'état
c. Visualisation / situationnel sensibilisation / alarmante
d. La stabilité du système
e. Régulation de la tension
f. Contrôle de la fréquence
g. Analyse post-mortem / capacité de lecture des
h. Le paramètre d'estimation / modèle de validation
i. L'analyse prédictive / regard vers l'avenir
j. Suivi d'oscillation
k. L'îlotage surveillance / contrôlée îlotage / restauration
l. Contrôle des ressources renouvelables
m. Optimisation du système
n. Régulation de la charge

CHAPITRE II
La Sûreté de Fonctionnement (SdF)

2.1 Introduction

La sûreté de fonctionnement est un concept imagine et propose vers le années 1980 pour définir globalement les performances opérationnelles des systèmes numériques programmes (Desroches, 2003).

La sûreté de fonctionnement d'un système est une activité qui a deux objectifs principaux indissociables :

1. La réussite de la mission ou de l'activité pour laquelle le système a été conçu et est impliqué. Elle est mesurée par l'atteinte de ses objectifs techniques et opérationnels. Ceci ne couvre que les évènements de nature aléatoire et par conséquent vient en complément du dimensionnement de la capacité intrinsèque du système à réussir sa mission qui dépend directement des activités d'ingénierie.
2. La sécurité de la mission ou de l'activité qui répond à la non-occurrence d'évènements pouvant diminuer ou porter atteinte à l'intégrité du système et de son environnement pendant toute la durée de la mission ou de l'activité que celle-ci soit réussie, dégradée ou échouée.

   La sécurité couvre les événements de nature aléatoire (*danger*) ou volontaire (*menace*). Généralement, ce deux objectifs sont complémentaires. Dans le cas contraire, il faut prévoir la mise en place d'une politique de compromis entre réussite technique et sécurité pour anticiper les cas où les objectifs de l'une des composantes viendraient en opposition avec ceux de l'autre. Ce compromis se fait généralement au profit de la sécurité qui reste prioritaire.

2.2 FMDS (Fiabilité Maintenabilité Disponibilité Sécurité)

Dans les domaines techniques, les activités de base de la sureté de fonctionnement sont définies par les quatre caractéristiques complémentaires comme dans la figure 2.1 suivantes (CEI, 1990) ;

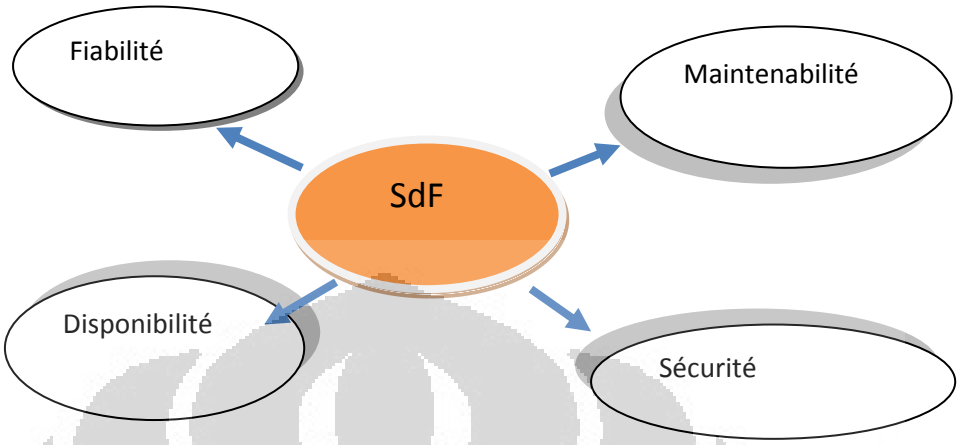


Figure 2.1 Le concepts FMDS
(Source : Chevassu , 2010, p 8)

La sûreté de fonctionnement est une notion générique qui mesure la qualité de service délivré par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée. Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système, mesurée par les grandeurs probabilistes associées: fiabilité, maintenabilité, disponibilité, sécurité (Figure 2.1).

2.2.1 Fiabilité : Aptitude d'un système à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps déterminé. Ou capacité d'un système à fonctionner pendant un certain temps sans panne; elle se caractérise par le temps moyen de bon fonctionnement.

Taux de défaillance est le nombre de défauts par unité de temps. Simplement mettre le taux de défaillance peut être exprimé comme le rapport du nombre de défaillances dans l'intervalle de temps spécifié par le temps total de fonctionnement du système ou sous-système.

Certains indicateurs vont caractériser le fonctionnement prévu du système, tels que le MTTF, le MDT et le MUT. Le MTTF (*Mean Time To [first] Failure*) est l'estimation de la durée moyenne s'écoulant entre la mise en service du système et la survenance de la première panne. Le MDT est le temps moyen

séparant la survenance d'une panne et la remise en état opérationnel du système. Il se décompose en plusieurs phases (intersections, 2004) ;

a. durée de détection de la panne (1),
b. durée de diagnostic de la panne (2),
c. durée d'intervention jusqu'au début de la réparation (3),
d. durée de la réparation (4),
e. durée de remise en service du système (5).

Le MUT est le temps moyen qui sépare une remise en service opérationnelle du système de la survenance de la panne suivante.

Ces deux derniers indicateurs ne sont pertinents que dans le cas de systèmes réparables. Leur somme MUT+MDT représente le temps moyen qui sépare deux pannes consécutives du système. On le note MTBF, comme *Mean Time Between Failures* (Figure 2.2).

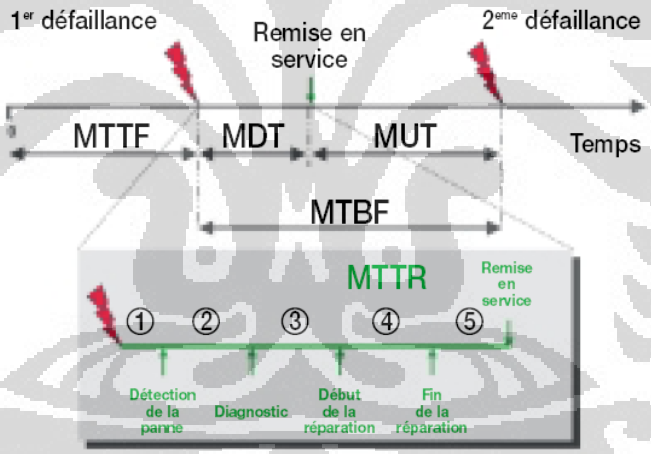


Figure 2.2 Durées moyennes associées à la SdF
(Source : Villemeur, 1988)

La fonction taux de défaillance permet la détermination du nombre de défaillances se produisant par unité de temps. Le taux de défaillance est mathématiquement donnée par

$$\lambda(t) = \frac{f(t)}{R(t)} \qquad (1.1)$$

Le taux de défaillance d'un système est élevée au début de la période d'exploitation, avant de retomber à une valeur constante et, en tant que dernière étape, d'augmenter de nouveau. Une courbe très généralisée pour les taux de défaillances de composants au cours du temps est la courbe en baignoire (Figure 2.3).

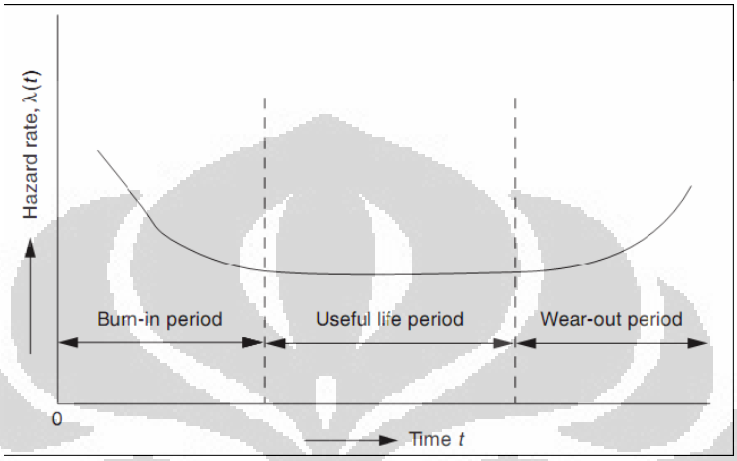


Figure 2.3. Courbe en baignoire
(Source : Barabady, 2005, p 30)

2.2.2 Maintenabilité : Aptitude d'un système à être maintenu ou rétabli, en un temps donné, dans un état de fonctionnement bien défini lorsque les opérations de maintenance sont accomplies avec des moyens donnés, suivant un programme déterminé. La maintenance est l'action de mise en état du matériel; elle peut être préventive, afin d'augmenter la fiabilité du système, ou bien être curative, consécutive au diagnostic d'un défaut

2.2.3 Disponibilité : Aptitude d'un système à être en état d'accomplir une fonction requise, dans des conditions données, à un instant donné, en supposant que la fourniture des moyens extérieurs soit assurée. Faculté d'un matériel ou d'un système à pouvoir fonctionner chaque fois que cela est nécessaire, chaque fois que l'on le sollicite, c'est-à-dire que l'on assure une fiabilité totale pendant les phases de fonctionnement. La disponibilité nécessite des opérations de maintenance préventive afin de prévenir tout vieillissement ou défaillance.

Formulations disponibles sont les suivants:

$$A = \frac{MTBF}{MTBF + MTTR} \tag{1.2}$$

Avec :

MTBF (*Mean Time Between Failure*) : temps moyen entre deux pannes.

MTTR (*Mean Time To Failure*) : temps moyen de travaux de réparation.

Disponibilité : disponibilité de l'équipement de fonctionner dans les heures totales de fonctionnement.

2.2.4 Sécurité : Aptitude d'un système à ne pas générer, dans des conditions données, des événements critiques ou catastrophiques. Ce terme regroupe les caractéristiques concernant l'utilisation du procédé et ses dangers potentiels pour l'utilisateur ou pour le matériel.

2.3 Analyse Fonctionnelle

Parmi les quelques références que je résume les étapes de l'analyse des fonctions d'un système est divisé en quatre étapes, comme suit;

a. Etape 1 Analyse fonctionnelle et dysfonctionnelle ou évaluation prévisionnelle.

   Dans cette étape du procédé mis en œuvre; définit les fonctions du système et analyser la faillite de tous éléments. Identifier les risques (évènements indésirables/redoutes) et rechercher les défaillances possibles.

b. Etape 2 Modélisation et analyse qualitative

   Les prochaines étapes sont la modélisation, et ensuite faire une analyse des causes de défaillance global. Cette étape se termine par une étape d'analyse qualitative.

c. Etape 3 Analyse quantitative

   Dans la troisième étape du processus de sélection est effectuée à partir des données opérationnelles et la fiabilité, la disponibilité et la sécurité, et effectuer des calculs mathématiques, les formules et dérivés intégrante simples pour des simulations complexes avec le programme.

d. Etape 4 Synthèse

L'étape finale contient une synthèse de l'analyse à l'étape précédente en examinant l'évolution des données et des résultats de simulation du calcul à prendre aussi en une conclusion.

2.4 Méthodes d'Analyse Qualitative des Systèmes

Les méthodes qualitatives d'analyse de la SdF ont toujours été utilisées pour aider à identifier toutes les défaillances possibles qui pourraient survenir au sein d'un système, et les risques généraux associés à chacune de ces échecs.

Le plus largement utilisé, méthode qualitative, est des modes de défaillance et leurs effets (AMDE), parfois aussi connu sous le nom des modes de défaillance, des effets et de leur criticité (AMDEC). Le but de l'AMDEC est d'examiner un système en termes de ses sous-systèmes, des assemblages, et ainsi de suite, jusqu'au niveau des composants, afin d'identifier toutes les causes et les modes de défaillance et les effets de ces défaillances. Cela se fait généralement en identifiant les cinq caractéristiques suivantes ;

a. comment chaque partie peut éventuellement échouer,
b. ce qui pourrait produire ces modes de défaillance,
c. quelles pourraient être les effets de ces défaillances,
d. comment les défaillances être détecté, et
e. quelles dispositions sont prévues pour compenser ce l'échec dans la conception (Wallace, 2000).

2.5 Méthodes d'Analyse Quantitative des Systèmes

Application des probabilités à l'évaluation de la SdF d'un système ; diagrammes de fiabilité, arbre défaillances, arbre d'évènements, graphe d'états, etc. Dans son livre La Gestion des Risque, Alain Desroches explique certaines méthodes sont souvent utilisées dans la sûreté de fonctionnement l'analyse d'un système sont ;

2.5.1 Arbre d'événements

Il a pour objectif de décrire le scenario d'accident produit par un enchainement de défaillances suite a l'occurrence d'un événement initiateur.

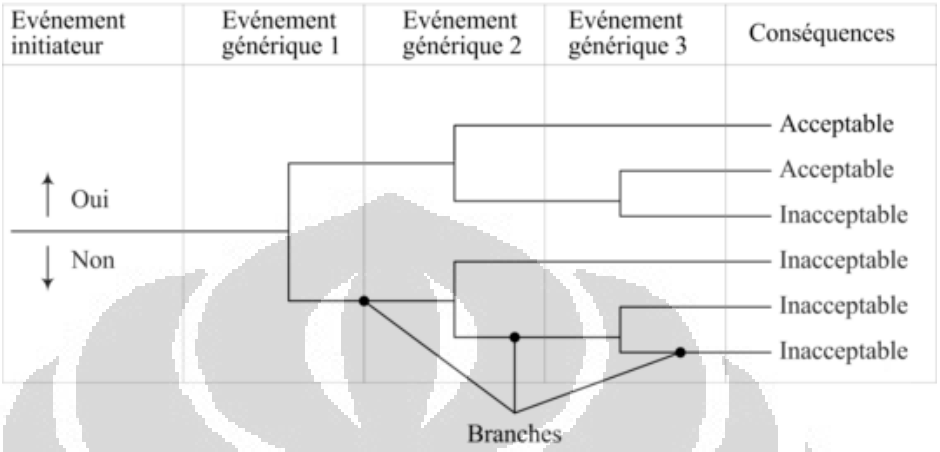


Figure 2.4 : Schématisation d'un arbre d'événement
(inspirée de Mortureux, 2005, p17)

2.5.2 Diagramme cause conséquences

Son objectif est identique à celui de l'arbre d'évènements maïs sa flexibilité de construction devrait le faire utiliser avant la méthode de l'arbre d'évènements (Leroy, 1992)

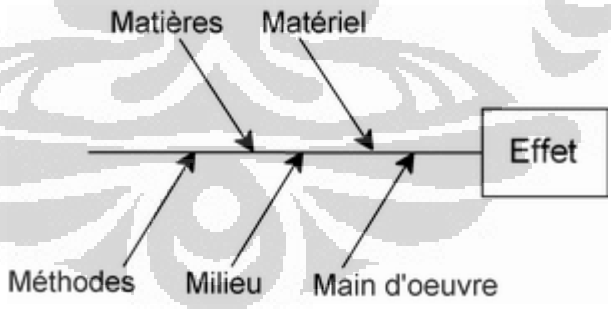


Figure 2.5 : Diagramme cause conséquences

2.5.3 Diagramme de fiabilité

La méthode des diagrammes fiabilité est la première méthode mise au point pour effectuer des calculs de fiabilité et disponibilité. Un diagramme de fiabilité est un diagramme de succès d'une mission, sa construction est assez simple :

a. les éléments dont la défaillance entraine l'échec de la mission sont représentés en série
b. les éléments dont la défaillance n'entraine l'échec de la mission qu'en association avec la défaillance d'autre élément sont représentés en parallèle.

Exemple de diagramme de fiabilité peut être vu dans la figure 2.6.

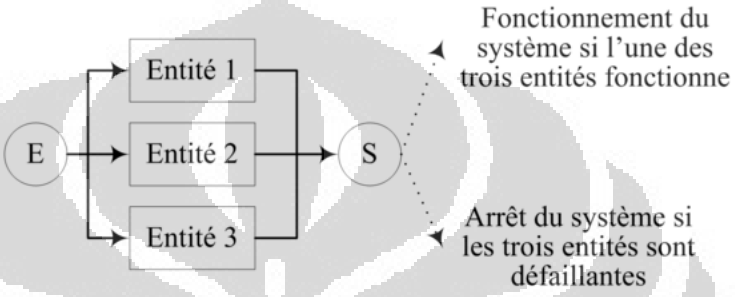


Figure 2.6: Exemple de diagramme de fiabilité en parallèle
(Source : http://www.unit.eu/cours/cyberrisques/etage_3_aurelie/co/Module_Etage_3_synthese_37.html)

2.5.4 Arbres des défauts

Les arbres des défauts sont la représentation graphique d'une équation booléenne qui ont pour objectif de représenter de manière arborescente les causes d'occurrence d'un évènement unique appelé évènement redouté.

2.5.5 Graphes de Markov

Les graphes de Markov sont la représentation graphique d'un système d'équations différentielle linières du primaire degré. La construction d'un graphe de Markov impose alors de considérer que ;

a. La probabilités instantanées de transition d'un état du système a un autre état sont des constantes,
b. La probabilité de passer de l'état Ei à l'état Ej ne dépend pas du temps ni de la manière dont Ei a été atteint, mais seulement de la présence dans l'état Ei (c'est pour cette raison que les graphes de Markov sont aussi dénommes processus sans mémoire du passe).

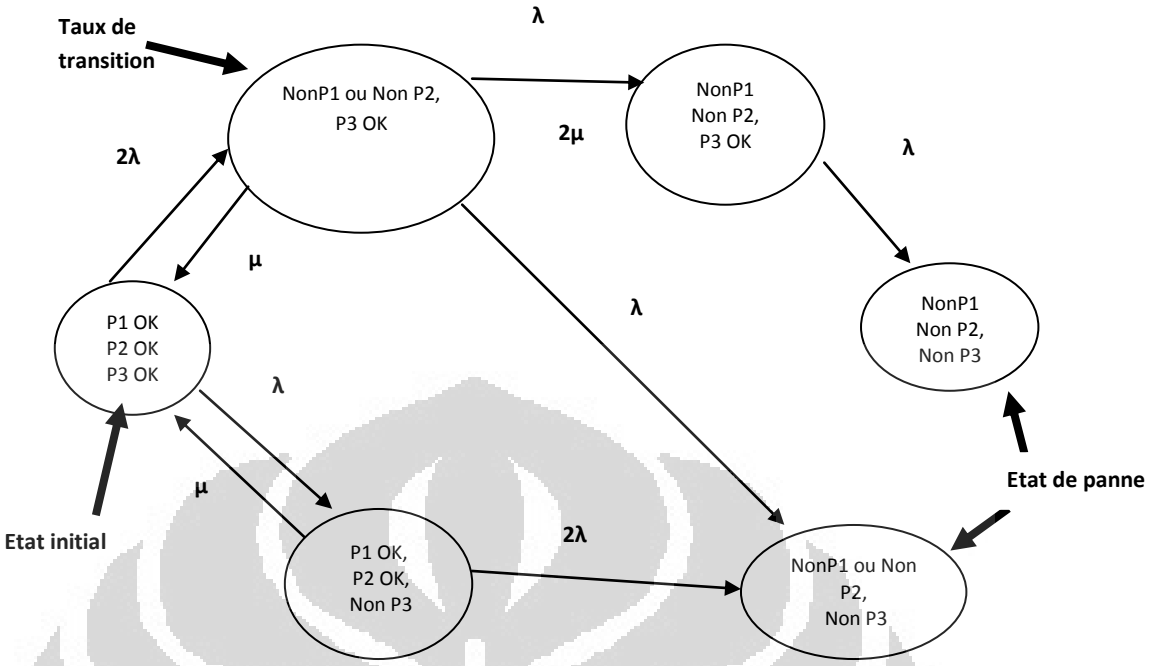


Figure 2.7 : Schématisation Les graphes de Markov
(Source : Desroches, 2003, p69)

2.5.6 Réseau de Petri

Un réseau de Petri élémentaire est constitué de places, de transitions, d'arcs et de messages. Places sont représentées graphiquement par des cercles, les places peuvent être marquées à l'aide d'une ou plusieurs marques appelées « jetons ».

Transitions sont représentées graphiquement par des segments de droite, les transitions ont deux états possibles (valides ou non valides). Arcs sont représentés par des flèches, les arcs sont de deux types selon qu'ils font le lien entre une place et une transition (arc amont) ou entre une transition et une place (arc aval).

2.5.7 Simulation de Monte Carlo

Lorsque le système a étudier est complexe (du fait de sa taille ou des lois régissant son évolution), les méthodes analytiques ne permettent pas d'en modéliser le comportement finement.

La modélisation du comportement est alors effectuée par une méthode (réseau de Petri par exemple) qui ne sert que de support à la simulation de Monte Carlo.

2.6 Qualité de l'énergie, fiabilité et disponibilité

De l'avis de Richard E. Brown dans le livre "*Electric Power Distribution Reliability*" et Ali A. Chowdhury dans son livre "*Power Distribution System Reliability*", à partir d'un point de vue du client, un problème de qualité de puissance peut être défini comme toute électrique fournir affection qui provoque des appareils d'un dysfonctionnement ou empêche leur utilisation. Du point de vue utilitaire, un problème de qualité de puissance pourrait être perçu comme non-conformité avec les différentes normes telles que la tension RMS ou harmoniques. En fait, la puissance est égale au produit instantané de courant et de tension et de formuler une définition satisfaisante de la qualité de l'énergie est problématique.

Qualité de l'énergie est mieux pensé que la qualité de tension. Le mieux qu'un utilitaire peut faire est de fournir aux clients une source de tension sinusoïdale parfaite. Utilitaires n'avons aucun contrôle sur le courant consommé par les utilisations finales et devrait être indifférent à généralement ondes de courant. Courant de charge peut effectuer de tension car il interagit avec des impédances du système, mais la tension est la mesure ultime de la qualité de l'alimentation.

Qualité de l'alimentation parfaite est une sinusoïde parfaite à fréquence constante et d'amplitude. Moins que la qualité de puissance parfait se produit quand une onde de tension est déformée par des transitoires ou harmoniques, les changements de son amplitude ou dévie en fréquence.

Interruptions des clients sont des préoccupations de qualité de puissance, car ils sont une réduction de la grandeur de la tension à zéro. La fiabilité est surtout préoccupée par les interruptions des clients et, par conséquent, un sous-ensemble de la qualité de l'alimentation. Bien qu'il n'y ait un accord général que la qualité de puissance comprend la fiabilité, la frontière qui sépare les deux n'est pas bien définie. Interruptions soutenus (plus de quelques minutes) ont toujours été classés comme un problème de fiabilité, mais de nombreux utilitaires ont classé

interruptions momentanées (moins de quelques minutes) comme un problème de qualité de l'alimentation. Les raisons en sont;

a. interruptions momentanées sont le résultat de pratiques d'exploitation intentionnelle,
b. ils n'ont pas générer un grand nombre de plaintes de clients et,
c. ils sont difficiles à mesurer. Aujourd'hui, interruptions momentanées sont un problème important client et la plupart des ingénieurs de distribution les considérer comme un problème de fiabilité.

Disponibilité est défini comme le pourcentage de temps d'une source de tension est ininterrompue. Son complément, indisponibilité, est le pourcentage de temps une source de tension en interrompu. Depuis la disponibilité et l'indisponibilité traité strictement avec des interruptions, ils sont classés comme un sous-ensemble de la fiabilité. La hiérarchie de la qualité de la puissance, la fiabilité et la disponibilité est illustré à la figure 2.8.

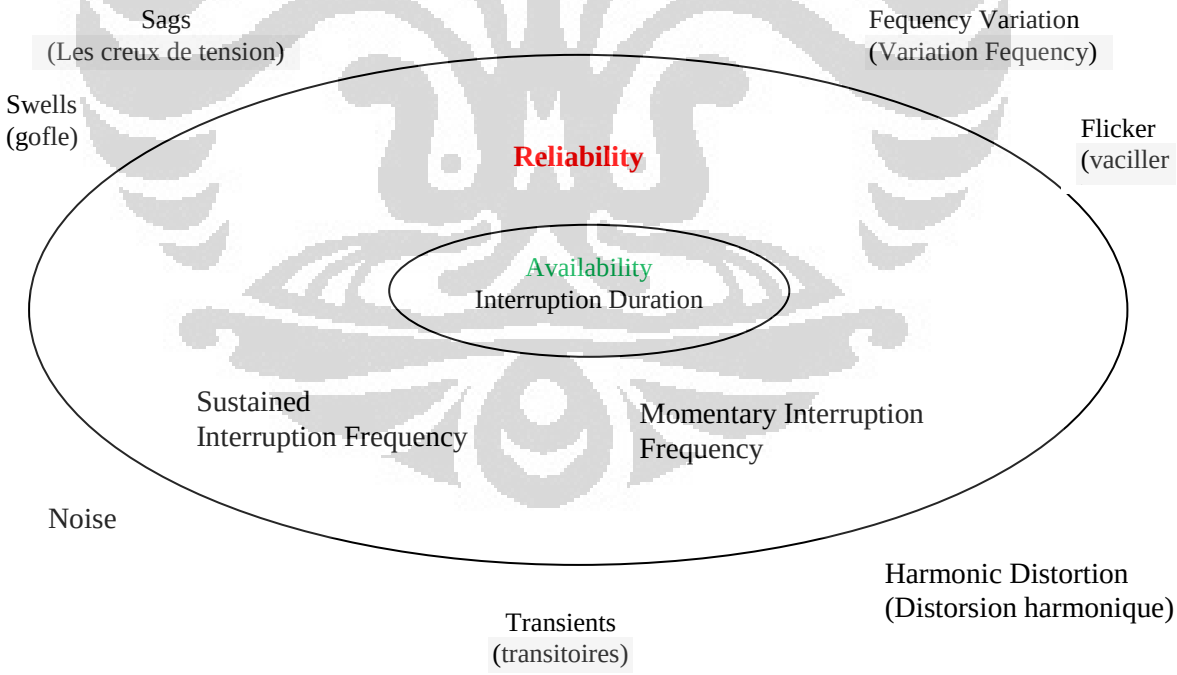


Figure 2.8 Fiabilité traite avec des interruptions, et les meilleures disponibilités, avec la probabilité d'être dans un état interrompu.

