وزارة التعليـم العالـي والبحـث العلمـي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITÉ BADJI MOKHTAR- ANNABA

جامعـــــة باجـــــي مختـــــار -عنابـة

Faculté : Sciences de L'Ingéniorat

Département : Électromécanique

Thèse

Présentée en vue de l'obtention du diplôme de : DOCTORAT LMD

Modélisation des performances fiabilistes des systèmes instrumentés de sécurité

Présentée et soutenue publiquement : Le 12 Avril 2021

Option : Sécurité industrielle

Par :

Hanane OMEIRI

Devant le jury :

Président :	Pr.	Elias HADJADJ AOUEL	U- Badji Mokhtar. Annaba
Rapporteur de thèse :	Pr.	Brahim HAMAIDI	U- Badji Mokhtar. Annaba
Co-rapporteur de thèse :	Pr.	Fares INNAL	U- 20 Août 1955. Skikda
Examinateur :	Pr.	Mohamed KARA	U- Larbi Tébessi. Tébessa
Examinateur :	Pr.	Abdallah KABOUCHE	U- Badji Mokhtar. Annaba

Résumé

Les systèmes instrumentés de sécurité (SIS) constituent une barrière de sécurité nécessaire pour faire face aux risques inhérents aux systèmes et procédés techniques. La fonction assignée aux SIS est la détection des dérives dangereuses du procédé et le déclenchement des actions nécessaires à l'évitement des accidents potentiels. La norme CEI 61508 offre une approche structurée fondée sur l'identification des dangers afin d'établir les exigences de sécurité pour les SIS. Elle vise à concevoir et exploiter les SIS avec un degré de fiabilité conforme à ces exigences. Un SIS peut être amené à fonctionner selon trois modes : faible demande, forte demande et demande continue. Leurs attributs respectifs sont connus sous les noms de « probabilité moyenne de défaillance à la demande (PFD_{avg}) » et de « probabilité de défaillance par heure (*PFH*) ». Notre travail offre une meilleure explication du contenu de la norme CEI 61508. Ceci facilite l'investigation des résultats fournis par la même norme. Nous avons vérifié les formules analytiques relatives à la *PFH* en poussant l'exploration de l'architecture 2oo3 vu son usage très courant. Par la suite, nous avons proposé une formulation originale permettant de comptabiliser la contribution de l'imperfection des tests périodiques. Ceci a été réalisé en utilisant plusieurs outils et méthodes voir l'arbre de défaillances, les graphes de Markov et les réseaux de Petri.

Mots-clés : norme CEI 61508, sécurité fonctionnelle, systèmes instrumentés de sécurité, arbre des défaillances, modèles markoviens, réseaux de Petri.

Abstract

Safety Instrumented Systems (SIS) constitute a necessary safety barrier to face the risks inherent in technical systems and processes. The function assigned to SISs is the detection of dangerous upsets in the process and the initiation of the necessary actions to avoid potential accidents. IEC 61508 provides a structured approach based on hazard identification to establish safety requirements for SIS. It aims at designing and operating the SIS within reliability confidence that meets these requirements. A SIS can be made to operate in three modes: low demand, high demand and continuous demand. Their respective attributes are known as «Average Probability of Failure on Demand (PFD_{avg}) » and «Probability of Failure per Hour (*PFH*) ». Our work offers a better explanation of the content of IEC 61508 standard. This facilitate the investigation of the results provided by the same standard. We have verified the analytical formulas related to the *PFH* by more exploring the 2oo3 architecture given its very common use. Subsequently, we proposed an original formulation allowing the calculation of imperfect tests contribution. This has been achieved using several tools and methods including fault tree, Markov graphs and Petri nets.

Keywords: IEC 61508 standard, functional safety, safety instrumented system, fault tree, markovian models, Petri nets.

ملخص

تشكل أنظمة السلامة المجهزة (SIS) حاجز أمان ضروريًا للتعامل مع المخاطر الكامنة في الأنظمة والعمليات التقنية. تتمثل الوظيفة المنوطة بـ SIS في اكتشاف الانحرافات الخطرة في العملية وبدء الإجراءات اللازمة لتجنب الحوادث المحتملة. يمثل المعيار IEC 61508 نهجًا منظمًا يعتمد على تحديد المخاطر لتحديد متطلبات السلامة لنظام معلومات السلامة. يهدف المعيار إلى تصميم وتشغيل نظام السلامة المجهز (SIS) بدرجة من الموثوقية وفقًا لهذه المتطلبات. يمكن جعل نظام السلامة المجهز (SIS) يعمل بثلاثة أوضاع: انخفاض الطلب, ارتفاع الطلب والطلب المستمر. تُعرف السمات الخاصة بكل منها باسم «متوسط احتمال العطب عند الطلب (PFD_{avg}) » و«احتمال العطب في الساعة (*PFH*) » يقدم عملنا شرحًا أفضل لمحتوى IEC 61508 سيسهل هذا التحقيق في النتائج المقدمة من طرف نفس المعيار. لقد تحققنا من الصيغ التحليلية المتعلقة بـ *PFH* من خلال استكشاف بنية 2oo3 نظرًا لاستخدامها الشائع جدًا. بعد ذلك، اقترحنا صياغة أصلية لحساب مساهمة النقص في الاختبارات الدورية. تم تحقيق ذلك باستخدام العديد من الأدوات والأساليب بما في ذلك شجرة الأعطاب , نماذج ماركوف وشبكات بيتري.

الكلمات المفتاحية: معيار IEC 61508، السلامة الوظيفية، أنظمة السلامة المجهزة، شجرة الأعطاب، نماذج ماركوف، شبكات بتري.

Remerciements

Avant tout, je remercie Allah le tout puissant pour la volonté, la santé et la patience, qu'il m'a donné durant toutes mes années d'étude.

Je remercie Monsieur Brahim HAMAIDI mon directeur de thèse, Professeur à l'Université de Annaba et responsable du laboratoire de Génie Electromécanique. Cette thèse est le fruit d'une collaboration de plus de six années avec lui. C'est à ses côtés que j'ai compris ce que rigueur et précision voulaient dire.

Je tiens à remercier Monsieur Fares INNAL mon co-directeur de thèse, Professeur à l'Université de Skikda, qui m'a encadré tout au long de cette thèse et qui m'a fait partager ses brillantes intuitions. Qu'il soit aussi remercié pour sa gentillesse, sa disponibilité permanente et pour les nombreux encouragements qu'il m'a prodiguée.

Mes remerciements vont également à Monsieur Elias HADJADJ AOUEL, Professeur à l'université d'Annaba pour avoir accepté de présider le jury de soutenance.

J'exprime ma gratitude à Monsieur Mohamed KARA, Professeur à l'université de Tébessa et à Monsieur Abdallah KABOUCHE, Professeur à l'Université de Annaba, qui ont bien voulu être examinateurs.

Un grand merci aussi à tous le personnel du département d'Electromécanique.

A mes parents

A mon époux

A mes enfants

A mes frères

A ma famille

A mes copines

Table des matières

Abréviations, acronymes

AdD	Arbre des Défaillances
ALARP	As Low As Raisonably Practicable (aussi faible que raisonnablement possible)
ALOHA	Areal Locations of Hazardous Atmospheres
AM	Additional Mitigation (atténuation supplémentaire)
AMDEC	Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticité
BPCS	Basic Process Control System
DC	Diagnostic Coverage (Couverture du Diagnostic)
DCC	Défaillance de Cause Commune
E/E/EP	Electrique / Electronique / Electronique Programmable
ER	Evénement Redouté
EN	European Norm (Norme Européenne)
EUC	Equipment Under Control (équipement commandé)
FS	Failed State
GRIF	GRaphiques Interactifs pour la Fiabilité
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitation)
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Comission
IE	Evènement Initiateur
IPL	Independent Protection Layer
ISA	Instrument Society of America
ISO	International Organisation for Standardization
KooN	K out of N (K parmi N)
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection)
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance)
MIL STD	norme militaire américaine
MRT	Mean Repair Time
MTTR	Mean Time To Repair (durée moyenne de réparation)
NF	Norme Française
OHSAS	British Standard Occupational Health and Safety Assessment Series
PFD	Probability of Failure on Demand (probabilité de défaillance à la demande)
PFH	Probability of Failure per Hour (probabilité de défaillance par heure)

PST	Partial Stroke Testing
QRA	Quantitative Risk Assessment
RdP	Réseaux de Petri
RFF	Risk Reduction Factor (facteur de réduction du risque)
SC	Systematic Capability
SFF	Safe Failure Fraction (proportion des défaillances en sécurité)
SIF	Safety Instrumented Function (fonction instrumentée de sécurité)
SIL	Safety Integrity Level (niveau d'intégrité de sécurité)
SIS	Safety Instrumented System (Système Instrumenté de Sécurité)
WS	Working State

Listes des figures

Liste des tableaux

Introduction générale

1. Problématique

Les installations industrielles sont susceptibles de générer des phénomènes dangereux (incendie, explosion, rejets de matières dangereuses, etc.) dont les conséquences sont de plus en plus dévastatrices pour les cibles potentiels que sont les personnes, les biens et l'environnement. Cette réalité est imputable aux quantités importantes et propriétés dangereuses des matériaux utilisés et aux conditions de fonctionnement sévères (haute température, pression, etc.).

L'objectif de tout responsable industriel est non pas l'élimination complète des risques qui s'y associent, car une tâche impossible, mais plutôt l'assurance que ces risques sont maintenus à des niveaux acceptables. Pour ce faire, il est indispensable d'adopter une démarche de gestion des risques appropriée permettant à la fois d'identifier les mesures de maitrise nécessaires (barrières de sécurité) et de quantifier leur performance requise garantissant une réduction suffisante des risques.

Les systèmes instrumentés de sécurité (SIS : *Safety Instrumented System*) constituent une barrière d'une importance capitale dans ce processus de réduction des risques. En effet, les SIS garantissent un fonctionnement sûr des installations en surveillant d'une manière continue leurs paramètres opératoires (température, pression, débit, niveau, concentration, ...). Afin de garantir leur habilité à réduire les risques associés au processus protégé à un niveau tolérable donné, la norme CEI 61508 [CEI 61508, 2010] a été élaborée en tant que cadre technique dans le but d'encadrer leur conception et exploitation. Elle a été adoptée par de nombreuses réglementations nationales comme moyen recommandé pour obtenir un SIS de haute fiabilité. Principalement orientée vers la performance, la CEI 61508 ne fournit pas de règles prescriptives concernant le choix de la technologie du SIS, la configuration (architecture), les stratégies de tests, etc. Adoptant une approche basée sur les risques, elle établit une relation directe entre la réduction des risques à atteindre et les exigences de performance du SIS. Cette relation est caractérisée par l'introduction du concept de niveau d'intégrité de sécurité (SIL : *Safety Integrity Level*). Par conséquent, le SIL requis ou cible fait

référence aux performances nécessaires permettant au SIS de remplir la fonction de sécurité qui lui a été assignée de manière satisfaisante.

En matière de performance de nature probabiliste, la CEI 61508 spécifie deux mesures relevant du domaine de la sûreté de fonctionnement, en fonction de la fréquence à laquelle le SIS doit répondre aux événements dangereux (demandes) : la probabilité moyenne des défaillances dangereuses à la demande (PFD_{avg} *: average probability of dangerous failure on demand*) et la fréquence moyenne des défaillances dangereuse (*PFH : probability of failure per hour*). La première mesure est appropriée pour le SIS sollicité à faible fréquence (inférieure ou égale à une fois par an), tandis que la seconde est pertinente lorsque cette fréquence est élevée (plus d'une fois par an) ou continue.

La quantification de ces deux mesures nécessite la prise en compte de plusieurs paramètres : la configuration ou l'architecture du système (KooN : K-out-of-N), les taux de défaillances, les intervalles de tests périodiques, les stratégies de test, les temps de réparation et les défaillances de cause commune (DCC). Afin de faciliter cette quantification, de multiples formules mathématiques spécifiques aux configurations usuelles ou généralisées ont été fournies dans des documents officiels, tel que la CEI 61508, ou proposées dans la littérature [Innal, 2008 ; Chebila et Innal, 2015]. Néanmoins, les formulations déjà existantes présentent quelques lacunes. Nous nous limiterons dans le cadre de cette thèse à deux d'entre elles :

- Considération inadéquate des défaillances dangereuses détectées, en particulier dans le cas de la *PFH*. En effet, la nouvelle édition de la CEI 61508 fournit des formules *PFH* rendant compte de l'éventualité de la mise à l'arrêt automatique du procédé surveillé (shutdown) en cas de détection d'une défaillance dangereuse dans le SIS qui s'y associe. Néanmoins, la tentative de la CEI 61508 reste incomplète et fournirait des résultats non conservatifs, ce qui est dangereux d'un point de vue sécuritaire.
- Non considération de l'imperfection des tests périodiques (tests fonctionnels). L'imperfection d'un test périodique est due à l'écart entre les conditions supposées et les conditions réelles selon lesquelles ce test est effectué. A ce titre, nous tenterons d'intégrer cet aspect dans les formules relatives à la PFD_{avg}. Il convient de noter que cette non considération conduirait à des valeurs de PFD_{avg} sous estimées ou non conservatives (approche optimiste).

2. Objectifs

En fonction de ce qui précède, les objectifs de cette thèse sont résumés ci-après.

- Le premier objectif consiste à mieux comprendre la démarche de gestion de la sécurité fonctionnelle telle que décrite dans la norme CEI 61508, qui représente le document normatif central pour la conception et l'exploitation des SIS.
- Le second objectif est de vérifier la cohérence des formules relatives à la *PFH* fournies dans la CEI 61508 et d'en proposer de nouvelles formulations qui s'affranchissent du premier inconvénient cité à la fin du précédent paragraphe : considération de la mise à l'arrêt automatique du procédé surveillé suite à l'occurrence d'une défaillance dangereuse du SIS.
- Le troisième et dernier objectif de cette thèse de doctorat consiste en une étude approfondie des formules relatives à la PFD_{avg} en prenant en compte la contribution des tests imparfaits et partiels. A cette occasion nous essayerons de proposer une généralisation inédite de ces formules.

3. Organisation du mémoire

Afin de réaliser les objectifs précités, ce manuscrit a été scindé en quatre chapitres.

Le premier chapitre est consacré aux principaux concepts utilisés dans la thèse, notamment : la sécurité des processus, la sécurité fonctionnelle, les systèmes instrumentés de sécurité. La démarche de la norme CEI 61508 sera également fournie en détail. Une étude de cas liée à un réservoir de stockage de butane sera ensuite présentée pour mieux illustrer cette démarche.

Le deuxième chapitre traite l'inclusion adéquate de la capacité à conduire le procédé surveillé dans un état de sécurité suite à la détection d'une défaillance dangereuse au sein du SIS. A ce titre, nous étudierons la cohérence des formulations relatives à la *PFH* données dans la CEI 61508 à l'aide des chaines de Markov. Notons que ces formules ne concernent que des architectures communément utilisées. Par la même occasion, nous développerons de nouvelles formules *PFH* pour ces mêmes architectures, toujours en utilisant l'approche markovienne.

Dans le troisième chapitre, nous conduirons une étude comparative des résultats numériques que produisent les différentes formules liées à la *PFH* présentes dans la littérature et les formules nouvellement développées dans le deuxième chapitre. Cette comparaison est effectuée en se référant aux valeurs numériques dérivées des modèles de Markov multi-phases, proposées au chapitre précédent, et les réseaux de Petri (RdP) animés par simulation de Monte Carlo. En effet, nous ferons un ultime recours à un autre type de modèles comportementaux (RdP stochastiques) afin de consolider cette comparaison numérique. Par ailleurs, des généralisations pour chaque ensemble de formules *PFH* seront proposées. Ces généralisations permettent de s'affranchir du champ restreint des formulations propres à quelques architectures et donc de calculer la *PFH* de n'importe architecture *KooN*. La dernière partie de ce chapitre est dédiée à une étude détaillée de la configuration 2oo3 par la considération d'un éventail plus large des données d'entrée et par le traitement d'un système dédié.

Le quatrième chapitre concerne les SIS fonctionnant en mode faible demande. Il sera d'abord réservé à une revue bibliographique relative aux notions de tests partiels et imparfaits. Ensuite, nous présenterons les différentes formules analytiques de la PFD_{avg} incluant les tests partiels et/ou imparfaits retrouvées dans la littérature. Puis, nous proposerons une formulation originale permettant de comptabiliser la contribution de l'imperfection des tests périodiques. Nous donnerons également une modélisation « *holistique* » fondée sur les arbres des défaillances (AdD) conduits par les chaines de Markov. Finalement, nous réaliserons une comparaison des résultats numériques fournies par la formule établie et le modèle holistique proposé.

Dans une dernière partie, une conclusion générale rappelle les conclusions et les apports de notre travail. Des perspectives de recherche concernant les performances probabilistes relatives aux SIS y sont également proposées.

Chapitre 1

Démarche de la norme CEI 61508

1.1. Introduction

L'introduction de nouvelles technologies et la complexité croissante des systèmes industriels actuels rendent l'assurance de la sécurité des cibles potentielles (personnes, biens et environnement), dans l'éventualité d'une situation dangereuse, une tâche très difficile. Ainsi, l'automatisation de cette tâche est de plus en plus indispensable. Les systèmes de sécurité automatisés sont désormais appelés système instrumenté de sécurité [CEI 61511, 2016 ; CEI 61508, 2010]. L'évaluation de leur fiabilité devrait être réalisée le plus en amont possible avant et pendant leur mise en œuvre. Dans cette optique, la CEI 61508 a été développée et représente aujourd'hui le document normatif central pour la conception et l'exploitation des SIS.

Le présent chapitre est d'abord réservé aux principales notions de base figurant dans cette thèse. Ensuite, la démarche CEI 61508 de maitrise des risques en utilisant les SIS est décrite avec suffisamment de détail. Finalement, une étude de cas liée à un réservoir de butane est étalée pour mieux comprendre cette démarche.

1.2. Notions de base

Afin de simplifier la lecture de ce document, nous commençons tout d'abord par un éclaircissement relatif aux principaux termes utilisés.

1.2.1. Notion de système

Bien intégré dans le langage quotidien, le terme système peut avoir plusieurs définitions. Nous nous limiterons aux suivantes.

Selon Rob Dekkers [Dekkers, 2015], un système se constitue des éléments perceptibles dans la réalité totale (univers), définis par les objectifs de l'enquêteur. Tous ces éléments ont au moins une relation avec un autre élément au sein du système et peuvent avoir des relations avec d'autres éléments dans la réalité totale.

L'auteur Le Moigne [Le Moigne, 1984] définit le système comme *« un objet doté de finalité qui, dans un environnement exerce une activité et voit sa structure interne évoluer au fil du temps, sans qu'il perde pourtant son identité»*. Alors selon cet auteur, le système se considère comme :

- Quelque chose identifiable ;

- Qui fait quelque chose (activité) ;
- Dans quelque chose (finalité, projet) ;
- Par quelque chose (structure) ;
- Et qui se transforme dans le temps (évolution).

En lisant les deux définitions précédentes, on peut conclure que la définition de Le Moigne est la plus générale, vu qu'elle dépasse la simple relation entre les éléments du système (vue étroite).

1.2.2. Notion de danger

Selon le référentiel OHSAS 18001 [OHSAS 18001, 2007], un danger est une source, situation, ou acte susceptible de nuire à la personne en termes de blessures ou d'atteinte à la santé, ou des deux en même temps.

Nous retrouvons ce point de vue au niveau de la nouvelle norme relative aux systèmes de management de la santé et de la sécurité au travail [ISO 45001, 2018] : un danger *une source susceptible de causer traumatisme et pathologie*. La norme ISO 45001 définit les traumatismes et pathologies en termes *d'effets négatifs sur l'état physique, mental ou cognitif d'une personne*.

Ces deux définitions ne mentionnent qu'une seule cible potentielle qui est la personne dans son lieu de travail. Dans un cadre plus général incorporant les accidents majeurs ou technologiques, la définition du mot danger devra mentionner plus de cibles, notamment les biens matériels et l'environnement naturel.

Jean-Marie Flaus [Flaus, 2013] considère le danger comme *« un potentiel de dommages ou de préjudices. Le plus souvent pour les risques technologiques, un danger est associé à un système ou à un dispositif mettant en jeu une énergie importante, ou à une substance capable de donner naissance à une réaction chimique ou biologique créant des dommages»*. Ici, le terme dommage et d'une portée générale et pourrait ainsi concerné toute sorte de cibles.

Le danger est donc une caractéristique intrinsèque des produits chimiques, des énergies, des organismes biologiques, des systèmes (plus globalement) qui les rendent susceptibles de causer des dommages. *Exemples :* un produit acide, une énergie électrique, un bruit etc.

Dans ce contexte, l'identification d'un danger est un processus de recherche de l'existence d'un danger et de définition de ses caractéristiques [OHSAS 18001, 2007].

1.2.3. Notion de risque

La norme ISO 31000 indique qu'un risque est souvent exprimé en termes de combinaison des *conséquences* d'un *événement* et de sa *vraisemblance*. Les termes clés de cette définition sont décrit ci-après [ISO 31000, 2009] :

- *Evénement* : occurrence ou changement d'un ensemble particulier de circonstances.
- *Conséquence* : effet d'un événement affectant des objectifs. Les objectifs peuvent avoir différents aspects (financiers, santé et sécurité ou environnementaux). L'ISO 31000 définit un effet comme étant un écart positif ou négatif par rapport à une attente. Dans le cadre de cette thèse, seuls l'aspect négatif est considéré (événement *dangereux, redouté, indésirable ou non souhaité*).
- *Vraisemblance* : possibilité que quelque chose se produise. Cette possibilité peut être décrite au moyen de termes mathématiques (telle une probabilité ou une fréquence sur une période donnée).

L'idée de combinaison se retrouve également dans la définition fournie par OHSAS 18001 [OHSAS 18001, 2007] : combinaison de la vraisemblance d'occurrence d'un *événement dangereux* ou d'une exposition et la gravité de blessure ou de maladie pouvant être causés par cet événement ou cette exposition.

Mathématiquement le risque est souvent représenté par l'équation suivante :

$$R = P \cdot G \tag{1.1}$$

Où P signifie la probabilité d'occurrence d'un évènement dangereux et G est la gravité des conséquences de cet évènement.

Par ailleurs, dans le cadre de l'évaluation quantitative des risques (QRA : *Quantitative Risk Assessment*), une définition très commune du mot risque consiste à le représenter par le triplet suivant [Kaplan et Garrick, 1981 ; NASA, 2011] :

- Que peut-il mal passé (scénario) ?
- Combien est-il fréquent (vraisemblance) ?
- Quelles sont les conséquences associées ?

La réponse à la première question est un ensemble de scenarios d'accidents. La seconde question nécessite l'évaluation des fréquences de ces scenarios, tandis que la troisième quantifie leurs conséquences (figure 1.1). Les scenarios d'accidents débutent avec un événement

initiateur (IE) qui perturbe le système et cause une déviation dans son fonctionnement souhaité. Ensuite, l'analyse se poursuit par la détermination des événements pertinents pour l'évolution du scenario et ayant un effet favorisant ou limitant la progression de l'accident (fonctionnement ou défaillances des barrières de sécurité, possibilité d'ignition, exposition, etc.). Puis, les fréquences des scenarios ayant des conséquences indésirables supposées sont déterminées. Finalement, ces conséquences indésirables sont estimées.

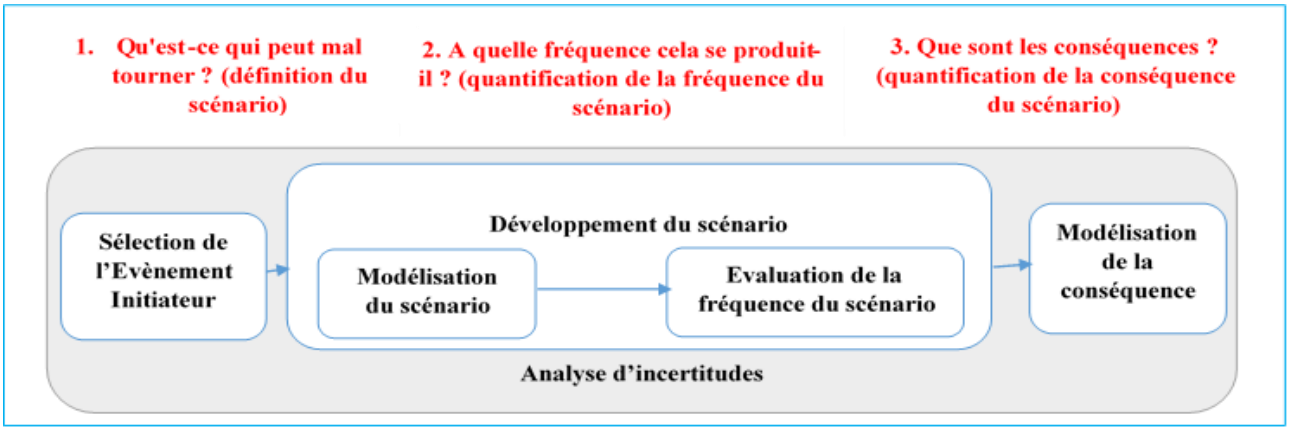

Figure 1.1 : Implémentation de la définition du risque dans le cadre du QRA [NASA, 2011]

Ce processus est fourni d'une manière plus complète et plus détaillée au niveau de la norme ISO 31000 [ISO 31000, 2009], telle que donnée dans la figure 1.2. Les différentes étapes de ce processus sont expliquées brièvement ci-après en se référant à cette même norme :

- *Etablissement du contexte* : définition des paramètres externes et internes à prendre en compte et définition du domaine d'application ainsi que les *critères de risque*. Les critères de risque sont les termes de référence vis-à-vis desquels l'importance d'un risque est évaluée. Ils peuvent être issus de normes, de lois, de politiques et d'autres exigences. La figure 1.3 donne un exemple de définition de ces critères.
- *Identification du risque* : identification des sources de risque (des dangers), des événements, de leurs causes et de leurs conséquences potentielles.
- *Analyse du risque* : détermination des conséquences et de leur vraisemblance, ainsi que d'autres attributs du risque. Il convient de prendre en compte les moyens de maitrise existants. L'analyse peut être qualitative, semi-quantitative, quantitative ou une combinaison des trois.
- *Evaluation du risque* : comparaison des résultats de l'analyse du risque (niveau de risque) avec les critères de risque afin de déterminer si le risque est acceptable ou tolérable.