(Source : Brown, 2003, p 47)

CHAPITRE III
ETAT DE L'ART

Ce chapitre commence par définir le concept de système de contrôle de *smart grid*. Nous allons développer cette idée avec des études de cas. Explication du concept de systèmes de contrôle, en particulier WAMS et WAPS, nous allons comparer le chapitre suivant.

3.1 Générale

La Sureté de Fonctionnement de la *smart grid* est déterminée à partir de la plupart des caractéristiques de chacun des chercheurs, des institutions, et les gouvernements ont leurs propres normes. Bien que maintenant dans certains pays commencent à faire quelques normes de *smart grid*, les États-Unis et l'Union européenne est devenu un pionnier de cette activité.

Smart grid introduit des technologies modernes de l'information, tels que les réseaux de communications bidirectionnels numériques, la technique de contrôle d'automatisation et les compteurs intelligents, dans le réseau électrique traditionnel pour fournir fiables, efficace et pratique des services d'approvisionnement en électricité à des clients partout dans le pays entier. *Smart grid* peut aussi atteindre les caractéristiques de la réponse rapide de la demande, auto-guérison, l'hébergement de la production d'énergie distribuée, etc. (Zeng, Jiang, Lin, Shen 2012).

En général, les caractéristiques de système de contrôle de la *smart grid* sont comme suit:

1. *Self-healing* et maintenabilité : il a une capacité à être auto-guérison en permanence si une erreur survient, la détection rapide et le diagnostic de la rapide ainsi, par l'intervention de l'opérateur et sans opérateur.
2. Forte et fiable: chaque élément du *smart grid* sera considéré comme des exigences de sécurité pour assurer un certain degré d'intégration et d'équilibre dans l'ensemble du système.

3. Compatible et Sécurité : Systèmes et dispositifs utilisés pour soutenir les grands réseaux et de petits réseaux. L'utilisation de la technologie devrait également être facile pour les consommateurs ainsi que des générateurs

3.2 *Control Center Networks* au *Smart Grid*

Comme une infrastructure indispensable pour la vie future, *smart grid* est mise en œuvre pour économiser l'énergie, réduire les coûts et augmenter la fiabilité. Dans un *smart grid*, de contrôle des réseaux de centres ont attiré une grande attention, parce que leur sécurité et de sûreté de fonctionnement problèmes sont cruciales pour l'ensemble du *smart grid*. (Zeng, Jiang, Lin, Shen, 2012)

3.2.1 Schéma de système de contrôle du *smart grid*

L'architecture du centre de contrôle peut être illustré à la figure 3.1, il y a une certaine N réseau sous-station qui connecté avec WAN au centre de contrôle. Dans les centres de contrôle, les serveurs SCADA, bases de données et serveurs d'applications connectées au réseau local et protégés par des *firewall*.

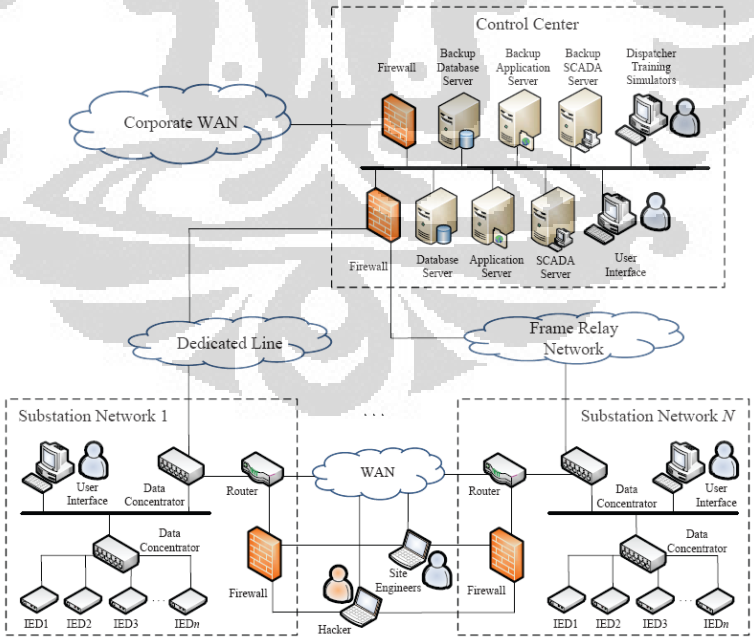


Figure 3.1. Schéma de système de contrôle du *smart grid.*
(Source : Zeng et al, 2012, p2)

Centre de contrôle de réseaux de *smart grid* sont ce qui est le cerveau humain, et la fiabilité des réseaux de centres de contrôle est un facteur important qui doit être sérieusement envisagée. Certains serveurs critiques dans les réseaux de centres de contrôle, par exemple, acquisition et de contrôle des données (SCADA), base de données, et serveurs d'applications, peuvent souffrir de diverses défaillances et les attaques malveillantes par des pirates et des terroristes initialisés. Plus catastrophique, une variété d'outils d'attaque est disponible sur l'Internet gratuitement, ce qui rend facile pour les adversaires de détruire les composants critiques. Par conséquent, les réseaux de centres de contrôle doivent être conçus avec une grande fiabilité (Chen, 2010).

3.2.2 Sûreté de fonctionnement Système Contrôle Centre

L'évaluation de fiabilité des réseaux de centres de contrôle est également très critique à un *smart grid*. Pour les réseaux de centres de contrôle dans un réseau intelligent, en particulier la fiabilité et la disponibilité, parce que le contrôle des réseaux de centres ne portent pas de perturbations.

3.2.2.1 Modélisation

Ten et al. utilisent pour attaquer l'arbre afin d'identifier les vulnérabilités du système SCADA, et ils accomplissent la même tâche en utilisant un autre outil impressionnant, c'est à dire, réseaux de petri stochastiques (SPN), au niveau du système, le niveau des scénarios, et les points d'accès de niveau.

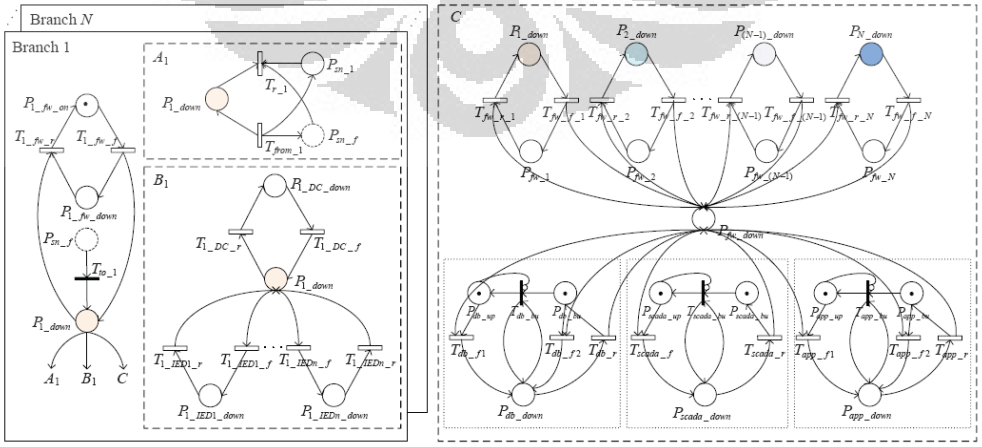


Figure 3.2. Le modèle SPN du centre contrôle
(Source : Zeng et al, 2012, p5)

Zhen et al. construisent le modèle général *Stochatic Petri Net* (SPN) de fiabilité pour les réseaux de centres de contrôle dans la figure 3.2. SPN est un outil graphique mathématique, qui est universellement appliquée à l'évaluation du rendement et d'analyse de fiabilité des différents systèmes distribués. SPN peut être définie comme une période de cinq ;

(1) $P = \{P_1, P_2, \cdots, P_k\}$ est l'ensemble endroit, qui décrié the stipule de réseaux ou les conditions de transitions,

(2) $T = \{T_1, T_2, \cdots, T_l\}$ est l'ensemble fini de transitions, l'exécution de ce qui modifie les états de réseaux,

(3) $F = (P \times T) \cup (T \times P)$ est un ensemble d'arc, et des transitions reliant les endroits,

(4) $\lambda = \{\lambda_1, \lambda_2, \cdots, \lambda_l\}$ est l'ensemble des taux de combustion associées aux transitions. En SPN, chaque cadence de tir λi ($i = 1, \cdots, l$) est exponentiellement-distribués,

(5) $M_0 = \{M_{01}, M_{02}, \cdots, M_{0k}\}$ est un marquage initial, qui représente l'état initial des réseaux.

Pour chaque réseau station, il y a deux façons pour les attaquants: détruire le firewall, et d'attaquer d'autres réseaux station compromis, qui sont représentés par des transitions séparément $T_{i\_fw\_f}$ et T_{sn_f}. Les pirates peuvent lancer des attaques suivantes ;

(1) de détruire le concentrateur de données (DC) ou IED,

(2) pénétrant réseaux station d'autres, et

(3) d'attaquer le centre de contrôle.

Ces attaques sont respectivement désigner par les transitions $T_{i\_DC\_f}$, $T_{i\_IEDi\_f}$, T_{from_i} et $T_{fw\_f\_i}$. Si le *firewall* du centre de contrôle est perturbé, l'état de ce qui est désigné par le P place, alors que l'attaquant peut encore détruire les serveurs d'applications, serveurs SCADA ou de bases de données. Zen et al imagée par la zone en pointillés à deux stratégies de sauvegarde sont utilisés pour les serveurs critiques dans le modèle général.

La formule proposée par Zhen et al. pour la fiabilité et la disponibilité sont les suivantes:

$$Rel(t) = 1 - Ex(\sum_{i=1}^{t} \lambda_i, t) = e^{-\sum_{i=1}^{t} \lambda_i, t} \tag{3.1}$$

où *λi* est la cadence de tir de la transition dont le tir causes de réseaux cibles de quitter les États fiables.

Pour connaître la disponibilité, nous pouvons aussi avoir deux types d'états, à savoir, la maîtrise précise que les réseaux cibles sont disponibles et la *MA* indique que les réseaux de centres de contrôle ne sont pas disponibles, et *bi* est le coefficient. Ensuite, la disponibilité état d'équilibre et de la disponibilité transitoires est respectivement

$$A(t) = \sum_{i} b_i \pi_i(t), M_i \in \mathcal{M}_{\mathcal{A}} \tag{3.2}$$

3.2.2.2 Etudes Cas

Zhen et al. décrivent dans un simple étude de cas les réseaux virtuels du centre de contrôle avec un IED (n = 1) dans une sous-station (N = 1) et seuls les serveurs SCADA, qui sont censés pour illustrer la procédure d'analyse de fiabilité et de la méthode de l'état-espace explosion d'évitement.

Dans la figure. 3.2, il décrit les lieux et les transitions omis pour les limitations de l'espace. Paramètres λ_1, λ_2, • • •, λ_{10} que le taux de tir de la transition $T_{1\_fw\_f}$, $T_{1\_fw\_r}$, $T_{1\_DC\_f}$, $T_{1\_DC\_r}$, $T_{1\_IED1\_f}$, $T_{1\_IED1\_r}$, $T_{fw\_f\_1}$, $T_{fw\_r\_1}$,T_{scada_f}, et T_{scada_r}, obtenu par l'analyse de grands volumes de statistiques et est calculé comme la fréquence moyenne d'apparition des événements. Puis simplifiée pour la méthode équivalente CTMC, montré dans la figure. 3,3.

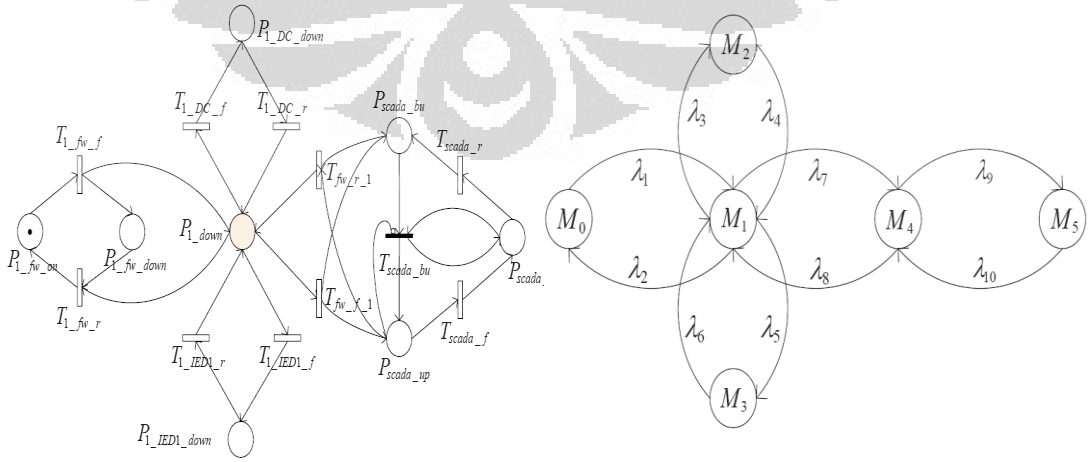


Figure 3.3. Le modèle SPN du cas et équivalent CTMC
(Source : Zeng et al, 2012, p6)

Avec les probabilités état stationnaire et transitoire, Zhen et al calculent la fiabilité et la disponibilité. Pour la fiabilité, on peut voir que seul l'état initial est fiable, et le taux de sortie de l'état fiable M_0 est λ_1. La fiabilité transitoire comme

$$R(t) = e^{-\lambda_1 t} \tag{3.3}$$

Pour connaître la disponibilité des réseaux, DC, les IED et les serveurs SCADA ne sont pas disponibles, dans le M2 Etats, M3, et, M5, respectivement. Disponibilité à l'état d'équilibre peut être calculée comme

$$\text{Ava} = 1 - (a1\pi2 + a2\pi3 + a3\pi5), \tag{3.4}$$

$$A(t) = 1 - (a1\pi2\,(t) + a2\pi3\,(t) + a3\pi5\,(t)), \tag{3.5}$$

où a1, a2 et a3 sont respectivement les poids de DC, IED, et le serveur SCADA.

Les résultats de l'équation simulation ci-dessus peut être illustré comme figure 3.4 que la fiabilité transitoire et la disponibilité diminue exponentielle avec le temps t, et les résultats près de l'état stationnaire fiabilité Rel = 0 et la disponibilité d'Ava = 0,9936.

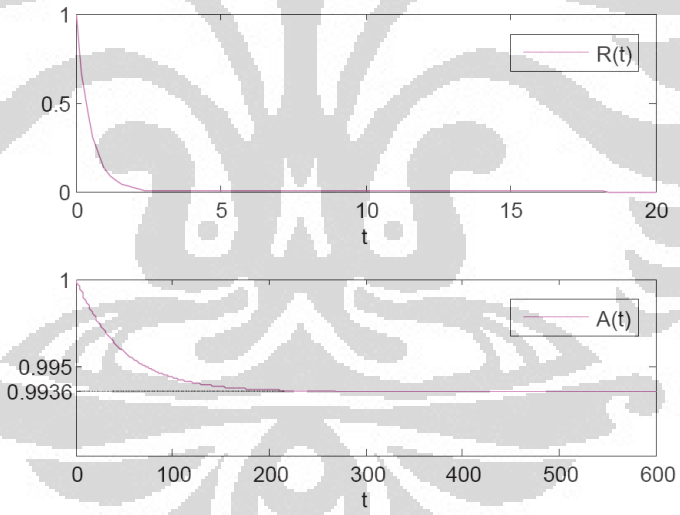


Figure 3.4. La fiabilité et la disponibilité transitoire
(Source : Zeng et al, 2012, p8)

3.3 WAMS (*Wide Area Measurement System*)

En tant que technologie clé dans un *smart grid*, le système de mesure dans une vaste zone (WAMS) va progressivement devenir une garantie importante pour la sécurité et la stabilité des systèmes électriques futurs (Wang et al, 2010).

3.3.1 La structure hiérarchique de WAMS

Comme une infrastructure d'information de la surveillance, de contrôle et les fonctions de protection dans la grille de transmission intelligente, le système de mesure large zone (WAMS) basé sur une unité de mesure de phaseur synchronisée (PMU) va progressivement devenir une garantie importante pour la sécurité et la stabilité des réseaux électriques (Wan et al, 2010).

Le WAMS peut être utilisé pour effectuer une surveillance en temps réel et de contrôle, dans les états de systèmes dynamiques et d'améliorer le niveau de sécurité du système car il utilise le système synchrone de haute précision d'horloge du système de positionnement mondial (GPS) pour construire un système unifié espace-temps ordonnée pour l'ensemble du système. Il comprend habituellement le PMU, les phaseurs de données concentrateur (PDC), centre de contrôle (CC), ainsi que les réseaux à grande vitesse de communication de données (Han, 2004).

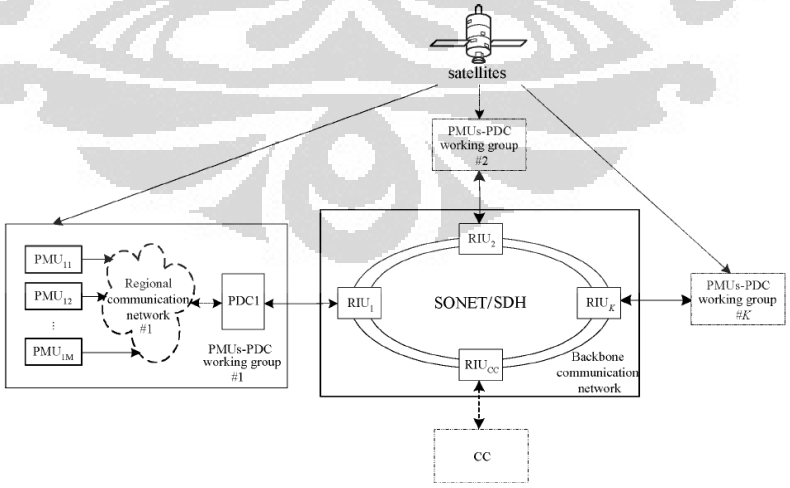


Figure 3.5. La structure hiérarchique de WAMS.
(Source : Wang et al, 2010, p1484)

Centre de Suivi de WAMS est principalement responsable du traitement des données de mesure et d'envoyer les ordres de commande. Plate-forme de Centre de Suivi est un temps réel de réception, la gestion, le système logiciel de traitement de données. Les équipements PMU qui sont installés dans des endroits différents à travers le réseau électrique peut acquérir des données en ligne synchrone à travers le temps accordé par les GPS. Après réception des données avec les informations de temps, le Centre de Suivi peut surveiller dynamiquement l'état en temps réel du réseau électrique tout entier. Les données acquises par le PMU installés dans les zones de protection différent est concentrée dans *Phasor Data Collector* (PDC), qui envoient ces données vers le haut au centre de suivi. Il y a deux types majeurs dans le réseau de transmission à large zone de réseau en anneau SDH et le réseau en étoile locale. Le large zone anneau SDH connecté avec le moniteur du Centre et les sous-stations qui peuvent fournir une bande passante suffisante et à grande vitesse des flux de données. Réseau en étoile entre PDC et le PMU est bon pour la connexion en temps réel du PDC et du PMU, et aussi pour l'expansion future du PMU (Liu et al, 2009).

3.3.2 Sûreté de fonctionnement du WAMS

Liu et al fournir une compréhension de base avant de WAMS a effectué une analyse de fiabilité, les hypothèses sont les suivantes:

a. La fiabilité de l'acquisition de données sous-systèmes est indépendante les unes des autres, et sa possibilité de fonctionnement normal est une constante.
b. Le traitement des données et l'application de logiciels dans le poste de travail principal sont indépendants les uns des autres.
c. La distribution des temps de réparation d'un système logiciel est supposé être l'exponentielle, le taux de réparation est une constante.
d. La possibilité qui sous-système apparaît deux ou plusieurs fautes ou des réparations pendant la durée du temps minuscule (t, t Δ t) est égale à zéro. Notamment, il devrait y avoir un seul permis pour faute ou à la réparation apparaissant au cours de Δ t minuscule.

e. La fiabilité de l'élément de réseau et le couloir de communication est indépendante les unes des autres.

Comprendre la fiabilité du système est la capacité du système à remplir une fonction spécifique dans un certain temps. L'ensemble du système WAMS est divisé en surveillance centre du système et le système d'acquisition de données. Dans des conditions normales, le système d'acquisition peut correctement obtenir et transmettre des données, et le Centre de surveillance est chargé de recevoir, d'analyse et de traitement des données. Donc, la fiabilité tout est décidé par le moniteur centre et sous-systèmes entre eux. Pour un système réparable, sa fiabilité peut être évaluée par le degré de fiabilité et de disponibilité. Le degré de fiabilité est la probabilité d'unités ou sous-système fonctionne normalement.

3.3.2.1 Modélisation WAMS générale

Une analyse de fiabilité d'une telle structure hiérarchique peut être effectuée en utilisant FTA comme indiqué dans la figure 3.6.

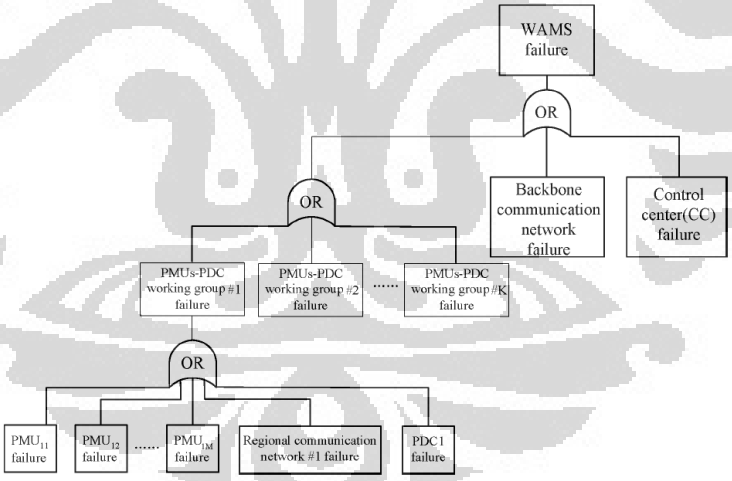


Figure 3.6. L'analyse par arbre de défaillance de WAMS.
(Source : Wang et al, 2010, p1484)

En 2010, Wang et al proposé la disponibilité de chaque groupe PMU-PDC qui travaillent dans les WAMS est calculé en

$$A_i = \left(\prod_{j=1}^{M_i} A_{ij}^{\mathrm{PMU}} \right) \cdot A_i^{\mathrm{RN}} \cdot A_i^{\mathrm{PDC}} \tag{3.6}$$

où Ai est la disponibilité du i_{th} PMU-PDC de groupe travail; A_{ij}^{PMU} est la disponibilité de *j*th PMU dans le *i*th PMU-PDC groupe de travail; M_i est le nombre de PMU dans le ith groupe; A_i^{RN} et A_i^{PDC} sont la disponibilité les valeurs du réseau de communication régionale et le dispositif *i* th de PDC. La disponibilité de WAMS entiers peuvent être calculées par

$$A_s = \left(\prod_{i=1}^{K} A_i\right) \cdot A_{\mathrm{BN}} \cdot A_{\mathrm{CC}} \tag{3.7}$$

K est le nombre de PMU-PDC groupe de travail dans les WAMS.