- *Traitement du risque* : processus destiné à modifier un risque (réduction du risque). Il engendre ou modifie les moyens de maitrise du risque. Les options de traitement peuvent inclure le refus du risque, l'élimination de la source de risque, une modification de la vraisemblance (mesure de prévention), une modification des conséquences (mesure de protection), etc. Nous tenons à préciser qu'un moyen de maitrise du risque signifie une *barrière de sécurité* telle que définit dans la première partie de la norme CEI 50126 [CEI EN 50126-1, 2019] : « *des moyens physiques ou non physiques, qui réduisent la fréquence d'un danger et/ou d'un accident potentiel résultant du danger et/ou atténuent la gravité des accidents potentiels résultant du danger* ». Pour plus de détail sur cette notion et celles qui s'y attachent, veuillez consulter la référence [Sklet, 2006].

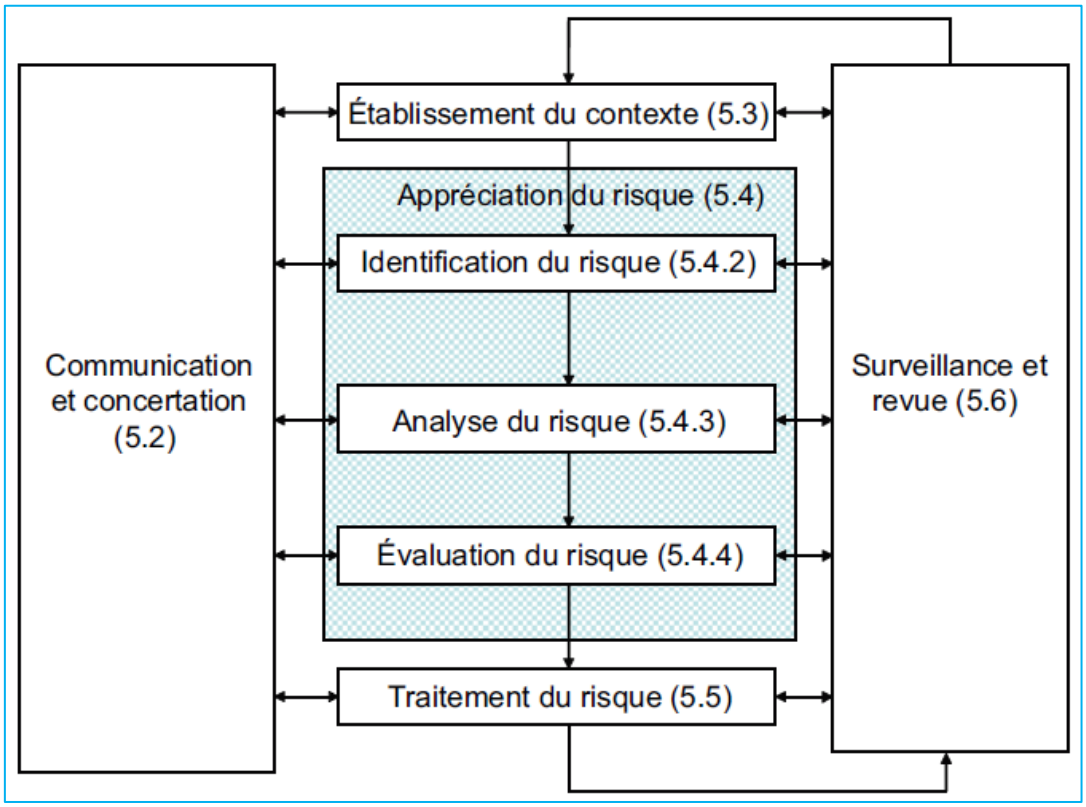

Figure 1.2 : Processus de management du risque [ISO 31000, 2009]

Pour mieux achever chacune des étapes du processus de management du risque, la norme CEI 31010 fournit de différentes techniques (figure 1.4).

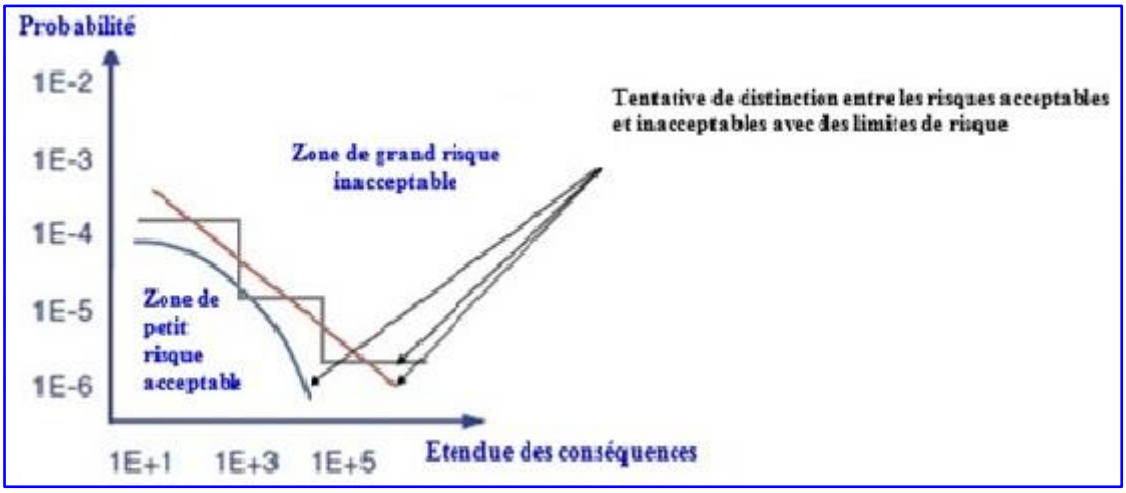

Figure 1.3 : Représentation du risque [Čepin, 2011]

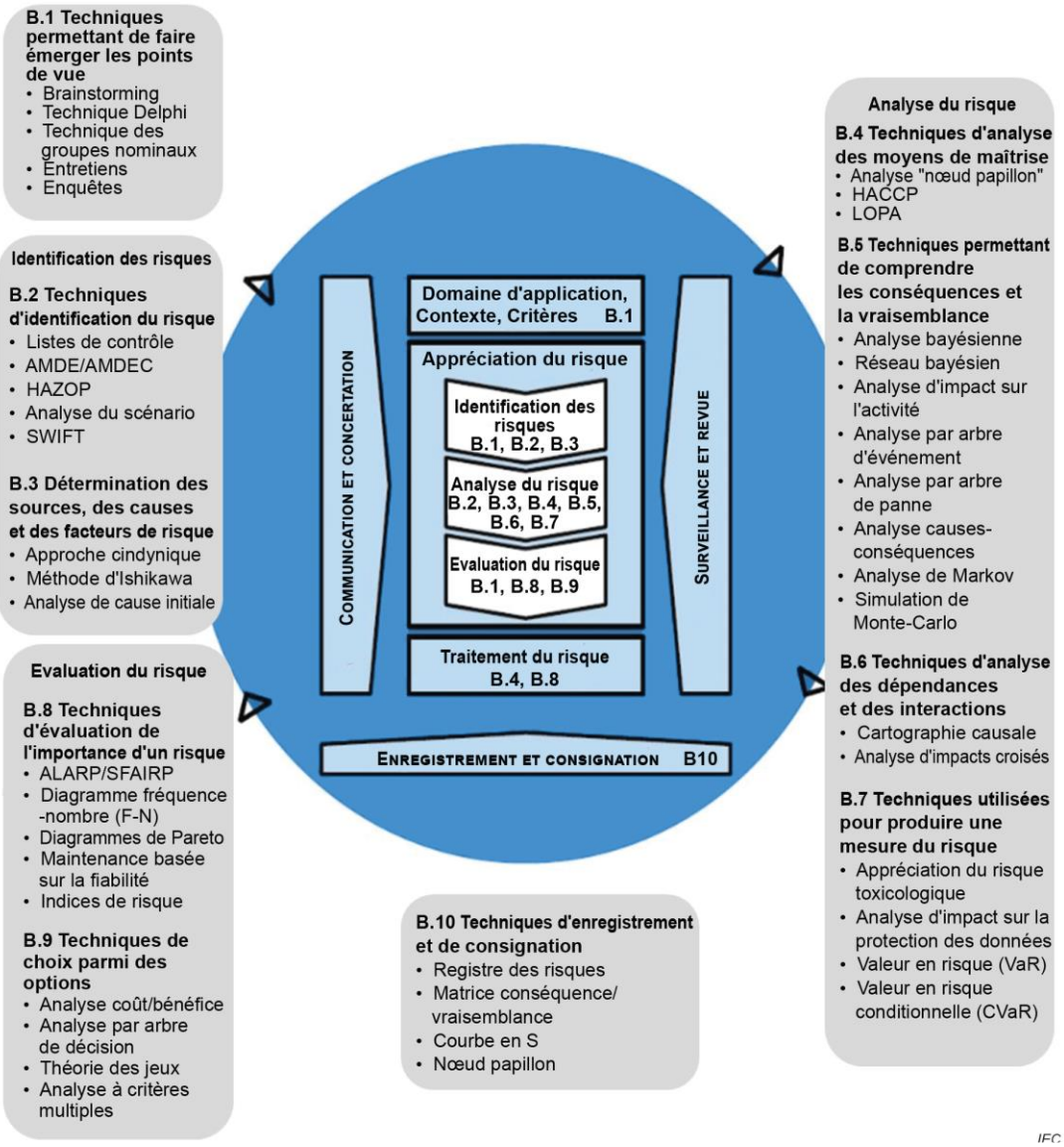

Figure 1.4 : Techniques relatives au processus de management du risque [CEI 31010, 2019]

1.2.4. Notion de sécurité

La norme [ISO/CEI Guide 51, 2014] définit la sécurité ainsi : « *absence de risque intolérable* ». Par ailleurs, la norme américaine [MIL-STD-882E, 2012] définit la sécurité comme : « *absence de conditions qui peuvent causer la mort, des blessures, des maladies professionnelles, des dommages ou la perte d'équipements ou de biens, ou des dommages à l'environnement* ».

En ce qui concerne la sécurité d'un système, l'auteur Fares Innal [Innal, 2008], la définit comme : *« l'aptitude d'un système à fonctionner ou à dysfonctionner sans engendrer d'évènement redouté à l'encontre de lui-même et de son environnement, notamment humain».*

Il convient de noter que la mesure de cette aptitude doit être effectuée en fonction des critères de risque applicables. Cette aptitude atteindrait donc son maximum en présence exclusive de risques négligeables ou acceptables (voire tolérables).

1.2.5. Sécurité fonctionnelle

La norme CEI 61508, dans son quatrième volume [CEI 61508-4, 2010], fournit la définition suivante : « *sous-ensemble de la sécurité globale se rapportant à l'EUC et au système de commande de l'EUC qui dépend du fonctionnement correct des systèmes E/E/PE relatifs à la sécurité et d'autres mesures de réduction de risque* ». Il convient de souligner que les mesures de réduction de risque sous-entendent les moyens de maitrise du risque.

L'EUC (*Equipment Under Control : équipement commandé*) est défini dans la même norme comme suit : « *équipements, machines, appareils ou installations utilisés pour la fabrication, le traitement, le transport, les activités médicales ou autres*». Le système de commande de l'EUC est un système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que l'EUC fonctionne de la façon souhaitée [CEI 61508-4, 2010].

La sécurité fonctionnelle ne concerne donc que les risques résultant des équipements commandés ou contrôlés, y compris leurs systèmes de commande, le système de commande de l'EUC étant séparé et distinct de l'EUC.

Les systèmes E/E/PE relatifs à la sécurité sont tout simplement les systèmes instrumentés de sécurité (*SIS*), objet principal de cette thèse (voir les définitions suivantes).

1.2.6. Systèmes instrumentés de sécurité

1.2.6.1. Définitions

Au niveau de la CEI 61508, les systèmes instrumentés de sécurité (SIS : *safety instrumented system*) sont désignés par la dénomination suivante : systèmes électriques/électroniques/électroniques programmables (E/E/EP) relatifs à la sécurité. Cette appellation nécessite d'être explicité :

- *Système E/E/EP* : système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs E/E/PE. Ce terme recouvre tous les éléments du système, tels que l'alimentation, les capteurs, et les autres dispositifs d'entrée, les autoroutes de données et les autres voies de communication, ainsi que les actionneurs et les autres dispositifs de sortie [CEI 61508-4, 2010].
- *Système relatif à la sécurité*. Un système qui à la fois :
  - met en œuvre des *fonctions de sécurité* requises pour atteindre ou maintenir un *état de sécurité* de l'EUC.
  - est prévu pour atteindre, par lui-même ou grâce à d'autres systèmes E/E/EP relatifs à la sécurité et autres mesures de réduction de risque, l'intégrité de sécurité nécessaire pour les fonctions de sécurité requises.
- *Fonction de sécurité* : fonction destinée à atteindre ou à maintenir un état de sécurité, par rapport à un événement dangereux spécifique [ISO/TR 12489, 2016].

  Les systèmes relatifs à la sécurité peuvent globalement être répartis en systèmes relatifs à la sécurité de commande et en systèmes relatifs à la sécurité de protection. Ils peuvent être conçus pour prévenir un événement dangereux ou pour réduire les effets de ce dernier (ou les deux à la fois).
- *Etat de sécurité* : état de l'EUC lorsque la sécurité est réalisée.
- *Intégrité de sécurité* : aptitude d'un système relatif à la sécurité à réaliser ses fonctions de sécurité requises dans toutes les conditions énoncées dans un environnement opérationnel et sur une durée déterminée [CEI EN 50126-1, 2019]. Les normes [CEI 61508-4, 2010], [CEI 61511-1, 2016] et [ISO/TR 12489, 2016] donnent des définitions semblables en réservant cette notion exclusivement aux SIS. Notons que les normes [CEI 61508-4, 2010] et [CEI 61511-1, 2016] utilise la notion de probabilité à la place d'aptitude. Dans le cadre de ce document nous adoptons le mot aptitude car plus généal. Selon cette aptitude, la norme CEI 61508 définit quatre niveaux d'intégrité de sécurité (SIL : safety integrity level)

distincts, correspondant à une gamme de valeurs d'intégrité de sécurité où le niveau 4 d'intégrité de sécurité possède le plus haut degré d'intégrité. Par ailleurs, l'intégrité de sécurité comprend :

- *Intégrité de sécurité du matériel :* partie de l'intégrité de sécurité d'un SIS qui se rapporte aux défaillances aléatoires du matériel en mode de défaillance dangereux (défaillances d'un SIS susceptibles de nuire à son intégrité de sécurité).
- *Intégrité de sécurité systématique* : partie de l'intégrité de sécurité d'un système relatif à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux.

La norme [CEI 61511-1, 2016] utilise le terme SIS et non pas système E/E/EP relatif à la sécurité et en donne la définition suivante : « *système instrumenté utilisé pour mettre en œuvre une ou plusi*eurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal (aux) ».

Un SIS, aussi appelé boucle de sécurité, se compose donc de n'importe quelle combinaison de (Figure 1.5) :

- éléments d'entrée (capteurs, détecteurs, etc.) qui surveillent l'évolution des paramètres représentatifs de l'installation (température, pression, débit, niveau, etc.).
- unités logiques (PLC, API, etc.) qui récoltent l'information en provenance du sous-système éléments d'entrée et réalisent le processus de prise de décision.
- éléments terminaux (vannes d'arrêt d'urgence, pompes, alarmes, etc.) qui agissent, sous l'ordre du sous-système unités logiques, sur l'installation pour neutraliser sa dérive en la mettant dans un état sûr.

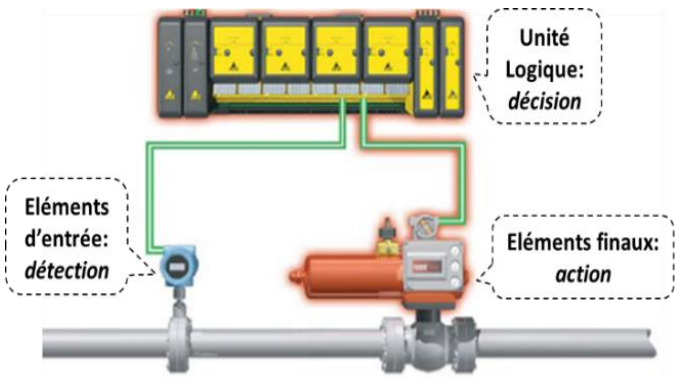

Figure 1.5 : Composition type d'un système instrumenté de sécurité

1.2.6.2. Modes de fonctionnement

La CEI 61508 définit trois modes de fonctionnement d'une fonction de sécurité [CEI 61508-4, 2010] :

- *Mode faible sollicitation* : la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations n'est pas supérieure à une par an.
- *Mode sollicitation élevée* : la fonction de sécurité n'est réalisée que sur sollicitation, afin de faire passer l'EUC dans un état de sécurité spécifié, et la fréquence des sollicitations est supérieure à une par an.
- *Mode continu* : la fonction de sécurité maintient l'EUC dans un état de sécurité en fonctionnement normal.

En considérant les caractéristiques des systèmes industriels actuels, nous pouvons avancer que les sollicitations dans le cadre du premier mode de fonctionnement sont des *événements indésirables,* tandis que celle relatives au deuxième mode sont des *événements faisant partie du fonctionnement normal* de l'EUC. La référence faite aux nombre de sollicitations par an est donnée sans aucune justification dans la CEI 61508.

1.3. Norme CEI 61508

La norme CEI 61508 représente le document normatif central pour la conception et l'exploitation des SIS. Elle présente une approche générique de toutes les activités liées au cycle de vie des SIS. Du fait de son aspect générique, elle a été déclinée en plusieurs normes filles spécifiques à chaque secteur d'application, voir figure 1.6 [ISO 26262, 2007].

En adoptant une approche fondée sur les risques, la CEI 61508 établie un lien direct entre la réduction du risque à réaliser et les exigences de performance pour le SIS (exigences en matière d'intégrité de sécurité). Cette relation est caractérisée par l'introduction de la notion de niveau d'intégrité de sécurité (SIL). Les SIL sont utilisés pour spécifier les exigences concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux SIS. Le SIL requis se réfère donc à la performance requise pour le SIS lui permettant de remplir la fonction de sécurité qui lui a été assignée d'une manière satisfaisante. A ce titre, la CEI 61508 spécifie deux principales mesures cibles de défaillance (objectifs chiffrés de défaillance), selon le nombre de sollicitations de la fonction de sécurité du SIS (modes de fonctionnement) :

- **La probabilité moyenne de défaillance dangereuse de la fonction de sécurité en cas de sollicitation (*PFD_{avg}*: *average probability of dangerous failure on demand*)**. Cette mesure est appropriée pour les fonctions de sécurité faiblement sollicitées : *mode de fonctionnement à faible sollicitation*. Cette mesure est l'indisponibilité moyenne d'un SIS pour réaliser la fonction de sécurité spécifiée sur sollicitation de l'EUC ou de son système de commande. L'indisponibilité moyenne sur un intervalle de temps donné [t_1, t_2] est généralement exprimée par :

$$U(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U(t)\, dt \qquad (1.2)$$

U(*t*) représente l'indisponibilité instantanée du SIS : « *probabilité qu'une entité ne soit pas en mesure de réaliser une fonction requise dans des conditions données à un moment donné, en supposant l'existence des ressources externes requises* » [IEC 60050-192, 2015].

Dans le cadre de la PFD_{avg}, le calcul est souvent effectué pour $t_1 = 0$ et $t_2 = T$ (durée de vie du SIS).

$$PFD_{avg} = U(0,T) = \frac{1}{T} \int_0^T U(t)\, dt \qquad (1.3)$$

- **La fréquence moyenne de défaillance dangereuse de la fonction de sécurité (*PFH* : *probability of failure per hour*)**. Cette mesure est convenable pour les fonctions de sécurité fortement sollicitées : *mode de fonctionnement à sollicitation élevée* ou *mode de fonctionnement continu*. Cette quantité représente la fréquence moyenne d'une défaillance dangereuse d'un SIS pour réaliser la fonction de sécurité spécifiée pendant une période de temps donnée. Formellement, la *PFH* est la moyenne de l'intensité de défaillance inconditionnelle *w*(*t*) (fréquence de défaillance) :

$$PFH = w(0,T) = \frac{1}{T} \int_0^T w(t)\, dt \qquad (1.4)$$

Avec :

$$w(t) = \lim_{dt \to 0} \frac{P(\text{Entité tombe en panne entre } t \text{ et } t+dt / E)}{dt} \qquad (1.5)$$

L'événement *E* signifie que l'entité était en état de marche à l'instant $t = 0$.

La correspondance entre les niveaux SIL et ces deux performances probabilistes est indiquée au tableau 1.1 [CEI 61508, 2010].

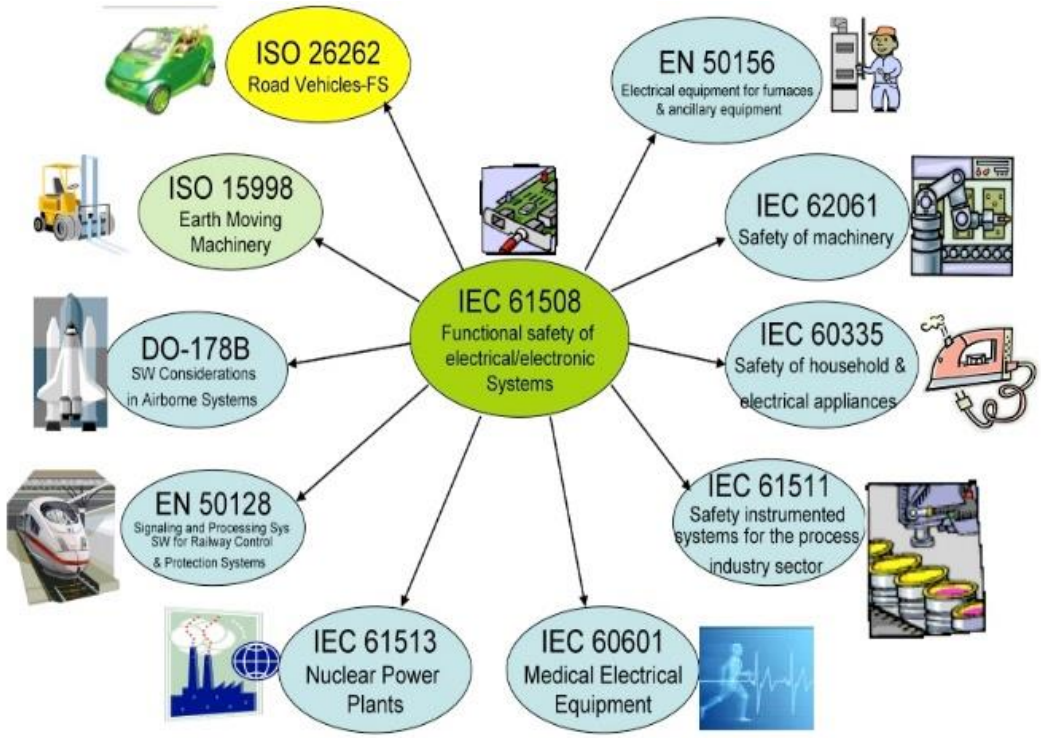

Figure 1.6 : Déclinaison de la norme CEI 61508 en normes filles

Tableau 1.1 : Niveaux d'intégrité de sécurité (SIL) en fonction des PFD_{avg} et PFH

SIL	$\boldsymbol{PFD_{avg}}$	$\boldsymbol{PFH}$
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$

1.4. Démarche de la norme CEI 61508

Cette section est réservée à une explication relative à la démarche de la norme CEI 61508. Cette démarche se résume dans la figure 1.7, où trois principales étapes sont à distinguer. Nous allons les décrire brièvement dans ce qui suit.

1.4.1. Première étape : Analyse et évaluation des risques

Pendant cette étape, l'ensemble des situations dangereuses (scénarios d'accident) est établi en termes de gravité et de vraisemblance (fréquence d'occurrence), afin d'en comparer la criticité (niveau de risque) à une valeur limite constituant l'objectif de sécurité à atteindre

(critère de risque). Si cette criticité excède la valeur-seuil précitée, il sera alors nécessaire de la réduire. L'ampleur de cette réduction est déclinée en prescriptions particulières de sécurité allouées aux différents moyens de réduction de risques : SIS et autres mesures de réduction (soupape de sécurité, par exemple). Pour les SIS, ces prescriptions sont établies en termes de fonctions de sécurité à réaliser et de niveaux d'intégrité de sécurité (SIL cible ou requis) correspondants (objet de la deuxième étape). Plus la réduction de risque à réaliser est importante, plus le SIL requis est élevé. Ce constat souligne l'importance et le rôle capital que jouent l'analyse et l'évaluation des risques dans la démarche CEI 61508. Il est à noter que la détermination des scenarios d'accidents peut être effectuée en utilisant des méthodes classiques telles que l'AMDEC et HAZOP (voir figure 1.4).

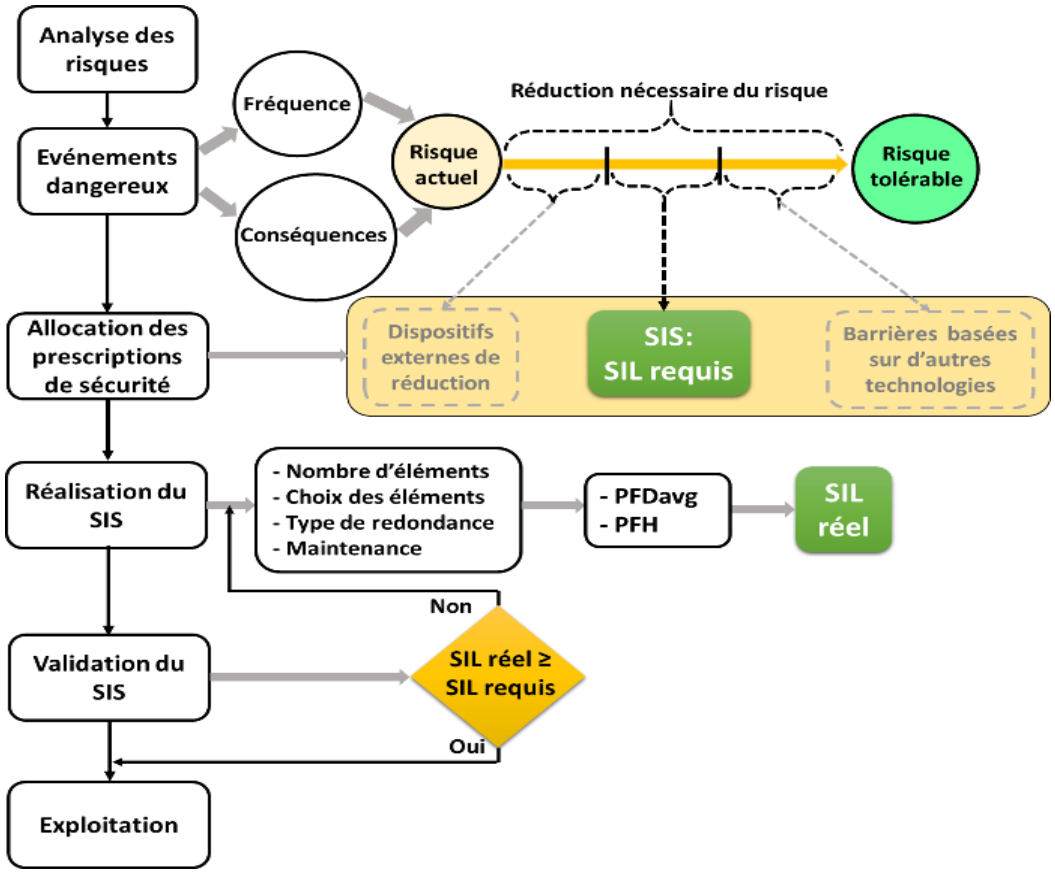

Figure 1.7 : Démarche de la CEI 61508 : risque et niveau d'intégrité de sécurité

1.4.2. Deuxième étape : Allocation du niveau d'intégrité de sécurité (SIL requis)

Cette allocation est conduite selon certaines méthodes particulières permettant de définir le SIL requis pour une fonction de sécurité : *SIL qui doit être atteint par un SIS afin de réaliser la réduction nécessaire du niveau de risque*. Sont décrites ci-dessous les deux méthodes les plus

souvent utilisées à cet effet : graphe de risque et LOPA *(layer of protection analysis)*. Elles sont plus ou moins adaptées en fonction du niveau de détail des analyses de risques réalisées.

1.4.2.1. Graphe de risque

Cette méthode est qualifiée de qualitative. Quand une méthode qualitative est adoptée, un certain nombre de paramètres de simplification doivent être introduits. Ils permettent de qualifier le phénomène dangereux (accident) en fonction des connaissances disponibles. La méthode du graphe de risque s'appuie sur quatre paramètres :

C : la conséquence de l'événement dangereux. Les conséquences pourraient être des dommages liés à la santé et la sécurité des personnes, perte de matériels ou de production, ou des dommages environnementaux,

F : la fréquence et la durée d'exposition aux dangers,

P : la possibilité d'éviter l'événement dangereux,

W : la fréquence de l'occurrence de l'événement dangereux sans moyen de protection.

Les paramètres *C*, *F*, *P* et *W* doivent être soigneusement définis pour chaque événement dangereux. Les documents [CEI 61508, 2010 ; Summers, 1998] fournissent de simples conseils sur la façon de caractériser chacun de ces paramètres.

Un calibrage de chacun d'entre eux peut être nécessaire pour prendre en compte les particularités de l'entreprise, la réglementation et les normes du secteur d'application. Comme montré sur la figure 1.8 [CEI 61508, 2010], le graphe des risques associe des combinaisons spécifiques de paramètres de risque aux niveaux d'intégrité de sécurité requis.

La technique du graphe de risque repose fortement sur l'expertise du personnel de l'entreprise pour caractériser le risque associé à un événement dangereux donné. Les avantages de cette approche sont sa simplicité, sa rapidité et ses ressources limitées requises pour son exécution en faisant un outil de dépistage utile [Stavrianidis et Bhimavarapu, 1998]. Cependant, le SIL requis peut facilement varier d'un seul niveau en raison des incertitudes liées aux paramètres de risque (en fonction de l'expertise des analystes). De plus, en raison de son caractère qualitatif, le graphe de risque n'offre pas un outil approprié pour une prise de décision efficace privilégiant des approches quantitatives.

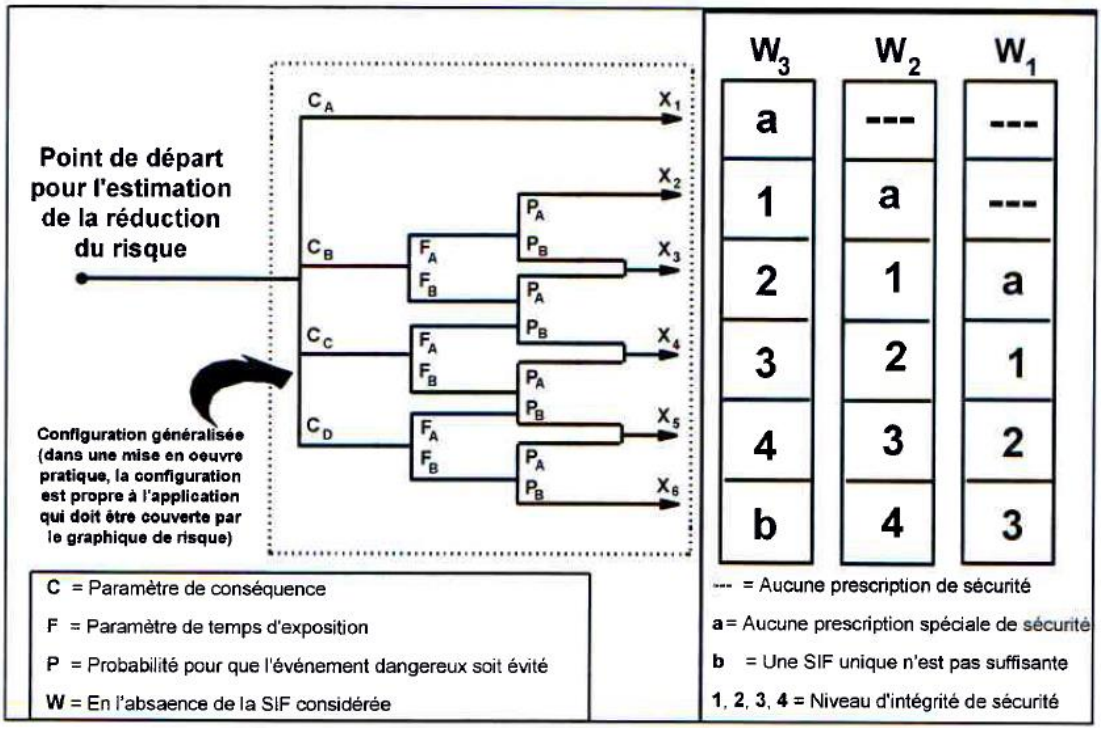

Figure 1.8 : Schéma général du graphe de risque [CEI 61508, 2010]

1.4.2.2. Analyse des couches de protection (LOPA: Layer Of Protection Analysis)

LOPA est une méthode semi-quantitative couramment utilisée pour la détermination du SIL requis. La méthode commence avec les données développées dans l'identification des dangers (généralement l'étude HAZOP) et rend compte de chaque danger identifié en documentant les causes initiatrices et les couches de protection qui empêchent ou atténuent le danger. Son principe est d'estimer la fréquence de l'événement dangereux (événement d'impact) grâce à la quantification des causes initiatrices (fréquences des événements initiateurs) et des probabilités de défaillance à la sollicitation de chaque couche de protection [CEI 61508, 2010 ; CEI 61511, 2003 ; Dowel, 1998]. La réduction du risque est alors évaluée à la lumière de la fréquence tolérable (critère de risque ou cible de sécurité). Une condition majeure à satisfaire est l'indépendance des différentes couches de protection (IPL: *independant protection layer*) les uns des autres et des événements initiateurs [CCPS, 2001 ; Innal *et al.*, 2014]. La figure 1.9 montre un exemple de format de feuille de calcul pouvant être utilisé pendant une étude LOPA [CEI 61508, 2010].

1	2	3	4	5			6	7	8	9	10
				Protection layers (PLs)							
Impact event description *F.2*	Severity level *F.3*	Initiating cause *F.4*	Initiation likelihood F.5	General design F.6.1	Control system F.6.2	Alarms, etc. F.6.3	Additional mitigation, restricted access F.7	Additional mitigation F.8	Intermediate event likelihood F.9	PFD_{avg} required for E/E/PES (and SIL) F.10	Tolerable Mitigated event likelihood F.11
Overspeed of rotor leading to fracture of casing	Loss of life of persons located adjacent to casing, fatalities will not exceed 2	Speed control system fails	0,1	1	1	1	0,1	0,1	10^{-3}	$5{\cdot}10^{-3}$ (SIL 2 with a minimum PFD_{avg} of $5{\cdot}10^{-3}$)	10^{-5}
		Loss of load	1	1	0,1	1	0,1	0,1	10^{-3}		
		Clutch failure	0,1	1	0,1	1	0,1	0,1	10^{-4}		
					0,1 credit given to control system		Occupancy limited, persons not present 90 % of the time	Fatality will only occur if fragments contact persons	Total $2{,}1{\cdot}10^{-3}$		Tolerable frequency if fatalities do not exceed 5

Figure 1.9 : Exemple de tableau LOPA

La fréquence d'un événement dangereux (avec gravité ou conséquence *C*) pour chaque cause *i* (colonne 8 de la figure 1.9) peut être formulée comme suit [Omeiri *et al.*, 2015] :

$$f_C^i = f_{IE}^i \cdot \left(\prod_j PFD_j^i\right) \cdot \left(\prod_k AM_k^i\right) \quad (1.6)$$

Où f_C^i est la fréquence de la conséquence *C* (liée à un événement dangereux donné) due à la *i*ème cause. f_{IE}^i est la fréquence de la *i*ème cause (événement initiateur : IE). PFD_j^i est la PFD_{avg} de la *j*ème couche de protection qui protège contre la conséquence *C* induite par la *i*ème cause. AM_k^i est le *k*ème facteur d'atténuation supplémentaire (AM : *Additional Mitigation*) pour la conséquence *C* compte tenu de la *i*ème cause (par exemple, accès restreint, réduction de la probabilité d'inflammation, etc.).

La fréquence totale d'un événement dangereux engendrant la conséquence *C* est calculée en ajoutant les fréquences calculées pour chaque cause :

$$f_C = \sum_i f_C^i = \sum_i \left[f_{IE}^i \cdot \left(\prod_j PFD_j^i\right) \cdot \left(\prod_k AM_k^i\right)\right] \quad (1.7)$$

La réduction du risque requise allouée à la fonction de sécurité du SIS est obtenue en comparant f_C avec la fréquence du risque tolérable f_C^t (la conséquence *C* ne doit pas se produire avec une fréquence supérieure à *x* fois par an). Dans le cas où la fonction de sécurité assurée par le SIS est faiblement sollicitée, sa mesure cible de défaillance peut être obtenue ainsi :

$$f_C \leq f_C^t \Rightarrow PFD_{avg}^{max} \leq \frac{f_C^t}{\sum_i \left[f_{IE}^i \cdot \left(\prod_{j \neq SIS} PFD_j^i\right) \cdot \left(\prod_k AM_k^i\right)\right]} \quad (1.8)$$

La PFD_{avg}^{max} est la valeur maximale autorisée pour le SIS, tel que la réduction du risque nécessaire soit réalisée et le risque tolérable soit donc atteint. Le SIL associé peut être obtenu à partir du tableau 1.1. Notons que l'équation (1.8) n'est valable que si la fonction de sécurité du SIS concerné intervient pour l'ensemble des événements initiateurs *i*. Dans le cas contraire, une manipulation attentive de l'équation (1.7) permettrait d'obtenir facilement la quantité PFD_{avg}^{max}. Pour le mode de fonctionnement sollicitation élevée et mode continu, la *PFH* du SIS serait la fréquence d'un événement initiateur *i* donné. L'obtention de la *PFH* cible, PFH^{max}, peut être effectuée en faisant un bon usage de l'équation (1.7).

Comme indiqué précédemment, la méthode LOPA repose fortement sur l'hypothèse de l'indépendance. Cela étant, la fréquence calculée serait sous-estimée si une cause de défaillance commune existe parmi les causes initiatrices et les couches de protection. En outre, l'incohérence dans l'assignation des SIL vient souvent d'un manque de clarté ou d'incertitude relative aux valeurs numériques utilisées. Des techniques quantitatives plus rigoureuses telles que l'arbre de défaillances ou les chaines de Markov peuvent être nécessaires pour représenter la performance réelle d'un équipement spécifique. Cependant, LOPA reste une méthode simplifiée qui nécessite moins de ressources qu'une technique élaborée, donnant des résultats légèrement conservatifs [Dowell, 1998].

1.4.3. Troisième étape : Réalisation, validation et exploitation du SIS (SIL réel)

Une fois le SIL requis est déterminé, reste à concevoir le SIS assurant la fonction de sécurité qui lui a été désignée et devant respecter les prescriptions attachées à ce SIL requis. Pour ce faire, la norme CEI 61508 montre que l'observation simultanée des trois prescriptions suivantes est nécessaire :

- ***Prescriptions qualitatives :*** permettant de tenir compte des exigences relatives aux défaillances systématiques : défaillances de *conception* et d'*interactions*. Les défaillances de conception ne peuvent généralement être éliminées que par une modification de la conception ou du processus de fabrication. Des exemples typiques de ces défaillances sont les défauts de conception du logiciel et du matériel. Les défaillances d'interactions sont initiées par les erreurs humaines lors de l'exploitation, la maintenance, etc. Le respect de ses prescriptions permet d'accomplir l'intégrité de sécurité systématique de la fonction de sécurité. A cet égard, la CEI 61508 introduit la notion de capabilité systématique (*SC* : *Systematic Capability*) : une mesure, exprimée sur une échelle de SC 1 à SC 4, de la confiance dans le fait que l'intégrité de sécurité

systématique d'un élément satisfait aux exigences du niveau SIL spécifié. Cela dit, une capabilité systématique de SC N pour un élément, par rapport à la fonction de sécurité spécifiée, signifie que l'intégrité de sécurité systématique de SIL N a été respectée. La [CEI 61508-2, 2010] donne de détail concernant le calcul de SC d'une combinaison d'éléments.

- ***Prescriptions probabilistes* :** consistant au calcul de la PFD_{avg} (mode de fonctionnement faible sollicitation) ou de la *PFH* (fonctionnement en sollicitation élevée ou en continu). Ces deux grandeurs ne doivent pas dépasser les mesures cibles définies au cours de l'étape d'allocation des niveaux d'intégrité de sécurité. Ce calcul nécessite la considération de plusieurs paramètres : architecture du système (nombre d'éléments utilisés et leur configuration), taux de défaillances, couverture du diagnostic, intervalles de tests périodiques, temps de réparation et défaillances de cause commune. Ces paramètres sont définis dans le chapitre suivant. Afin de guider les analystes, la CEI 61508 propose des formules analytiques simplifiées, valables sous certaines hypothèses [Innal, 2008], pour effectuer ces calculs probabilistes. Il est à noter que les méthodes quantitatives classiques, telle que l'arbre de défaillances (AdD), sont plus adaptées du fait de leur large domaine de validité. De nombreuses formulations ont ensuite été proposées. Nous les évoquerons dans la suite de ce manuscrit.

- ***Prescriptions complémentaires*** : la détermination du SIL de manière probabiliste, via le calcul de la PFD_{avg} ou de la *PFH*, n'offrirait pas la garantie d'une précision suffisante selon la norme CEI 61508. Il conviendrait donc de confirmer ou de corriger la valeur ainsi trouvée pour le SIL (réel) en appliquant l'une des deux procédures suivantes :

  - ***Route 1_H : Contraintes architecturales***. Les contraintes architecturales représentent une première estimation de la capacité d'un système instrumenté à accomplir sa fonction en analysant son architecture. Cette procédure est basée sur les concepts de *tolérance aux anomalies du matériel* (*HFT* : *hardware fault tolerance*) et de *proportion de défaillances en sécurité* (*SFF* : *safe failure fraction*). Une $HFT = M$ signifie que $(M + 1)$ anomalies sont susceptibles de provoquer la perte de la fonction de sécurité. La *SFF* d'un sous-système est définie par le rapport du taux moyen des défaillances en sécurité (λ_S) plus les défaillances dangereuses détectées (λ_{DD}) au taux de défaillance moyen total du sous-système :

$$SFF = (\lambda_s + \lambda_{DD})/(\lambda_s + \lambda_D) \quad (1.9)$$

Cette procédure s'appuie sur le tableau 1.2 [CEI 61508-2, 2010].

Tableau 1.2 : Contraintes architecturales sur les SIS du type A (resp. B)

SFF	HFT		
	0	**1**	**2**
< 60 %	SIL 1 (non autorisé)	SIL 2 (SIL 1)	SIL 3 (SIL 2)
60 % - < 90 %	SIL 2 (SIL 1)	SIL 3 (SIL 2)	SIL 4 (SIL 3)
90 % - < 99 %	SIL 3 (SIL 2)	SIL 4 (SIL 3)	SIL 4 (SIL 4)
≥ 99 %	SIL 3 (SIL 3)	SIL 4 (SIL 4)	SIL 4 (SIL 4)
Un SIS peut être considéré du type A si son comportement en présence d'anomalies est bien déterminé, si les modes de défaillance de ses constituants sont bien définis et si les données concernant leurs défaillances, issus du retour d'expérience, sont connus avec une bonne fiabilité. Un SIS peut être considéré du type B si une des trois conditions régissant le type A n'est pas satisfaite.			

- ***Route 2_H : Propagation d'incertitudes.*** Cette seconde procédure est fondée sur le principe de propagation d'incertitudes classique. A ce titre, la norme CEI 61508 stipule que « *Si la route 2_H est choisie, alors les incertitudes relatives aux données de fiabilité doivent être prises en compte lors du calcul de la mesure cible de défaillance (c'est-à-dire PFD_{avg} ou PFH) et le système doit être amélioré jusqu'à ce qu'il y ait une confiance supérieure à 90% que la mesure cible de défaillance est atteinte* » [CEI 61508-2, 2010].

  Pour des raisons d'exhaustivité, nous rappelons brièvement les étapes clés d'une procédure de propagation d'incertitudes en utilisant la méthode de Monte Carlo :

  1. Etablir la distribution de probabilité pour chaque paramètre utilisé (cette distribution reflète les incertitudes attachées à ce paramètre : uniforme, log-normale, …).
  2. Générer aléatoirement une valeur pour chacun des paramètres (selon leurs distributions).
  3. Evaluer la PFD_{avg} ou la *PFH*. La valeur obtenue est une réalisation d'une variable aléatoire *X*.
  4. Répéter les étapes 2 à 3 *n* fois (par exemple, $n = 1000$) produisant *n* valeurs (PFD_{avg} ou *PFH*) indépendantes. Ces valeurs représentent un échantillon aléatoire.
  5. Générer des statistiques à partir de l'échantillon obtenu : moyenne, écart-type, intervalle de confiance, etc.

La confiance selon laquelle la PFD_{avg} ou PFH obtenue appartient à un SIL requis donné peut être établi en vérifiant si la borne supérieure de l'intervalle de confiance ($X_{90\%}$) est incluse dans l'intervalle du SIL requis (tableau 1.1) et au plus égale à la PFD_{avg} ou PFH autorisée (PFD_{avg}^{max} ou PFH^{max}). En outre, une mesure directe de cette confiance est l'évaluation de la fonction de répartition relative à l'échantillon obtenu. Dans le cas de PFD_{avg}, nous pouvons écrire :

$$F\left(PFD_{avg}^{max}\right) = p(X \leq PFD_{avg}^{max}) \quad (1.10)$$

Il convient de préciser que la CEI 61508 maintient des contraintes d'architecture minimales, même si la route 2_H est utilisée (voir tableau 1.3). De plus, elle exige que les composants de type B doivent avoir un DC ≥ 60%. Aussi, pour les éléments de type A uniquement et si l'utilisateur apporte les justifications nécessaires, le HFT peut être réduit de 1 dans le tableau 1.3. Notons que la SFF n'est plus nécessaire.

Tableau 1.3 : Contraintes architecturales sur les SIS dans le cadre de la route 2_H

SIL requis	**HFT**	
	Type A (sans justification) et B (DC ≥ 60%)	**Type A (avec justification)**
1	0	0
2 (PFDavg)	0	0
2 (PFH)	1	0
3	1	0
4	2	1

1.5. Illustration de la démarche de la CEI 61508

Dans ce qui suit, l'approche CEI 61508 est illustrée sur un système réel : un réservoir de stockage de butane, décrit dans la section suivante.

1.5.1. Description du cas d'étude : réservoir de stockage de butane

Le système choisi pour illustrer la démarche de la CEI 61508 fait partie de la section stockage et réfrigération de l'unité GPL du complexe GL1K (Skikda) [SOFREGAZ, 1995]. Cette section reçoit du propane et du butane en provenance de l'unité de séparation, des unités 5P et 6P et de la raffinerie de Skikda (RA1K). Seul le stockage de butane est traité dans ce document. Un schéma simplifié du réservoir de stockage de butane (TK411 : 20000 tonnes)

ainsi que le cycle réfrigérant associé est représenté à la figure 1.10. Le butane est stocké dans le réservoir sous sa forme liquéfiée à –10 °C. Au sein du réservoir, une certaine quantité de butane s'évapore en continu (BOG: *boil-off gas*). Cette évaporation est principalement provoquée par un apport de chaleur externe et/ou des fluctuations de niveaux de liquide (opérations de remplissage et déchargement). En conséquence, cette évaporation peut conduire à une augmentation de la pression à l'intérieur du réservoir. Dans ce qui suit nous allons décrire brièvement les différents niveaux de protection du réservoir vis-à-vis du risque de surpression.

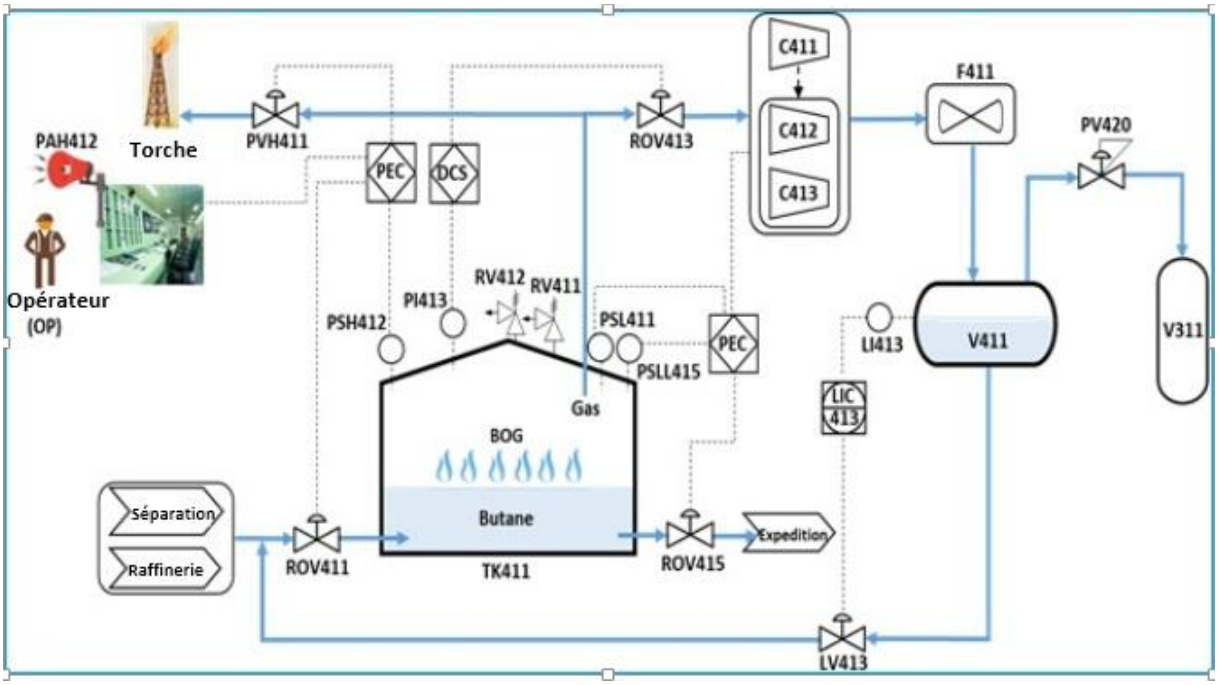

Figure 1.10 : Réservoir de butane et son cycle réfrigérant

- ***Conception du réservoir :*** en vue de prévenir le réchauffement dû à l'air ambiant, le réservoir est composé d'une double cuve et d'un toit suspendu. Des matériaux calorifuges (perlite) occupent l'espace entre les parois extérieure et intérieure. Aussi, de l'azote est injecté entre les parois via la vanne PCV461 (non représentée à la figure 1.10).

- ***Système de régulation de pression :*** ce système permet de maintenir la pression interne limitée aux valeurs de conception en réglant automatiquement la capacité des compresseurs. Selon la classification de la CEI 61508, ce système fonctionne en mode continu. Sa mesure de fiabilité appropriée est donc la *PFH* (fréquence de défaillance). La constitution du système de régulation est son fonctionnement sont donnés ci-après.

- *Système de Contrôle Distribué (DCS) :* il assure le contrôle de la pression à l'intérieur du réservoir en surveillant le signal de l'indicateur de pression (PI413) et en contrôlant le fonctionnement (ouverture et fermeture) de la vanne ROV413 afin de réguler automatiquement la capacité des compresseurs de sorte que la pression dans le réservoir soit comprise entre 25 à 60 mbar.
- *Boucle de réfrigération* : elle permet de récupérer et de liquéfier le BOG. Le butane gazeux arrivant du réservoir (via la vanne ROV413) est comprimé par les compresseurs C411, C412, C413 et condensé au niveau de l'aérocondenseur (F411). Le butane est ensuite envoyé dans un ballon (réservoir V411) avant d'être acheminé à nouveau vers le réservoir de stockage en passant par la vanne LV413. Le niveau du réservoir V411 est réglable automatiquement à mi-hauteur (indicateur de niveau LI413 et contrôleur LIC413). Le gaz non condensable dans le ballon V411 est amené au ballon de détente V311 (section propane) en passant par la vanne auto-régulatrice de pression PV420. Il convient de noter que seuls deux des compresseurs de refroidissement sont en marche, le troisième étant en réserve.