3.3.2.2 La disponibilité et Modélisation du centre de surveillance de WAMS

Lui et al utiliser une simplification de l'échec et les problèmes de réparation avec la chaîne de Markov. Le modèle souple de GO qui est proposé par *Goel-Okumoto* a une large application dans l'analyse la fiabilité des logiciels. Il est basé que le nombre moyen de panne logicielle avait été trouvé est proportionnelle au nombre de la défaillance n'avait pas été trouvé, ce que plus le nombre de défaillances est conforme à la distribution de Poisson. Donc, nous obtenons le taux d'échec est la suivante:

$$\lambda\,(t) = abe^{(-bt)} \tag{3.8}$$

Où a est le nombre total de défaillances devrait et b est le taux d'échec. Avec les conditions initiales P1(0)=1; P0(0)=0 (l'équipement peut normalement travailler lors du démarrage, la probabilité de son échec est égal à zéro); Yuan connaître la disponibilité du Centre de Surveillance au temps t.

$$A_m\,(t) = [\int \mu .\, \exp(\mu x - a.\, \exp(-bx))\, dx + \exp(-a)] \,.\, \exp\,(-\mu t + a.\exp\,(-bt)) \tag{3.9}$$

3.3.2.3 La fiabilité et la Modélisation du système de données acquisition

Il existe de nombreux types de raccordement, en acquisition de données sous-système, comme le bus, arbre, et l'anneau. Toutefois, la structure en étoile est largement utilisée dans la zone protégée, dans laquelle PDC (*Phasor Data Collector*) de transit des données qui ont acquis par le PMU de cette zone. L'analyse de fiabilité du système qui consistait par le PDC et le PMU devrait envisager toutes les unités de cette région. (Liu,2009)

R (t) est la valeur de dispositifs de mesure de **n**, et R_m est la fiabilité du modèle jugement, afin de la fiabilité de k/n système R_3 (t) est la suivante:

$$R_3(t) = R_m \sum_{i=k}^{n} \binom{n}{i} [R(t)]^i [1 - R(t)]^{n-i} \quad (3.10)$$

3.3.2.4 Disponibilité de communication SDH Anneau

Selon Liu et al qui construisent une modélisation de l'anneau de protection multiplex section 2-fibre qui est habituellement utilisé en WAMS. Dans la figure 1, il y a quatre éléments de réseau (NE) ou le réseau sous-station dans le modèle. Ainsi, la structure du réseau et de la modélisation du transfert de l'état de la communication comme suit ;

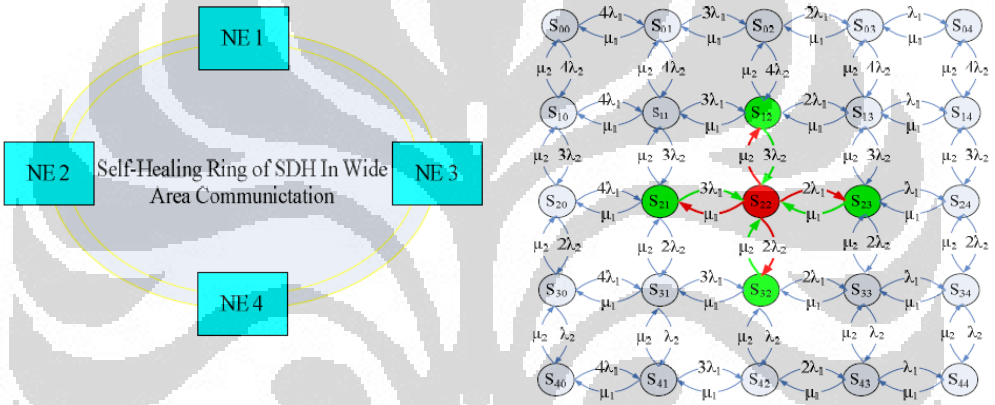


Figure 3.7 Auto-guérison anneau de SDH
(Source : LIU et al, 2009, p3)

Paramètres contenus dans le modèle peut être décrite comme suit ;

a. Le λ_1 est le taux d'échec de la NE dans le ring et λ_2 est le taux d'échec de la fibre entre les NE.
b. Le μ_1 est le taux de réparation de la NE et μ_2 est le taux de réparation de fibres.
c. S_{ij} est L'état du réseau après NE ou de la fibre est un échec. Où *i* se rapportent au nombre de NE qui est échec et *j* est le nombre de fibres.

Avec $P(S_{ij})$ est la probabilité de réseau lorsque le réseau est dans la état de S_{ij}, afin la disponibilité des réseaux de communication peut être formulée comme suit ;

$$A_{COM}(t) = PS(S_{0,0}) + P(S_{1,0}) \quad (3.11)$$

3.3.2.5 La fiabilité du réseau de communication de base

Dans la figure 3.8, le réseau de communication WAMS est une épine dorsale SHRN quatre nœuds de l'anneau-structure et double passage. Wang et al utiliser le réseau de quatre nœuds comme un exemple pour l'explication. Le réseau est divisé en quatre segments L1-L4 par quatre unités d'interface anneau (RIU) marqués avec RIU1 - RIU4. Chaque RIU peut être compacte représenté par une interface en série avec un commutateur. Il y a deux anneaux de fibres optiques dans le SHRN est l'anneau de fibres optiques primaires (P) et l'autre est l'anneau de fibres optiques d'attente (S) comme la sauvegarde.

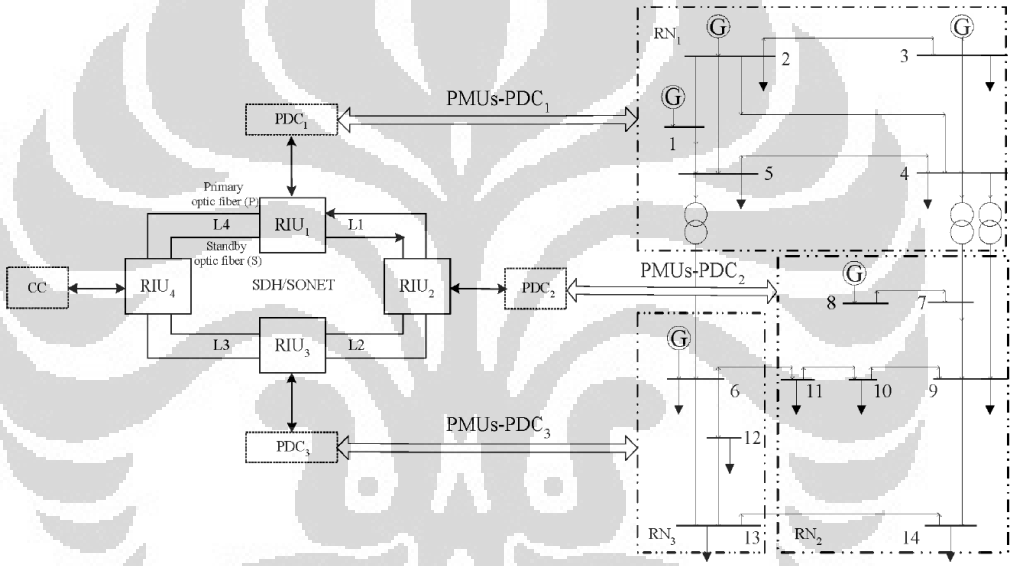


Figure 3.8. WAMS du IEEE 14 systèmes de bus.
(Source : Wang et al, 2010, p1484)

Disponibilité de l'OFS calculées par le modèle de Markov à taux d'échec et de réparation, la disponibilité de chaque interface de RIU noté avec A_{Mi}. Alors que le taux d'échec et de réparation désigné par λ_{Mi} et μ_{Mi} . Une fois les modèles de fiabilité de l'OFS et les interfaces de communication RIU sont obtenus, les indices de fiabilité quatre du réseau de communication épine dorsale peut être calculée comme suit (Wang, 2010) :

$$A_{\mathrm{BN}} = \left(\prod_{i=1'}^{4} A_{Mi}\right) \cdot A_F \tag{3.12}$$

$$U_{\mathrm{BN}} = 1 - A_{\mathrm{BN}} \tag{3.13}$$

$$\lambda_{\mathrm{BN}} = \sum_{i=1}^{4} \lambda_{Mi} + \lambda_F \tag{3.14}$$

$$r_{\mathrm{BN}} = \frac{\left(\sum_{i=1}^{4} \lambda_{Mi} r_{Mi} + \lambda_F r_F\right)}{\lambda_{\mathrm{BN}}} \tag{3.15}$$

3.3.2.6 La fiabilité d'OFS

Le diagramme de markov de transition d'état de la L1 est représenté dans la figure. 3.9, où l'état indiqué par un nombre à trois chiffres binaires représente un état de combinaison des pannes de cause commune et indépendante. Les trois chiffres binaires de gauche à droite correspondent respectivement à la panne de cause commune de deux fibres optiques, d'une panne indépendante de la fibre optique, et veille panne indépendante de la fibre optique primaire, où 0 indique que la panne correspondante, et 1 sinon.

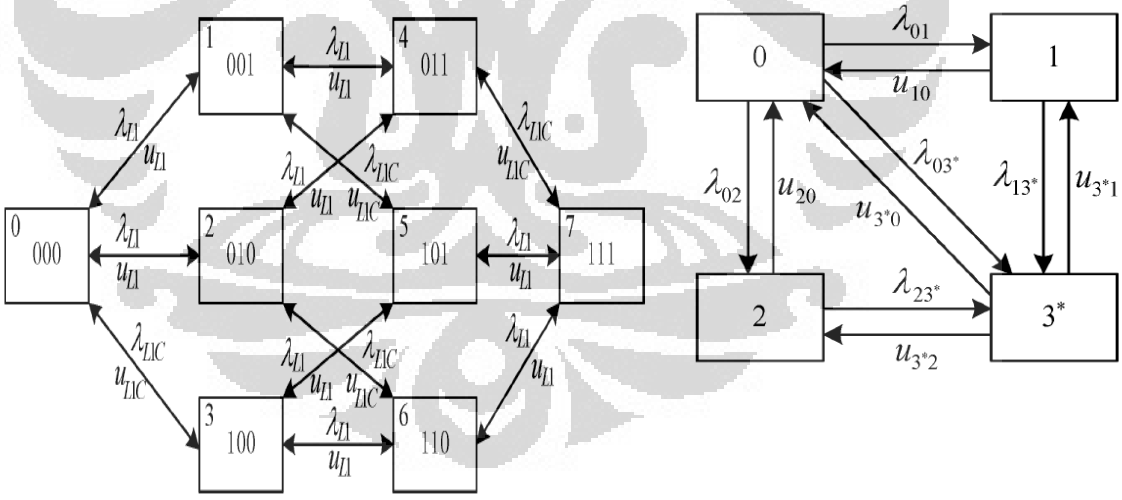


Figure 3.9 Diagramme de transition d'état des deux fibres optiques en L1 et d'équivalents de quatre l'espace d'état
(Source : Wang et al, 2010, p1486)

Les indices de fiabilité des autres états non disponibles peuvent être calculés de la même manière. Depuis les états énumérés sont mutuellement

exclusives, après les indices de fiabilité de tous les états non disponibles dans G_U sont obtenus, l'indisponibilité et la disponibilité de l'OFS peut être calculée par

$$U_F = \sum_{s \in G_U} P(s) \tag{3.16}$$

$$A_F = 1 - U_F. \tag{3.17}$$

la fréquence de défaillance de l'OFS est

$$F_F = \sum_{s \in G_U} f(s) \tag{3.18}$$

et le temps moyen de réparation est

$$r_F = \frac{U_F}{F_F} \tag{3.19}$$

Par conséquent, le taux d'échec de l'OFS peut être calculée par

$$\lambda_F = \frac{F_F}{A_F} \tag{3.20}$$

3.3.2.7 La fiabilité du *Optimal Load Shedding* (OLS)

Aminifar dans son revue, intitulé «Impact de dysfonctionnement WAMS sur le système d'évaluation de la fiabilité d'alimentation » examen de la fiabilité du contrôle non seulement les outils, mais l'opérateur au centre de contrôle. Ce concept est une combinaison d'évaluation de fiabilité des systèmes électriques et WAMS avec un terme appelé les OLS.

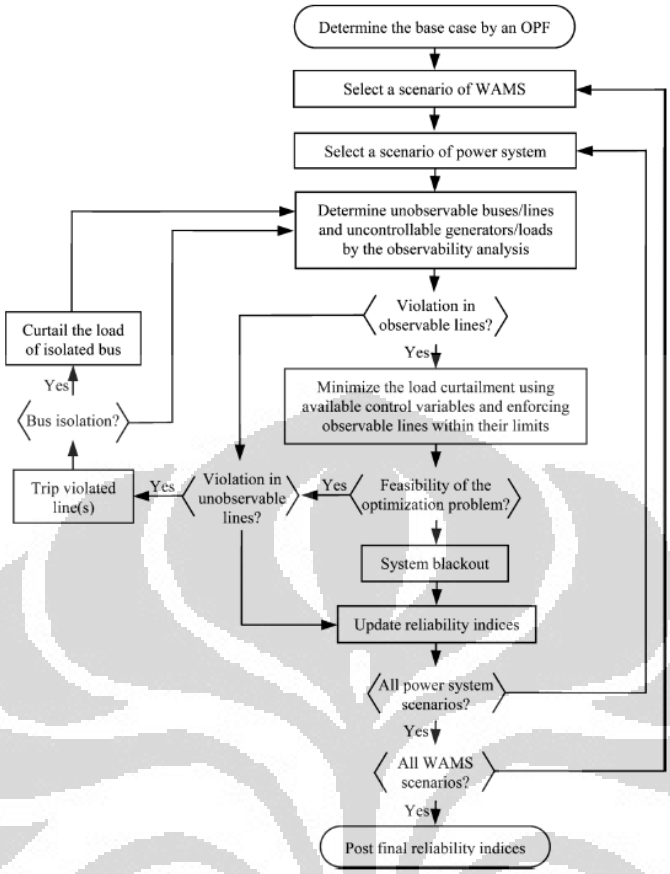


Figure 3.10 Algorithme proposé pour évaluation fiabilité conjointe du système l'électrique
(Source : Aminifar et al., 2012, p3)

Etape 1: La première étape consiste à déterminer une OPF cas de base.

Étape 2: La boucle extérieure effectue une itération sur des scénarios WAMS. La première série de scénarios est tronqué à un niveau maniable. L'évaluation de la fiabilité du système électrique composite est effectuée pour chaque scénario.

Étape 3: La boucle intérieure considère des scénarios de systèmes d'alimentation dans lequel la réduction est appliquée à nouveau scénario.

Étape 4: Un compte d'analyse d'observabilité pour arrêts forcés dans les niveaux du système de surveillance et de la puissance. Dans cette analyse, la mesure d'un courant PMU ligne donnée offre une mesure de *voltage* indirect associé à l'extrémité de la ligne d'autres.

Étape 5: Avec le cas de violations dans les régions observables, l'opérateur du système pré découpe actions correctives pour les atténuer. Ces actions

sont simulées par un délestage optimal (*optimal load shedding* = OLS) algorithme d'optimisation.

Étape 6: Cette étape simule le rôle du système de protection dans le déclenchement des lignes surchargées. Toute violation de la région inobservable est vérifiée à ce stade. Dans le cas, les lignes violées sera déclenché par le système de protection.

Étape 7: Les bus isolés sont identifiés, leurs unités de production sont fermées, et les charges respectives sont réduites. Depuis, le système passe à un nouveau point de fonctionnement, l'algorithme retourne à l'étape 5 pour vérifier d'autres violations.

Étape 8: Les indices de fiabilité sont mises à jour sur la base de réductions de charges dans le scénario et la probabilité d'occurrence de ce scénario. (Wood 1996).

Pour en savoir la fiabilité du traitement le cas de violations dans les régions observables, l'opérateur du système pré découpe actions correctives pour les atténuer. Le problème OLS peut être calculé par les formules suivantes :

$$\min f^s = \sum_{n \in B} LS_n^s \tag{3.21}$$

$$PF_l^s = \frac{SL_l^s}{x_l} \sum_{n \in B} A_{nl} \delta_n^s; \quad l \in L \tag{3.22}$$

$$\sum_{i \in G_n} SU_i^s (P_i^{bc} + \Delta P_i^s) - \sum_{\substack{l \in L \\ n \in B}} A_{nl} PF_l^s = PD_n - LS_n^s \tag{3.23}$$

$$-\overline{PF}_l \le PF_l^s \le \overline{PF}_l; \quad l \in OL \tag{3.24}$$

$$\underline{P}_i - P_i^{bc} \le \Delta P_i^s \le \bar{P}_i - P_i^{bc}; \quad i \in G_n,\ n \in CB \tag{3.25}$$

$$0 \le LS_n^s \le PD_n; \quad \forall n \in CB \tag{3.26}$$

$$\Delta P_i^s = 0; \quad \forall i \in G_n, \quad \forall n \in B - CB \tag{3.27}$$

$$LS_n^s = 0; \quad \forall n \in B - CB \tag{3.28}$$

Avec ;

f^s : Fonction objectif OLS du scénario s.

LS_n^s : Délestage au niveau du bus *n* dans le scénario *s*.

PF_l^s : Le flux de puissance de la ligne *l* dans le scénario *s*.

d_n^s : Angle de phase de tension de bus *n* dans le scénario *s*.

dP_i^s : Réexpédition de puissance de unité *i* dans le scénario *s*.

3.3.2.8 ÉTUDE DE CAS DU WAMS

3.3.2.8.1 Étude de cas un système de neuf bus (IEEE 9 bus system)

1. Cas n ° **1: les contingences du système électrique avec WAMS fiables.**

Comme le montre la figur 3.11, le réseau WAMS alloué pour la surveillance du système / commande comprend trois unités de gestion installés au bus 4, 6, et 8. Ces dispositifs de rendre le réseau totalement observable, alors que les bus 5, 7, 9 ont PMU mesures redondantes. Les données sur la fiabilité des composants WAMS sont données dans le tableau 3.1. (Aminifar et al, 2012)

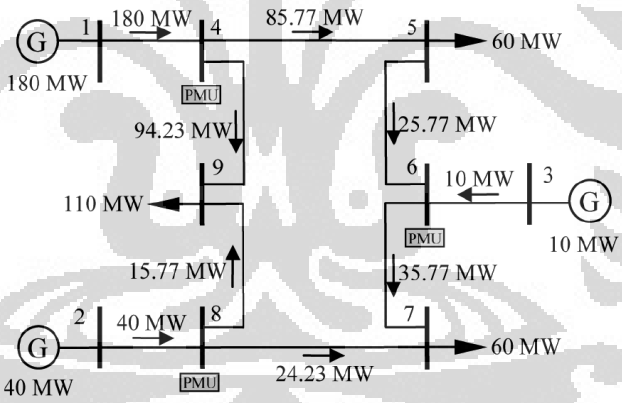


Figure. 3.11. Schéma unifilaire de l'IEEE 9 systèmes de bus.
(Source : Aminifar et al., 2012, p4)

Tableau 3.1 Génératrices de données de l'unité

	Unit located at bus		
	1	2	3
$\underline{P}_i$ [MW]	0	0	0
$\overline{P}_i$ [MW]	220	40	120
P_i^{bc} [MW]	180	40	10
Availability	0.98	0.96	0.99

(Source : Aminifar et al., 2012, p4)

Tableau 3.2 Répartition de la demande du système

	Demand located at bus		
	5	7	9
PD_n [MW]	60	60	110
% total	26.09	26.09	47.82

(Source : Aminifar et al., 2012, p4)

Tableau 3.3 Données de réseau de transport

Line		x_l [p.u.]	$\overline{PF}_l$ [MW]	Availability
From	To			
1	4	0.170	250	0.9907
2	8	0.143	120	0.9965
3	6	0.189	140	0.9942
4	5	0.085	110	0.9952
4	9	0.140	160	0.9943
5	6	0.206	110	0.9905
6	7	0.137	110	0.9976
7	8	0.241	55	0.9944
8	9	0.097	55	0.9954

(Source : Aminifar et al., 2012, p4)

Tableau 3.4. Données WAMS fiabilité des composants

Component	Availability
PMU [15]	0.995497
Current Transformer (CT) [16]	0.999584
Potential Transformer (PT) [16]	0.998542
Communication link [17]	0.999

(Source : Aminifar et al., 2012, p5)

Cette affaire est la référence de comparaison pour quantifier l'impact des dysfonctionnements WAMS sur le système de puissance, les indices de fiabilité. Tableau 3.5 donne les indices de fiabilité pour les points de charge et le système puissance.

Tableau 3.5 Cas n ° 1, les indices de fiabilité

	Load point bus			System
	5	7	9	
EDNS [MW]	0.386	0.178	1.699	2.263
% total	17.06	7.87	75.07	100

(Source : Aminifar et al., 2012, p5)

2. Cas n ° **2: Peu de risques communs du système de pouvoir et de WAMS.**

Ce cas simule un ensemble de contingences communes dans le système de puissance et WAMS. (Aminifar et al, 2012)

D'urgence 1: PMU au bus n ° 4 et la ligne 1-4 (ou à l'unité génératrice de bus 1) sont sur panne. Cette contingence simule l'instabilité de la fréquence et le potentiel de la condition panne d'électricité.

D'urgence 2: PMU au bus n ° 6 et la ligne 1-4 sont sur panne. Cette contingence simule l'impact de la disponibilité WAMS sur le délestage. Du point de vue système électrique, cette éventualité est similaire à la contingence 1.

D'urgence 3: PMU au bus n ° 8 et la ligne 6-7 sont sur panne. Cette contingence simule des pannes en cascade et l'isolement de bus.

D'urgence 4: Le PMU au bus n °8 et unité de production au bus n °2 sont sur panne. Cette contingence simule la situation que le système en défaut reste en bonne santé. Suite à la panne de l'unité génératrice de 2, l'unité de mou au système de bus n °3 compense la perte de production et de la solution nouvelle puissance de débit ne viole pas les limites de transmission.

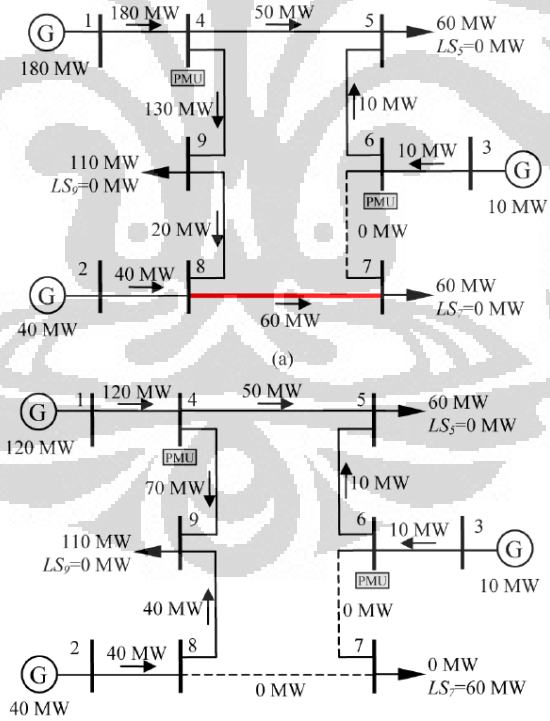


Figure 3.12 Cas n °2 panne *Precascading* pour éventualités de cas n° 3 et panne *Poscascading*
(Source : Aminifar et al., 2012, p5)

3. Cas n ° **3: Toutes les contingences de système électrique et de WAMS.**

Dans ce cas, toutes les éventualités liées au système puissance à la fois et le réseau WAMS sont considérés, y compris quatre états analysés dans le cas précédent. Ce cas est comparable à l'affaire 1, dans lequel le réseau WAMS a été supposé être totalement fiable. L'indice de fiabilité charge ponctuelle varie dans l'intervalle allant grande de 2,82 à 20,78% (Aminifar et al, 2012).

3.3.2.8.2 ÉTUDE DE CAS ET DISCUSSION: IEEE 57-BUS SYSTEME

1. Cas n ° **1: les contingences du système électrique, avec un WAMS fiables.**

EDNS dans l'affaire 1 représente la fiabilité du système repose sur l'analyse d'évaluation classique. Fiabilité indice de système EDNS 1,63 (Aminifar et al, 2012).

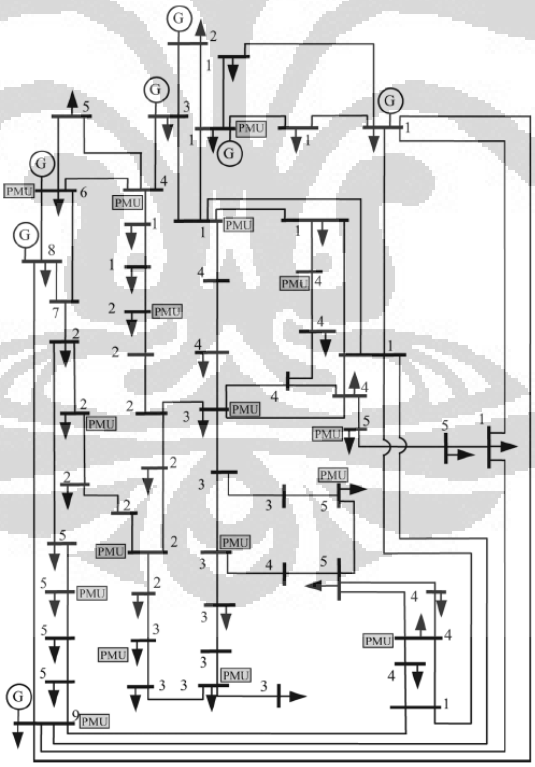


Figure 3.13. IEEE 57 systèmes de bus .
(Source : Aminifar et al., 2012, p7)

2. Cas n ° **2: Toutes les contingences de système électrique et de WAMS.**

EDNS dans l'affaire 2 montre une augmentation de 41% par rapport à celui de l'affaire 1. Ainsi l'incorporation de la défaillance de composants WAMS, comme prévu, fournit un indice de système plus global de fiabilité (Aminifar et al, 2012).