- ***Evacuation d'urgence.*** Dans le cas d'une défaillance du système de régulation, le gaz d'évaporation excédant sera évacué vers la torche pour être brulé. En effet, lorsque la pression dans le réservoir monte au-dessus de 65 mbar, un détecteur haute pression (PSH412) commande l'évacuation du gaz à la torche via la vanne de réglage PVH411 activée par le PEC (programmable electronic controller). Le PEC entraine également la fermeture de la vanne d'alimentation en butane (ROV411). L'alarme (PAH412) se declenche dans la salle de contrôle permettant ainsi à un opérateur (OP) d'effectuer les opérations requises. Il est à noter que le système de torche sera défaillant en cas de défaillance de la vanne d'injection d'azote (PCV 461 non représentée à la figure 1.10), puisque cette défaillance conduit à la présence d'azote à l'intérieur du réservoir. Rappelons que l'azote est injecté entre les parois du réservoir de stockage afin d'éviter son réchauffement dû à l'air ambiant.

  Le système d'évacuation d'urgence fonctionne en mode faible sollicitation selon la classification de la CEI 61508. Cela dit, la PFD_{avg} est sa mesure de fiabilité appropriée. Le but premier de cette illustration est de vérifier sa conformité vis-à-vis des exigences issues de l'analyse des risques.

- ***Soupapes de surpression.*** En ultime secours, en cas de franchissement non contrôlé de la pression au dernier seuil de protection (70 mbar), deux soupapes de sécurité (RV411 et RV412) s'ouvrent et rejettent le gaz directement à l'atmosphère. Le fonctionnement des deux vannes est nécessaire pour dégager la totalité de la suppression.

- ***Système de sécurité contre les basses pressions :*** le réservoir de stockage de butane est équipé de deux détecteurs pour prévenir tout risque du aux basses pressions :
  - *Détecteur basse pression* (PSL411) qui commande l'arrêt automatique des compresseurs et la fermeture de la vanne de soutirage (ROV415), via l'unité logique PEC, lorsque la pression dans le réservoir s'abaisse au-dessous de 20 mbar.
  - *Détecteur très basse pression* (PSLL415) qui engendre les mêmes actions liées au détecteur PSL411 lorsque la pression dans le réservoir s'abaisse au-dessous de 15 mbar. Ces deux détecteurs n'ont pas un lien direct avec la surpression, mais leurs fonctionnements intempestifs peuvent la provoquer suite à l'arrêt non souhaité des compresseurs.

1.5.2. Analyse et évaluation des risques

Comme nous l'avons déjà signalé, la première étape dans la démarche de la CEI 61508 consiste en une analyse et évaluation des risques permettant d'identifier et de quantifier les dangers potentiels du système étudié (réservoir de butane dans notre cas). Pour ce faire, nous avons d'abord mis à profit la méthode HAZOP qui représente un outil formalisé s'appuyant sur l'analyse des déviations des paramètres caractéristiques du système (débit, pression, température, etc.) dans le but d'identifier les situations conduisant à des accidents (conséquences). Un extrait de l'étude HAZOP relative à la déviation « *plus de pression à l'intérieur du réservoir* » est donné au tableau 1.4.

Tableau 1.4 : Extrait des tableaux HAZOP

Déviation	N°	Cause	Conséquences	Barrières	Cotation	
					G	**P**
Plus de pression à l'intérieur du réservoir	1	Plus de débit à l'entrée du bacTK411	-Perte de confinement par montée en pression critique dans le bac de stockage -Feu de nappe, VCE, flash fire	-Compresseurs C411, C412 et C413 permettant de réguler la pression dans le bac de stockage -Sécurité sur pression haute dans le bac TK411 (PSH 412) entrainant la décompression automatique du bac vers le circuit de torche (ouverture de la vanne PVH411) et la fermeture de la vanne d'alimentation ROV411	4	3

				-Soupapes RV411 et RV412 tarées à 0.07 bar relatif		
	2	Présence de légers dans le butane	Idem que conséquence n°1	Idem que barrières n°1	4	3
	3	Défaillance du système de régulation de pression (soutirage insuffisant ou nul des compresseurs)	Idem que conséquence n°1	Idem que barrières n°1 à l'exception des compresseurs	4	3
	4	Isolation thermique défaillante	Idem que conséquence n°1	Idem que barrières n°1	4	3
	5	Défaillance de la vanne de régulation de pression d'azote vers l'inter-paroi (vanne PCV461 bloquée ouverte)	-Passage d'azote dans la cuve interne provoquant une montée en pression -Extinction de la torche en cas d'ouverture de la vanne PVH 411 due à la présence d'azote dans le gaz	Idem que barrières n°1 à l'exception du circuit de torche	1	5

Les échelles de gravité et de fréquence utilisées sont données respectivement dans les tableaux 1.5 et 1.6.

Tableau 1.5 : Gravité des conséquences d'événements dangereux

Niveau de gravité	**Zone délimitée par le seuil des effets létaux significatifs (SELS)**	**Zone délimitée par le seuil des effets létaux (SEL)**	**Zone délimitée par le seuil des effets irréversibles sur la vie humaine (SEI)**
5. Désastreux	Plus de 100 personnes exposées	Plus de 1000 personnes exposées	Plus de 10 000 personnes exposées
4. Catastrophique	Entre 10 et 100 personnes exposées	Entre 100 et 1000 personnes exposées	Entre 1 000 et 1 0000 personnes exposées
3. Important	Entre 1 et 10 personnes exposées	Entre 10 et 100 personnes exposées	Entre 100 et 1 000 personnes exposées
2. Sérieux	Au plus 1 personne exposée	Au plus 10 personnes exposées	Entre 10 et 100 personnes exposées
1. Modéré	Aucune personne exposée	Au plus 1 personne exposée	Moins de 10 personnes exposées

Tableau 1.6 : Fréquence d'occurrence d'événements dangereux

Echelle	**1**	**2**	**3**	**4**	**5**
Qualitative	*Possible mais extrêmement improbable*	*Très faible*	*Faible*	*Modérée*	*Elevée*
Quantitative (par an)	$F < 10^{-5}$	$10^{-4} > F > 10^{-5}$	$10^{-3} > F > 10^{-4}$	$10^{-2} > F > 10^{-3}$	$F > 10^{-2}$

Afin d'apprécier l'ampleur des conséquences, nous donnons dans la figure 1.11 les zones d'effets liés aux scenarios «*feu de nappe*» et «*flash fire*» obtenues à l'aide du logiciel ALOHA [EPA et NOAA, 2006].

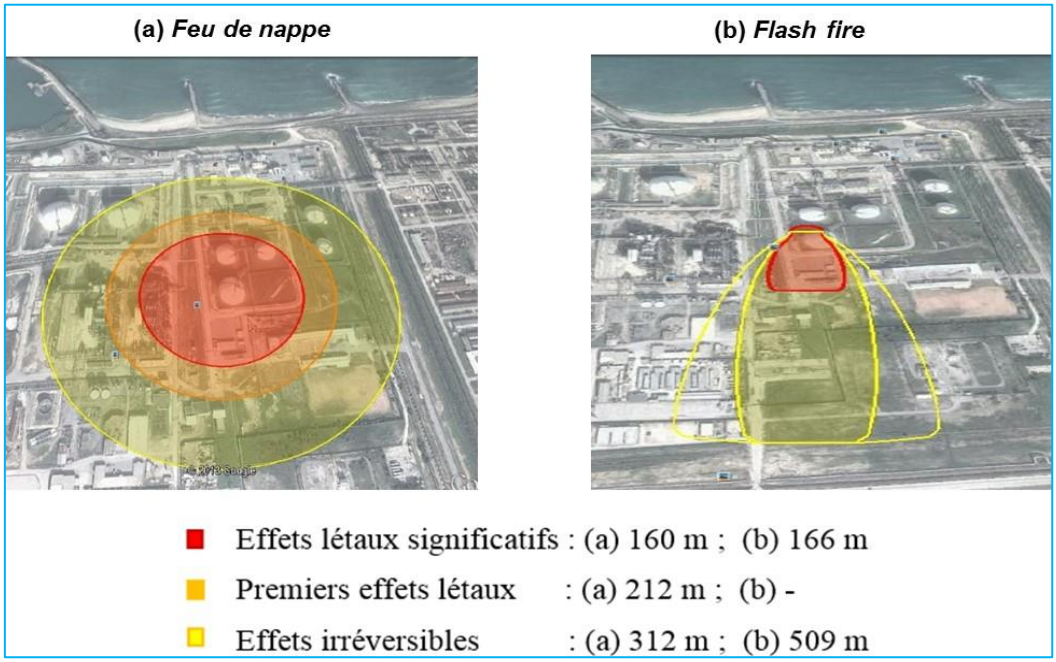

Figure 1.11 : Zones menacées par les effets thermiques

1.5.3. Allocation du niveau d'intégrité de sécurité (SIL requis)

1.5.3.1. Méthode qualitative : graphe de risque

Dans ce qui suit, ne nous nous intéressons qu'à la cause N°3 de la déviation considérée : *défaillance du système de régulation de pression*. Comme nous l'avons déjà mentionné, sa mesure de performance appropriée est la *PFH*. La fréquence d'une telle défaillance (la défaillance d'une boucle de contrôle) est généralement considérée comme élevée (W_3). L'analyse des risques, basée sur le tableau 1.5 et la figure 1.11, a indiqué que les événements

dangereux potentiels peuvent entraîner plusieurs blessures graves (C_B). La fréquence d'exposition est très élevée du fait de l'ampleur des distances d'effets et de la présence permanente de personnes à l'intérieur de ces zones, donc F_B. Aussi, la possibilité d'éviter les effets de l'accident est quasiment nulle, puisque les accidents sont à cinétique rapide (P_B). L'utilisation conjointe de ces paramètres d'entrée (C_B, F_B, P_B et W_3) et la figure 1.8 conduit à un **SIL3** (SIL requis). Cette méthode est simple à utiliser, mais le SIL requis obtenu peut facilement varier d'un niveau à cause des incertitudes liées aux données. Par conséquent, la cohérence des résultats dépend fortement de l'expertise des analystes.

1.5.3.2. Méthode semi-quantitative : LOPA

Cette méthode est plus précise et donc plus fiable si les données numériques liées aux évènements initiateurs et défaillances des barrières de sécurité sont disponibles. Pour l'étude de cas considérée, nous avons les éléments suivants :

- Basé sur une matrice de risque de l'entreprise, la fréquence tolérable correspondant à un événement dangereux de gravité 4 est défini à 1E-5/an.
- L'événement initiateur est la défaillance du système de régulation de pression composé de trois boucles de contrôle (DCS, PEC (arrêt intempestif des compresseurs) et LIC413), trois compresseurs (C411, C412 et C413), l'aérocondenseur F411 et le régulateur autonome de pression PV420. La fréquence de défaillance d'une seule boucle de contrôle est en moyenne prise égale à 1E-1/an. La même valeur peut être attribuée à la vanne PV420. Le retour d'expérience montre que le bloc compresseur défaille presque une fois chaque 5 ans (≈ 2E-1/an), tandis que l'aérocondenseur tombe en panne presque deux fois au cours de la même période (≈ 4E-1/an). Comme les éléments du système de régulation de pression sont en série, la fréquence totale est obtenue en additionnant leurs fréquences correspondantes : f_{IE} = 1/an.
- Les barrières de sécurité non-instrumentées qui interviennent afin d'empêcher le développement de cette surpression en un accident sont l'action de l'opérateur (OP) (averti par l'alarme PAH412) et les deux soupapes de sécurité (RV411 et RV412). Toutefois, aucun crédit n'est accordé à l'action de l'opérateur, car en effet cette barrière possède deux éléments en commun avec le système instrumenté de sécurité (PSH412, PEC). Donc, cette barrière ne respecte pas la condition d'indépendance. Seules les deux soupapes sont à considérer dans ce qui suit. La probabilité moyenne de défaillance d'une soupape est estimée à 1E-2. De plus, l'ouverture des deux soupapes est nécessaire afin

que la surpression soit évacuée à l'atmosphère. Cela dit, la probabilité moyenne de défaillance des deux soupapes $PFD_{soupapes} \approx$ 2E-2.

- Le facteur d'atténuation supplémentaire considéré est la probabilité d'ignition supposée être égale à 6E-1.

L'équation (1.6) permet d'écrire :

$$f_C = 1.2E-2.6E-1 = 1.2E-2/an \quad (1.11)$$

Cette valeur est bien supérieure à la valeur maximale autorisée (1E-5/an). Une réduction supplémentaire de cette fréquence s'impose donc. Evidemment, cette réduction est réalisée par le système instrumenté de sécurité (évacuation d'urgence), qui doit avoir une probabilité moyenne de défaillance maximale déterminée conformément à l'équation (1.8) :

$$PFD_{avg}^{max} = 1E-5/1.2E-2 = 8.33E-4 \quad (1.12)$$

La lecture de cette valeur au niveau du tableau 1.1 donne un SIL3. Notons que ce résultat est celui obtenu par la méthode graphe de risque. Néanmoins, la méthode LOPA est plus précise car elle fournit la PFD_{avg} maximale autorisée : 8.33E-4. Si l'on se réfère uniquement au résultat du graphe de risque, cette valeur serait prise égale à une valeur approchant la borne supérieure de l'intervalle correspondant au SIL3, par exemple : 9.99E-4. On peut remarquer que le résultat de LOPA est plus restrictif (donc conservatif) que celui induit par le graphe de risque.

1.5.3.3. Méthode quantitative : arbre de défaillances

La méthode LOPA s'appuie sur des valeurs génériques issues du retour d'expérience, d'où la nomination semi-quantitative. Elle ne tient pas compte de l'architecture et du type des éléments concernés : redondance, taux de défaillance, temps de réparation, tests, etc. Dans la suite nous allons exploiter la méthode arbre des défaillances (AdD) afin de fournir un résultat plus crédible quant à la fréquence d'accident. L'AdD correspondant est donné à la figure 1.12.

Les différents taux de défaillance (λ) utilisés sont groupés au tableau 1.7. Ces données sont issues de bases de données reconnues [SINTEF, 2006 ; OREDA, 2002] et les données spécifiques de l'usine. Nous supposons que les différents composants possèdent le même taux de réparation μ = 1/8 = 0.125 h^{-1}.

Il convient de préciser que le comportement dysfonctionnel des trois compresseurs ne peut être rendu correctement à l'aide de l'AdD (événement #4 de la figure 1.12) du fait de la

dépendance induite par la mise en attente de l'un des compresseurs. Pour y remédier, nous mettant à profit le graphe Markovien de la figure 1.13.

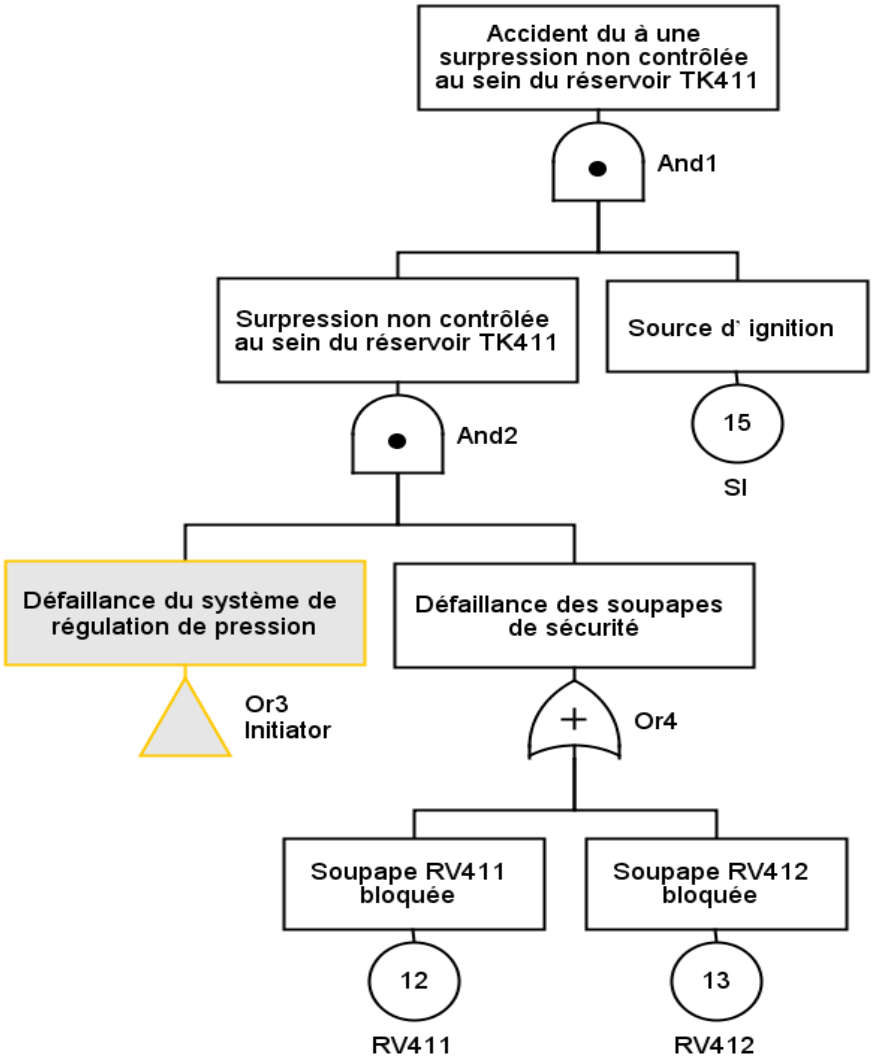

Figure 1.12 : AdD relatif à l'évènement indésirable « *Accident due à une surpression non contrôlée au sein du réservoir TK411* ».

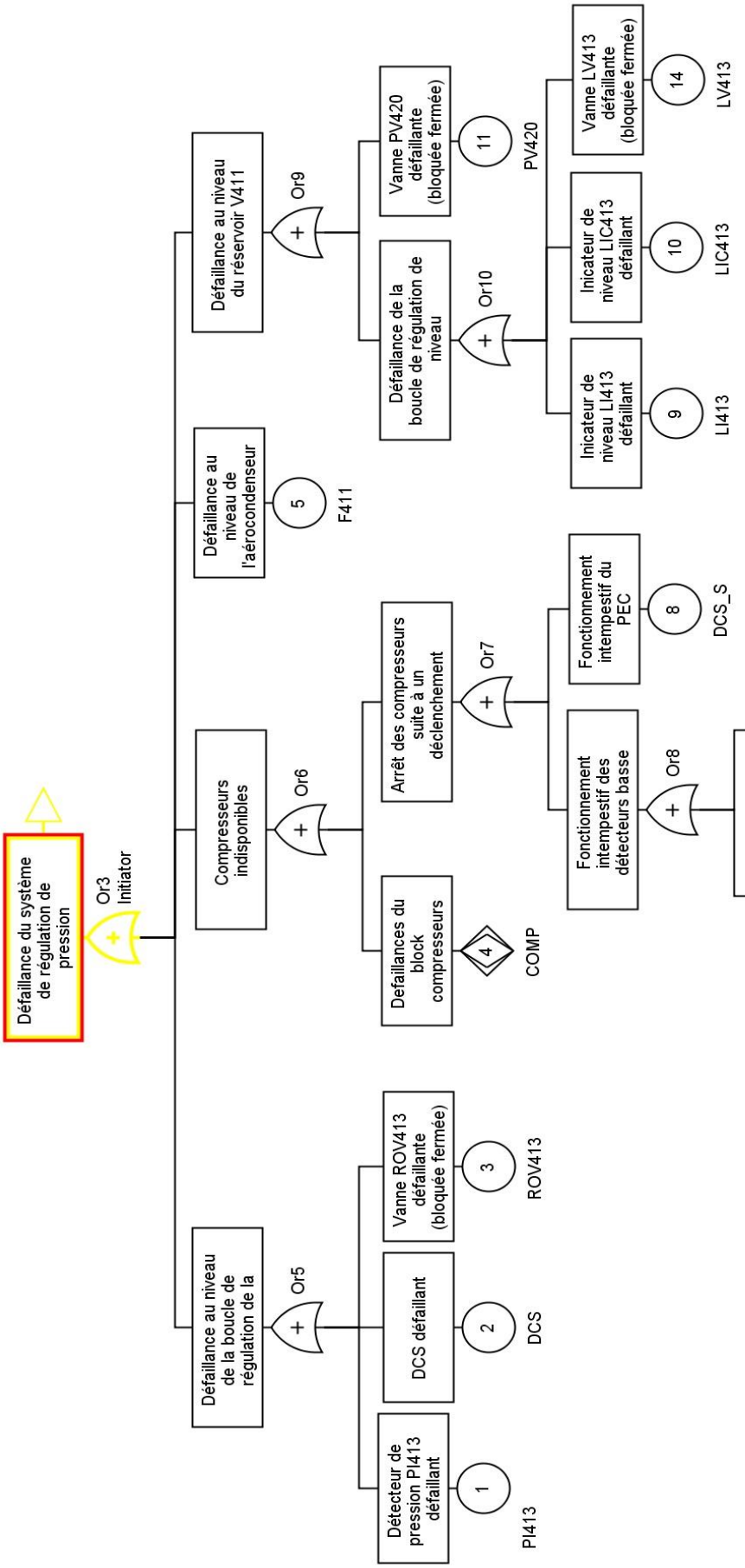

Figure 1.12 : (suite)

Tableau 1.7 : Les différents taux de défaillance

Composant	λ (h^{-1})	Composant	λ (h^{-1})
PI413	5E-6	LI413	6.3E-6
PSL411	1.1E-6	LIC413	2E-5
PSLL415	1.1E-6	ROV413	2.1E-6
DCS	1.5E-5	LV413	4.3E-6
PEC _S	1E-5	PV420	1E-5
C411 C412 C413	2.5E-4	Deux compresseurs sont en fonctionnement. Le troisième étant en attente. Il démarre automatiquement des que l'un des deux premiers tombe en panne. Sa probabilité de refus de démarrage G = 0.01. Il existe également une possibilité de défaillance commune entre les compresseurs : β = 0.1.	
FV411	5E-5		
RV411 RV412	2.9E-6	Ces défaillances ne sont révélées que lors des tests périodiques effectués chaque six mois (4380 *h*).	
IS	0.6	Probabilité constante pour la source d'ignition.	

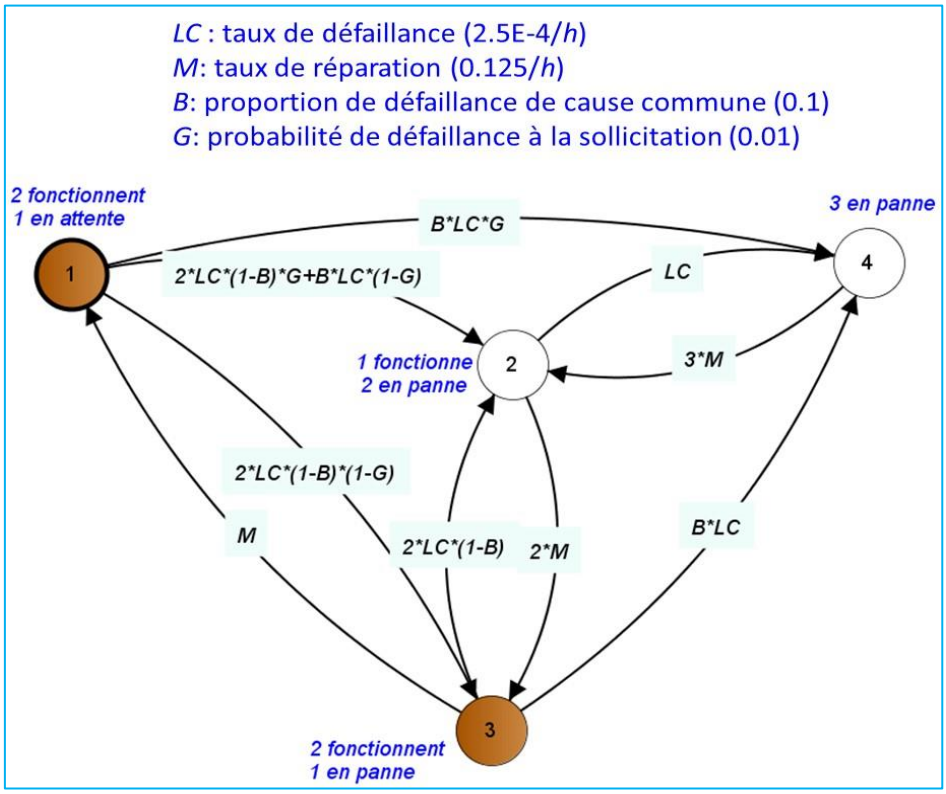

Figure 1.13 : Modèle markovien relatif aux compresseurs

La fréquence de l'accident est calculée à partir de l'arbre de défaillance précédent en utilisant les formules suivantes :

$$\begin{cases} f_C(t) = f_{And1}(t) = f_{And2}(t) \cdot P_{IS}(t) \\ f_{And2}(t) = f_{Or3}(t) \cdot p_{Or4}(t) \\ p_{Or4}(t) = p_{RV411}(t) + p_{RV412}(t) - p_{RV411}(t) \cdot p_{RV411}(t) \end{cases} \quad (1.13)$$

Où :

$$p_{RVi}(t) = 1 - e^{-\lambda_i \cdot \left[t - Int\left(\frac{t}{T}\right) \cdot T\right]} \quad (1.14)$$

T est l'intervalle du test périodique et *Int* () fournit la partie entière. L'équation (1.14) représente la probabilité de défaillance d'un composant dont les défaillances sont révélées par le test périodique. $f_{Or3}(t)$, qui représente la fréquence de défaillance du système de régulation de pression, est dérivée à partir de la relation suivante [Dutuit et Rauzy, 2005] :

$$f_{Or3}(t) = \sum I_{Bi}(t) \cdot w_i(t) = \sum I_{Bi}(t) \cdot A_i(t) \cdot \lambda_i \quad (1.15)$$

Dans l'équation (1.15), $I_{Bi}(t)$, $w_i(t)$ et $A_i(t)$ correspondent, respectivement, au facteur d'importance de Birnbaum [Birnbaum, 1969], la fréquence de défaillance (intensité de défaillance inconditionnelle) et la disponibilité du composant *i* au temps *t*. $I_{Bi}(t)$ est obtenu comme suit :

$$I_{Bi}(t) = p_{Or3/(i=failed)} - p_{Or3/(i=operational)} \quad (1.16)$$

Les différentes disponibilités, $A_i(t)$, sont données par la formule connue suivante:

$$A_i(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} \cdot e^{-(\lambda+\mu)\cdot t} \quad (1.17)$$

Pour l'événement # 4 de la figure 1.12, c'est-à-dire COMP, nous calculons directement son *w* (t) à partir du graphe markovien grâce à l'équation (1.18) :

$$w(t) = \sum_{i \in WS} P_i(\infty) \cdot \sum_{i \in FS} \lambda_{i \to j} \quad (1.18)$$

Où *WS* signifie "états de marche : *working states*" et *FS* signifie "états de pannes : *failed states*". En outre, $\lambda_{i \to j}$ représente le taux de défaillance partant d'un état de marche et arrivant dans un état de panne. Pour notre cas, l'équation (1.18) permet d'écrire :

$$w_{COMP}(t) = p_1(t) \cdot [2\lambda_C(1-\beta)\gamma + \beta\lambda_C(1-\gamma) + \beta\lambda_C\gamma] + p_3(t) \cdot [2\lambda_C(1-\beta) + \beta\lambda_C] = \lambda_C \cdot [p_1(t) \cdot (2\gamma - 2\beta\gamma + \beta) + p_3(t) \cdot (2-\beta)] \quad (1.19)$$

$p_1(t)$ et $p_3(t)$ sont les probabilités d'être dans les états 1 et 3, respectivement.

En se basant sur l'ensemble des équations précédentes, le calcul de la fréquence de l'accident a été effectué à l'aide du logiciel GRIF [GRIF, 2020]. La fréquence de l'accident obtenue s'élève a : 1.032E-2 / an. Cette valeur est supérieure à la valeur de seuil (1E-5 / an). Par conséquent, une réduction de risque est nécessaire. Elle doit être assurée par le système d'évacuation d'urgence dont la PFD_{avg} ne doit pas dépasser 1E-5/1.032E-2 = 9.690E-4. Ce résultat correspond également à un SIL3.

Les trois méthodes précédentes ont conduit au même SIL requis : SIL3. Toutefois, les valeurs correspondantes à la PFD_{avg} maximale diffèrent légèrement. L'approche LOPA a fourni le résultat le plus contraignant, tandis que le graphe de risque a donné la valeur la moins exigeante. Cette conclusion est propre à notre cas d'étude et ne doit en aucun cas être généralisée.

1.5.4. Evaluation du SIL du système d'évacuation d'urgence

Le but de cette étape est la détermination du SIL effectif du système instrumenté de sécurité, constitué des éléments suivants : PSH412, PEC, PVH411, torche (défaillance de la pompe d'injection d'azote (PCV461), PAH412 et l'opérateur). Nous supposons que l'ensemble des prescriptions qualitatives (défaillances systématiques) permet d'atteindre les spécifications d'intégrité de sécurité systématique liées au SIL requis identifié précédemment (SIL3). Reste donc à vérifier les prescriptions complémentaires et probabilistes. Les différentes données de fiabilité utilisées sont regroupées dans le tableau 1.8, où λ_{DU} représente le taux des défaillances révélées lors des tests périodiques et λ_{DD} représente le taux des défaillances détectées immédiatement suite à leur occurrence. Les probabilités de défaillance correspondantes sont respectivement données par l'équation (1.14) et le complément de l'équation (1.17).

Tableau 1.8 : Données de fiabilité relatives au système d'évacuation d'urgence

Composant	**λ_{DU} (h^{-1})**	**Tests (h)**	***SFF* (%)**	**Type**
PSH412	3E-7	4380	75	A
PEC	1E-6	8760	95 ; DC = 90 %	B
PVH411	2.8E-6	4380	62	A
PCV461 (torche)	λ_{DD} = 8E-7 h^{-1} (défaillance détectée), μ = 0.125 h^{-1}		70	A
PAH412	6E-6	4380	50	A
OP	1E-2 (probabilité constante)			

1.5.4.1. Quantification de la PFD_{avg}

La quantification de la PFD_{avg} est effectuée à l'aide de l'arbre de défaillances illustrée à la figure 1.11. Comme mentionné précédemment, la CEI 61508 fournit un ensemble de formules simplifiées pour certaines configurations spécifiques afin d'effectuer cette quantification sous plusieurs hypothèses spécifiques. Cependant, la méthode arbre de défaillance est plus précise en raison de son large domaine de validité [Innal, 2008].

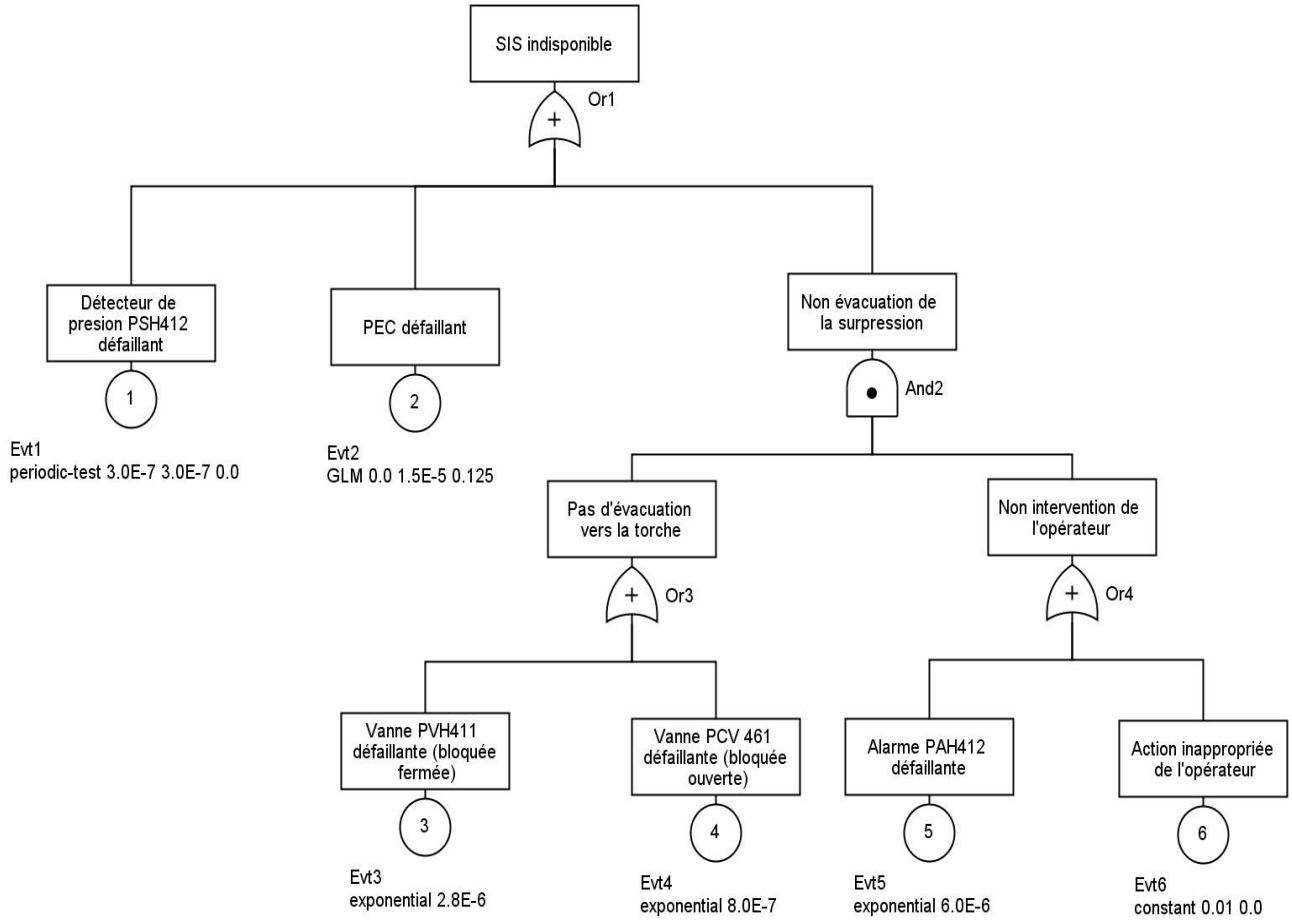

Figure 1.14 : AdD relatif à l'indisponibilité du SIS (système d'évacuation d'urgence)

La PFD_{avg} issue de cet AdD est 3.01E-3. Cette valeur est supérieure aux valeurs cibles obtenues précédemment avec les méthodes graphe de risque (9.99E-4), LOPA (8.33E-4) et AdD (9.690E-4). Elle correspond à un SIL2. Par conséquent, la fonction de sécurité fournie par le SIS ne peut être en mesure d'assurer la réduction nécessaire du risque afin d'atteindre le niveau tolérable. La PFD_{avg} peut être réduite, entre autres, en limitant l'intervalle de tests périodiques à un mois (730 h) au lieu de six mois (4380 h) : PFD_{avg} = 4.88E-4. Cette nouvelle valeur est conforme à l'ensemble des exigences précédentes. Une autre possibilité d'amélioration consiste

à créer une redondance en ajoutant un deuxième capteur de pression et une deuxième unité PEC. Cela conduit à une PFD_{avg} = 2.01E-4. Cette valeur est obtenue avec un facteur de cause commune β = 0.01 pour les deux : capteurs de pression et unités PEC [Chebila et Innal, 2014].

1.5.4.2. Contraintes d'intégrité de sécurité matérielle

Comme déjà mentionné, nous avons le choix entre deux alternatives :

- ***Route*** $\mathbf{1_H}$ **:** *contraintes architecturales*. L'utilisation conjointe des tableaux 1.2 et 1.8 permettent de définir le SIL pour les différents composants du SIS tel qu'il est présenté dans la figure 1.15. Notons que le SIL affecté à l'opérateur (OP) est directement déduit du tableau 1.1 en se basant sur la probabilité correspondante (tableau 1.8). Certaines règles de fusion sont nécessaires pour comprendre la dérivation du SIL pour *n* éléments : le SIL minimal pour les éléments en série et le SIL maximal + (*n* – 1) pour les éléments en parallèles (voir [CEI 61508-2] pour plus de détail). Le SIL global du SIS étudié est donc SIL2. Cela signifie que l'amélioration de l'architecture du SIS est nécessaire pour atteindre le SIL requis (SIL3). Afin d'augmenter le SIL global du SIS, il est nécessaire d'améliorer son maillant faible (bloc capteur + PEC). En s'appuyant sur le tableau 1.2, l'ajout d'un deuxième capteur de pression et d'une deuxième unité logique PEC (redondance) est requis afin d'atteindre le SIL3. Il est à noter que la première option utilisée pour réduire la PFD_{avg} (réduction de l'intervalle de test périodique) n'aura aucun impact positif sur les contraintes architecturales, car le SIL correspondant reste toujours SIL2.

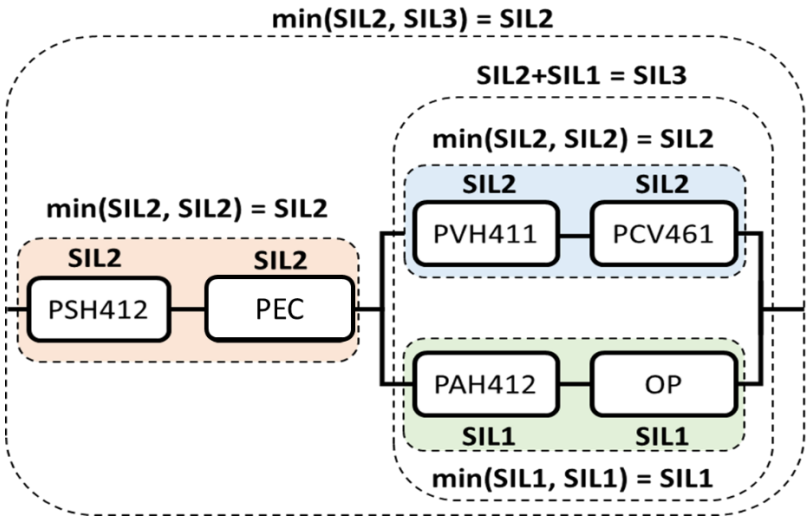

Figure 1.15 : Contraintes architecturales relatif au SIS (route 1_H)

- ***Route* 2_H :** *propagation d'incertitudes*. Cette procédure, rappelons-le, nécessite la prise en compte des incertitudes entachant les différents taux de défaillances. Néanmoins, certaines contraintes et conditions sont à respecter (voir la fin du paragraphe 1.4.3). Les conditions mentionnées sont satisfaites : le DC du PEC (type B) = 90 % > 60%. Aussi, nous supposons qu'il existe les justifications nécessaires pour l'ensemble des composants type A. Le tableau 1.3 nous permis ainsi de calculer le SIL correspondant (voir figure 1.16) : SIL2. Encore une fois, l'amélioration de l'architecture du SIS est nécessaire pour atteindre le SIL requis (SIL3). Cela peut être obtenu en ajoutant seulement une deuxième unité logique PEC (redondance), car son SIL (SIL2) limite le SIL global obtenu.

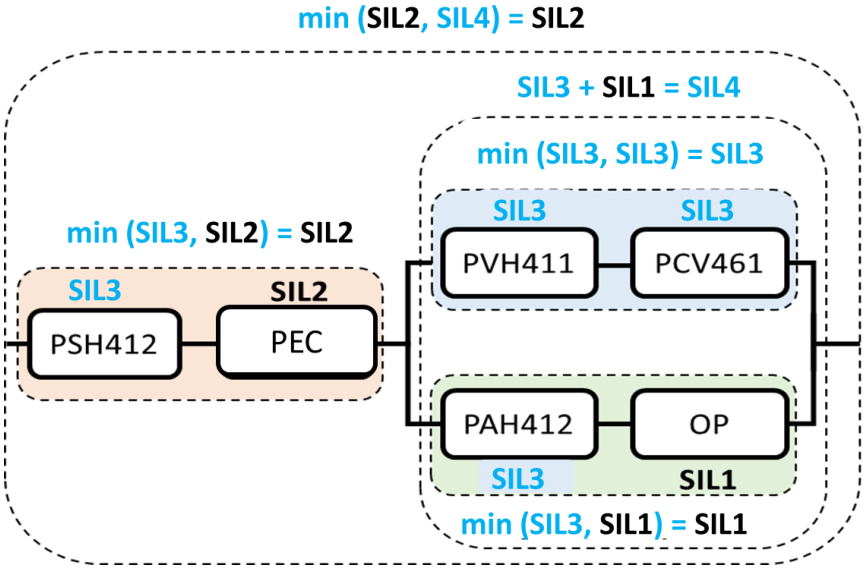

Figure 1.16 : Contraintes architecturales relatif au SIS (route 2_H)

Par ailleurs, afin de rendre compte des incertitudes entachant les différents taux de défaillances des composants, nous supposons qu'ils peuvent varier selon une distribution log-normale (*m*, *FE*) : le taux de défaillance est inclus dans l'intervalle [*m/FE*, m. *FE*], *m* se réfère aux valeurs moyennes données au tableau 1.8 et *FE* est le facteur d'erreur. Nous le fixant dans notre cas à 5 (valeur conservative). En modifiant l'AdD de la figure 1.14 par l'ajout d'un deuxième PEC (facteur de cause commune β = 0.01), le logiciel GRIF nous a fourni l'intervalle de confiance [0%, 90%] relatif à la PFD_{avg} (1E +5 itérations) = [9.009E-5, 1.771E-3]. La figure 1.17 décrit la *PFD* dépendant du temps et les incertitudes associées.

La borne supérieure de l'intervalle de confiance (1.771E-3) appartient à la zone SIL2 (voir tableau 1.1). Donc, elle n'est pas conforme aux exigences du SIL requis identifié (SIL3). Cela

étant, une amélioration supplémentaire du SIS s'impose. Si l'on réduit le l'intervalle entre tests périodique du composant PSH412, on obtient l'intervalle de confiance suivant : [4.061E-5, 6.267E-4]. La borne supérieure de cet intervalle correspond à la zone SIL3 et est inférieure aux PFD_{avg} maximales admissibles données par les méthodes graphe de risque (9.99E-4), LOPA (8.33E-4) et AdD (9.690E-4). Compte tenu de cette seconde amélioration, la fonction de sécurité assurée par le SIS répond donc aux exigences du SIL requis.

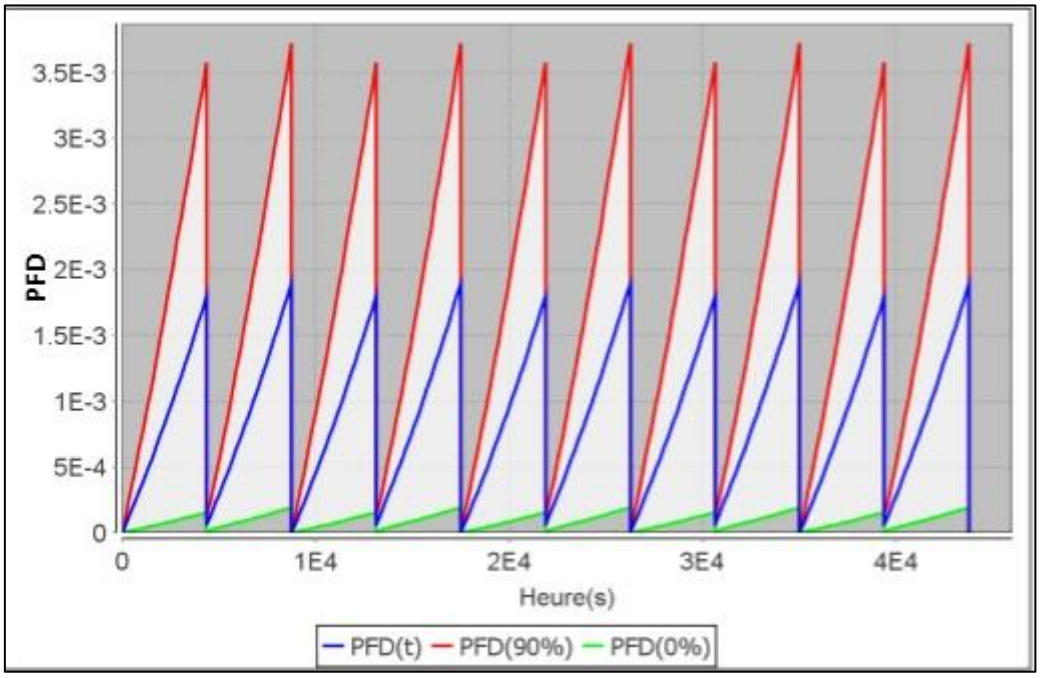

Figure 1.17 : *PFD*(*t*) relative au SIS et les incertitudes associées

1.6. Conclusion

L'objectif de ce premier chapitre était d'abord de rappeler certaines notions de base relatives à la sécurité d'une manière générale, et à la sécurité fonctionnelle plus particulièrement. Ensuite, nous avons mis en exergue l'approche de la norme CEI 61508 dédiée à la sécurité fonctionnelle et ayant pour objet principale la maitrise des risques des évènements dangereux associés aux équipements contrôlés en utilisant des barrières de sécurité instrumentées (SIS).

Nous avons dans un premier temps introduit ses principales étapes : analyse et évaluation des risques, détermination de la réduction du risque affectée au SIS (SIL requis) et évaluation de la performance réelle de ce dernier (SIL réel). Pour chacune de ces étapes, nous avons présentés succinctement les lignes directrices associées en s'appuyant sur la CEI 61508. Ensuite, nous l'avons illustré sur un système consistant en un réservoir de butane situé au niveau de l'unité GPL du complexe GNL1K (Skikda). Plus précisément, nous avons d'abord décrit le fonctionnement des différentes barrières de sécurité intervenant pour empêcher toute surpression au sein du réservoir. L'illustration a été poursuivie par une analyse des risques conduite à l'aide de la méthode HAZOP. Elle a montré que la défaillance du système de régulation de pression du réservoir constitue une source importante pour le déclenchement du processus accidentel. Ensuite, l'application de trois méthodes de détermination de la réduction nécessaire du risque (graphe de risque, LOPA et AdD), qui doit être assurée par le système d'évacuation d'urgence (SIS), a aboutie au même SIL (SIL3), bien que les valeurs cibles relative à la PFD_{avg} (PFD_{avg}^{max}) diffèrent légèrement. Finalement, l'évaluation de la performance du SIS en termes de PFD_{avg} et de contraintes d'architectures a montré que le système d'évacuation d'urgence n'est pas conforme aux exigences du SIL3. A ce titre, certaines modifications ont été proposées, entre autres : tests périodiques plus fréquents, ajout d'un deuxième détecteur haute pression et l'installation d'une deuxième unité logique dédiée à la sécurité (PEC).

Chapitre 2

Vérification de la validité des formules de la CEI 61508 relatives à la PFH à l'aide des graphes de Markov

2.1. Introduction

Comme nous l'avons étalé au chapitre précédent, les SIS jouent un rôle primordial dans la protection des personnes, des biens et de l'environnement contre les évènements dangereux générés par les installations industrielles. Il est donc important d'évaluer leurs indicateurs de performance d'une manière adéquate et suffisamment précise. Pour ce faire, rappelons-le, la norme CEI 61508 considère deux mesures de fiabilité : (*i*) la probabilité moyenne de défaillance dangereuse à la sollicitation (*PFD*) et (*ii*) la probabilité de défaillance dangereuse par heure (*PFH*). Ce chapitre concerne exclusivement la *PFH* qui représente la fréquence de défaillance d'un SIS fortement ou continuellement sollicité.

La norme CEI 61508 (deuxième édition) fournit dans son volume 6 des formules analytiques relatives à la mesure de *PFH* pour certaines configurations *KooN* : 1oo1, 1oo2, 2oo2, 1oo3 et 2oo3. Ces formules ont été dérivées, sans aucune explication, sous l'hypothèse selon laquelle le SIS met l'équipement à protéger (*EUC*) dans un état de repli de sécurité (*shutdown*) suite à la détection d'une défaillance dangereuse du SIS. Il convient de noter que la prise en compte de cette hypothèse est tout à fait logique et donc justifiée, car en effet une défaillance dangereuse empêche le SIS d'accomplir sa fonction de sécurité. Ainsi, un SIS fonctionnant en forte demande ou en demande continue doit avoir une capacité d'arrêt d'urgence automatique afin d'éviter toute situation dangereuse immédiate.

L'objectif principal assigné à ce chapitre est de vérifier la validité des formules de la norme CEI 61508 relatives à la *PFH* en mettant à profit des modèles markoviens multi-phases et classiques. Pour ce faire, le reste de ce chapitre est organisé comme suit. Tout d'abord, les différents paramètres et concepts utilisés sont présentés pour mieux comprendre les différentes formulations analytiques. Ensuite, les formules fournies par la CEI 61508 sont rappelées et comparées aux nouvelles formules obtenues à l'aide des modèles markoviens. En effet, les chaines de Markov constituent une approche pratique permettant d'établir des expressions analytiques relatives à la *PFH* pour les configurations considérées. En outre, les divergences entre les formules nouvellement dérivées et celles données par la CEI 61508 sont explicitées. Finalement, de différentes comparaisons des résultats numériques issus des formules de la CEI 61508, des modèles markoviens et des nouvelles formules établies sont conduites.

2.2. Concepts et paramètres utilisés

Pour une meilleure compréhension des différentes formules analytiques fournies dans ce chapitre, nous présentons d'abord les différents paramètres qui s'y associent.

2.2.1. Configuration ou architecture *KooN*

Chaque sous-système du SIS (S, LS, FE) peut être considéré comme une configuration *KooN* (Figure 2.1) : le fonctionnement de *K* canaux identiques parmi *N* est nécessaire pour qu'un sous-système fonctionne. C'est-à-dire que la défaillance de *N*–*K*+1 canaux entraîne la défaillance du sous-système. Cela dit, une configuration *KooN* met automatiquement l'équipement à protéger (EUC) dans un état sûr lors de la détection de *N*–*K*+1 défaillances. Cette capacité de détection est traitée dans le paragraphe suivant.

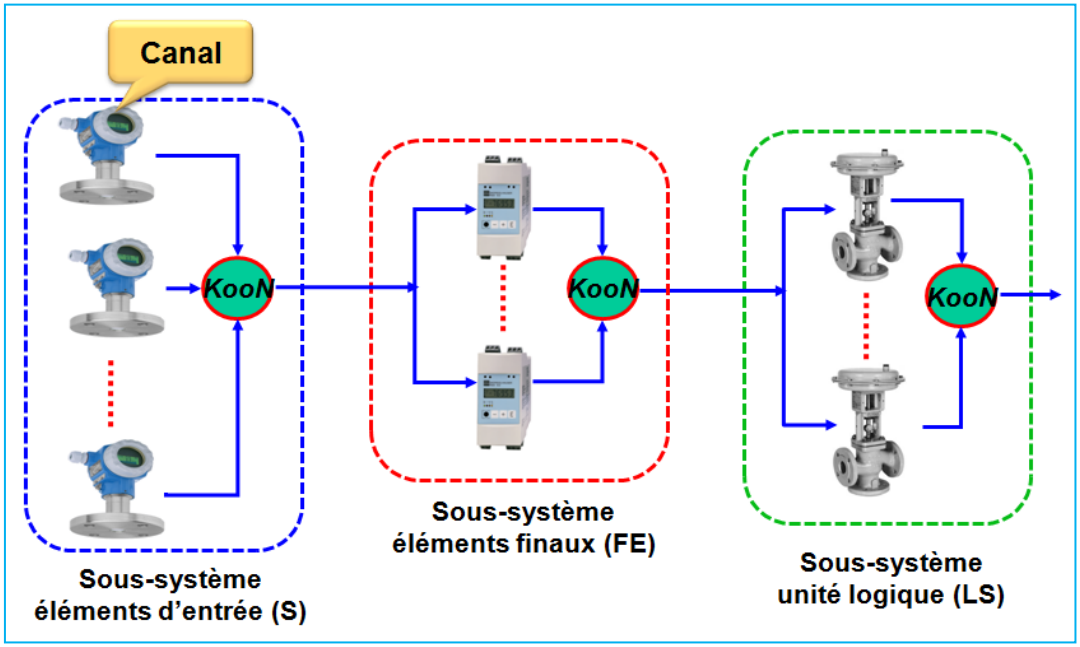

Figure 2.1 : Configuration *KooN*

2.2.2. Classification des défaillances

La quantification de la *PFH* est faite sur la base des défaillances Dangereuses (D) aléatoire du matériel [CEI 61508, 2010], caractérisée par un taux de défaillance constant λ_D. Ces défaillances sont divisées davantage en défaillances dangereuses détectées (DD) et défaillances dangereuses non détectées (DU). Cette nouvelle partition est caractérisée par les taux de défaillances définis ci-après.

$$\begin{cases} \lambda_{DD} = DC.\lambda_D \\ \lambda_{DU} = (1 - DC).\lambda_D \end{cases} \quad (2.1)$$

Où *DC* représente la couverture de diagnostic : $0 \leq DC \leq 1$.