Ainsi, les principaux bus de points de charge, avec des exigences supérieures à 25 MW, sont adoptés et leurs indices de fiabilité respectifs sont détaillés dans le tableau 3.6. Par souci de comparaison, l'indice de fiabilité est employé depuis de délestage montant influe directement sur cet indice.

Tableau 3.6 Principaux indices de charge de point fiabilité dans le cas n °2

Bus # n	PD_n [MW]	$EDNS_n$ [MW]
1	55	0.0219
3	41	0.0238
6	75	0.0293
8	150	0.0588
9	121	0.0493
12	377	1.8793
16	43	0.0175
17	42	0.0184
18	27.2	0.0118
47	29.7	0.0135

(Source : Aminifar et al., 2012, p7)

3. Cas n °**3: Identique au cas n ° 2, mais la contrôlabilité est totalement fiable.**

Indice de fiabilité du système EDNS 1,80. Dans le cas n °3, il est supposé que WAMS est juste en charge de la surveillance du système et le contrôle des actions sont rendues par un autre média qui n'est pas touchées par les défaillances WAMS. Comme prévu, dans ce cas, l'indice de la fiabilité du système EDNS est supérieur à celle de l'affaire 1. Cela est dû à l'incorporation des déficits d'observabilité associés aux défaillances WAMS. Au contraire, la comparaison des cas 2 et 3 révèle que les déficits comptables de contrôlabilité aggraveraient la fiabilité du système. (Aminifar et al, 2012).

3.4 WAPS

Cette section aborde le concept de système WAPS et sa fiabilité, allant de l'architecture du système, la modélisation, à la formulation.

3.4.1 SPS (*Special Protection System*)

Le système de protection spéciale (SPS), ou des régimes de protection spéciale, est un système de protection automatique qui est conçu pour détecter des conditions anormales ou système prédéterminé, et prendre des mesures correctives pour maintenir la fiabilité du système (NERC, 2010).

3.4.1.1 L'architecture de tous les SPS conceptuel numérique

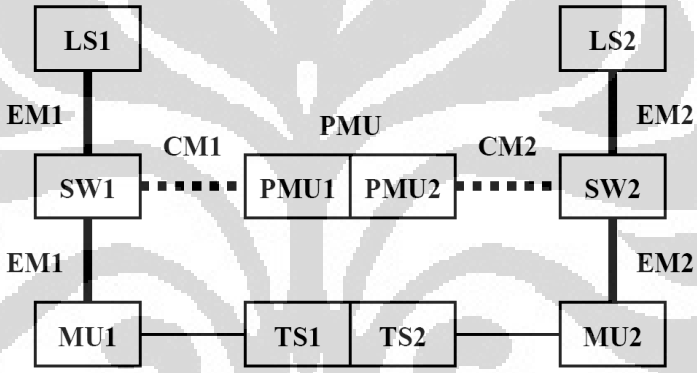


Figure 3.14 Architecture de tous les SPS conceptuel numérique
(Source : Jiang et Singh, 2011, p2)

Dans l'architecture de la figure 3.14, chaque ensemble peut remplir la fonction à plein SPS de manière indépendante et se compose d'un solveur logique numérique (LS), un commutateur Ethernet (SO), l'Ethernet supports de communication (EM), les dispositifs de l'unité de fusion (MU), une source de synchronisation du temps (TS), les équipements de phaseurs unité de mesure (PMU), et les médias numériques les canaux de communication (CM) pour le PMU. Dans le détail, les composants TS1, MU1, EM1, SW1, LS1, PMU1 et CM1 constituent un ensemble de composants SPS tout en TS2, MU2, EM2, SW2, LS2, PMU2, et CM2 forment l'autre ensemble (Jiang et al, 2011).

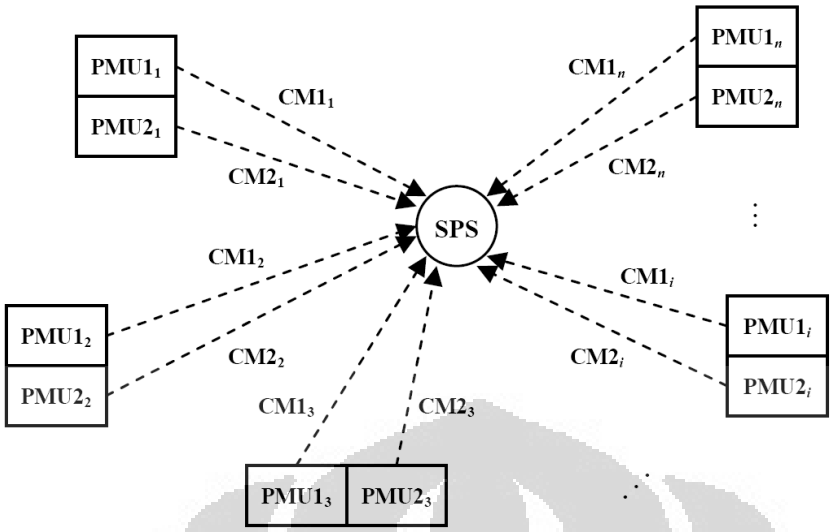


Figure 3.15 Illustration de la PMU de configuration de mise en œuvre pour SPS (Source : Jiang et Singh, 2011, p2)

PMU sont préférés pour les applications futures SPS en particulier dans les cas où l'information d'une grande surface est nécessaire pour déterminer la logique de l'alarme SPS et d'actionnement. PMU redondance est également nécessaire en raison de son importance unique dans la collecte de données. Ainsi, deux équipements PMU sont considérés pour chaque emplacement comme le montre la figure 3.15, où PMU_{1i} et PMU_{2i} sont sauvegarde mutuelle les uns aux autres pour i emplacement. Par conséquent, PMU_1 et PMU_2 la figure 3.26 ne sont pas deux unités individuelles, mais deux groupes de jeux PMU. En particulier, PMU_1 est le groupe d'appareils PMU_{1i} (i = 1,2, L, n) et PMU_2 est le groupe d'appareils PMU_{2i} (i = 1,2, L, n). De même, CM1 et CM2 dans la figure 3.26 sont également deux groupes de supports de communication numériques CM_{1i} canaux (i = 1,2, L, n) et CM_{2i} (i = 1,2, L, n), respectivement comme indiqué dans la figure 3.15. (Jiang et al, 2011)

3.4.1.2 Évaluation de la fiabilité du SPS en Utilisant La méthode de réduction de réseau

Par conséquent, nous pouvons tracer le diagramme bloc de fiabilité de la proposition de l'architecture SPS selon les relations fonctionnelles des composants comme le montre la figure 3.16 (Jiang et al, 2011).

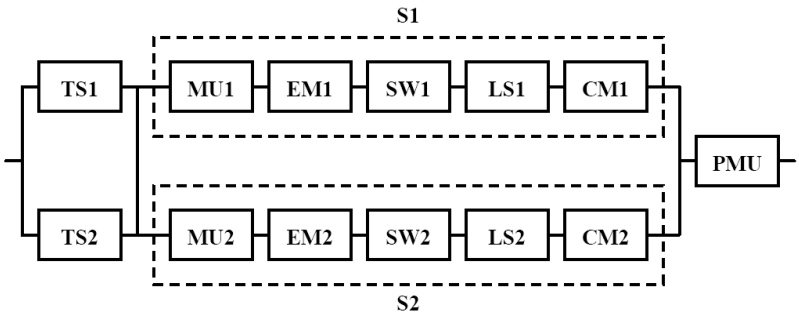
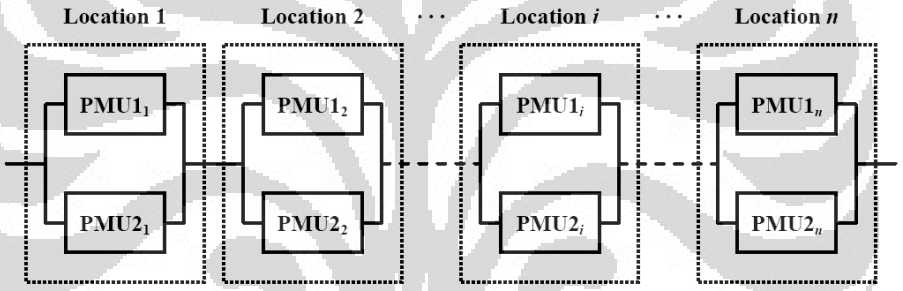


Fig. 3.16. Bloc-diagramme de SPS fiabilité
(Source : Jiang et Singh, 2011, p3)

En fait, le PMU, CM1, et CM2 dans la figure 3.15 sont des composantes conceptuellement globales, y compris, tous les emplacements nécessaires PMU pour la mise en œuvre SPS. Selon les hypothèses de configuration précédente, leur schéma de la fiabilité, peut être détaillé comme dans la figure 3.17.



(a) Agrégats component PMU

(b) agrégats component CM1

(c) agrégats component CM2

Figure 3.17 Schéma Fiabilité des composants agrégés
(Source : Jiang et Singh, 2011, p3)

3.4.1.3 Formulation SPS

La fiabilité du système de SPS (probabilité de succès SPS) est

$$p_{SPS,s} = \frac{\mu_{TS}\mu_S\mu_{PMU}}{(\lambda_{TS}+\mu_{TS})(\lambda_S+\mu_S)(\lambda_{PMU}+\mu_{PMU})} \tag{3.29}$$

Le taux de défaillance du système de SPS est $\lambda_{SPS} = \lambda_{TS} + \lambda_S + \lambda_{PMU}$

La fréquence de défaillance du système SPS

$$f_{SPS,f} = \frac{\mu_{TS}\mu_S\mu_{PMU}(\lambda_{TS}+\lambda_S+\lambda_{PMU})}{(\lambda_{TS}+\mu_{TS})(\lambda_S+\mu_S)(\lambda_{PMU}+\mu_{PMU})} \tag{3.30}$$

Le temps de cycle moyen de SPS est

$$MCT = \frac{1}{f_{SPS,f}} = \frac{(\lambda_{TS}+\mu_{TS})(\lambda_S+\mu_S)(\lambda_{PMU}+\mu_{PMU})}{\mu_{TS}\mu_S\mu_{PMU}(\lambda_{TS}+\lambda_S+\lambda_{PMU})} \tag{3.31}$$

La moyenne les temps d'arrêt (MDT) de SPS est

$$MDT = \frac{(\lambda_{TS}+\mu_{TS})(\lambda_S+\mu_S)(\lambda_{PMU}+\mu_{PMU}) - \mu_{TS}\mu_S\mu_{PMU}}{\mu_{TS}\mu_S\mu_{PMU}(\lambda_{TS}+\lambda_S+\lambda_{PMU})} \tag{3.32}$$

Le temps moyen avant défaillance (MTTF) représente le temps moyen entre pannes de système ou de perte de service. Pour des raisons d'éviter la confusion, le concept même est parfois exprimé comme la moyenne des temps (MUT) dans la modélisation du système à la réparation.

$$MTTF = MUT = MCT - MDT = \frac{1}{\lambda_{SPS}} = \frac{1}{\lambda_{TS}+\lambda_S+\lambda_{PMU}} \tag{3.33}$$

Comme nous observons dans la figure. 3.18, composants MU1, EM1, SW1, LS1, et CM1 comprennent le sous-système S1 d'une structure série. Si nous considérons S1 comme un nouveau composant composite en utilisant le concept de taux de transition équivalente à nouveau, cette composante composite aura les mêmes valeurs de taux d'échec et de réparation, les probabilités de succès et états de panne, et les fréquences de succès rencontré et états de défaillance que l'sous-système d'origine. De même, nous pouvons utiliser un autre composant composite pour représenter le sous-système série S2 formé par les composants MU2, EM2, SW2, LS2, et CM2. Ensuite, le bloc-diagramme de fiabilité peut être réduit à un système plus simple, comme indiqué dans la figure 3.18 (Jiang et al, 2011).

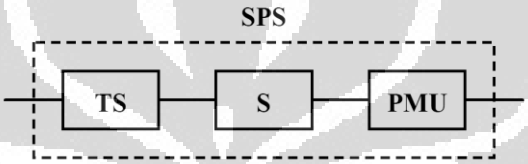


Figure 3.18. Simplifié SPS schéma de fiabilité
(Source : Jiang et Singh, 2011, p4)

Basé sur le modèle de paramètres en continu de processus de Markov, on peut dériver la formule ultime pour le calcul de MTTFF en utilisant la matrice taux de transition du système comme suit (Jiang et al, 2011) :

$$MTTFF = p_{+}(0)(-R_{11})^{-1}U_{k} \tag{3.34}$$

3.4.2 CSWAP

La structure hiérarchique de l'CSWAP est montré dans la figure. 3.19, et sur cette base, le modèle de fiabilité des CSWAP hiérarchique pourrait être construit en utilisant l'arbre de défaillances (FTA) (Hui Dai et al, 2011).

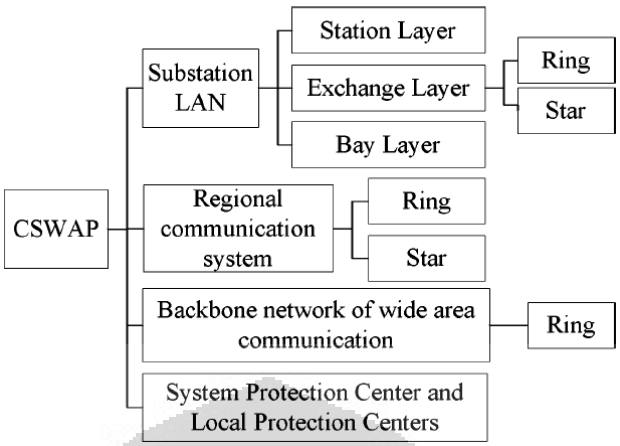


Figure 3.19. La structure hiérarchique de la fiabilité du système de communication de WAPS.
(Source : Hui Dai et al, 2011, p2525)

En règle générale, le réseau de communication interne de postes pourrait également être divisé en trois couches:

1) la couche centrale (SL),

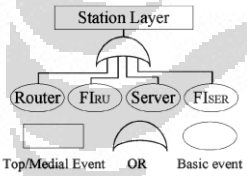


Figure 3.20 Modèle AdD de la couche centrale
(Source : Hui Dai et al, 2011, p2525)

2) la couche d'échange (EL),

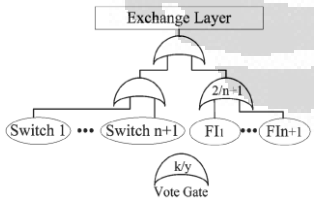


Figure 3.21 Modèle AdD de la couche d'anneau de change
(Source : Hui Dai et al, 2011, p2525)

3) la couche baie (BL).

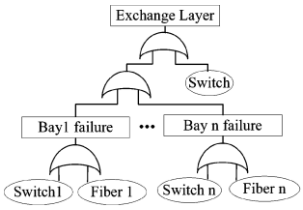


Figure 3.22 Modèle AdD de la couche d'étoiles d'échange
(Source : Hui Dai et al, 2011, p2525)

3.4.2.1 Fiabilité de la Réseau de communication, modèle de la LPC

La fonction principale de la LPC est de collecter et compiler les informations à partir des postes au sein d'une région responsable, et le transmet à la CPS au moyen d'équipements de réseau, telles que les ponts du réseau (NB). Un certain LPC composé de quatre ponts du réseau est illustré à la figure 3.23. (Hui Dai et al, 2011)

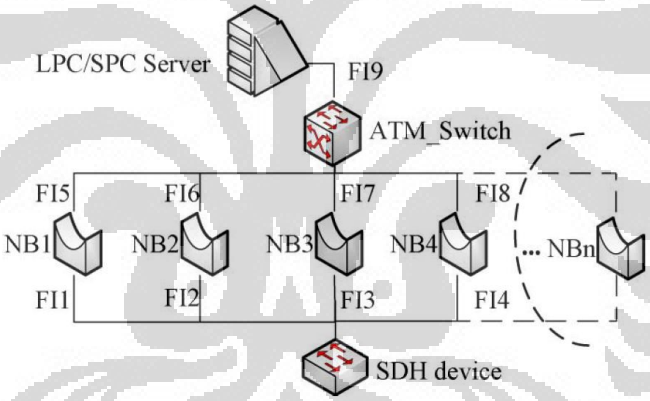


Figure 3.23. Structure de communication de la LPC.
(Source : Hui Dai et al, 2011, p2526)

Le modèle de fiabilité de la LPC est montré dans la figure 3.24.

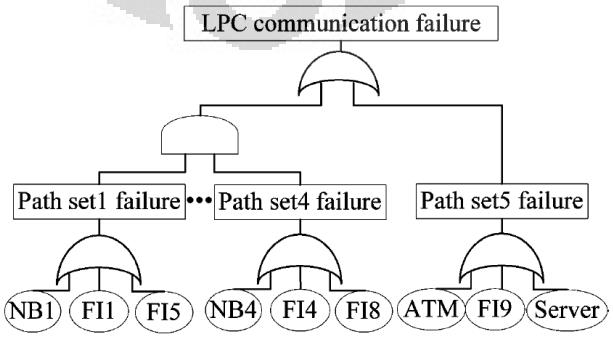


Figure 3.24 Fiabilité de communication, AdD modèle de la LPC.
(Source : Hui Dai et al, 2011, p2526)

3.4.2.2 La fiabilité du réseau *Backbone* Wide-Area et le Réseau régional

Actuellement, le réseau fédérateur de communication du système d'alimentation est principalement le réseau en anneau SDH. Nous prenons le bidirectionnel, anneau de structure, et double-passant de fibres optiques (BRDOF) réseau représenté dans la figure 3.25 (Hui Dai et al, 2011).

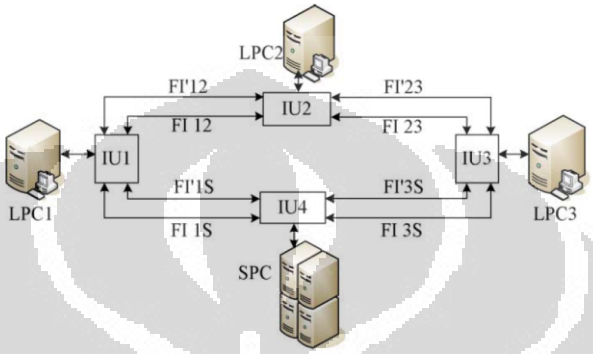


Figure 3.25. Structure du réseau fédérateur.
(Source : Hui Dai et al, 2011, p2526)

Le modèle de fiabilité correspondant AdD est montré dans la figure. 3.26.

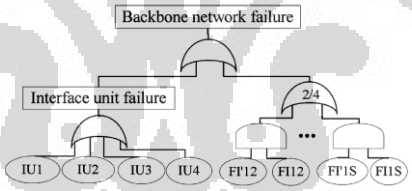


Figure 3.26. Communication de fiabilité AdD modèle du réseau fédérateur.
(Source : Hui Dai et al, 2011, p2526)

3.4.2.3 Formulation

1) Fonction cumulative de probabilité de défaillance: La donne la probabilité cumulative que le système ne parvient pas à donner le fonctionnement du système au (Hui Dai et al, 2011)

$$\mathrm{CFP}(t) = \Pr(T \leq t), T > 0, \mathrm{CFP}(0) = 0 \tag{3.35}$$

2) L'état d'équilibre Disponibilité: L'indice de disponibilité l'état d'équilibre donnant de longue durée la fiabilité de l'CSWAP pourrait être exprimée mathématiquement par

$$A = \frac{\text{MTBF}}{(\text{MTBF} + \text{MTTR})} \tag{3.36}$$

3) Indice Importance composant Probabilité: Afin d'analyser l'effet de la variation du taux de défaillance sur le taux du composant défaillance du système, l'indice d'importance composante probabilité est introduit pour identifier les composants qui altèrent de manière significative la fiabilité de la CSWAP. Elle est définie comme la dérivée partielle de manque de fiabilité du système par rapport à la probabilité de défaillance de composant.

$$I_i^{pr}(t) = \frac{\partial F(t)}{\partial F_i(t)} = \Pr\{g_{yk} = 1\} - \Pr\{g_{yk} = 0\} \tag{3.37}$$

4) Mettre fin à la simulation, le calcul des indices de fiabilité. MTTR et MTBF est calculé en

$$\text{MTTR} = \frac{\left(\sum_{l=1}^{m} T_{F,l}\right)}{\sum_{l=1}^{m} F_l} \tag{3.38}$$

$$\text{MTBF} = \frac{\left(\sum_{l=1}^{m} T_{N,t}\right)}{\sum_{l=1}^{m} N_l}. \tag{3.39}$$

5) L'estimation point de PCP pourrait être obtenu par

$$\text{CFP}(t) = \Pr(T \le t) \approx \frac{1}{T_s} \sum_{l=1}^{N} T_{F,l}, T_s \le t \tag{3.40}$$

3.4.3 ÉTUDE DE CAS DU WAPS

Assomption des paramètres pour le même type des composants, qui sont présentés dans le tableau 3.7. En outre, les paramètres de granulats composants PMU, CM1, et CM2 sont donnés directement. Les résultats de calcul de certains indices de fiabilité SPS sont figurent au tableau 3.7 (Hui Dai et al, 2011)

Tableau 3.7 Paramètres de fiabilité des composants.

Components	Failure rate (1/year)	Repair rate (1/year)
TS1 / TS2	0.01	876
MU1 / MU2	0.01	876
EM1 / EM2	0.01	876
SW1 / SW2	0.01	876
LS1 / LS2	0.01	876
CM1 / CM2	0.03	876
PMU	0.006	786

(Source : Jiang et Singh, 2011, p7)

Tableau 3.8 Les indices de fiabilité SPS

Reliability indices	Calculated values
Probability of SPS failure	0.0000076
Frequency of SPS failure (1/year)	0.00601
Mean time to first failure (MTTFF) (years)	166.4

(Source : Jiang et Singh, 2011, p7)

Tableau 3.9 Les indices de fiabilité pour différents taux de défaillance des composants

Reliability indices	Original	Two times	Three times	Five times
Probability of SPS failure	0.0000076	0.000015	0.000023	0.000038
Frequency of SPS failure (1/year)	0.00601	0.0120	0.0181	0.0303
MTTFF (years)	166.4	83.02	55.24	33.02

(Source : Jiang et Singh, 2011, p7)

Les taux de défaillance des composants ont une influence sur la fiabilité des SPS. Tableau 3.9 montre des résultats différents indices de fiabilité de SPS en augmentant tous les taux de défaillance des composants à deux, trois et cinq fois de leurs valeurs d'origine tout en gardant leurs taux de réparation de la même qu'avant.

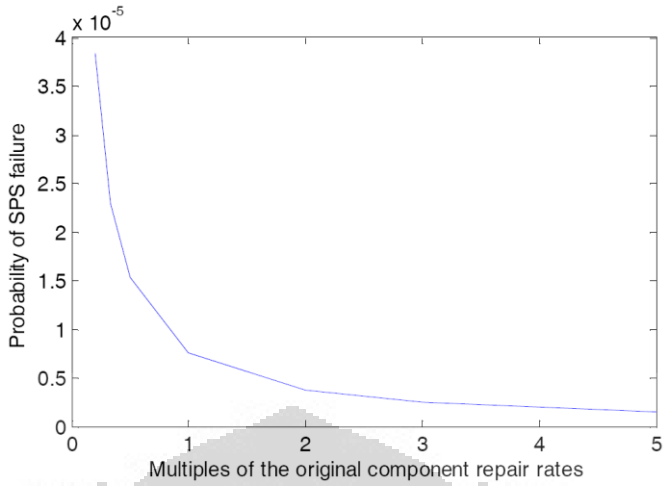


Figure 3.27. Probabilité de défaillance SPS pour différents taux de réparation des composants
(Source : Jiang et Singh, 2011, p7)

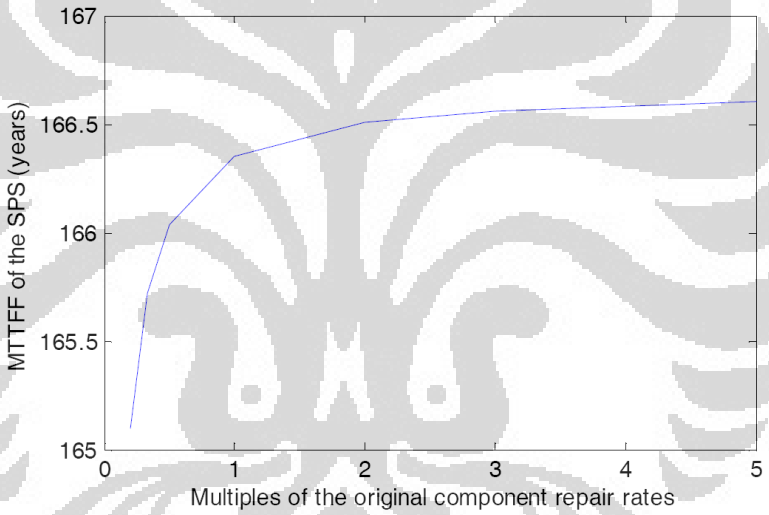


Figure 3.28. MTTFF du SPS pour les différents taux de réparation des composants
(Source : Jiang et Singh, 2011, p7)

Figure 3.27 et figure 3.28 illustrent la tendance de la probabilité de défaillance SPS et MTTFF du SPS, respectivement, en changeant tous les taux de réparation de composants dans des multiples des données d'origine en même temps.