Par ailleurs, les défaillances DD sont annoncées immédiatement par les tests de diagnostic et restaurées dans un temps moyen noté *MTTR* (*Mean Time to Restoration*). *DC* représente la couverture de diagnostic : la capacité du canal à détecter en ligne les défaillances dangereuses. Les défaillances DU sont plus critiques, car elles restent cachées jusqu'au prochain test périodique (intervalle entre deux tests périodiques consécutifs = T_1). Une fois détectée, une défaillance DU est réparée dans un temps moyen de réparation *MRT* (*Mean Repair Time*). La figure 2.2 explicite ces dernières considérations et fournie les profils de l'indisponibilité $Q(t)$ obtenus dans le cas d'un seul canal.

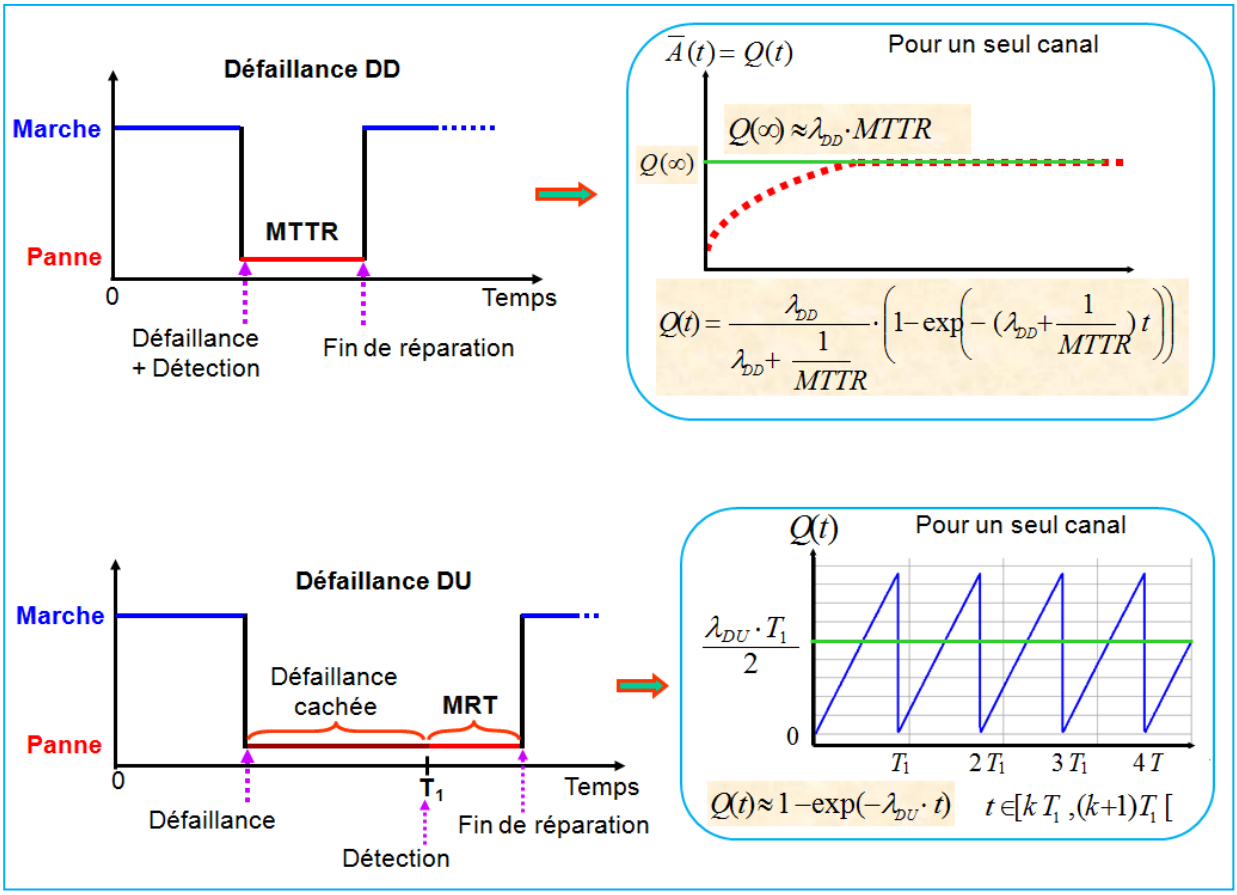

Figure 2.2 : Processus de réparation des défaillances DD et DU

2.2.3. Défaillances de cause commune (DCC)

Une DCC (*CCF : Common Cause Failure*) est le résultat d'un événement qui affecte simultanément plusieurs ou tous les éléments d'un système redondant, ce qui entraîne la perte de la fonction requise. Le modèle du facteur β [Hokstad et Rausand, 2008 ; Chebila et Innal, 2014] est utilisé dans ce document pour caractériser les DCC, d'autant plus qu'il est suggéré dans la norme CEI 61508. Selon ce modèle, le taux de défaillance total (λ) d'un composant est décomposé en deux contributions : indépendante (*ind*) et dépendante (*DCC*) :

$$\lambda = \lambda^{ind} + \lambda^{DCC} = (1-\beta)\lambda + \beta\lambda \qquad (2.2)$$

Avec : $\beta = \lambda^{DCC}/\lambda$.

En appliquant l'équation (2.1) aux deux modes de défaillance mentionnés précédemment (DD et DU), on obtient (Figure 2.3) :

$$\begin{cases} \lambda_{DD} = \lambda_{DD}^{ind} + \lambda_{DD}^{DCC} = (1-\beta_D)\lambda_{DD} + \beta_D\lambda_{DD} \\ \lambda_{DU} = \lambda_{DU}^{ind} + \lambda_{DU}^{DCC} = (1-\beta)\lambda_{DU} + \beta\lambda_{DU} \end{cases} \qquad (2.3)$$

où β et β_D représentent respectivement la proportion des défaillances dangereuses de cause commune non détectées et détectées.

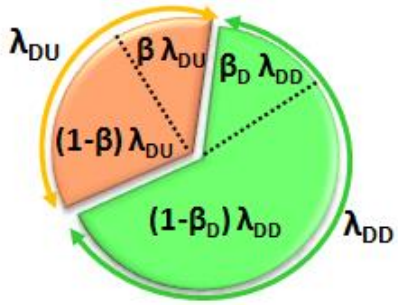

Figure 2.3: Répartition des taux de défaillances dangereuses

2.3. Vérification des formules de la CEI 61508 relatives à la *PFH*

Dans cette section, les formules de la *PFH* données par la CEI 61508 pour les configurations 1oo1, 1oo2, 2oo2, 1oo3 et 2oo3 sont présentées et étudiées à l'aide des modèles markoviens multi-phases et classiques. Avant d'entamer cette tâche de vérification, nous tenons à rappeler très brièvement quelques éléments relatifs au graphe de Markov.

Les chaînes ou graphes de Markov, nommées d'après le mathématicien russe Andrey Markov, représentent le comportement d'un système donné en décrivant les différents états

qu'il peut occuper et en indiquant comment il transite d'un état à un autre (transitions) dans le temps. Le système est supposé occupé un et seulement un de ces états à tout moment. En outre, l'évolution future du système dépend uniquement de son état actuel et non pas de son passé : *propriété de Markov*.

Les probabilités des états peuvent être déterminées en utilisant la relation suivante :

$$\frac{dP(t)}{dt} = P(t) \cdot Q \qquad (2.4)$$

où P représente le vecteur de probabilités des états et Q est la matrice de transition.

Les probabilités limites ou stationnaires peuvent être tout simplement obtenues comme suit :

$$P(\infty) \cdot Q = 0 \qquad (2.5)$$

Il convient d'indiquer que le comportement des systèmes testés périodiquement, suivi sur une durée de plusieurs périodes de test, ne peut être correctement rendu par un modèle markovien classique. Il nécessite l'usage d'un modèle markovien multi-phases [Dutuit *et al.*, 2008 ; Innal, 2008 ; Mechri *et al.*, 2013] qui peut être approché par un modèle classique à travers la détermination des taux de restauration à partir de ses états de défaillance partielle ou totale [Innal, 2008 ; Innal *et al.*, 2015]. La raison derrière l'approximation est que le modèle de Markov classique s'avère très utile pour l'établissement de formules simplifiées et compréhensibles.

Les probabilités des différents états d'un modèle markovien multi-phases pourraient facilement être obtenues en mettant à jour les probabilités d'états au début de chaque nouvelle période de test $P(b_{i+1})$ à partir de celles obtenues à la fin de la période précédente $P(e_i)$. Cette mise à jour nécessite l'emploi d'une matrice d'enchainement ou de passage M tel que :

$$P(b_{i+1}) = M \cdot P(e_i) \qquad (2.6)$$

2.3.1. Configuration 1oo1

2.3.1.1. Description

Cette architecture basique est composée d'un seul canal et, par conséquent, toutes défaillances dangereuses (détectées et non détectées) entraînent la perte de la fonction de sécurité. Cependant, suite à la détection d'une défaillance dangereuse (détection automatique par les tests en ligne : *watchdog*, etc.), le SIS conduit l'EUC dans en état de repli de sécurité. Cette

architecture s'appelle généralement 1oo1D. Le bloc-diagramme de fiabilité correspondant à cette architecture est donné à la figure 2.4 (a), tandis que le circuit électrique relatif à son principe de fonctionnement est présenté à la figure 2.4 (b). Le schéma électrique est fondée sur le « *principe du courant au repos* » (*de-energised to trip*). Les systèmes basés sur ce principe sont appelés systèmes normalement alimentés et sont conçus de manière à couper l'alimentation électrique suite à la détection d'une défaillance [Goble, 1998 ; Charpentier, 2002]. Cette première architecture est modélisée par deux relais câblés en série : commutateur de sortie (*output switch*) et relais de coupure (*cut-off relay*). Ces deux relais sont fermés en fonctionnement normal. Le commutateur de sortie devrait s'ouvrir (mise hors tension) en cas de situation dangereuse. Toute défaillance DD ou DU garderait ce commutateur fermé. Néanmoins, une défaillance DD conduit le système protégé dans un état sûr par l'ouverture du relais de diagnostic.

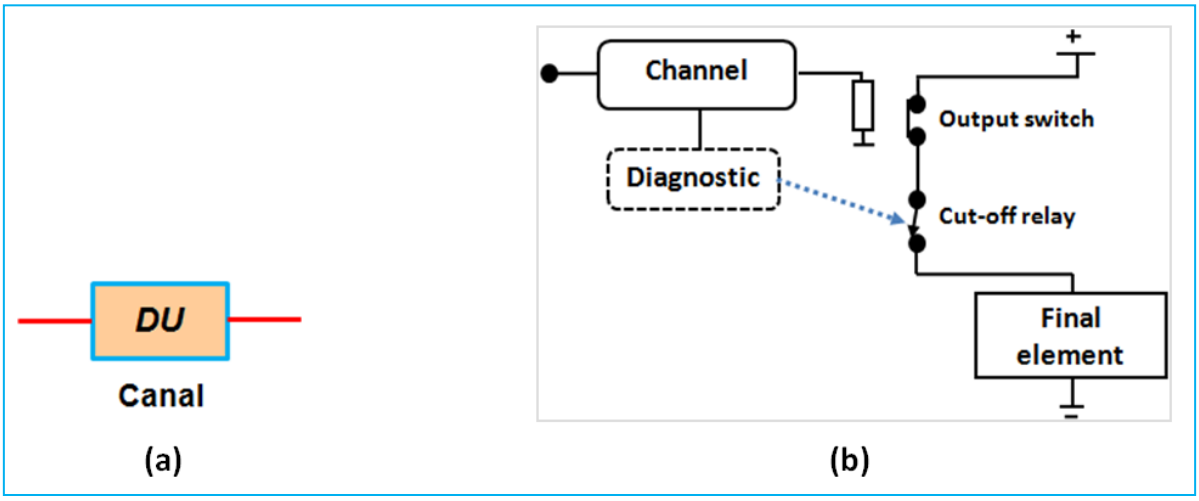

Figure 2.4 : (a) Bloc-diagramme de fiabilité et (b) circuit électrique de principe correspondant à la configuration 1oo1 (avec arrêt automatique)

La formule de la *PFH* fournie par la norme pour cette configuration est la suivante :

$$PFH_{1oo1} = \lambda_{DU} \quad (2.7)$$

2.3.1.2. Modèles markoviens

Les modèles markoviens multi-phases et approchés (classique) pour la configuration 1oo1 sont respectivement représentés sur les figures 2.5 (a) et (b). Notons que *MTTRsd* représente la durée moyenne de remise en service de l'*EUC* suite à un shutdown.

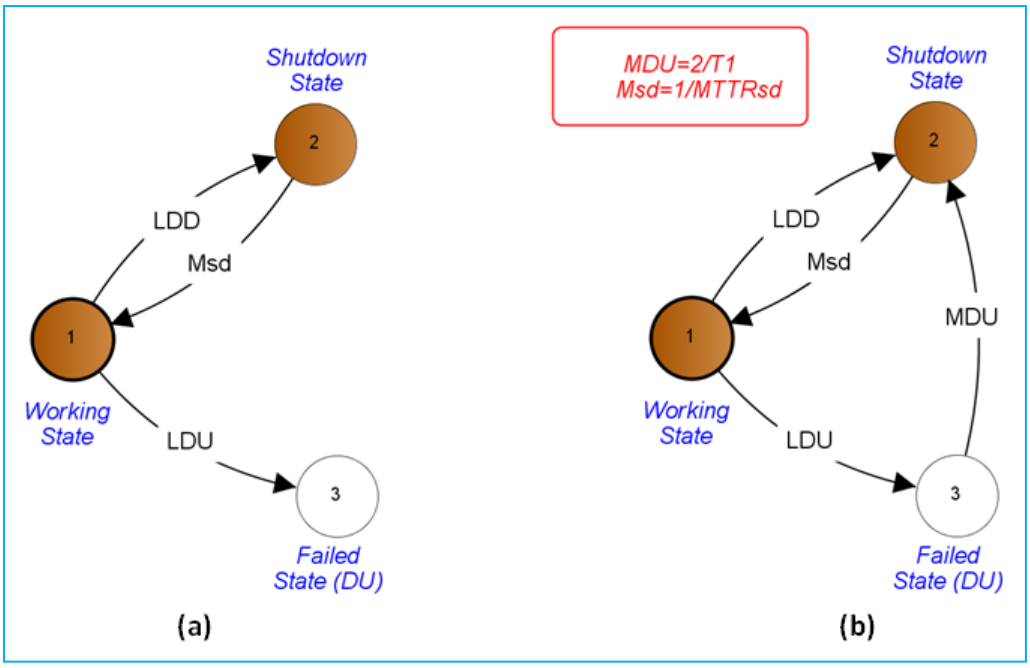

Figure 2.5 : Modèles markoviens relatifs à la configuration 1oo1 : (a) multi-phases et (b) classique ou approché

Pour le modèle markovien multi-phases, les probabilités au début de chaque période de test sont calculées ainsi :

$$\begin{bmatrix} P_1(b_{i+1}) \\ P_2(b_{i+1}) \\ P_3(b_{i+1}) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} P_1(e_i) \\ P_2(e_i) \\ P_3(e_i) \end{bmatrix} \Rightarrow \begin{cases} P_1(b_{i+1}) = P_1(e_i) \\ P_2(b_{i+1}) = P_2(e_i) + P_3(e_i) \\ P_3(b_{i+1}) = 0 \end{cases} \quad (2.8)$$

2.3.1.3. Formulation de la *PFH*

L'exploitation du modèle markovien approché nous permet d'établir la formule de la *PFH* correspondante en se basant sur la relation suivante [Omeiri *et al.*, 2015] :

$$PFH = \sum_{i \epsilon WS} P_i(\infty) \sum_{j \epsilon FS} \lambda_{i \to j} \quad (2.9)$$

Où WS signifie "états de marche : *working states*" et FS signifie "états de pannes : *failed states*". En outre, $\lambda_{i \to j}$ représente le taux de défaillance partant d'un état de marche et arrivant dans un état de panne. Pour le système 1oo1, l'équation (2.9) permet d'écrire :

$$PFH_{1oo1} = P_1(\infty)\lambda_{DU} \quad (2.10)$$

En déterminant $P_1(\infty)$ à partir du modèle approché, l'équation (2.10) peut être réécrite sous la forme suivante :

$$PFH_{1oo1} = \left[\frac{\mu_{DU}\cdot\mu_{sd}}{\mu_{DU}\cdot\mu_{sd}+\mu_{DU}\cdot\lambda_{DD}+\mu_{sd}\cdot\lambda_{DU}}\right]\cdot\lambda_{DU} \quad (2.11)$$

où : $\mu_{DU} = 1/\left(\frac{T_1}{2} + MRT\right)$ et $\mu_{sd} = 1/MTTR_{sd}$.

Dans le cadre des SIS, nous pouvons négliger les taux de défaillance devant les taux de réparation ($\lambda << \mu$). La relation (2.11) peut donc être réduite comme suit :

$$PFH_{1oo1} \approx \left[\frac{\mu_{DU}\cdot\mu_{sd}}{\mu_{DU}\cdot\mu_{sd}}\right]\cdot\lambda_{DU} = \lambda_{DU} \quad (2.12)$$

On peut facilement remarquer que la quantité donnée par la relation (2.12) est la même que celle fournie par l'égalité (2.7). Par conséquent, pour la configuration 1oo1, la formule fournie par la norme CEI 61508 est valide et très légèrement conservative par rapport à celle issue du modèle markovien approché (donnée par l'équation (2.11)).

2.3.2. Configuration 2oo2

2.3.2.1. Description

Cette configuration se compose de deux canaux identiques, de sorte que la fonction de sécurité requiert le fonctionnement des deux canaux. Ainsi, une défaillance dangereuse dans l'un des deux canaux conduit à l'inhibition de la fonction de sécurité. En outre, la détection de toute défaillance dangereuse provoque le déclenchement de cette fonction. Le bloc-diagramme de fiabilité et le schéma électrique de principe correspondant à cette configuration sont respectivement donnés à la figure 2.6 (a) et (b). Le schéma électrique montre clairement que toute défaillance DD coupe l'alimentation du circuit en ouvrant les deux relais de diagnostic. Par conséquent, un état dangereux (circuit bloqué sous tension) ne se produit que si au moins l'un des deux canaux subit une défaillance DU.

La formule de la *PFH* correspondante fournie par la norme CEI 61508 est :

$$PFH_{2oo2} = 2\lambda_{DU} \quad (2.13)$$

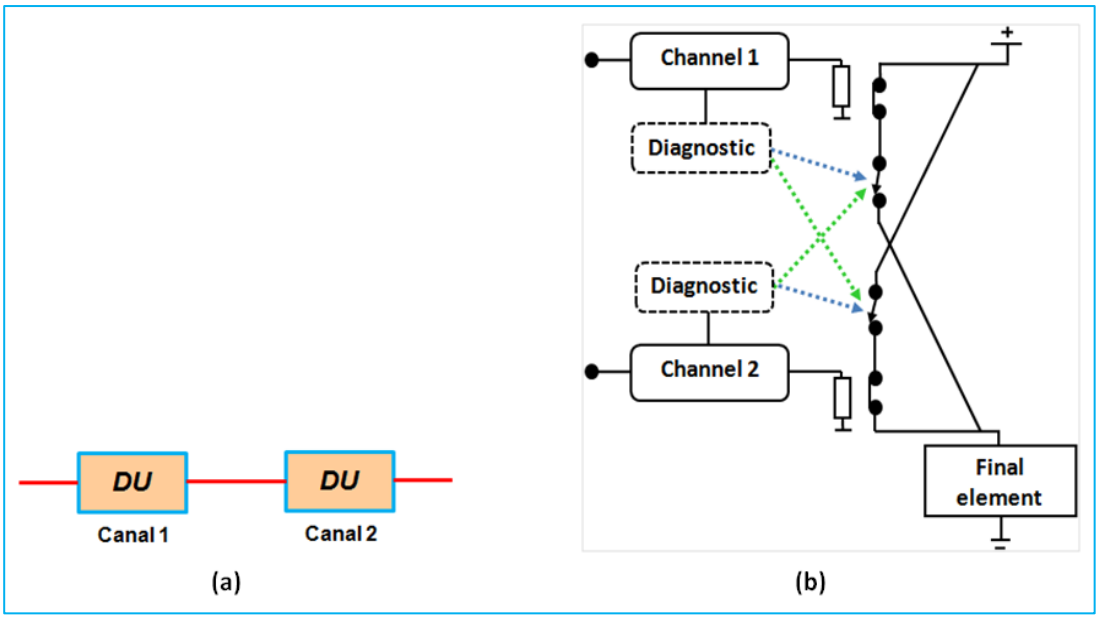

Figure 2.6 : (a) Bloc-diagramme de fiabilité et (b) circuit électrique de principe correspondant à la configuration 2oo2 (avec arrêt automatique)

2.3.2.2. Modèles markoviens

Les modèles markoviens multi-phases et approchés (classique) pour la configuration 2oo2 sont respectivement représentés au figures 2.7 et 2.8.

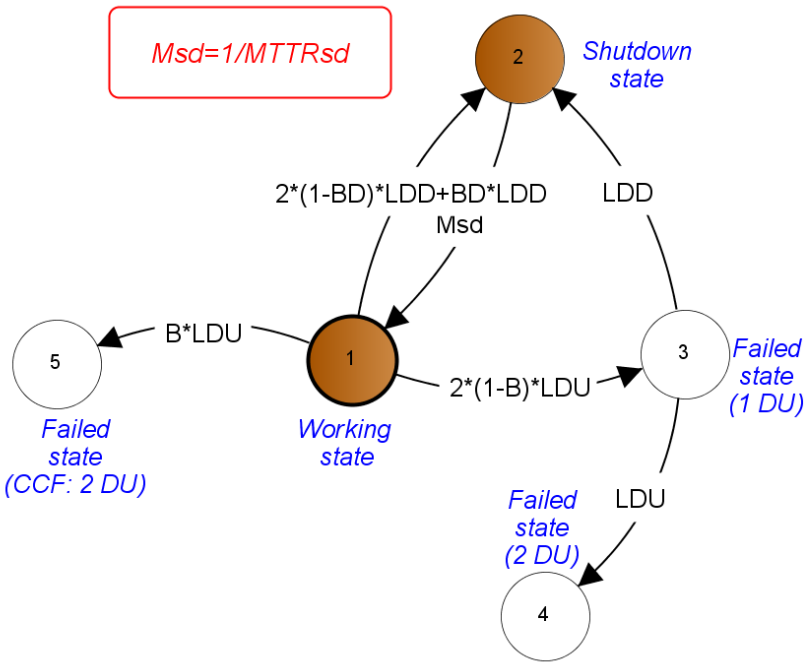

Figure 2.7 : Modèle markovien multi-phases relatif à la configuration 2oo2

Les probabilités au début de chaque période de test sont calculées comme suit :

$$\begin{cases} P_1(b_{i+1}) = P_1(e_i) \\ P_2(b_{i+1}) = P_2(e_i) + P_3(e_i) + P_4(e_i) + P_5(e_i) \\ P_3(b_{i+1}) = P_4(b_{i+1}) = P_5(b_{i+1}) = 0 \end{cases} \quad (2.14)$$

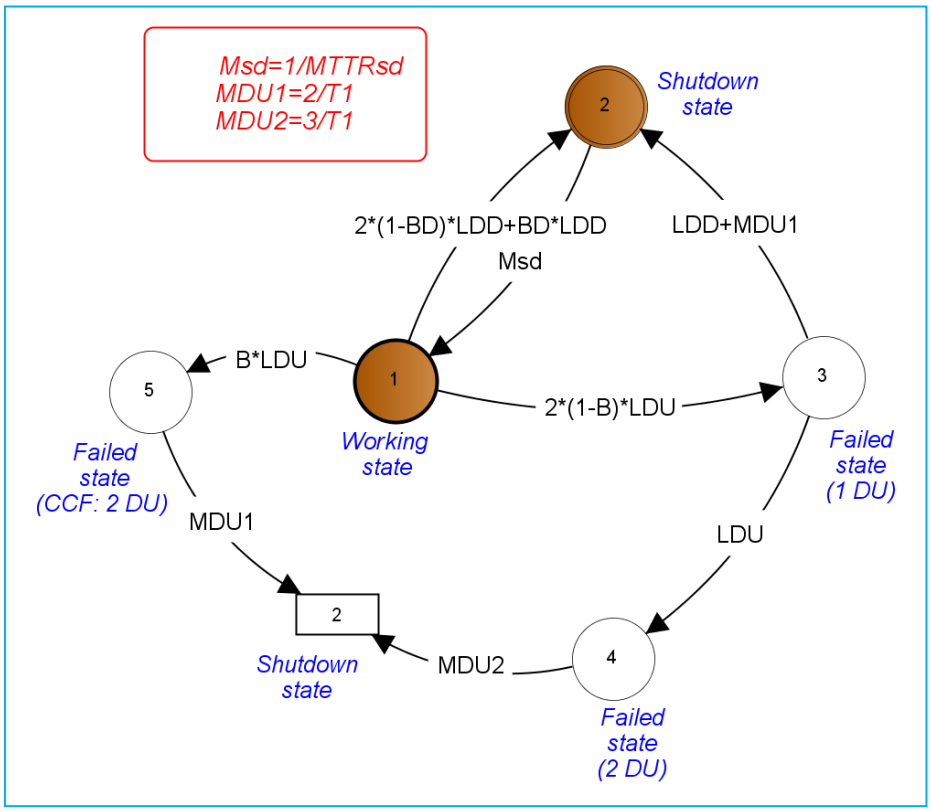

Figure 2.8 : Modèle markovien approché relatif à la configuration 2oo2

2.3.2.3. Formulation de la *PFH*

L'utilisation conjointe du modèle de Markov approché et de l'équation (2.9) permet l'écriture suivante :

$$PFH_{2oo2} = P_1(\infty) \cdot [2(1-\beta)\lambda_{DU} + \beta\lambda_{DU}] = P_1(\infty) \cdot (2-\beta)\lambda_{DU} \approx (2-\beta)\lambda_{DU} \quad (2.15)$$

La formule de la *PFH* obtenue (équation (2.15)) est légèrement différente de celle de l'équation (2.13). Compte tenu des possibles valeurs qui pourraient être attribuées au facteur β, nous pouvons valider la formule de la CEI 61508 pour cette deuxième configuration qui maintient le caractère conservatif mentionné dans le cas de la configuration 1oo1.

2.3.3. Configuration 1oo2

2.3.3.1. Description

Cette configuration est composée de deux canaux identiques fonctionnant en parallèle. Il est donc nécessaire que chacun des canaux subisse une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande émanant de l'*EUC*. Selon l'hypothèse de mise en état de sécurité, le SIS conduit l'*EUC* vers un état sûr dans le cas de détection de défaillances dangereuses dans les deux canaux. Le bloc-diagramme de fiabilité ainsi que le schéma électrique de principe correspondant à cette configuration sont respectivement donnés aux figures 2.9 et 2.10. Le schéma électrique montre que la coupure de l'alimentation du circuit, dans le cas d'une défaillance de l'architecture, requière l'ouverture des deux relais de diagnostic. Cela n'est possible qu'avec la présence d'une défaillance DD dans chaque canal.

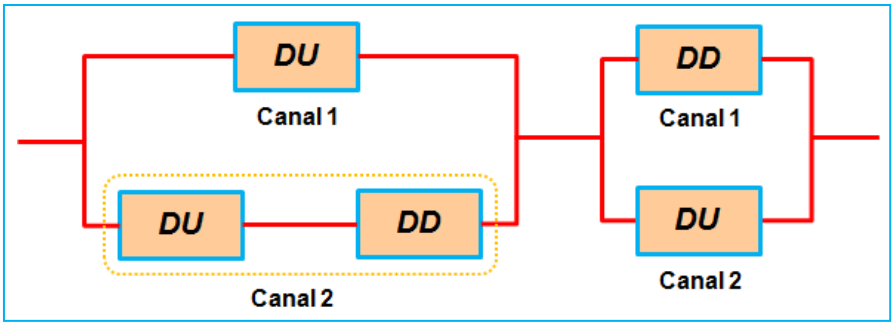

Figure 2.9 : Bloc-diagramme de fiabilité correspondant à la configuration 1oo2

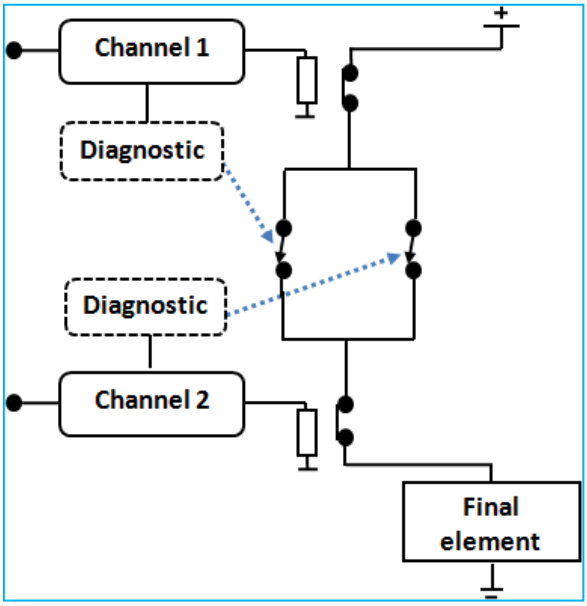

Figure 2.10 : Circuit électrique de principe correspondant à la configuration 1oo2

La formule de la *PFH* correspondante donnée par la norme CEI 61508 est rappelée ci-après :

$$PFH_{1oo2} = 2 \cdot [(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}] \cdot t_{CE} \cdot (1-\beta)\lambda_{DU} + \beta\lambda_{DU} \quad (2.16)$$

Avec : $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$ (2.17)

2.3.3.2. Modèles markoviens

Les modèles markoviens multi-phases et approchés pour la configuration 1oo2 sont respectivement représentés au figures 2.11 et 2.12.

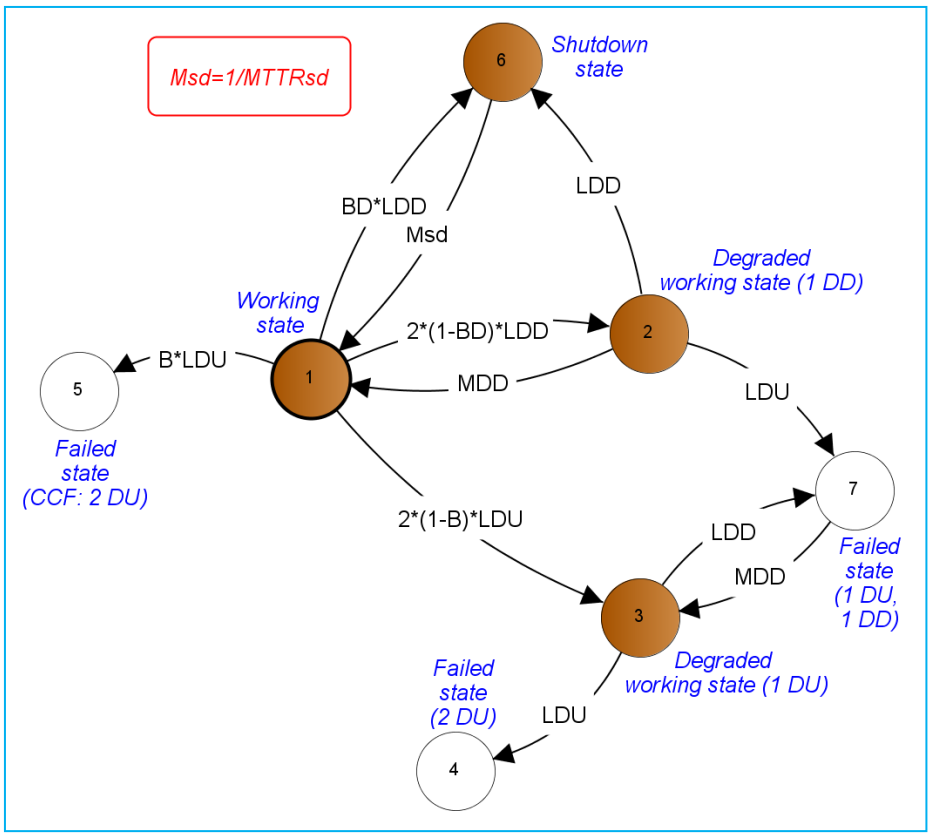

Figure 2.11 : Modèle markovien multi-phases relatif à la configuration 1oo2

Les probabilités au début de chaque période de test sont calculées comme suit :

$$\begin{cases} P_1(b_{i+1}) = P_1(e_i) \\ P_2(b_{i+1}) = P_2(e_i) + P_3(e_i) \\ P_6(b_{i+1}) = P_4(e_i) + P_5(e_i) + P_6(e_i) + P_7(e_i) \\ P_3(b_{i+1}) = P_4(b_{i+1}) = P_5(b_{i+1}) = P_7(b_{i+1}) = 0 \end{cases} \quad (2.18)$$

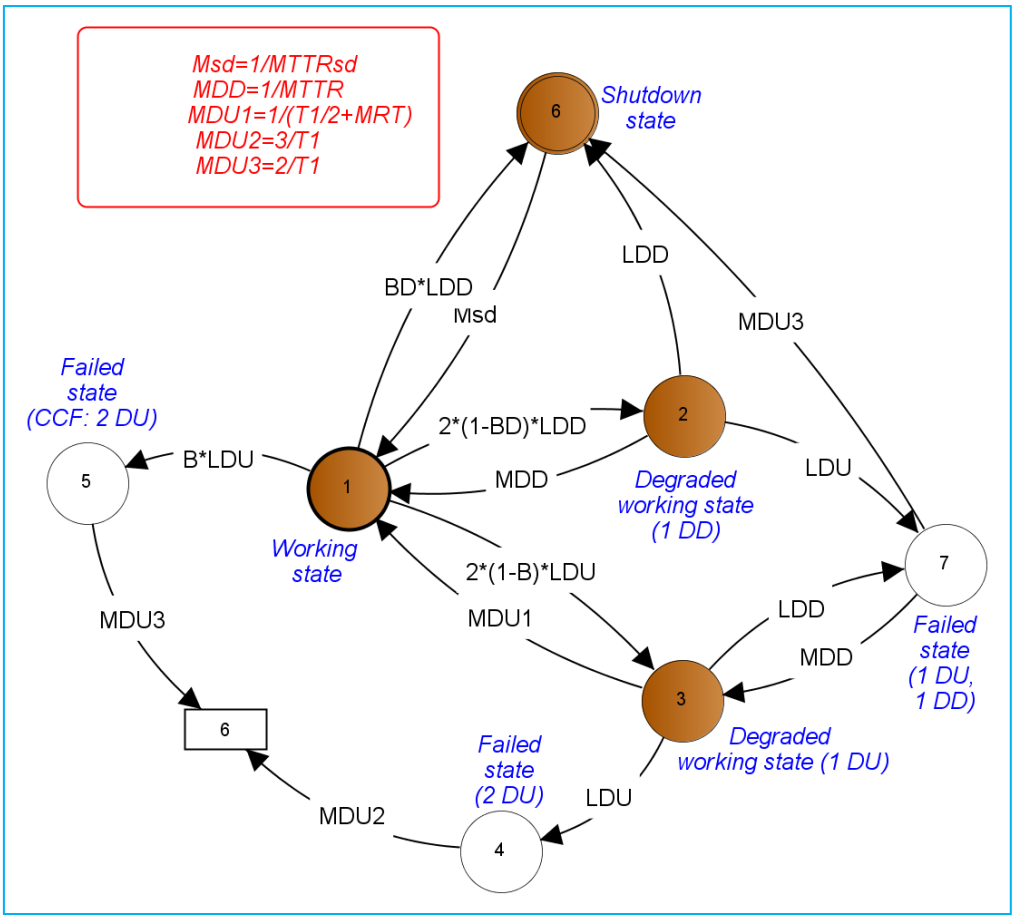

Figure 2.12 : Modèle markovien approché relatif à la configuration 1oo2

2.3.3.3. Formulation de la *PFH*

En appliquant l'équation (2.9) au modèle markovien de la figure 2.12 on obtient la formule de la *PFH* suivante :

$$PFH_{1oo2} = P_1(\infty) \cdot \beta\lambda_{DU} + P_2(\infty) \cdot \lambda_{DU} + P_3(\infty) \cdot [\lambda_{DD} + \lambda_{DU}] \qquad (2.19)$$

Les probabilités des états 1, 2 et 3 au régime stationnaire (probabilités limites ou asymptotiques) sont données par l'équation (2.20).

$$\begin{cases} P_1(\infty) \approx 1 \\ P_2(\infty) \approx \frac{2(1-\beta_D)\cdot\lambda_{DD}}{\mu_{DD}} = 2(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \\ P_3(\infty) \approx \frac{2(1-\beta)\cdot\lambda_{DU}}{\mu_{DU1}} = 2(1-\beta)\cdot\lambda_{DU}\left(\frac{T_1}{2}+MRT\right) \end{cases} \qquad (2.20)$$

Une fois que les probabilités de l'équation (2.20) sont insérées dans l'équation 2.15, nous obtenons :

$$PFH_{1oo2} \approx \beta\lambda_{DU} + 2(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR\cdot\lambda_{DU} + 2(1-\beta)\cdot\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]\cdot[\lambda_{DD}+\lambda_{DU}] \quad (2.21)$$

Afin de comparer efficacement les formules données par les équations (2.16) et (2.21), nous réécrivons l'équation (2.21) sous une forme similaire à la formule fournie dans la CEI 61508 (équation 2.16):

$$\begin{aligned} PFH_{1oo2} &\approx 2\left[(1-\beta)\cdot\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]+(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR\right]\cdot\lambda_{DU}+\beta\lambda_{DU}+ \\ &\quad 2(1-\beta)\cdot\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]\cdot\lambda_{DD} \\ &= 2[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]\cdot t_{CE1}\cdot\lambda_{DU}+\beta\lambda_{DU}+2(1-\beta)\cdot\lambda_{DU}\cdot \\ &\quad \left[\frac{T_1}{2}+MRT\right]\cdot\lambda_{DD} \end{aligned} \quad (2.22)$$

Avec : $t_{CE1} = \frac{\lambda_{DU}^{ind}}{\lambda_D^{ind}}\left[\frac{T_1}{2}+MRT\right]+\frac{\lambda_{DD}^{ind}}{\lambda_{DU}^{ind}}MTTR$ (2.23)

$$\lambda_{DD}^{ind} = (1-\beta_D)\lambda_{DD};\ \lambda_{DU}^{ind} = (1-\beta)\lambda_{DU};\ \lambda_D^{ind} = \lambda_{DD}^{ind}+\lambda_{DU}^{ind}$$

L'examen de la relation (2.22) montre que ses premiers termes de la sommation sont presque similaires à la formule de la norme CEI 61508 (équation 2.16). Le t_{CE} donné par l'équation (2.17), comme clairement indiqué dans la CEI 61508, est calculé sur la base de la configuration 1oo1, où aucune DCC n'est possible. C'est pourquoi il n'y a aucune mention des facteurs (β et β_D) dans l'équation (2.17). Cependant, la quantité correcte est le t_{CE1} donnée par l'équation (2.23) car il prend la spécificité de la configuration 1oo2 liée à l'occurrence possible des DCC. Si nous ignorons les facteurs β, les premiers termes de la sommation dans l'équation (2.23) seraient égaux à la formule de la PFH_{1oo2} donnée dans la CEI 61508. Néanmoins, la formule dérivée du modèle markovien (équation 2.23) contient un terme supplémentaire : $2(1-\beta)\lambda_{DU}\left[\frac{T_1}{2}+MRT\right]\lambda_{DD}$. Il représente une séquence de défaillance commençant par une défaillance DU suivie d'une défaillance DD : état 1 → état 3 → état 7 (voir figure 2.12). Il convient de noter qu'aucun arrêt de sécurité consécutif à cette séquence de défaillances n'est absolument pas possible, puisqu'il n'existe qu'une seule défaillance DD. Par conséquent, la formule de la *PFH* donnée dans la CEI 61508 est formellement erronée car elle ne tient pas compte de la séquence de défaillance mentionnée ci-dessus. Ainsi, la formule de la CEI 61508 pourrait conduire à des résultats sous-estimés (non-conservatifs) ce qui est dangereux d'un point de vue sécuritaire.

2.3.4. Configuration 2oo3

2.3.4.1. Description

Cette configuration se compose de trois canaux connectés en parallèle avec vote majoritaire 2oo3 pour les signaux de sortie : la fonction de sécurité nécessite au minimum le fonctionnement de deux canaux parmi les trois. Par conséquent, une défaillance dangereuse d'au moins deux canaux empêche le SIS d'exécuter sa fonction de sécurité. En conséquence, le SIS met l'EUC dans un état sûr aussitôt qu'une défaillance dangereuse dans deux canaux quelconques est détectée. Le bloc-diagramme de fiabilité correspondant à cette configuration est donné à la figure 2.13, tandis que schéma électrique associée est présenté à la figure 2.14. Les commutateurs de sortie et les relais de diagnostic sont fermés en fonctionnement normal. Les commutateurs de sortie doivent s'ouvrir en cas de situation dangereuse. Toute défaillance DD ou DU garderait ces commutateurs fermés. Avec l'aptitude d'arrêt d'urgence automatique, les défaillances DD (au moins deux défaillances DD) mettraient immédiatement l'*EUC* dans un état sûr, car les relais de diagnostic correspondant s'ouvriraient.

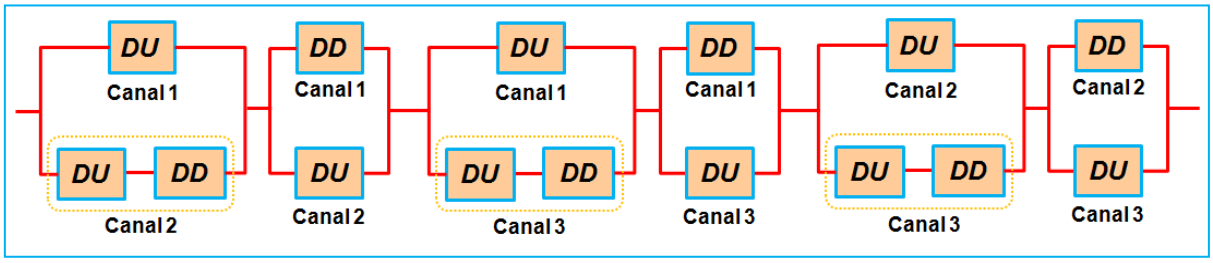

Figure 2.13 : Bloc-diagramme de fiabilité relatif à la configuration 2oo3

La formule de la *PFH* correspondante fournie par la norme CEI 61508 est donnée ci-dessous :

$$PFH_{2oo3} = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}] \cdot t_{CE} \cdot (1-\beta)\lambda_{DU} + \beta\lambda_{DU} \qquad (2.24)$$

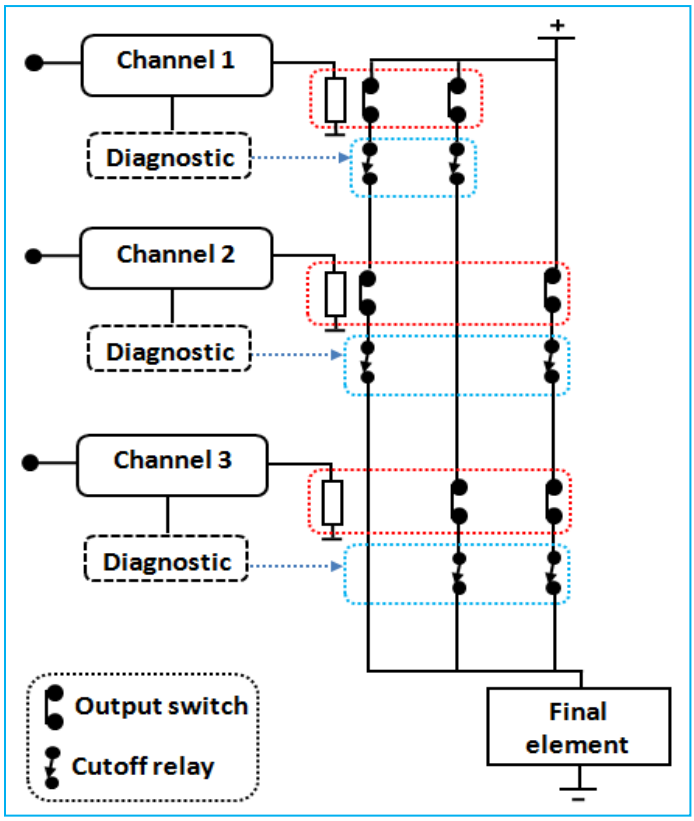

Figure 2.14 : Schéma électrique de principe relatif à la configuration 2oo3

2.3.4.2. Modèles markoviens

Les graphes de Markov multi-phases et approchés relatifs à l'architecture 2oo3 sont respectivement représentés aux figures 2.15 et 2.16. Pour le modèle multi-phases, les probabilités au début de chaque période de test sont calculées comme suit :

$$\begin{cases} P_1(b_{i+1}) = P_1(e_i) \\ P_2(b_{i+1}) = P_2(e_i) + P_3(e_i) \\ P_j(b_{i+1}) = 0,\ j = 4,5,7,8,9 \\ P_6(b_{i+1}) = \sum_{j=4}^{9} P_j(e_i) \end{cases} \quad (2.25)$$

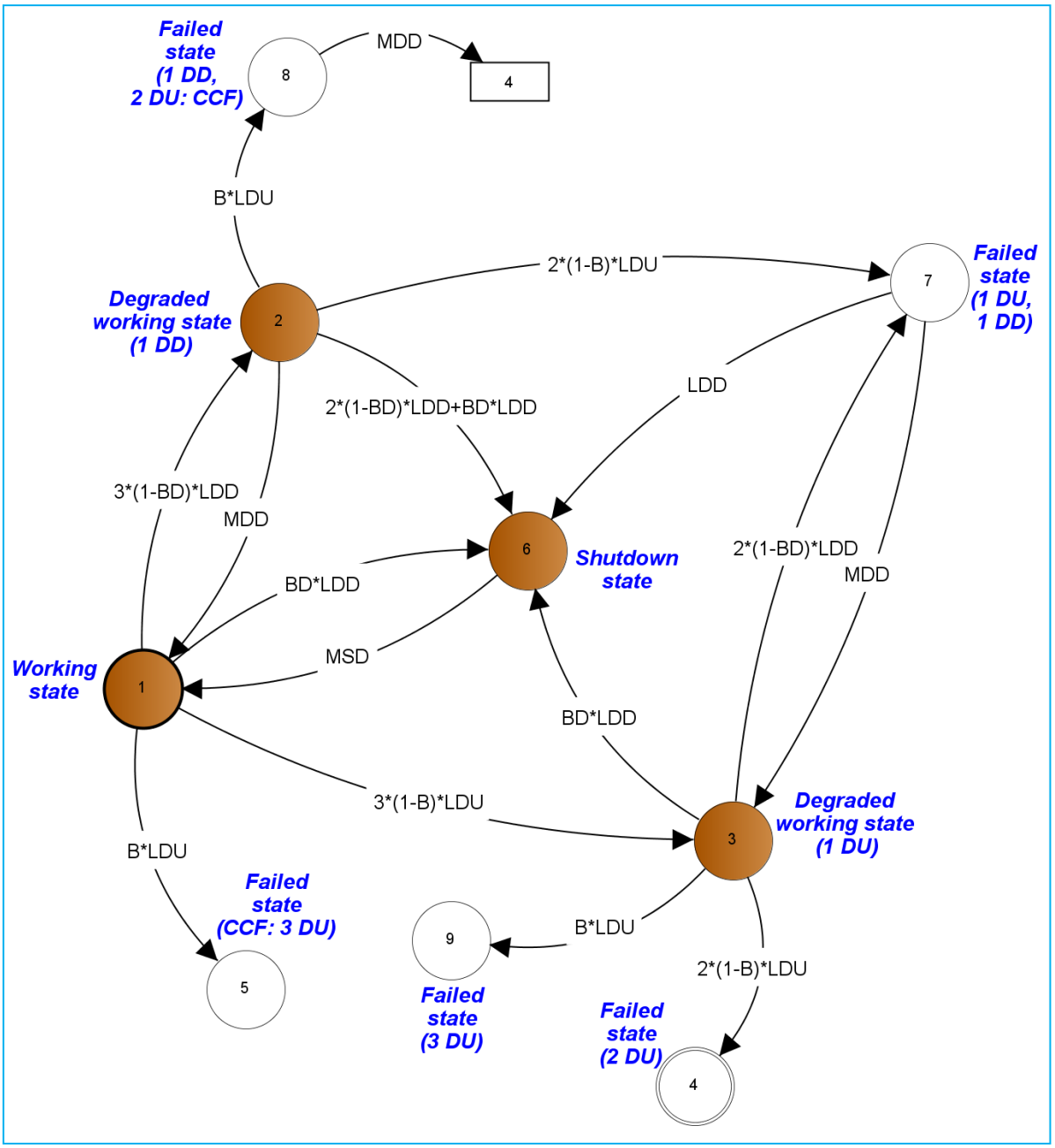

Figure 2.15 : Modèle markovien multi-phases relatif à la configuration 2oo3

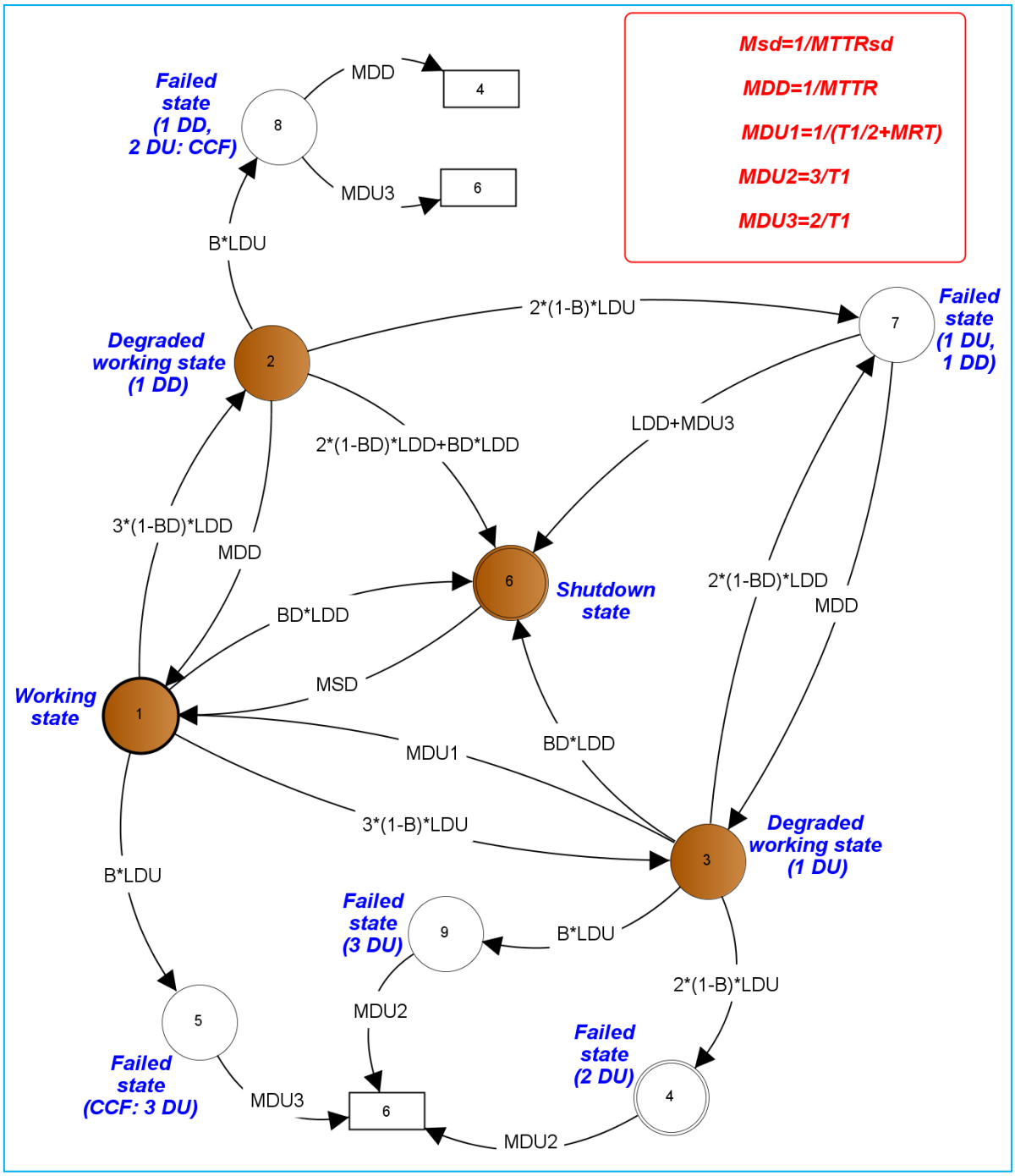

Figure 2.16 : Modèle markovien approché relatif à la configuration 2oo3

2.3.4.3. Formulation de la *PFH*

L'équation (2.9) permet de dériver la formule de la *PFH* liée à la configuration 2oo3 :

$$PFH_{2oo3} = P_1(\infty)\cdot\beta\lambda_{DU} + P_2(\infty)\cdot[2(1-\beta)\lambda_{DU} + \beta\lambda_{DU}] + P_3(\infty)\cdot[2(1-\beta)\lambda_{DU} + 2(1-\beta_D)\lambda_{DD} + \beta\lambda_{DU}] \quad (2.26)$$