CHAPITRE IV

ETUDE COMPARATIVE

4.1 Introduction

Ce chapitre résume le concept, la modélisation et le calcul de la fiabilité des résultats de plusieurs cas de WAMS et WAPS, pour faciliter l'analyse comparative des titres de revues seront désignés par trois caractères comme suit;

1. *Control center*
2. WAMS
3. WAPS

L'analyse de la SDF commence par une comparaison des concepts de système de contrôle du *smart grid* qui ont fait son résumé dans le chapitre 3. Cela commence par une analyse comparative des revues dans les discussions sur le concept proposé, et les discussions de sa fiabilité. La disponibilité des outils utilisés et que l'échantillon de cas à une partie de la discussion. Dans cette section des outils sont utilisé, il sera de discuter des outils qui sont souvent utilisés pour faire les concepts de modélisation et des outils ou logiciels utilisés pour la simulation.

Sur la base des instructions de l'IEEE, pour étudier le système de contrôle de *smart grid*, il est nécessaire de comprendre ce que signifie la fiabilité dans le secteur de l'électricité, ainsi que l'industrie des TIC. Les exigences pour communiquer efficacement de fiabilité divers des concepts :

1. Livraison fiable de l'énergie électrique en toute sécurité.
2. Fiabilité de la livraison des données.
3. Nature itérative de la conception.
4. Opération d'urgence de l'équipement de *smart grid.*

Lors de l'évaluation de la fiabilité et les performances de l'information et de la technologie informatique dans les systèmes d'électricité, il est important de tenir compte des effets d'environnements réels. Les listes suivante de facteurs ont le potentiel de dégrader les performances de certains réseaux de données:

1. Météo
2. Les interférences électromagnétiques

3. Problèmes de sécurité
4. Accidents
5. Emplacement/Géographie
6. D'autres événements majeurs touchant de vastes étendues

4.2 Analyse Comparative de Processus

En général, l'analyse sûreté de fonctionnement des plusieurs revues sont les suivantes;

1. Etape 1 : Définition du système
2. Etape 2 : Identification des risques du système
3. Etape 3 : Modélisation du système et formulation mathématique
4. Etape 4 : Analyse qualitative et quantitative
5. Etape 5 : Etude de cas
6. Etape 6 : Synthèse et évaluation

Cette étape est conforme à la théorie dans la littérature.

4.3 Analyse Comparative SdF de Contrôle Center

Le processus analyse SdF du contrôle de la *smart grid* effectué Zeng et al qui est un exemple simple d'application de l'analyse de fiabilité et disponibilité d'un système. Les étapes de la discussion en conformité avec d'autres chercheurs basées sur l'ingénierie de la fiabilité d'un système complexe. Nous avons essayé en utilisant le guide de livre La Gestion Des Risques, qui se divise en quatre étapes, comme suit ;

4.3.1 Evaluation Prévisionnelle

Analyse du système de contrôle recommandé par le NIST, provoquer à les recherches par certains scientifiques, y compris Zeng et al de la Département of Computer Science et Technologie, l'Université de Tsinghua, à Beijing et Département de Engineering électrique et informatique, Université de Waterloo, Canada. Ils donnent suggestions sur les stratégies de serveur de sauvegarde du centre de contrôle. C’est une brillante idée de faire en sorte le centre de contrôle faiblement à tout moment.

Caractéristiques du centre de contrôle qui est fiable et sécuritaire, avec le concept de deux stratégies pour le serveur de sauvegarde critique, devrait être lancé rapidement faire face à la suppression des interférences des pirates et des terroristes et la perturbation de vol d'électricité. Cette réaction a entraîné des perturbations étendue et l'échec peut être évité.

4.3.2 Modélisation et analyse qualitative

Bien que le concept qui a recommandé par NIST est déjà équipé d'un pare-feu pour protéger le centre de contrôle mais il y a toujours la possibilité de hackers ont réussi à travers la sous-station du centre de contrôle et faire des dommages via le WAN. Possibilité de défaillance du système est aussi causée par la panne ou de dysfonctionnement du serveur principal.

Modèle proposé par Zen et al utilisant une logique mathématique simple, à savoir le SPN. Avec SPN décrit un processus dynamique dans le système peut être décrit par un simple, et facile à comprendre, Modèle proposé par Zen et al utilisant une logique mathématique simple, à savoir le SPN. Avec SPN décrit un processus dynamique dans le système peut être décrit par un simple, et facile à comprendre, donc « *two backup strategies* » peut comprendre as serveur de secours si la perturbation a eu lieu dans le centre de contrôle.

4.3.3 Analyse quantitative

En modélisant la défaillance et les risques qui peuvent survenir dans le composant essentiel est un centre de contrôle du serveur, le Zen et al déjà ont été conçu un système de contrôle dans le centre de contrôle pour rendre le serveur de sauvegarde qui est toujours *standby*. S'il y a une défaillance, le serveur ombre qui va sauvegarder le système afin de ne pas avoir un impact important sur la distribution de l'électricité.

Dans la figure 3.3 Modèle SPN est réalisée à une formule mathématique à l'analyse CTMC et ensuite calculé sa fiabilité et sa disponibilité.

4.3.4 Synthèse

A partir des résultats de simulation obtenus les résultats que: de la figure 3.4, Zen et al présentent la fiabilité et la disponibilité sont transitoires diminue de

façon exponentielle avec le temps *t*. En outre, ils ont respectivement approché la fiabilité l'état d'équilibre Rel (Fiabilité) = 0 et de la disponibilité Ava (disponibilité) = 0,9936.

Enfin, les réseaux de centres de contrôle avec grande disponibilité l'état d'équilibre sont plus fiables et plus fiables que ceux avec les petits l'état d'équilibre de disponibilité.

4.4 Analyse comparative WAMS

WAMS est un sujet très populaire pour la recherche du système de contrôle *smart grid*, il y a plus de 35 revues qui traitent les WAMS, mais il y a seulement 4 revues complètes avec la étape de la modélisation et la formulation, d'autres seulement dans la forme de l'utilisation proposé de la méthode, sans discussion plus approfondie et une solution mathématique pour appuyer le processus d'évaluation et de vérification des études de cas. Wang et al, Liu et al, Aminifar et al, Zhang et al, ont concept complémentaire de WAMS.

A partir du concept d'un réseau mondial vers le bas pour les composants et les moyens de communication sont abordés dans les quatre revues. La méthode utilisée a été modifiée. Nous pouvons analyser par étapes comme suit;

4.4.1 Evaluation Prévisionnelle

WAMS comme le cœur du système de contrôle *smart grid* doit être garanti sa sécurité et le toujours fiable pour le suivi en temps réel et pour maintenir la stabilité du système électrique. Par conséquent besoin d'une infrastructure sûre et fiable pour toutes les conditions sur le terrain tel que la géographie extrême. Wang et al proposer une variante de dispositif qui peut être compté à soutenir le modèle de WAMS SDH.

Dans son article, Liu et al a déclaré que le système WAMS est divisé en deux sous-systèmes: du centre de contrôle du système, et du système d'acquisition de données. Dans ce système de communication, également modélisé comme un système d'évaluation supplémentaire. L'analyse du système d'acquisition de données prend des mesures de phaseurs de PMU et PDC, sont installés dans divers domaines de la protection, comme un objet d'étude, ci-après dénommé un

système sous des PDC. Cette section a contribué à assurer que le suivi dynamique en temps réel avant un moniteur central dans le centre de contrôle. En plus de la surveillance sous LIU et al également proposé corridor de communication, pour soutenir une distribution de l'électricité stable et sans coupures.

Point de vue différent, Aminifar et al, qui se penche sur WAMS, qu'il appelait SMT, comme la commande centrale et de l'acquisition par une partie de la principale SCADA. Cette section est importante de sorte que le dysfonctionnement aurait été fatal. Équilibrer l'offre, la demande et la charge du système de transmission sera particulièrement préoccupante dans la discussion de la fiabilité de WAMS chaque sous-section avec un OLS (charge optimale délestage).

4.4.2 Modélisation et analyse qualitative

Analyse qualitative de WAMS utilise Arbre de Défaillance pour décrire la défaillance de WAMS. Il est très facilement compris par le système en haut vers le bas. Représentation de la défaillance, dans chaque section que le PMU, le PDC du centre de contrôle et de réseau de communication a un rôle majeur sur le défaut global du système tel que décrit par la porte logique OU.

Une autre représentation de l'évaluation fiabilité algorithme, ce qui explique le processus de réduction, si une certaine partie de WAMS perturbé s'il y a une certaine partie de WAMS, qui a un trouble. Il a été illustré par un OLS sur le SCADA.

4.4.3 Analyse quantitative

La plupart des chercheurs en ingénierie de la fiabilité et les experts de la distribution d'énergie en utilisant la modélisation de Markov. La modélisation de Markov permet de simuler les processus dynamiques dans la distribution et de décrire les paramètres qui ne sont pas si variés. Après quelques hypothèses et simplifications conceptuelles facteur de structure concept, cette étude a corroboré par des études de cas réels sur l'IEEE 9 systèmes de bus jusqu'à l'IEEE 57 systèmes de bus.

Par conséquent, la fiabilité et la disponibilité dans le temps est noté dans le dérivé et intégral, puis la méthode de Monte Carlo peut également être utilisé pour simuler le règlement de la prévision de la fiabilité de WAMS. En raison des

itérations répétées et de la complexité du Monte-Carlo ne peut se faire pour processus de calcul sans ordinateur.

4.4.4 Synthèse

Processus de modélisation, avec Markov et de Monte Carlo sont très simple. Par conséquent, il doit être corroboré par des études de cas détaillées et réelle du système de bus qui recommandée par IEEE. Modélisation Monte Carlo pour le système OLS est pris en charge par l'application sur l'IEEE 9 systèmes de bus jusqu'à l'IEEE 57 systèmes de bus sont en mesure de décrire comment l'équilibre entre le chargement de bus pour éviter de mal fonction de WAMS. Pour les résultats de simulation obtenus avec l'IEEE 9 systèmes de bus de la disponibilité de WAMS est la suivante:

a. PMU : 0.995497
b. *Current Transformator* : 0.999584
c. *Potential Transformator* : 0.998542
d. *Communication link* : 0.999000

Que pour l'IEEE 57 système de bus, la disponibilité allant de 0,95 à 0,98, en fonction de la taille et la capacité de puissance du système de bus.

Bien que l'analyse du processus de Markov est simulé avec les systèmes de bus IEEE14 qui représentent le système de distribution intermédiaire. Ces systèmes sont largement utilisés dans la plupart des villes dans le monde. Pour l'étude de cas, l'acquisition de données et de la communication dans le centre de contrôle corridor varié avec μ le taux de défaillance différente de 0,5 à 0,9 produit une valeur maximale de 0925 tandis que la disponibilité des valeurs fiables de chaque système de sous-zone est différent de 0638 jusqu'à 0,9996.

4.5 Analyse comparative WAPS

Certains chercheurs de séparer les fonctions de surveillance et de protection de WAMS et WAPS, mais certains chercheurs les combiner en un seul dans WAMS. Kai Jiang et al proposent un système entièrement numérique WAPS, tandis que Hui Dai et al revoient les systèmes de protection dans plus de contrôle sur la synchronisation à la sous-station des composants individuels de WAPS.

4.5.1 Evaluation Prévisionnelle

Système de contrôle de la base du processus nécessite une bonne protection, qui craignait la perturbation de ce système est l'inexactitude de synchronisation de l'heure tel qu'évalué par Jiang et al. Alors que d'autres facteurs sont également importants afin de protéger la communication dans lequel chaque couche de chaque station et des composants donnés contribué à l'échec de la fonction des WAP, y compris les interférences en Ethernet.

4.5.2 Modélisation et analyse qualitative

Jiang et al utilisent le diagramme de la fiabilité pour analyser l'évaluation de modélisation de WAPS, avec hypothèses sont valables pour qu'un système complexe de WAPS que figure 3.15 simplifiée soit dans figure 3.18. Alors Hui Dai et al préfèrent un très simple arbre de défaillance par les ingénieurs électriciens, car elle utilise des portes logiques.

Analyse avec l'arbre de défaillance qui est simple et complet a été utilisé pour l'analyse de fiabilité des réseaux de communication, le « *back bone network* » et de la communication WAPS comme un tout.

4.5.3 Analyse quantitative

L'analyse quantitative de WAPS utilise l'outil de Monte Carlo pour la discussion de CSWAP qui est complexe et il procède à l'évaluation des études de cas avec l'IEE 11 systèmes de bus.

Pendant ce temps, Jiang et al préfèrent utiliser la modélisation de Markov pour la discussion complète numérique de fiabilité du système WAPS. Avec le paramètre applications MTTF, MTTFF et WAPS devenu plus facile à comprendre en regardant le temps de réparation et de temps la perturbation d'un système.

4.5.4 Synthèse

Discussion avec les indicateurs de performance de la fiabilité du système MTTFF suivies par des études de cas qui contiennent beaucoup des hypothèses ne sont pas favorisés par l'ingénieur électricien. Cependant cela peut refléter la possibilité de réparation et de temps pour réparer un système. A partir des exemples donnés assomption obtenu pour WAPS est l'interférence possible avec

0.0000076 perturbations de fréquence est 0,00601 qui a été obtenu MTTFF de 166,4 par année.

Attendu que Hui Dai et al. ont autres propositions détaillant avec simulation de formulations qui ont été obtenus à partir de la modélisation, testé le IEEE 11 systèmes de bus dans lequel chaque zone pour obtenir une valeur comprise entre 0,9468 à 0,9536 tandis que pour les programmes de sorte que le système dans son ensemble est obtenue par la faible disponibilité de 0,89513 discussion sur cela est dû à la couverture analyse est trop large.

4.6 Comparaison étape analyse qualitative

La méthode est souvent utilisée dans l'analyse qualitative sont;

1. Arbre de Défaillances (en Anglais FTA)
2. Réseaux de Petri Stochastiques (en Anglais SPN)
3. Algorithme
4. Diagramme de la fiabilité (en Anglais RBD)

4.7 Comparaison étape analyse quantitative

Phase décisive dans la phase d'analyse du SDF est le modèle de probabilité et le traitement des données. Les nombreux chercheurs sont utilisant le de la méthode de Markov est simple, mais beaucoup aussi utiliser itérations répétées de l'exactitude des données avec Monte-Carlo ou même avec un SPN. Dans l'ensemble, les méthodes couramment utilisées sont :

1. Chaine de Markov
2. Monte Carlo Simulation
3. Réseaux de Petri Stochastiques (en Anglais SPN)

4.8 Comparaison étape synthèse

L'utilisation d'études de cas réels et standard de la preuve permettra de renforcer la fiabilité et la disponibilité d'un système de synthèse dans le chapitre 4 du présent la plupart des chercheurs utilisent utilisant les systèmes standard IEEE 14 systèmes de bus, mais certains sont à partir de l'IEEE 9 systèmes de bus, l'IEEE 11 systèmes de bus jusqu'à l'IEEE 57 systèmes de bus.

CONCLUSION

Sur certains chercheurs au sujet du réseau intelligent et ingénierie de la fiabilité, il peut être conclu que;

1. En général, les étapes l'analyse SdF du système de contrôle *smart grid* sont les suivantes:
   a. évaluation initiale,
   b. modélisation,
   c. analyse qualitative,
   d. analyse quantitative et,
   e. étape de synthèse.
2. Dans les étapes de l'analyse qualitative, les outils qui sont souvent utilisés;
   a. Arbre de Défaillances (FTA)
   b. Diagramme de la fiabilité (RBD)
   c. Algorithme
3. Dans les étapes de l'analyse quantitative, les outils qui sont souvent utilisés;
   a. Chaine de Markov
   b. Monte Carlo Simulation
   c. Réseaux de Petri Stochastiques (SPN)
4. Dans les concepts de FMDS, les facteurs de sécurité et les facteurs de maintenance sont souvent discutés séparément mais ils sont inclus dans la discussion sur les probabilités de défaillance pour garantir la sécurité et l'état de santé du système.

BIBLIOGRAPHIES

Ali A. Chowdhury, POWER DISTRIBUTION SYSTEM RELIABILITY Practical Methods and Applications, John Wiley & Sons, Canada, 2009.

Aminifar et al, Impact of WAMS Malfunction on Power System Reliability Assessment, IEEE Transactions on Smart Grid, 2012.

Brown, Richard E., Electric Power Distribution Reliability, Marcek Dekker, New York, 2002.

Barlow, Richard E, Engineering Reliability, SIAM, Philadelphia, 1998.

Chakrabortty, Aranya, Control and Optimization Methodes for Electric Smart Grids, Springer, New York, 2012.

Desroches Alain, La gestion des risques, principes et pratiqués, Lavoisier, Paris, 2003.

Fang et al, Smart grid – The New and Improved Power Grid : A survey, IEEE, 2011.

Groupement des industries de l'équipement électrique du contrôle-commande et des services associés, Livre Blanc Réseaux Électriques Intelligents, Paris, 2010.

Gerard Landy, AMDEC Guide Practique, 1 re edition, Afnor, Paris, 2011.

Hruz, modeling and Control of Discrete-event Dynamic Systems, Springer, London, 2007.

Hui Dai et al, Reliability Evaluation of communication Network in Wide-Area protection, IEEE Transactions on Power Delivery, 2011.

IEEE, IEEE Guide for Smart Grid, IEEE Standards Coordinating Committee 2011, New York, 2011.

Jiang et al, Reliability Evaluation of a Conceptual All-digital Special protection System architecture for the Future Smart Grid, IEEE, 2011.

LUI et al, Reliability analysus of Wide Area Measurement System based on the Centralized Distributed model, IEEE, 2009.

Mortureux Y. La sûreté de fonctionnement : méthodes pour maîtriser les risques, Paris, 2005.

Moslehi Khosrow, kumar Ranjir, A reliability Persective of the Smart Grid, IEEE Transactions Smart Grid, 2010.

Niel Eric, Maitrise des risques et sûreté de fonctionnement des systèmes de production, Lavoisier, Paris 2002.

Villemeur Alain, Sûreté de Fonctionnement des systèmes industriels, Collection de la Direction des Etudes et Recherches d'Electricité de France, Eyrolles, 1988.

Widerman, R Max, Risk Management, PMI, Pennisylvania, 1992.

Wang et al, Reliability Analysis of Wide-Area measurement System, IEEE Transactions on Power Delivery, 2010.

Zhang et al, Reliability Evaluation of Phasor Measurement Unit Using Monte Carlo Dynamic Fault Tree Method, IEEE transaction on Smart Grid, 2012.

Zheng et al, Dependability Analysis of Control Center Networks in Smart Grid using Stochastic Petri Nets, IEEE Transactions on Parallel and Distributed Systems, 2012.

http://www.connaissancedesenergies.org Réseau intelligent (*Smart Grid*).

ANNEXE 1

Arbre de Défaillances (AdD)/ Fault Tree Analysis (FTA).

1. Introduction

Objectif : déterminer la raison initiale d'apparition d'un évènement non désire et la probabilité que celui-ci survienne.

Méthodologie : procédure bien dénie. Procède par combinaison de fautes menant à l'événement non désire. Evènement non désire ou événement redoute.

Méthode d'analyse :

a. Déductive (contrairement à l'AMDE(C) qui est inductive) ;
b. Relativement simple ;
c. Basée sur un modelé graphique.

Méthode née en 1962 chez Bell Labs et conçue par H.A. Watson. Contrat de l'U.S. Air Force Ballistics Systems Division pour évaluer le système de mise à feu du Minute man I Intercontinental Ballistic Missile (ICBM). A été ensuite développée et formalisée surtout par la société Boeing. Ensuite, depuis 1965, emploi fréquent dans de nombreux domaines industriels (aéronautique, nucléaire, chimie, ...).

Quand faire une FTA ?

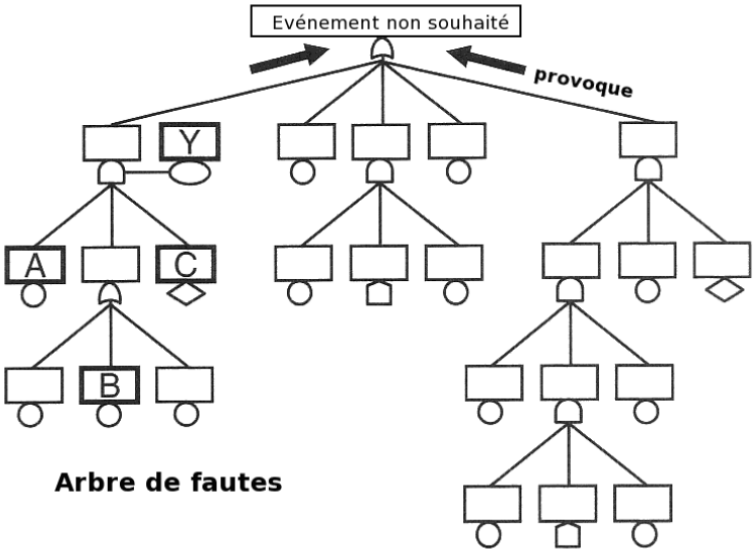
Proactive : avant mise en service du produit ; renforcer la confiance qu'on a dans le produit.

Réactive : comprendre la survenue d'une défaillance a posteriori (analyse post-mortem).

2. Principe de la méthodologie

a. Partir d'un événement non souhaite (racine de l'arbre).
b. Construire un diagramme logique représentant les combinaisons d'évènements. Pondérer les probabilités de ces événements.
c. En déduire les «cut sets« (combinaisons d'événements menant a l'événement racine).

3. Les étapes de la méthode



Arbre de fautes

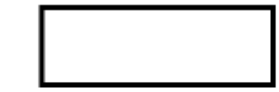
8 étapes essentielles :

1. Comprendre l'architecture et le fonctionnement du système ;
2. Déterminer un événement non souhaite (pertinent !) ;
3. Définir les réglés et limites d'analyse ;
4. Construire l'arbre des fautes suivant la méthodologie ;
5. Identifier les « cut sets » et les probabilités ;
6. S'assurer que l'arbre est correct et complet (versus système) ;
7. Faire évoluer l'arbre au fur et à mesure des modifications du système ;
8. Documenter l'analyse.

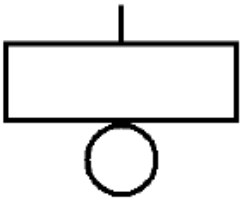
Un aperçu de la représentation

a. Utilisation d'un formalisme graphique bien établi.
b. Chaque nœud doit être documenté.
c. Chaque forme de nœud a une sémantique précise.

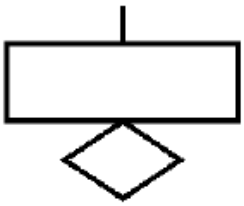
4. Représentation des événements de base



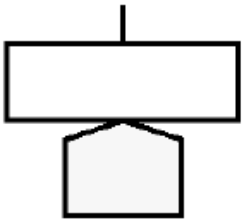
Noeud de documentation (texte simple).



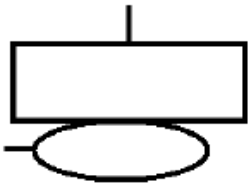
Noeud de défaillance primaire
(inhérente au composant).



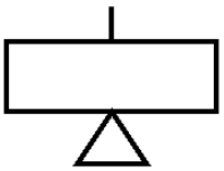
Noeud de défaillance secondaire
(induite par une défaillance externe au composant).



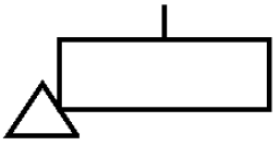
Noeud d'événement normal
(attendu en fonctionnement nominal du système).



Noeud de restriction conditionnelle ou de probabilité.



Noeud de "transfert".
Indique qu'un sous-arbre défini ailleurs vient se greffer
en dessous du noeud courant.



Noeud de "transfert".
Indique que le sous-arbre étiqueté est "exporté" et utilisé
ailleurs.

5. Combiner les conditions

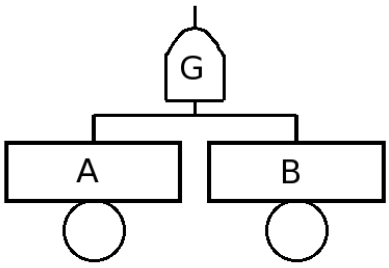
a. Cause d'un _événement non souhaité pas forcément simple.

b. Peut faire intervenir plusieurs défaillances.

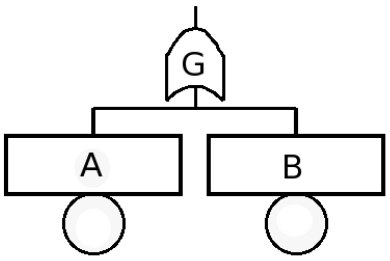
c. On combine alors les nœuds par des « gate nodes » (Expressions logiques simples).

Représentation des combinaisons

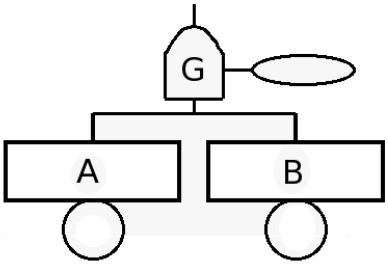
Porte "AND".
Sortie survient ssi les 2 entrées surviennent.



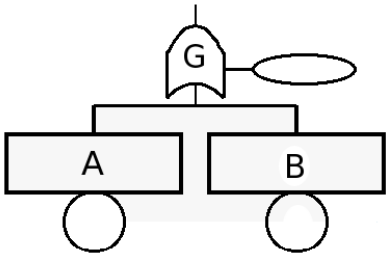
Porte "OR".
Sortie survient si au moins 1 entrée survient.



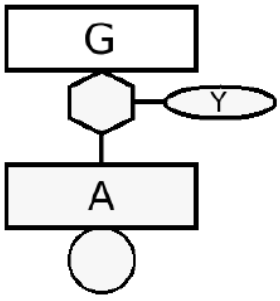
Porte "priority AND".
Sortie survient si les 2 entrées surviennent,
et A survient avant B.



Porte "XOR".
Sortie survient si 1 et 1 seule des entrées survient.



Porte "inhibit".
Sortie survient si entée survient
et condition attachée satisfaite.

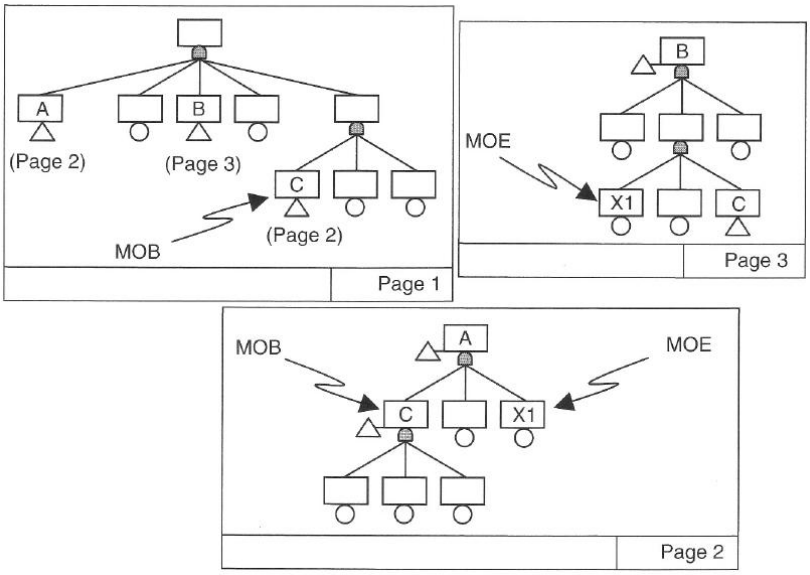


6. Définitions

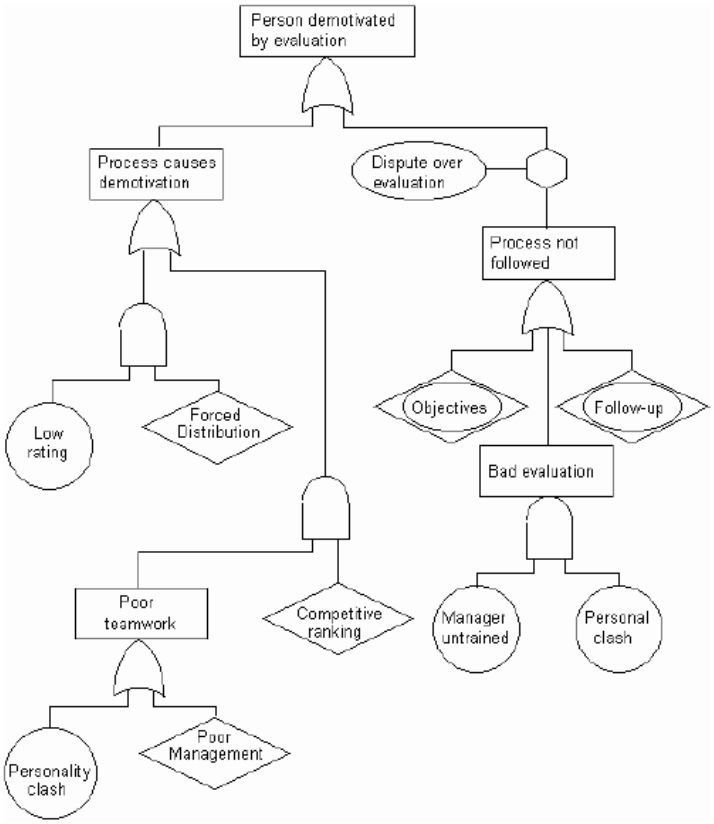
Objectif : donner un vocabulaire précis aux concepts manipulés dans un “ Fault Tree “.

1. Cut Set (CS) : combinaison d'événements menant à l'événement racine.
2. Minimal Cut Set (MCS) : combinaison réduite au maximum d'évènements menant a l'événement racine.
3. Cut Set Order : nombre d'éléments dans un CS.
4. Multiple Occuring Event (MOE) : événement de base du FT apparaissant à différents endroits dans le FT.
5. Multiple Occuring Branch (MOB) : branche du FT apparaissant à différents endroits dans le FT.
6. Failure : apparition d'une défaillance inhérente à un composant (exemple : transistor « grille »).
7. Fault : occurrence ou existance d'un état non désiré d'un composant, d'un sous-système ou du système.
8. Primary Fault/Failure : défaillance d'un composant qui ne peut pas être raffinée.
9. Secondary Fault/Failure : défaillance d'un composant due à une action extérieure sur le système.
10. Command Fault/Failure : élément « commandé » pour défaillir ou forcé dans un état fautif.
11. Critical Path : CS menant à la racine de l'arbre avec la plus forte probabilité.

7. Intérêts des nœuds de transfert : modularité



8. Système d'évaluation du personnel



Bibliothèque :

Delahaye, David, Cours de Sûreté de Fonctionnement, CNAM, 2009

ANNEXE 2

Diagramme de Fiabilité (Reliability Bloc Diagram (RBD))

1. Introduction

Le BDF est une représentation des éléments qui participent à la réalisation des diverses fonctions d'un produit, sous la forme de blocs rectangulaires, en série ou parallèle, liés entre eux. Le fonctionnement est assuré tant que la chaîne n'est pas rompue par la défaillance de certains blocs. La fiabilité de la chaîne est calculée et différentes redondances sont simulées pour augmenter sa fiabilité.

Les types de redondances sont :

a. la redondance active M parmi N : les N éléments en redondance fonctionnent simultanément, sachant que seulement M éléments sont nécessaires pour assurer le service attendu.

b. la redondance passive M parmi N : M-N éléments sont des éléments de rechange.

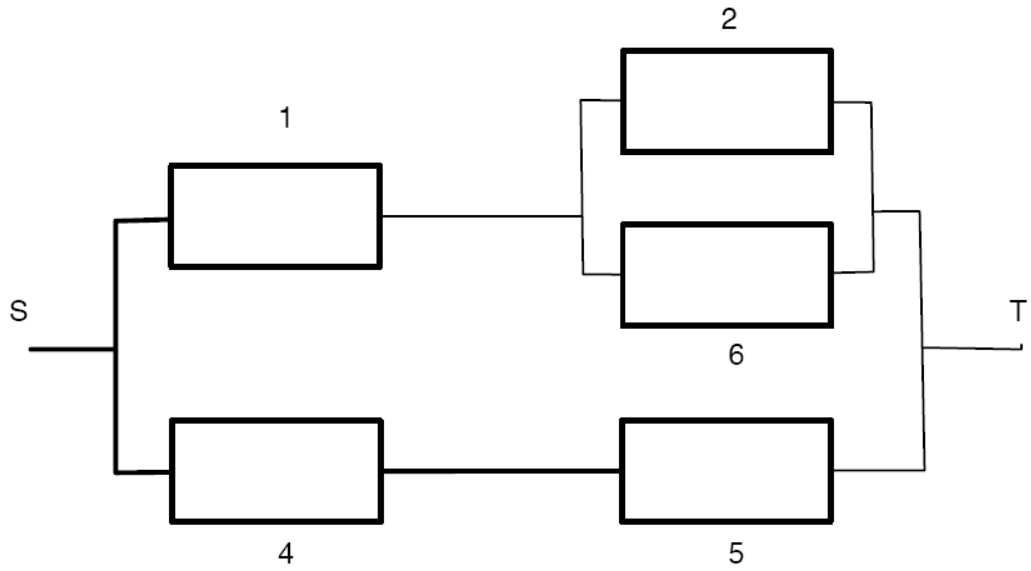
- ✓ Une représentation graphique du système et de la fiabilité.
- ✓ Chaque composant est représenté par un bloc.
- ✓ Sert à déterminer si le système est UP ou DOWN en fonction des états des composants.
- ✓ Idée intuitive : un bloc peut être vu comme un switch qui est fermé quand le composant est UP et ouvert quand le composant est DOWN.
- ✓ Il y a une entrée dans le diagramme S et une sortie T.

2. Définition

- ✓ C'est un modèle reposant sur la logique et non pas sur les états.
- ✓ Modèle Statique : pas de représentation du temps ni de l'ordre entre des événements successifs.
- ✓ Hypothèse d'Indépendance des pannes des différents composants.
- ✓ Pas de pannes arrivant conjointement ou de pannes provoquées par la panne d'un autre composant.

3. Structure

Le système est UP s'il y a au moins un chemin passant par des éléments UP et reliant S à T.



4. Logique

- ✓ **Le comportement du système par rapport à la panne est modélisé par les connexions entre blocs.**
- ✓ **Si tous les composants sont nécessaires, les modéliser en série**
- ✓ **Si un seul des composants est nécessaire, les modéliser en parallèle.**
- ✓ **S'il en faut au moins K parmi N, utiliser la structure "K out of N"**

a. Blocs en Série

n composants indépendants en série.

E_i le composant i fonctionne.

$R_s = P(E_1 \setminus E_2 \setminus : : : \setminus E_n)$

A cause de l'indépendance :

$$P(E_1 \cap E_2 \cap \ldots \cap E_n) = \prod_{i=1}^{n} P(E_i)$$

En notant $R_i = P(E_i)$, on obtient :

$$R_s = \prod_{i=1}^{n} R_i$$

On remarque que $R_s < \min(R_i)$. Le système est moins fiable que sa composante la moins fiable.

b. Blocs en Parallèle

n composants indépendants en parallèle.

E_i le composant i fonctionne.

$R_s = P(E_1 [E_2 [: : : [E_n)$

Le système est en panne si tous les composants sont en panne :

c. Systèmes Série-Parallèles

Décomposition récursive : un système série-parallèle (SP) est soit :

- ✓ un bloc isolé
- ✓ plusieurs sous-systèmes SP en série
- ✓ plusieurs sous-systèmes SP en parallèle

Utilise la décomposition récursive de la construction pour obtenir la fiabilité.

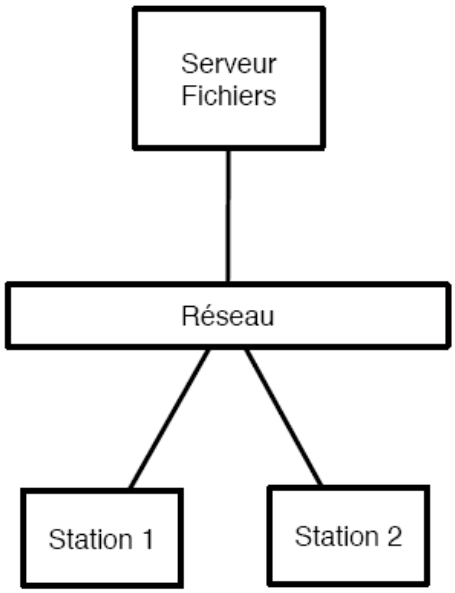
Exemple simple : n étages en série, chaque étage composé de m composants en parallèle tous identiques :

$$R_{sp} = (1 - (1 - R)^m)^n$$

5. Exemple : Station de Travail/ serveur de Fichiers

- ✓ Un serveur de fichiers,
- ✓ Deux stations de Travail identiques
- ✓ Un réseau pour les connecter. On suppose que le réseau est fiable.
- ✓ Le système est opérationnel si le serveur de fichiers est opérationnel et au moins une des deux stations de travail est opérationnelle.

a. Représentation de l'exemple



b. Etude de la fiabilité de l'exemple

R_w fiabilité d'une station de travail

R_f fiabilité du serveur de fichiers

R_{fsw} fiabilité du système

$R_{fsw} = (1 - (1 - R_w)^2) R_f$

ANNEXE 3

Chaine de Markov

1. Introduction

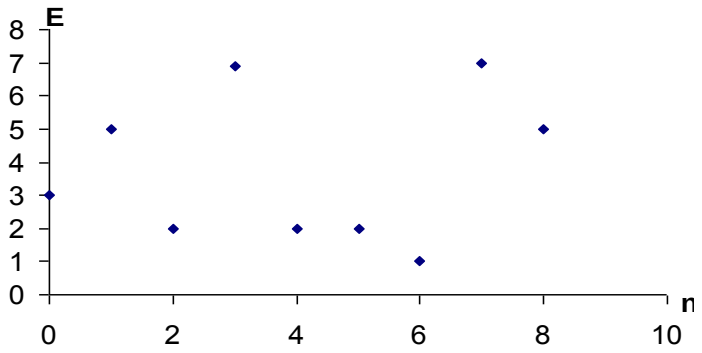
Nous considérons deux exemples de processus stochastiques à espace d'état discret

a. Chaînes de Markov à temps discret (CMTD)
b. Chaînes de Markov à temps continu (CMTC)

Chaînes de Markov : analyse préliminaire à l'étude des systèmes de files d'attente

2. Les chaînes de Markov à temps discret (CMTD)

- ✓ Processus stochastique $\{Xn\}$ n $_{\in}E$ à espace d'état discret et à temps discret
- ✓ E est l'espace d'états, De dimension finie ou infinie (mais dénombrable car discret)



- Définition : $\{X_n\}_{n\in E}$ est une chaîne de Markov à temps discret ssi

$$P\left[X_n = j \,\middle|\, X_{n-1} = i_{n-1}, X_{n-2} = i_{n-2}, \ldots, X_0 = i_0\right] = P\left[X_n = j \,\middle|\, X_{n-1} = i_{n-1}\right]$$

- La probabilité pour que la chaîne soit dans un certain état à la nième « étape » du processus ne dépend que de l'état du processus à l'étape précédente (j = n-1), et pas des états dans lesquels il se trouvait aux étapes antérieures (j = 0, …, n-2)
- Autrement dit :
  - Une chaîne de Markov est un système pouvant évoluer entre n états X_i définis par le repère X = (X_1, X_2, … X_n),

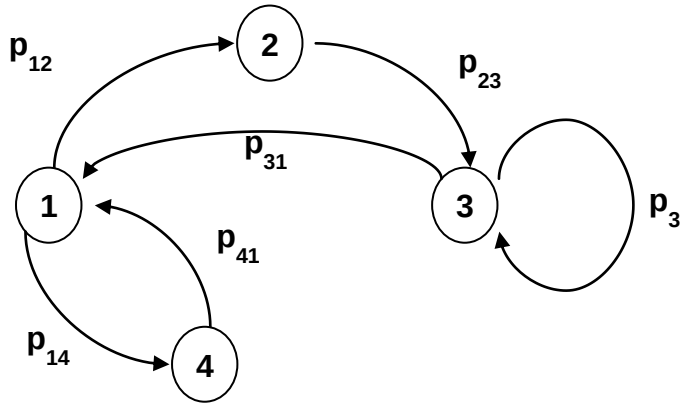
- Le passage d'un état X_i à un état X_j ou transition, ne dépend que de ces deux états et s'effectue selon la probabilité conditionnelle $Prob(X_j/X_i) = p_{ij}$

$$\sum_{j \in E} p_{ij} = 1 \text{ et } \quad p_{ij} \geq 0$$

- Matrice de transition $P \in [P_{i,j}]_{\ i,\ j \in E}$
  - Matrice carrée d'ordre fini ou infini, selon que l'espace d'état est fini ou infini

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1j} & \cdots \\ p_{21} & p_{22} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{i1} & \cdots & \cdots & p_{ij} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

- Représentation graphique
  - Graphe orienté
  - On associe à chaque état un nœud
  - On associe à chaque transition possible entre chaque état un arc pondéré par la probabilité de transition
- Exemple :



E = {1,2,3,4}

p23 = p41 = 1

P12 + p14 = 1 et p31 + p33 = 1

$$P = \begin{pmatrix} 0 & p_{12} & 0 & p_{14} \\ 0 & 0 & 1 & 0 \\ p_{31} & 0 & p_{33} & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

3. Les chaînes de Markov à temps continu (CMTC)

3.1 Exercice

Un syst`eme clients-serveur re¸coit en moyenne 1000 requˆetes par seconde, arrivant selon un processus de Poisson. Il dispose d'un unique serveur pouvant traiter en moyenne 2000 clients par seconde. On suppose que le temps de service d'un client est distribut´e selon la loi exponentielle.

Q 1.1 – Calculer la probabilit´e que le temps de service d´epasse 2 ms.

Q 1.2 – Quelle est le pourcentage de clients rejet´es pour un syst`eme ne comportant pas de file d'attente.

Q 1.3 – Mˆeme question pour un syst`eme comportant une file d'attente de 1 place. Calculer le taux d'application du serveur.

Q 1.4 – Mˆeme question pour un syst`eme comportant une file d'attente de 2 places

3.2 Solution

Fig. 1 – File d'attente comportant 0 (resp. 1) place.

Q 1.1 – En choisissantt la milli–seconde comme unit´e de temps, on trouve $\lambda = 1$ client/ms et $\mu = 2$ client/ms. On pose $a := \lambda/\mu = 1/2$.

Le temps de service TS d'un client suit la loi exponentielle de param`etre μ donc

Prob $\{TS > t\} = \exp(-\mu t)$.

Pour $t = 2$, on trouve Prob $\{TS > 2\} = \exp(-4) = 0.0183$.

Q 1.2 – Le calcul de la distribution stationnaire de la chaine de Markov figurant en figure

1 (a) conduit à résoudre le système linéaire $\lambda\ \pi_0 = \mu\pi_1$ et $\pi_0 + \pi_1 = 1$. Le calcul donne

$$\begin{cases} \pi_0 &= \dfrac{\mu}{\lambda+\mu} &= \dfrac{1}{1+a} &= \dfrac{2}{3} \\ \pi_1 &= \dfrac{\lambda}{\lambda+\mu} &= \dfrac{a}{1+a} &= \dfrac{1}{3} \end{cases}$$

Le pourcentage de clients rejetés est $\boxed{\pi_1 = 33.3\%}$.

Q 1.3 – Le calcul de la distribution stationnaire de la chaine de Markov figurant en figure 1 (b) conduit à résoudre le système linéaire $\lambda\ \pi_0 = \mu\pi_1$, $\lambda\ \pi_1 = \mu\pi_2$ et $\pi_0 + \pi_1 + \pi_2 = 1$. Le calcul donne

$$\begin{cases} \pi_0 &= \dfrac{1}{1+a+a^2} &= \dfrac{4}{7} \\ \pi_1 &= \dfrac{a}{1+a+a^2} &= \dfrac{2}{7} \\ \pi_2 &= \dfrac{a^2}{1+a+a^2} &= \dfrac{1}{7} \end{cases}$$

Le pourcentage de clients rejetés est π_2 et le taux d'occupation du serveur est π_0.

Q 1.4 – Le calcul de la distribution stationnaire de la chaine de Markov $M/M/1/3$ conduit à résoudre le système linéaire $\lambda\ \pi_0 = \mu\pi_1$, $\lambda\ \pi_1 = \mu\pi_2$, $\lambda\ \pi_2 = \mu\pi_3$ et $\pi_0 + \pi_1 + \pi_2 + \pi_3 = 1$. Le calcul donne

$$\pi_k = \frac{a^k}{1+a+a^2+a^3}, \qquad k = 0 \ldots 3\ .$$

Le pourcentage de clients rejetés est $\boxed{\pi_3 = \frac{1}{15}}$ et le taux d'occupation du serveur est $\boxed{\pi_0 = \frac{8}{15}}$.

Bibliographie :

Marangé, Pascale, Module Analyse de systèmes de production, Univ- Nancy, 2008.

Petiot, Michel, Chaines de Markov en temps continu, 15 septembre 2010

ANNEXE 4

Simulation de Monte Carlo

1. Introduction

La méthode de Monte Carlo : est une technique numérique pour solutionner des problèmes mathématiques en simulant des variables aléatoires. Il n'y a pas un consensus absolu sur une définition précise de ce qu'est une technique de type Monte Carlo, mais la description la plus habituelle consiste à dire que les méthodes de ce type se caractérisent par l'utilisation du hasard pour résoudre des problèmes centrés sur un calcul. Elles sont en général applicables à des problèmes de type numérique, ou bien à des problèmes de nature elle-même probabiliste.

De manière générale, la simulation permet d'étudier et expérimenter un système donné dont on connaît les interactions complexes, de mesurer les effets de certains changements dans les intéractions sur le comportement du système, d'expérimenter de nouvelle situations.
Lorsque dans la simulation intervient un élément aléatoire, on parle de simulation aléatoire.
Les exemples d'application sont très variés, citons par exemple :
– la simulation de files d'attente, de réseaux,
– la simulation de portefeuilles d'actifs en finance,
– la comparaison d'estimateurs en statistique,
– la recherche d'état stationnaire en physique, en économie.
Remarquons de plus que si l'on cherche une représentation fidèle des phénomènes observés, on est rapidement confronté à des difficultés dues aux *calculs non explicites*. Les techniques de simulation vont nous permettre d'approcher numériquement ces calculs. Nous allons développer ici *les méthodes de Monte-Carlo* qui ont pour essence l'utilisation d'expériences répétées pour évaluer une quantité, résoudre un système déterministe. Ces méthodes peuvent servir pour :
– le calcul d'intégrale,
– la résolution d'équations aux dérivées partielles,
– la résolution de système linéaire,
– la résolution de problèmes d'optimisation (algorithme du recuit simulé).

2. Méthodes de Monte-Carlo et Chaînes de Markov

Nous avons mis en évidence un certain nombre de méthodes pour simuler un variables aléatoire de loi π donnée. Mais il y a des cas où la loi π n'est pas facilement explicitable. On rencontre ce problème par exemple pour les lois d'équilibres de systèmes infinis de particules, l'espace d'état étant un espace fini de cardinal important. La méthode de rejet peut aussi conduire à des simulations lente si la probabilité de rejet est trop grande. Les méthodes de Monte-Carlo par chaîne de Markov vont permettre de pallier à ces problèmes.

L'objectif est toujours de calculer $\int f(x)d\pi(x)$ où π est une loi donnée. On sait que la loi des grands nombres s'étend aux processus stationnaires ergodiques et donc si $(X_n, n \geq 0)$ est un tel processus, si X_0 a pour loi π et si $f(X_0)$ est intégrale, alors :

$$\lim_{n\to+\infty} \frac{f(X_0) + \cdots + f(X_n)}{n} = E\left(f(X_0)\right) = \int f(x)\,d\pi(x) \text{ presque sûrement.} \qquad (3.1)$$

Mais comme on ne sait pas simuler X_0 selon la loi π, on n'a guère avancé.

Considérons cependant l'exemple d'un processus AR(1) :

$$X_n = aX_{n-1} + U_n \text{ avec } U_n \text{ i.i.d. et } |a| < 1. \qquad (3.2)$$

La solution stationnaire X_n de cette équation s'écrit $\sum_{p=0}^{+\infty} a^p U_{n-p}$ et est ergodique.

Soit maintenant X_n^x la solution de 3.2 satisfaisant $X_0 = x$. Il est facile de montrer par récurrence que :

$$X_n^x - X_n^y = a^n(x - y),$$

et donc les trajectoires se rapprochent et oublient leur point de départ. De même $X_n^x - X_n = a^n(x - X_0)$ tend vers 0 quand n tends vers $+\infty$. Par suite, si f est uniformément continue :

$$\lim_{n\to+\infty} f(X_n^x) - f\left(X_n\right) = 0 \text{ p.s.}$$

et donc la moyenne de Césaro aussi :

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{i=1}^{n} f(X_i^x) - f\left(X_i\right) = 0 \text{ p.s..}$$

On en déduit donc que pour tout point de départ x :

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{i=1}^{n} f(X_i^x) = E\left(f(X_0)\right) \text{ p.s..}$$

La chaîne de Markov X_n^x d'état initial x est facile à simuler et conduit à une approximation de $\mathbf{E}\left(f(X_0)\right)$. Cet exemple très simple donne l'idée d'une démarche générale. Soit π une loi donnée, on va chercher à construire une chaîne de Markov qui sera stationnaire et ergodique si la loi initiale est π et dont les trajectoires, pour tout état initial x, auront un comportement asymptotique analogue aux trajectoires de la solution stationnaire. En d'autres termes, pour tout x, les trajectoires issues de x, vérifieront la loi forte des grands nombres :

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{i=1}^{n} f\left(X_i^x\right) = \int f(x)d\pi(x),$$

que l'on cherche à évaluer. Il faudra ensuite étudier la vitesse de convergence.

3.1 Chaîne de Markov et ergodicité

Les notations sont celles du cours de première année. On rappelle que $(X_n, n \geq 0)$ est une chaîne de Markov si la loi de l'état X_{n+1} ne dépend des valeurs passées $(X_0, \ldots, X_n)$ que par X_n.

On suppose l'espace d'états E discret et l'on considère sur E une matrice de transition $Q = (Q(x,y); x, y \in E)$. Cela signifie que Q est telle que :

- $Q(x,y) \geq 0$ pour tout $(x,y) \in E^2$,
- $\sum_{y\in E} Q(x,y) = 1$, pour tout $x \in E$.

Une suite $(X_n, n \geq 0)$ de variables aléatoires à valeurs dans E est appelée une *chaîne de Markov de matrice de transition* Q si, pour tout $x_1, \cdots, x_n \in E$:

$$\begin{aligned}\mathbf{P}\left(X_{n+1} = x | X_0 = x_0, X_1 = x_1, \ldots, \ldots, X_n = x_n\right) &= \mathbf{P}\left(X_{n+1} = x | X_n = x_n\right)\\ &= Q(x_n, x).\end{aligned}$$

Il est alors facile de voir que :

- $\mathbf{P}(X_0 = x_0, X_1 = x_1, \ldots, \ldots, X_n = x_n) = \pi_0(x_0)Q(x_0,x_1)\ldots Q(x_{n-1}, X_n)$,
- $\mathbf{P}(X_n = x_n)\sum_{x_0\in E} \pi_0(x_0)Q^n(x_0,x_n) = (\pi_0 Q^n)(x_n)$, où Q^n est définie au sens de la multiplication des matrices.

Par suite, si la loi initiale de la chaîne de Markov est π_0, la loi de X_n est $\pi_0 Q^n$.

On dira que la probabilité π_0 est invariante pour Q si :

$$\pi_0 Q = \pi_0. \tag{3.3}$$

Proposition 3.1.1 *Soit π un probabilité sur un espace E discret et soit $\bar{X}_n$ la chaîne de Markov de matrice de transition Q et de loi initiale π. Alors, il y a équivalence entre :*

1. *π est un loi invariante pour Q,*
2. *la chaîne $(\bar{X}_n, n \geq 0)$ est un processus stationnaire au sens strict.*

Démonstration : La fait que 2 implique 1 est clair, puisque a loi de $\bar{X}_1$ (égale à πQ) est identique à celle de X_0 (égale à π).

Pour démontrer que 1) implique 2), notons que :

$$\begin{aligned}\mathbf{P}(\bar{X}_1 = x_1, \ldots, \bar{X}_n = x_n) &= \sum_{x_0} \pi(x_0)Q(x_0,x_1)Q(x_1,x_2)\ldots Q(x_{n-1},x_n)\\ &= (\pi Q)(x_1)Q(x_1,x_2)\ldots Q(x_{n-1},x_n)\\ &= \pi(x_1)Q(x_1,x_2)\ldots Q(x_{n-1},x_n)\\ &= \mathbf{P}(X_0 = x_1, \ldots, X_{n-1} = x_n).\end{aligned}$$

Ceci prouve que les lois de $(\bar{X}_1, \ldots, \bar{X}_n)$ et de $(\bar{X}_0, \ldots, \bar{X}_{n-1})$ sont identiques. Le processus $(X_n, n \geq 0)$ est donc stationnaire au sens strict. ∎

On va supposer dorénavant que la chaîne de Markov que l'on considère admet une probabilité invariante π. Pour que les trajectoires issues des divers points aient des comportements analogues, il faut imposer à la matrice de transition Q d'être *irréductible*, c'est à dire que :

- pour tout $x \in E$ et pour tout $y \in E$ il existe un entier $n > 1$ tel que :

$$\mathbf{P}(\bar{X}_0 = x, \bar{X}_n = y) = Q^n(x, y) > 0.$$

Ceci signifie que l'on peut aller (avec un probabilité strictement positive) de tout point de E à tout point de E en un nombre fini de coups.

On sait alors (voir cours de probabilité de première année) que :

- *soit* tous les états sont réccurents,
- *soit* tous les états sont transients.

Théorème 3.1.1 *Supposons que Q est irréductible et qu'il existe une probabilité π telle que $\pi Q = \pi$. Alors :*

1. *π est l'unique probabilité invariante,*
2. *tous les états sont réccurents,*
3. *si $(\bar{X}_n, n \geq 0)$ désigne la chaîne de Markov stationnaire au sens strict de loi initiale π, alors, pour toute fonction f telle que $\int |f(x)| d\pi(x) < +\infty$:*

$$\lim_{n \to +\infty} \frac{1}{n} \sum_{p=1}^{n} f\left(\bar{X}_p\right) = \int f(x) d\pi(x) \text{ p.s..}$$

4. *Pour tout point $x \in E$, si l'on note $(\bar{X}_n^x, n \geq 0)$ une chaîne de Markov d'état initial x :*

$$\lim_{n \to +\infty} \frac{1}{n} \sum_{p=1}^{n} f\left(\bar{X}_p^x\right) = \int f(x) d\pi(x) \text{ p.s..}$$

Conséquence : Si l'on sait construire une chaîne de Markov de matrice de transition irréductible et ayant π comme probabilité invariante, on pourra approximer $\int f d\pi$ par $\frac{1}{n} \sum_{p=1}^{n} f\left(X_p^x\right)$. Le problème du calcul de l'intégrale se ramène à celui de la simulation de la chaîne $(X_n^x, n \geq 0)$.

Remarque 3.1.2 Si π est une probabilité telle que, pour tout x, y :

$$\pi(x) Q(x, y) = \pi(y) Q(y, x),$$

on dit que la probabilité est une *probabilité symétrique*. Notez qu'une probabilité symétrique est forcément invariante puisque :

$$(\pi Q)(y) = \sum_{x \in E} \pi(x) Q(x, y) = \sum_{x \in E} \pi(y) Q(y, x) = \pi(y) \sum_{x \in E} Q(y, x) = \pi(y).$$

On dit alors que la chaîne est *réversible* car la loi de X_n sachant $\{X_{n-1} = x\}$ est égale à la loi de X_n sachant $\{X_{n+1} = x\}$.

Démonstration : Commençons par montrer que si Q est irréductible et si π est une probabilité invariante, alors, pour tout $x \in E$, $\pi(x) > 0$.

Pour cela remarquons que comme π est une probabilité, il existe un point y de E tel que $\pi(y) > 0$. Considérons maintenant un point arbitraire x de E. Comme Q est irréductible, il existe un $n > 1$ tel que $Q^n(y, x) > 0$. On a donc :

$$\pi(x) = \pi Q^n(x) = \sum_z \pi(z) Q^n(z, x) \geq \pi(y) Q^n(y, x) > 0.$$

Montrons maintenant que π est l'unique probabilité invariante. Soit π' une autre probabilité invariante. Alors $\pi''(x) = \min(\pi(x), \pi'(x))$ définit une mesure positive telle que :

$$\pi'' Q \leq \pi Q = \pi.$$

De même $\pi'' Q \leq \pi'$ et donc $\pi'' Q \leq \pi''$. Comme de plus, $\sum_{x \in E} \pi'' Q(x) = 1 = \sum_{x \in E} \pi''(x)$, on en déduit que $\pi'' Q = \pi''$.

Par suite $\Delta = \pi - \pi''$ est une mesure positive de masse totale finie telle que $\Delta Q = \Delta$. On peut alors déduire de la première partie de la démonstration que cette mesure est soit partout nulle, soit partout strictement positive. Ce qui prouve dans le premier cas que $\pi \leq \pi'$ et dans le second cas que $\pi' \leq \pi$. Dans les deux cas comme $\sum_{x \in E} \pi(x) = 1 = \sum_{x \in E} \pi'(x)$, ceci implique que $\pi = \pi'$. Ce qui prouve l'unicité de la probabilité invariante.

Montrons maintenant que tout les états sont récurrents. Commencions par supposer tout les états transients, alors, pour tout x et y on a :

$$\sum_{n \geq 0} \mathbf{1}_{\{X_n^x = y\}} < +\infty \text{ p.s.},$$

donc $\lim_{n \to +\infty} \mathbf{1}_{\{X_n^x = y\}} = 0$ p.s.. Et on en déduit, en utilisant le théorème de Lebesgue (puisque $\mathbf{1}_{\{X_n^x = y\}} \leq 1$), que :

$$\lim_{n \to +\infty} Q^n(x, y) = \lim_{n \to +\infty} \mathbf{E}\left(\mathbf{1}_{\{X_n^x = y\}}\right) = 0.$$

En utilisant encore une fois le théorème de Lebesgue, on montre que si π est la probabilité invariante, alors :

$$\lim_{n \to +\infty} \sum_{x \in E} \pi(x) Q^n(x, y) = 0.$$

Or, comme π est invariante $\pi(y) = \sum_{x \in E} \pi(x) Q^n(x, y)$ et l'on a vu que $\pi(y) > 0$ pour tout état y, ceci entraîne une contradiction. La chaîne étant irréductible tout les état sont donc récurrents.

On peut donc, utiliser le théorème ergodique du cours de première année pour montrer que, pour tout x et y :

$$\lim_{n \to +\infty} \frac{1}{n} \sum_{p=1}^{n} \mathbf{1}_{\left\{\bar{X}_p^x = y\right\}} = \mu(y) \text{ p.s.},$$

La limite $\mu(y)$ ne dépend pas du point de départ x et μ est soit nulle, soit une probabilité satisfaisant $\mu Q = \mu$.

Montrons que μ ne peut pas être nulle. Pour cela supposons que $\mu = 0$. Alors en appliquant le théorème de Lebesgue à $\frac{1}{n} \sum_{p=1}^{n} \mathbf{1}_{\left\{\bar{X}_p^x = y\right\}}$, qui reste clairement borné par 1, on obtient :

$$\lim_{n \to +\infty} \frac{1}{n} \sum_{p=1}^{n} Q^p(x, y) = \lim_{n \to +\infty} \mathbf{E}\left[\frac{1}{n} \sum_{p=1}^{n} \mathbf{1}_{\left\{\bar{X}_p^x = y\right\}}\right] = 0.$$

Soit π le probabilité invariante. Toujours en utilisant le théorème de Lebesgue, on obtient :

$$\lim_{n\to+\infty} \sum_x \pi(x) \left[\frac{1}{n}\sum_{p=1}^{n} Q^p(x,y)\right] = 0.$$

Donc comme, $\pi Q^p = \pi$:

$$\sum_x \pi(x) \left[\frac{1}{n}\sum_{p=1}^{n} Q^p(x,y)\right] = \frac{1}{n}\sum_{p=1}^{n} \pi Q^p(y) = \pi(y).$$

Ceci entraine une contradiction puisque $\pi(y) > 0$. μ est donc une probabilité et est donc égale à π, puisque nous avons vu qu'il existe une unique probabilité invariante.

Le résultat annoncé dans le lemme est prouvé pour $f = \mathbf{1}_{\{y\}}$. Il est relativement facile de l'étendre à f borné. L'extension au cas $\int |f(x)|\pi(dx) < +\infty$ est nettement plus technique aussi nous l'admettrons.

Si f est bornée par M, alors $g = f - M \geq 0$.

Soit $(g_k, k \geq 1)$ une suite de fonction à support fini telle que les g_k tendent en croissant vers g. Alors, d'après le résultat obtenu, on a, pour tout k :

$$\lim_{n\to+\infty} \frac{1}{n}\sum_{p=1}^{n} g_k\left(\bar{X}_p^x\right) = \sum_y g_k(y)\pi(y).$$

On en déduit donc que, pour tout k :

$$\liminf_{n+\infty} \frac{1}{n}\sum_{p=1}^{n} g\left(\bar{X}_p^x\right) \geq \sum_y g_k(y)\pi(y),$$

d'où, par passage à la limite :

$$\liminf_{n+\infty} \frac{1}{n}\sum_{p=1}^{n} g\left(\bar{X}_p^x\right) \geq \sum_y g(y)\pi(y),$$

Par linéarité on obtient alors :

$$\liminf_{n+\infty} \frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right) \geq \sum_y f(y)\pi(y).$$

Le même raisonnement, en utilisant la fonction $-f$ prouve que :

$$\limsup_{n+\infty} \frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right) \leq \sum_y f(y)\pi(y).$$

D'où le résultat annoncé pour une fonction borné f.

Pour montrer le résultat, lorsque la chaîne $(X_n, n \geq 0)$ part d'une probabilité arbitraire ν, il suffit de remarquer que :

$$\mathbf{P}\left[\frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p\right)\right] = \sum_{x\in E} \mathbf{P}\left(X_0 = x\right) \mathbf{P}\left[\frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right)\right].$$

Comme, pour tout x :

$$\mathbf{P}(X_0 = x)\,\mathbf{P}\left[\frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right)\right] = 1,$$

et comme $\sum_{x\in E}\mathbf{P}(X_0 = x) = 1$. Le résultat reste vrai pour toute loi initiale ν et en particulier pour π. ∎

Pour étudier la vitesse de convergence de $\frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right)$, nous allons imposer à la chaîne d'être apériodique.

Définition 3.1.3 Soit Q une matrice de transition. On note :

$$d(x) = \mathrm{PGCD}\{n, Q^n(x,x) > 0\}.$$

On dit que x est apériodique si $d(x) = 1$.

Si Q est irréductible et si un état est apériodique, tous les états sont alors apériodiques et l'on dit que la chaîne est apériodique.

Nous admettrons le théorème suivant.

Théorème 3.1.2 *Supposons que l'espace d'états* E *soit fini et soit* Q *une matrice de transition irréductible apériodique admettant une probabilité invariante* π.

1. *Il existe deux réels* α, M *avec* $\alpha < 1$ *et* $M < +\infty$ *tel que, pour tout* x *et pour tout* y *:*

$$|Q^n(x,y) - \pi(y)| < M\alpha^n.$$

2. *Pour tout* x *et pour toute fonction* f *définie sur* E *:*

$$\sqrt{n}\left(\frac{1}{n}\sum_{p=1}^{n} f\left(\bar{X}_p^x\right) - \sum_{y\in E}\pi(y)f(y)\right)$$ *converge en loi vers une gaussienne centrée de variance* $\bar{\sigma}^2$,

avec $\bar{\sigma}^2 < +\infty$.

Remarque 3.1.4 En pratique, la variance $\bar{\sigma}^2 < +\infty$ est beaucoup plus délicate à estimer que pour le théorème de la limite centrale classique.

Exercice 13 Soit E un espace d'états dénombrable (on peut aussi se placer dans un espace d'états abstrait au prix d'une extension de la notion de chaîne de Markov) et p et q des densités de probabilité , avec $0 < p \leq cq$, q étant une densité facilement simulable. On considère alors une suite Y_n, $n \geq 1$ de variables aléatoires indépendantes identiquement distribuées selon la loi q et indépendantes de la variable aléatoire X_0. On définit par récurrence :

$$X_{n+1} = \begin{cases} Y_{n+1} \text{ avec probabilité } \dfrac{p(Y_{n+1})}{cq(Y_{n+1})} \\ X_n \text{ avec probabilité } 1 - \dfrac{p(Y_{n+1})}{cq(Y_{n+1})} \end{cases}$$

1. En considérant une suite U_n de variables aléatoires indépendantes identiquement distribuées selon la loi uniforme sur $[0, 1]$ écrire X_{n+1} sous la forme $f(X_n, U_{n+1}, Y_{n+1})$ et en déduire que X_n est une chaîne de Markov.
2. Calculer la probabilité de transition $P(i, j)$ de X_n.
3. Calculer μP pour une probabilité μ et en déduire que la loi de X_n converge vers une unique probabilité invariante égale à p.
4. Quel rapport y-a-t-il entre cette chaîne et la méthode de rejet classique ?

Exercice 14 Soit $P(x, y)$ un noyau de transition d'une chaîne de Markov sur un espace d'état fini E. On suppose que :

$$P(x, y) \geq \alpha c(y), \text{ pour tout } y \in E, \tag{3.4}$$

où c est une mesure de probabilité et $\alpha > 0$.

1. Soit μ et μ' deux mesures de probabilité sur E. On note $|\mu - \mu'| = \sum_{x \in E} |\mu(x) - \mu'(x)|$. Montrer que l'on a :
$$|\mu P - \mu' P| \leq (1 - \alpha) |\mu - \mu'|.$$
2. Montrer que s'il existe une mesure de probabilité invariante, elle est forcément unique.
3. Soit $(X_n, n \geq 0)$ une chaîne de Markov de matrice de transition P. Montrer que quelle que soit la loi initiale de X_0, la loi de X_n converge vers une unique loi de probabilité invariante.
4. Montrer que les résultats précédents sont conservés si, il existe $l \geq 1$:
$$P^l(x, y) \geq \alpha c(y), \text{ pour tout } y \in E. \tag{3.5}$$
5. On considère maintenant l'algorithme de Métropolis. On suppose que $P(x, y) = P(y, x)$ et que l'équation (3.4) est vérifiée. On cherche à simuler une loi μ donnée à une constante près par :
$$\mu(x) = Ce^{-\beta H(x)}.$$
Écrire la probabilité de transition $\tilde{P}(x, y)$ sur E qui permet de construire l'algorithme de Métropolis.

Bibliographie :

Elie, Laura, Introduction aux Méthodes de Monte-Carlo, Septembre 2001

ANNEXE 5

Réseaux de Petri

1 Introduction

Cahier des charges ➔ Spécification formelle ➔Conception

Critique des modèles d'états

Souhaits :

Critique des modèles HDL

Simplicité

Expression du parallélisme

Analyse formelle

2 Définition d'un Réseau de Petri

2.1 Définition

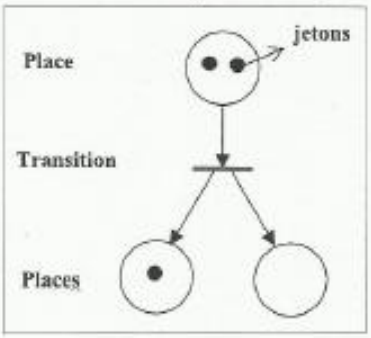
Quintuple : **R = (T, P, A, M_0)**

T : ensemble de **transitions** T = {t1, t2, …, tl}

P : ensemble de **places** P = {p1, p2, …, pm}

A : ensemble d'**arcs** A = {a1, a2, … , an} $A \subseteq \{PxT\} \cup \{TxP\}$

M_0 : marquage initial : {m(pi)} (entier ≥ 0 = nombre de **jetons** dans place.pi.)

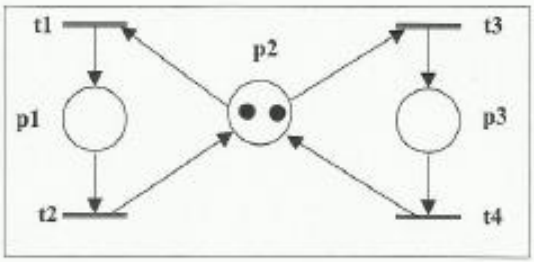


Expression du parallélisme :

évolution des *jetons* entre certaines *places* lors de tirs de *transitions*.

2.2 Exemple

T = {t1, t2, t3, t4}
P = {p1, p2, p3}
Arcs = {(p2, t1), (t1, p1), (p1, t2), (t2, p2), (p2, t3), (t3, p3), (p3, t4), (t4, p2)}
M_0 = [0 2 0]
1 2 3



Matrices de connexion :

arc p2 → t1

	t1	t2	t3	t4
p1	0	1	0	0
p2	1	0	1	0
p3	0	0	0	1

PRE

	t1	t2	t3	t4
p1	1	0	0	0
p2	0	1	0	1
p3	0	0	1	0

POST

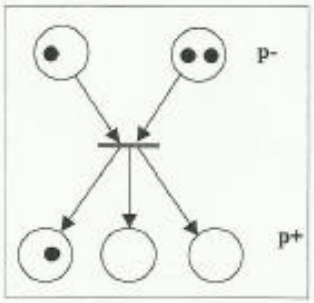
arc t4 → p2

2.3 Animation du graphe

Sensibilisation d'une transition

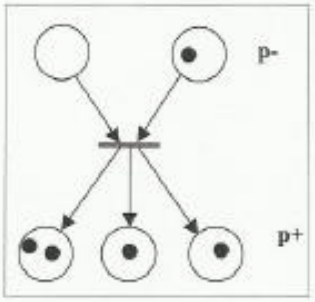
Une transition est sensibilisée ssi toute place prédécesseur contient au moins un jeton.

$\forall p \in P \quad M(p) \geq PRE(p,t)$



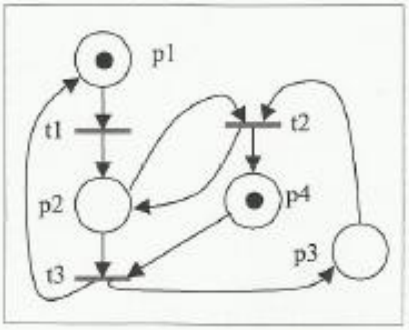
Tir d'une transition

On enlève 1 jeton de chaque place 'amont' et on ajoute 1 jeton à chaque place 'aval'.



Il n'y a pas conservation a priori du nombre de jetons dans le graphe

Graphe des marquages



Marquages successifs :

M0 1 0 0 1

M1 0 1 0 1

M2 1 0 1 0

M3 0 1 1 0

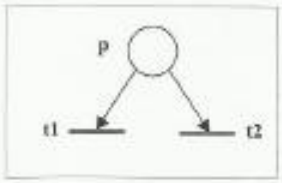
M1 : le graphe contient une boucle

3 Propriétés

3.1 Conflits et parallélisme

Structure potentiellement conflictuelle

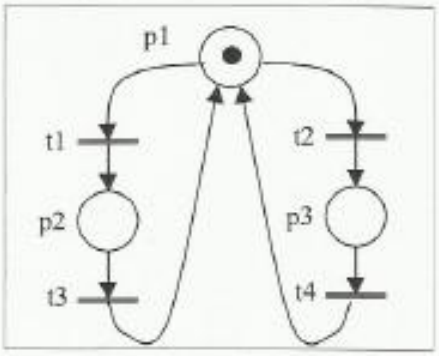
$t1$ et $t2$ sont en conflit structurel potentiel pour le partage des jetons de la place p.



Conflit relatif au marquage

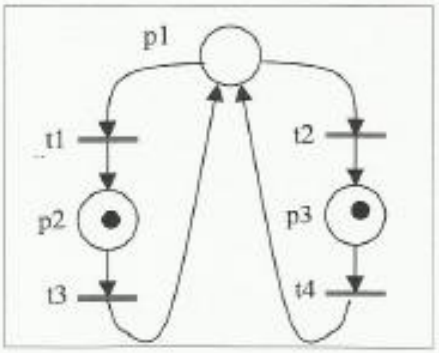
Structure potentiellement conflictuelle + marquage insuffisant

$t1$ et $t2$ en conflit pour le partage du jeton : non déterminisme du tir ($t1$ ou $t2$)



Parallélisme :

$t1$ et $t2$ sont tirées en parallèle



3.2 Réseau propre (réinitialisable)

SSI ∀marquage M_i accessible depuis M_0, ∃ une séquence de tirs conduisant à M_0.

3.3 Réseau vivant (sans blocage)

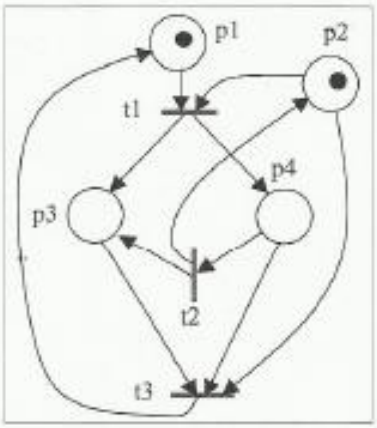
M0 → Mk

∀ ti ∃ séquence de tirs passant par ti

M0 = 1 1 0 0

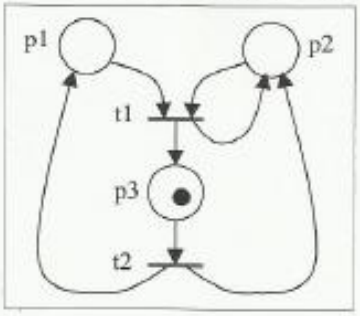
M1 = 0 0 1 1

M2 = 0 1 2 0 → blocage !



3.4 Réseau borné

Si ∀marquage M_i accessible depuis M_0, et $\forall\, p_j \in P \rightarrow M_i(p_j) \leq MAX$.



Marquages successifs :

M0 0 0 1
M1 1 1 0
M2 0 1 1
M4 1 2 0
M5 1 2 1
M6 1 3 1 … croissance infinie

Si MAX = 1 → **Réseau de Petri Sauf**

3.5 Réseau conforme

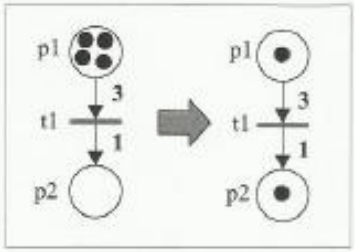
Réseau de Petri **vivant** et **sauf** : 1 jeton, sans blocage

3.6 Machine à états finie

Chaque transition n'a qu'une place amont et une place aval.

4 Extensions des réseaux de Petri

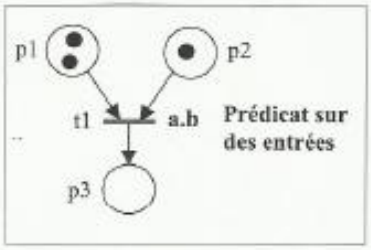
4.1 Réseaux de Petri à arcs étiquetés



4.2 Réseau de Petri interprété

Tir de la transition si :

1) transition sensibilisée
2) prédicat vrai (ab' = 1)



Bibliographie :

ANNEXE 6

Définitions et Commentaires

Acceptable, Terme anglais : "Acceptable"
Qualifie un événement jugé acceptable au regard d'objectifs de sûreté de fonctionnement.

Accident, Terme anglais : "Accident"
Evénement ayant des conséquences catastrophiques ou susceptible d'en avoir. Dans le nucléaire, l'accident est défini comme l'événement pouvant entraîner l'endommagement d'une ou plusieurs barrières et donc conduire à un relâchement de produits radioactifs et demandant la mise en service de systèmes de protection.

Amélioration de la sûreté de fonctionnement, Terme anglais : "Dependability Improvement"
Procédé intentionnellement destiné à produire une croissance d'une caractéristique de la sûreté de fonctionnement disponibilité, fiabilité, maintenabilité, sécurité, etc.) en vue d'atteindre des objectifs spécifiés par élimination de défaillance ou réduction de leur probabilité d'occurrence.

Analyse qualitative Terme anglais : Qualitative analysis :
L'analyse qualitative d'un système (ou analyse fonctionnelle) est l'étude systématique la plus complète possible des défaillance éventuelles de ce système et de leurs conséquences sur ses missions, dans toutes les configurations de fonctionnement envisageables (exemple : AMDE, arbre de défaillances)

Analyse quantitative Terme anglais : Quantitative analysis :
L'analyse quantitative consiste à calculer une probabilité (munie d'un intervalle de confiance) pour chaque événement indésirable mis en évidence par l'analyse qualitative; elle peut se compéter par l'évaluation de la contribution des défaillances élémentaires ou de celles de certains sous-systèmes de réalisation de cet événement

Analyse d'un système Terme anglais : "System Analysis"
Processus orienté vers l'acquisition, l'investigation et le traitement ordonnés d'informations spécifiques au système et pertinentes vis-à-vis d'une décision ou d'un objectif donné. Ce processus conduit à l'obtention d'un modèle et, éventuellement, à son évaluation quantitative.

Analyse de criticité de défaillance Terme anglais : "Criticality Analysis":
Analyse ayant pour objet d'évaluer le couple gravité/probabilité associé à une défaillance.

Analyse des modes de défaillance et de leurs effets (AMDE) Terme anglais : "Failure Modes and Effects Analysis" (FMEA)
Méthode d'analyse quantitative d'un système ayant pour objet d'identifier les modes de défaillance des composants du système, leurs causes et leurs effets.

Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) Terme anglais : "Failure Modes, Effects and Criticality: Méthode d'analyse d'un système qui comprend une analyse des modes de défaillance et de leurs effets, complétée par une analyse de criticité des modes de défaillance.

Analysis" (FMECA) Analyse préliminaire des risques Terme anglais : "Preliminary Hazard Analysis (PHA)" ; "Preliminary Risks Analysis"
Analyse ayant pour objet d'identifier et d'évaluer des risques (économiques, humains...) liés à l'utilisation d'un système, et ce de manière préliminaire à l'utilisation de méthodes d'analyse plus précises.

Arbre de défaillances Terme anglais : Fault tree :
C'est une méthode déductive qui consiste, en partant d'un événement unique et bien défini, à représenter graphiquement les combinaisons d'événements qui conduisent à sa réalisation. L'arbre des défauts sera formé de niveaux successifs tels que chaque événement soit généré à partir des événements du niveau inférieur par l'intermédiaire d'opérateurs logiques (portes logiques Et, Ou). Le processus déductif est poursuivi jusqu'à ce qu'on aboutisse à des événements élémentaires en général indépendants, pour lesquels on possède des données numériques statistiques (taux de défaillance).

A sûreté intégrée : Terme anglais : "Fail safe"
Qualifie une entité qui est conçue en vue d'éviter que ses défaillances n'entraînent des conséquences critiques ou catastrophiques. On parle aussi de "sécurité intrinsèque".

Composant Terme anglais : "Component"
C'est la plus petite partie d'un système qu'il est nécessaire et suffisant de considérer pour l'analyse d'un système.

Composant actif Terme anglais : "Active component"
Composant qui comporte des pièces mobiles dont la position est modifiée ou qui nécessite pour remplir sa fonction une variation de sa configuration ou de ses propriétés à l'aide d'une source d'énergie extérieure.

Composant critique Terme anglais : "Critical component"
Composant dont la défaillance, dans un état de fonctionnement donné d'un système, entraîne la défaillance de ce système.

Composant passif Terme anglais : "Passive component"
Composant n'entrant pas dans la définition des composants actifs et qui n'est soumis, par exemple, qu'à des variations de pression, de température, de débit de fluide ou de courant électrique lorsqu'il remplit sa fonction. Cette définition est utilisée dans le nucléaire.

Courbe en baignoire Terme anglais : Bath tub curve :
La variation de taux de défaillance d'un composant en fonction du temps, présente l'allure d'une baignoire

Danger Terme anglais : "Hazard" ; "Danger"
Situation pouvant nuire à l'homme, à la société ou à l'environnement.

Défaillance Terme anglais : "Failure"
Cessation de l'aptitude d'une entité à accomplir une fonction requise.

Défaillance à taux constant Terme anglais : "Random Failure"
Défaillance qui apparaît avec un taux sensiblement constant pendant la durée de vie utile de l'entité. Cette défaillance est généralement catalectique. Elle est encore appelée "défaillance aléatoire".

Défaillance catalectique Terme anglais : "Catastrophic Failure"
Défaillance qui est à la fois soudaine et complète.

Défaillance complète Terme anglais : "Complete Failure"
Défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, telle qu'elle entraîne une disparition complète de la fonction requise.

Défaillance de commande Terme anglais : "Command Failure"
Défaillance d'une entité dont la cause directe ou indirecte est la défaillance d'une autre entité et pour laquelle cette entité a été qualifiée et dimensionnée.

Défaillance d'usure Terme anglais : "Wearout Failure"
Défaillance qui apparaît avec un taux rapidement croissant par suite de processus inhérents à l'entité.

Défaillance non pertinente Terme anglais : "Non-relevant Failure"
Défaillance à exclure pour l'interprétation ou l'évaluation d'une mesure de la sûreté de fonctionnement. On parle aussi de "défaillance à ne pas prendre en compte".

Défaillance par dégradation Terme anglais : "Degradation Failure"
Défaillance qui est à la fois progressive et partielle. A la longue, une telle défaillance peut devenir une défaillance complète

Défaillance partielle Terme anglais : "Partial Failure"
Défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, mais telle qu'elle n'entraîne pas une disparition complète de la fonction requise. Les limites sont des limites spéciales spécifiées à cette fin .

Défaillance pertinente Terme anglais : "Relevant Failure"
Défaillance à prendre en compte pour interpréter ou évaluer une mesure de la sûreté de fonctionnement. On parle aussi de "défaillance à prendre en compte".

Défaillance progressive Terme anglais : "Gradual Failure" ; "Drift Failure"
Défaillance due à une évolution dans le temps des caractéristiques d'une entité. En général, une défaillance progressive peut être prévue par un examen ou une surveillance antérieur.

Défaillance de cause commune Terme anglais : "Common cause Failures"
Défaillances dépendantes ayant pour origine la même cause directe.

Défaillance de mode commun Terme anglais : "Commun mode Failures"
Défaillances de cause commune se manifestant par le même mode de défaillance des entités.

Défaut Terme anglais : "Defect"
Ecart entre une caractéristique d'une entité et la caractéristique voulue, cet écart dépassant les limites d'acceptabilité.

Démarche déductive Terme anglais : "Deductive approach"
Démarche dans laquelle on raisonne du plus général au plus particulier.

Démarche inductive Terme anglais : "Inductive approach"
Démarche dans laquelle on raisonne du plus particulier au plus général.

Densité de défaillance Terme anglais : "Failure density"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T de la première défaillance d'une entité soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité est en fonctionnement au temps t=0. Elle est notée U(t).

Densité de probabilité Terme anglais : "Probability density function"
C'est la dérivée, si elle existe, de la fonction de répartition d'une variable aléatoire. Elle est notée f(x).

Densité de réparation Terme anglais : "Repair density"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'achèvement de la réparation d'une entité soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité est défaillante au temps t=0. Elle est notée G(t).

Densité de transition Terme anglais : "Transition density"
C'est la dérivée, si elle existe, de la probabilité de transition.

Disponibilité Terme anglais : "Availability"
Aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné. Le terme de "disponibilité" est aussi employé pour désigner la mesure de la disponibilité.

Disponibilité (mesure de la) Terme anglais : "Availability"
Probabilité pour qu'une entité soit en état d'accomplir une fonction requise dans des conditions données et à un instant donné. Elle est généralement notée A(t) et est aussi dénommée "disponibilité instantanée".

Disponibilité asymptotique Terme anglais : "Steady-state availability" ; "Asymptotic availbility"
C'est la limite, si elle existe, de la disponibilité instantanée représentée par un modèle mathématique, quand on fait tendre le temps vers l'infini. Elle est notée $A(\infty)$.

Disponibilité moyenne Terme anglais : "Up time"
C'est la moyenne de la disponibilité instantanée sur un intervalle de temps donné [t1;t2]. Elle est notée Am (t1,t2). Terme anglais : "Mean availability" Durée de disponibilité : Période pendant laquelle une entité est en état d'accomplir sa fonction requise.

Durée de fonctionnement Terme anglais : "Operating time"
Période pendant laquelle une entité accomplit sa fonction requise.

Durée de vie utile Terme anglais : "Useful life"
Période commençant à un instant donné, pendant laquelle, dans des conditions données, une entité a un taux de défaillance acceptable, ou période précédant l'apparition d'une défaillance non réparable.

Durée d'indisponibilité Terme anglais : "Down time"
Période pendant laquelle une entité n'est pas en état d'accomplir sa fonction requise.

Entité Terme anglais : "Entity" ; "Item"
Tout élément, composant, sous-système, dispositif, équipement, unité fonctionnelle que l'on peut considérer individuellement.

Etat d'attente Terme anglais : "Standby state"
Etat d'une entité disponible et en état de non-fonctionnement pendant une période requise.

Etat de disponibilité Terme anglais : "Availability state"
Etat d'une entité caractérisée par son aptitude à accomplir une fonction requise.

Etat de fonctionnement Terme anglais : "Fault state"
Etat d'une entité dans lequel cette entité accomplit correctement une fonction requise.

Etat de panne Terme anglais : "Operating state"
Etat d'une entité caractérisée par une inaptitude à accomplir une fonction requise.

Evénement initiateur Terme anglais : Initiating event

C'est l'événement de tête d'un arbre d'événements. C'est généralement une défaillance qui déclenche l'action de systèmes de sécurité ou de sauvegarde (cela peut être la défaillance d'un système, une erreur humaine, le dépassement d'un seuil physique, etc.).

Evénement catastrophique Terme anglais : "Catastrophic event"
Evénement qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) d'un système en causant des dommages importants au dit système ou à son environnement et/ou entraîne pour l'homme la mort ou des dommages corporels.

Evénement critique Terme anglais : "Critical event"
Evénement qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) d'un système en causant des dommages importants au dit système ou à son environnement en ne présentant toutefois qu'un risque négligeable de mort ou de blessure.

Evénement Terme anglais : Event :
Dans les études de systèmes ou d'ensembles, l'événement peut être d'origine :
-Interne au système (panne d'un de ses éléments, déclenchement d'un signal, manipulation d'un opérateur…) ;
-Externe au système (séisme, panne du réseau électrique…) .

Evénement indésirable Terme anglais : "Undesirable event"
Evénement (de la vie d'une entité) ne devant pas se produire ou devant se produire avec une probabilité moins élevée au regard d'objectifs de sûreté de fonctionnement.

Evénement majeur Terme anglais : "Major event"
Evénement critique ou significatif.

Fiabilité Terme anglais : "Reliability"
-Aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant une durée donnée.
-Au sens commun, la notion de fiabilité correspond à la confiance de l'usager dans l'appareil qu'il utilise.
- La définition adoptée par les spécialistes s'énonce : caractéristique d'un dispositif, exprimé par la probabilité qu'il accomplisse une mission donnée, dans des conditions déterminées pendant une durée donnée.

Graphe d'états Terme anglais : "States graph"
Diagramme logique montrant les états de fonctionnement et de pannes d'un système, ainsi que leurs transitions.

Immaintenabilité Terme anglais : "Unmaintainability"
Inaptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits.

Inacceptable Terme anglais : "Unacceptable"
Qualifie un événement jugé inacceptable au regard d'objectifs de sûreté de fonctionnement.

Incident Terme anglais : "Incident"
Evénement ayant des effets ou des conséquences critiques ou susceptible d'en avoir.

Indépendance Terme anglais : Independance
L'hypothèse d'indépendance des défaillances des divers éléments d'un système peut être ainsi formulée : à tout instant, le taux de défaillance d'un quelconque élément du système est indépendant des défaillances passées ou à venir des autres éléments

Indisponibilité Terme anglais : "Unavailability"
Inaptitude d'une entité à accomplir une fonction requise, dans des conditions données et à un instant donné.

Indisponibilité (mesure de l') Terme anglais : "Unavailability" ; "Instantaneous unavailability"
Probabilité qu'une entité ne soit pas en état d'accomplir une fonction requise, dans des conditions données et à un instant donné. Elle est notée A (t). Elle est aussi dénommée "indisponibilité instantanée".

Indisponibilité asymptotique Terme anglais : "Steady-state unavailability" ; "Asymptotic unavailability"
C'est la limite, si elle existe, de l'indisponibilité instantanée représentée par un modèle mathématique, quand on fait tendre le temps vers l'infini. Elle est notée A (∞).

Indisponibilité moyenne Terme anglais : "Mean unavailability"
C'est la moyenne de l'indisponibilité instantanée sur un intervalle de temps donné [t1;t2]. Elle est notée Am (t1, t2).

Insécurité Terme anglais : "Unsafety"
Aptitude d'une entité à faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Maintenabilité Terme anglais : "Maintainability"
Aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise lorsque la maintenance est effectuée dans des conditions données avec des procédures et des moyens prescrits.

Maintenabilité (mesure de la) Terme anglais : "Maintainability"
Pour une entité donnée, probabilité qu'une maintenance accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t sachant que l'entité est défaillante au temps t = 0. Elle est notée M(t).

Maintenance Terme anglais : "Maintenance"
Combinaison de toutes les actions techniques et des actions administratives correspondantes, y compris les opérations de surveillance et de contrôle, destinées à maintenir ou à remettre une entité dans un état lui permettant d'accomplir une fonction requise.

Maintenance corrective Terme anglais : "Corrective maintenance"
Maintenance effectuée après la détection de panne et destinée à remettre une entité dans un état lui permettant d'accomplir une fonction requise.

Maintenance préventive Terme anglais : "Preventive maintenance"
Maintenance effectuée à intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'une entité.

MDT Terme anglais : "Mean down time"
Durée moyenne d'indisponibilité.

Mode de défaillance Terme anglais : "Failure mode"
Effet par lequel une défaillance est observée.

Mode de fonctionnement Terme anglais : "Functional mode"
Effet par lequel un fonctionnement est observé.

MTBF Terme anglais : "Mean time between failure"
Durée moyenne entre deux défaillances consécutives d'une entité réparée.

MTTF Terme anglais : "Mean time to failure" ; "Mean Time To First Failure"
Durée moyenne de fonctionnement d'une entité avant la première défaillance.

MTTR Terme anglais : "Mean time to repair"
Durée moyenne de réparation. Ce terme est parfois utilisé pour désigner la durée moyenne de maintenance corrective.

MUT Terme anglais : "Mean up time"
Durée moyenne de fonctionnement après réparation.

Maintenabilité Terme anglais : Maintenability
C'est le complément à 1 de la probabilité pour que le système ne soit pas réparé sur l'intervalle (0,t) sachant qu'il est défaillant à l'instant t=0

Mode de défaillance Terme anglais : Failure mode
Processus conduisant à la défaillance d'un élément. Il peut y avoir plusieurs processus entraînant la même défaillance d'un composant (exemple : vanne ouverte ou fermée). L'objectif des banques de données est de donner des taux de défaillances d'un composant pour différents modes de défaillance.

MTBF (moyenne des temps de bon fonctionnement) Terme anglais : MTBF (Mean Time Between Failures)
Temps moyen entre deux défaillances d'un système réparable

MTTR Terme anglais : MTTR (Mean Time to Repair)
Durée moyenne des temps de réparation

Panne Terme anglais : "Fault"
Inaptitude d'une entité à accomplir une fonction requise.

Panne intermittente Terme anglais : "Intermittent fault"
Panne d'une entité subsistant pendant une durée limitée après laquelle l'entité redevient apte à accomplir une fonction requise sans avoir été soumise à une opération de maintenance corrective.

Panne latente Terme anglais : "Latent fault"
Panne qui existe, mais qui n'a pas encore été détectée.

Panne permanente Terme anglais : "Permanent fault"
Panne d'une entité qui persiste tant que n'ont pas eu lieu les opérations de maintenance corrective.

Phaseur Terme Anglais : Phasor :
un **phaseur** est une représentation d'une grandeur fonction sinusoïdale du temps dans laquelle la valeur maximale de l'amplitude (**A**), la phase (**θ**) et la pulsation (**ω**) (donc la fréquence) ne dépendent pas du temps.

Probabilité de transition Terme anglais : "Transition probability" ; "Transition distribution"
Probabilité de quitter un état du système dans l'intervalle de temps [0;t] et de passer dans un autre état en une seule transition, sachant que l'on est entré dans le premier état à l'instant t=0.

Processus stochastique Terme anglais : "Random process"
Ensemble de variables aléatoires dépendant du temps, dont les valeurs sont régies par un ensemble donné de lois de probabilité multidimensionnelles qui correspondent à toutes les combinaisons des variables aléatoires. Le terme de "processus aléatoire" est aussi utilisé.

Porte logique Terme anglais : Logic gate
Une porte logique représente la relation logique entre les événements d'entrée et l'événement de sortie de la porte.

Porte ET Porte OU Terme anglais : AND gate OR gate
-L 'événement de sortie d'une porte ET n'est réalisé que si tous les éléments d'entrée le sont ;
-L'événement de sortie d'une porte OU est réalisé dès que l'un ou moins des éléments d'entrée est réalisé.

Qualité Terme anglais : "Quality"
Aptitude d'un produit ou d'un service à satisfaire les besoins des utilisateurs.

Redondance Terme anglais : "Redundancy"
Existence, dans une entité, de plus d'un moyen pour accomplir une fonction requise.

Redondance active Terme anglais : "Active redundancy"
Redondance selon laquelle tous les moyens d'accomplir une fonction requise sont mis en œuvre simultanément (Norme CEI-271-1974).

Redondance passive Terme anglais : "Standby redundancy"
Redondance où les différents moyens d'accomplir une fonction donnée ne sont pas mis en œuvre avant que ce ne soit nécessaire (Norme CEI-271-194).

Réparation Terme anglais : "Repair"
Partie de la maintenance corrective pendant laquelle des opérations sont effectuées sur l'entité.

Risque Terme anglais : "Risk"
Mesure du danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences.

Sûreté de fonctionnement Terme anglais : "Dependability"
Aptitude d'une entité à satisfaire à une ou plusieurs fonctions requises dans des conditions données. Ce concept peut englober la fiabilité, la disponibilité, la maintenabilité, la sécurité... ou des combinaisons de ces aptitudes. Au sens large, on considère la sûreté de fonctionnement comme la Science des Défaillances et des Pannes.

Sécurité Terme anglais : "Safety"
Aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Système réparable Terme anglais : Repairable system
Un système est dit "réparable" si, une défaillance s'étant produite, la réparation peut intervenir dans un délai suffisamment court pour éviter la détérioration grave ou la perte du système

Système non réparable Terme anglais : Non-repairable system
Dans le cas contraire, le système est dit «non réparable»

Taux de défaillance Terme anglais : "(Instantaneous) Failure rate"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'une défaillance soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, en sachant que l'entité n'a pas eu de défaillance sur $[0;t]$. Ce taux est noté $\Lambda(t)$.

Taux de défaillance asymptotique Terme anglais : "Steady-state failure rate"
C'est la limite, si elle existe, du taux de défaillance représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $\Lambda(\infty)$.

Taux de réparation Terme anglais : "Repair rate (instantaneous)"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'achèvement de la réparation (ou d'une opération de maintenance) d'une entité soit compris dans un intervalle de temps donné $[t;+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité a été en panne sur tout l'intervalle de temps $[0;t]$. Ce taux est noté $M(t)$.

Taux de réparation asymptotique Terme anglais : "Steady-state repair rate"
C'est la limite, si elle existe, du taux de réparation représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $M(\infty)$.

Taux de transition Terme anglais : "Transition rate"
C'est la limite, si elle existe, du quotient de la probabilité de quitter un état du système pour un autre état du système dans l'intervalle de temps $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro.

Tolérance aux fautes Terme anglais : "Fault tolerance"
Propriété d'un système qui le rend capable d'accomplir une fonction requise en présence decertaines défaillances ou pannes de ses composants.

Taux de défaillance Terme anglais : "(Instantaneous) Failure rate"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'une défaillance soit compris dans un intervalle de temps donné $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, en sachant que l'entité n'a pas eu de défaillance sur $[0;t]$. Ce taux est noté $\Lambda(t)$.

Taux de défaillance asymptotique Terme anglais : "Steady-state failure rate"
C'est la limite, si elle existe, du taux de défaillance représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $\Lambda(\infty)$.

Taux de réparation Terme anglais : "Repair rate (instantaneous)"
C'est la limite, si elle existe, du quotient de la probabilité conditionnelle pour que l'instant T d'achèvement de la réparation (ou d'une opération de maintenance) d'une entité soit compris dans un intervalle de temps donné $[t;+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro, sachant que l'entité a été en panne sur tout l'intervalle de temps $[0;t]$. Ce taux est noté $M(t)$.

Taux de réparation asymptotique Terme anglais : "Steady-state repair rate"
C'est la limite, si elle existe, du taux de réparation représenté par un modèle mathématique lorsqu'on fait tendre le temps vers l'infini. Il est noté $M(\infty)$.

Taux de transition Terme anglais : "Transition rate"
C'est la limite, si elle existe, du quotient de la probabilité de quitter un état du système pour un autre état du système dans l'intervalle de temps $[t;t+\Delta t]$, par la durée de l'intervalle de temps, lorsque Δt tend vers zéro.

Tolérance aux fautes Terme anglais : "Fault tolerance"
Propriété d'un système qui le rend capable d'accomplir une fonction requise en présence de certaines défaillances ou pannes de ses composants.

Taux de défaillance Terme anglais : Failure rate
C'est la probabilité conditionnelle par unité de temps qu'un dispositif survie à l'instant t, mesurée entre t et t + dt.
$\lambda(t)dt$ est la probabilité de défaillance du dispositif entre t et t+dt, sachant qu'il fonctionnait à l'instant t.
La fiabilité R(t) et le taux de défaillance □ (t) du dispositif sont liés par les relations :

R(t)=Exp (-□ 0t □ (t)dt et □ (t)dt=dR(t)/R(t)
Lorsque □ est constant, on a : R(t) = Exp (-□ t) : c'est la «loi exponentielle». Il existe d'autres expressions mathématiques de la fiabilité; loi normale, loi log normale, loi de Weibull, etc .

Taux de réparation μ Terme anglais : Repaire rate μ
C'est la probabilité conditionnelle par unité de temps pour qu'une réparation commencée à t=0 se termine entre t et t+dt, sachant que le matériel est resté en panne entre 0 et t