Les probabilités limites des états 1, 2 et 3 sont données ci-après.

$$\begin{cases} P_1(\infty) \approx 1 \\ P_2(\infty) \approx \frac{3(1-\beta_D)\cdot\lambda_{DD}}{\mu_{DD}} = 3(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \\ P_3(\infty) \approx \frac{3(1-\beta)\cdot\lambda_{DU}}{\mu_{DU1}} = 3(1-\beta)\cdot\lambda_{DU}\left(\frac{T_1}{2} + MRT\right) \end{cases} \quad (2.27)$$

En insérant ces quantités et réécrivant l'équation (2.26) sous une forme similaire à l'équation (2.24), nous obtenons :

$$PFH_{2oo3} \approx 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]\cdot t_{CE1}\cdot(1-\beta)\lambda_{DU} + \beta\lambda_{DU} + 6(1-\beta)\cdot\lambda_{DU}\cdot\left[\frac{T_1}{2} + MRT\right]\cdot(1-\beta_D)\lambda_{DD} + 3\left((1-\beta_D)\lambda_{DD}\cdot MTTR + (1-\beta)\lambda_{DU}\cdot\left[\frac{T_1}{2} + MRT\right]\right)\cdot\beta\lambda_{DU} \quad (2.28)$$

La même remarque faite pour la configuration 1oo2 est toujours valable en ce qui concerne la similitude des deux premiers termes de la sommation dans l'équation 2.28 et l'équation 2.24. De plus, l'équation 2.28 contient des termes supplémentaires. Il convient de noter que le dernier terme de la sommation dans l'équation 2.28 pourrait être négligé devant le second ($\beta\,\lambda_{DU}$). Cependant, le troisième terme de la sommation, c'est-à-dire $6(1-\beta)\cdot\lambda_{DU}\cdot\left[\frac{T_1}{2} + MRT\right]\cdot(1-\beta_D)\lambda_{DD}$ ne peut être négligé. Comme pour la configuration 1oo2, cette quantité représente une séquence de défaillance commençant par une défaillance DU suivie d'une défaillance DD : état 1 → état 3 → état 7 (voir la figure 2.16). Encore une fois, la formule de la *PFH* donnée dans la CEI 61508 est formellement fausse et fournirait des résultats non conservatifs.

2.3.5. Configuration 1oo3

2.3.5.1 Description

Cette configuration se compose de trois canaux connectés en parallèle. Par conséquent, une défaillance dangereuse de tous les canaux empêche le SIS d'exécuter sa fonction de sécurité. Ainsi, le SIS met l'EUC dans un état sûr suite à la détection d'une défaillance dangereuse dans les trois canaux. Le bloc-diagramme de fiabilité correspondant à cette configuration est donné à la figure 2.17. Le schéma électrique relatif au principe de l'architecture 1oo3, présenté à la figure 2.18, indique clairement l'ouverture automatique du circuit électrique consécutivement à la présence d'une défaillance DD dans chacun des trois canaux.

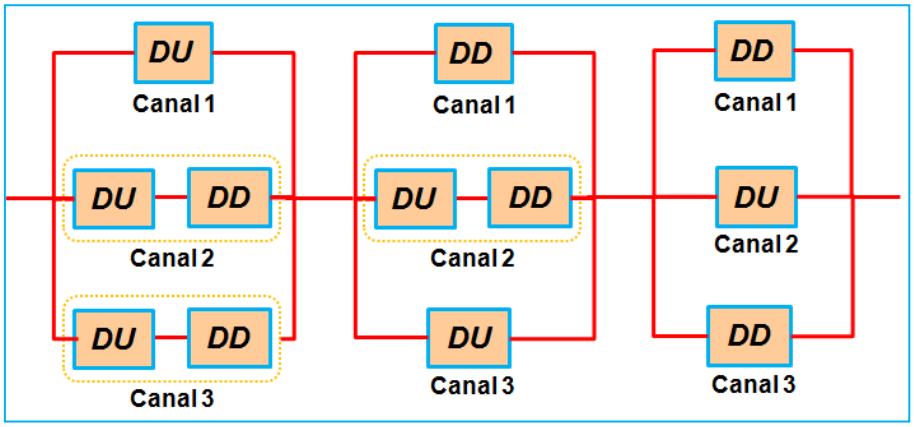

Figure 2.17 : Bloc-diagramme de fiabilité relatif à l'architecture 1oo3

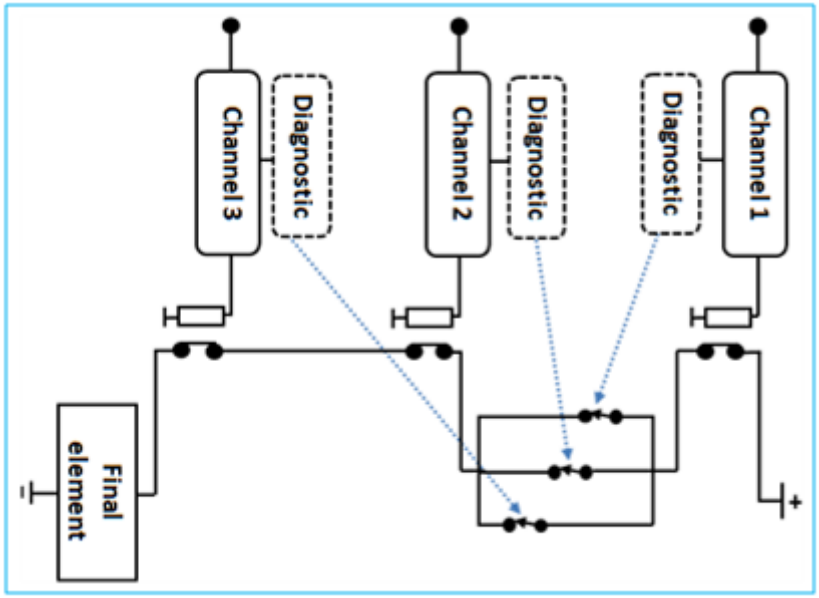

Figure 2.18 : Schéma électrique de principe relatif à l'architecture 1oo3

La norme CEI 61508 donne la formule *PFH* suivante de cette dernière configuration :

$$PFH_{1oo3} = 6\left[(1-\beta_D)\,\lambda_{DD} + (1-\beta)\,\lambda_{DU}\right]^2 \cdot t_{CE} \cdot t_{GE} \cdot (1-\beta)\,\lambda_{DU} + \beta\lambda_{DU} \qquad (2.29)$$

$$\text{Avec: } t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MRT\right] + \frac{\lambda_{DD}}{\lambda_D}\,MTTR \qquad (2.30)$$

2.3.5.2. Modèles markoviens

Le comportement de cette dernière configuration est donné par le modèle markovien multi-phases de la figure 2.19. Le modèle markovien approché qui s'y associe est fournie à la figure 2.20.

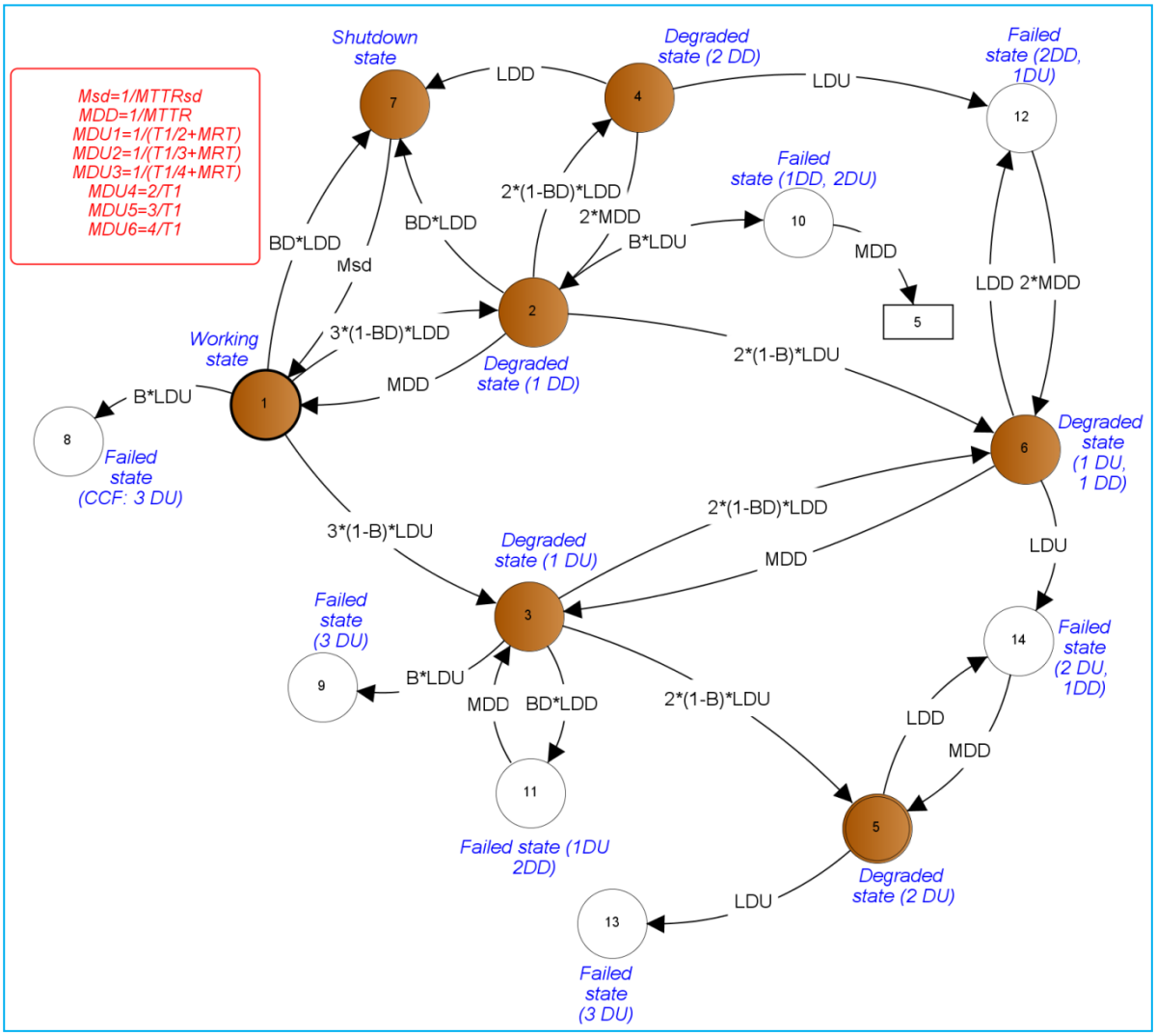

Figure 2.19 : Modèle markovien multi-phases relatif à la configuration 1oo3

Les probabilités au début de chaque période de test sont calculées comme suit :

$$\begin{cases} P_1(b_{i+1}) = P_1(e_i) \\ P_2(b_{i+1}) = P_2(e_i) + P_3(e_i) \\ P_4(b_{i+1}) = P_4(e_i) + P_5(e_i) + P_6(e_i) \\ P_7(b_{i+1}) = \sum_{j=7}^{14} P_j(e_i) \\ P_j(b_{i+1}) = 0,\ j \neq 1, 2, 4, 7 \end{cases} \quad (2.31)$$

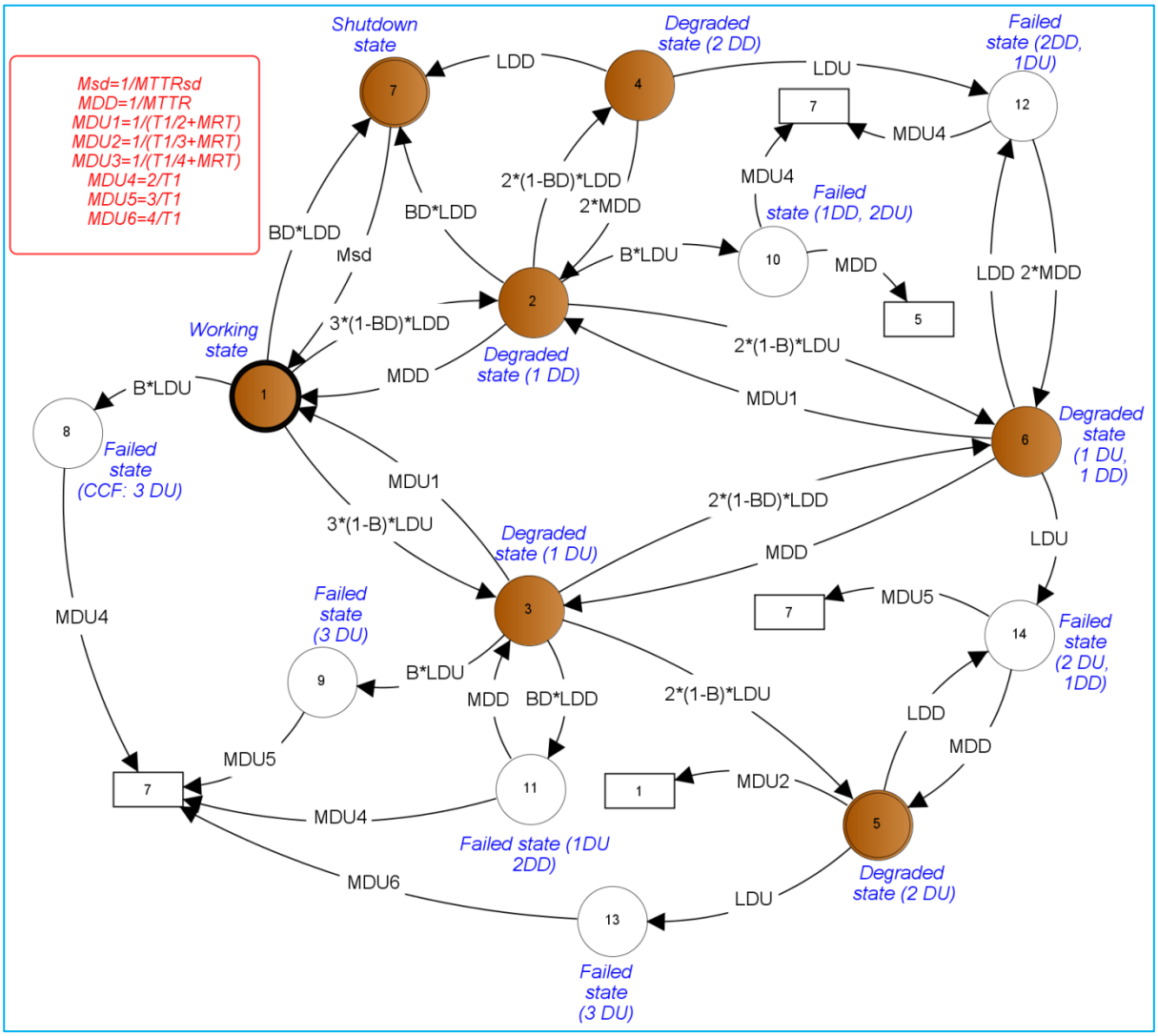

Figure 2.20 : Modèle markovien approché relatif à la configuration 1oo3

2.3.5.3. Formulation de la *PFH*

L'usage de l'équation (2.9) permet la détermination de la *PFH* liée à la configuration 1oo3 :

$$PFH_{1oo3} = P_1(\infty)\cdot\beta\lambda_{DU} + P_2(\infty)\cdot\beta\lambda_{DU} + P_3(\infty)\cdot[\beta\,\lambda_{DU} + \beta_D\,\lambda_{DD}] + P_4(\infty)\cdot\lambda_{DU} + P_5(\infty)\cdot[\lambda_{DU}+\lambda_{DD}] + P_6(\infty)\cdot[\lambda_{DU}+\lambda_{DD}] \quad (2.32)$$

Les probabilités limites des différents états sont données par les relations (2.33).

$$\begin{cases} P_1(\infty) \approx 1 \\ P_2(\infty) \approx \frac{3(1-\beta_D)\cdot\lambda_{DD}}{\mu_{DD}} = 2(1-\beta_D)\cdot\lambda_{DD}\cdot MTTR \\ P_3(\infty) \approx \frac{3(1-\beta)\cdot\lambda_{DU}}{\mu_{DU1}} = 2(1-\beta)\cdot\lambda_{DU}\left(\frac{T_1}{2}+MRT\right) \\ P_4(\infty) \approx \frac{3(1-\beta_D)^2\cdot\lambda_{DD}^2}{\mu_{DD}^2} = 3(1-\beta_D)^2\cdot\lambda_{DD}^2\cdot MTTR^2 \\ P_5(\infty) \approx \frac{6(1-\beta)^2\cdot\lambda_{DU}^2}{\mu_{DU1}\cdot\mu_{DU2}} = 6(1-\beta)^2\cdot\lambda_{DU}^2\left(\frac{T_1}{2}+MRT\right)\left(\frac{T_1}{3}+MRT\right) \\ P_6(\infty) \approx \frac{6(1-\beta)\cdot\lambda_{DU}\cdot(1-\beta_D)\cdot\lambda_{DD}}{\mu_{DU1}\cdot\mu_{DD}} = 6(1-\beta)\cdot\lambda_{DU}\cdot(1-\beta_D)\cdot\lambda_{DD}\cdot\left(\frac{T_1}{2}+MRT\right)MTTR \end{cases} \quad (2.33)$$

Après avoir inséré les différentes probabilités stationnaires et opéré certains arrangements, nous obtenons :

$$PFH_{1oo3} = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2\cdot t_{CE1}\cdot t_{GE1}\cdot\lambda_{DU} + \beta\lambda_{DU} + 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]\cdot(1-\beta)\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]\cdot t_{GE1}\cdot\lambda_{DD} + 3\left((1-\beta_D)\lambda_{DD}\cdot MTTR + (1-\beta)\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]\right)\cdot\beta\lambda_{DU} + 3(1-\beta)\lambda_{DU}\cdot\left[\frac{T_1}{2}+MRT\right]\cdot\beta_D\lambda_{DD} \quad (2.34)$$

Avec : $t_{GE1} = \frac{\lambda_{DU}^{ind}}{\lambda_D^{ind}}\left[\frac{T_1}{3}+MRT\right] + \frac{\lambda_{DD}^{ind}}{\lambda_D^{ind}}MTTR$ (2.35)

Comme pour la configuration précédente, l'examen des équations (2.29) et (2.34) montre que leurs deux premiers termes de sommation sont presque les mêmes. Nous tenons à noter que les raisons de la différence entre t_{GE} et t_{GE1} sont celles indiquées pour le cas de t_{CE} et t_{CE1}. Encore une fois de plus, la formule de *PFH* donnée par la relation (2.34) contient des termes supplémentaires par rapport à la relation (2.29). Par conséquent, la formule de la *PFH* donnée dans la CEI 61508 est formellement erronée et fournirait donc des résultats optimistes.

2.4. Résultats numériques

L'objectif de cette section est de vérifier numériquement la non-validité des formules de la norme CEI 61508 liées à la *PFH* pour certaines configurations. Les résultats numériques ont été obtenus en utilisant différentes approches : les formules de la CEI 61508, les modèles markoviens multi-phase (MMP), les modèles markoviens approchés (MA) et les nouvelles formules (NF) dérivées à partir de ces derniers modèles. Le jeu de paramètres utilisé est le suivant : λ_D = 5E-6 h^{-1} ; $MTTR = MRT = 8h$; $T_1 = 4380\ h$; $\beta = 2\beta_D = 0.1$; $MTTR_{sd} = 24h$. De différentes valeurs pour DC sont considérées.

2.4.1. Configurations 1oo1 et 2oo2

Les résultats obtenus pour ces configurations sont respectivement regroupés dans les tableaux 2.1 et 2.2. La figure 2.21 est fournie pour montrer que l'approximation des modèles MMP par des modèles MA sont correctes. En effet, ces deux dernières figures montrent explicitement que les valeurs limites des *PFH*, obtenues via les modèles MA, coïncident avec les *PFH* moyennes obtenues via les modèles MMP.

Tableau 2.1 : Résultats de la *PFH* pour la configuration 1oo1

DC	Approches			
	CEI 61508 : Eq. (2.7)	**MMP**	**MA**	**NF : Eq. (2.12)**
0	5E-6	4.945E-6	4.945E-6	5E-6
0.6	2E-6	1.991E-6	1.992E-6	2E-6
0.9	5E-7	4.994E-7	4.994E-7	5E-7
0.99	5E-8	4.999E-8	4.999E-8	5E-8

Tableau 2.2 : Résultats de la *PFH* pour la configuration 2oo2

DC	Approches			
	CEI 61508 : Eq. (2.13)	**MMP**	**MA**	**NF : Eq. (2.15)**
0	1E-5	9.30E-06	9.305E-6	9.50E-6
0.6	4E-6	3.768E-6	3.769E-6	3.8E-6
0.9	1E-6	9.478E-7	9.479E-7	9.5E-7
0.99	1E-7	9.496E-8	9.496E-8	9.5E-8

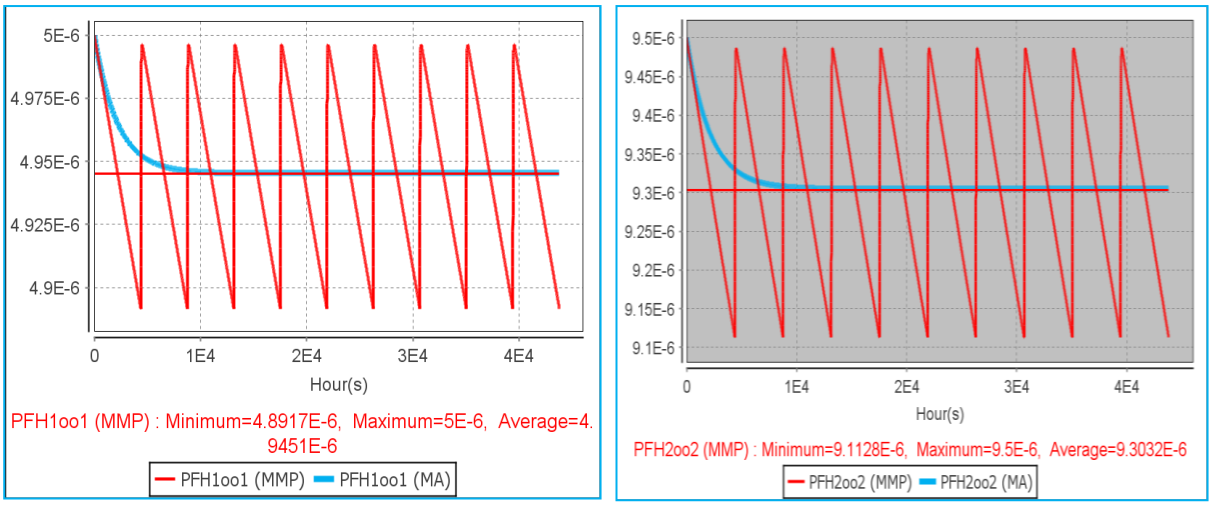

Figure 2.21 : Courbes relatives aux PFH_{1oo1} et PFH_{2oo2} (DC = 0)

L'inspection du tableau 2.1 montre que les résultats de la *PFH* découlant des approches MMP et MA sont presque identiques. En outre, ils sont très proches des résultats donnés par les formules analytiques (Eqs. (2.7) et (2.12)), qui sont légèrement conservatives.

Le tableau 2.2 montre que les résultats de la *PFH* obtenus à partir des MMP, MA et NF (Eq. 2.15) sont très proches. Les résultats induits par la formule de la CEI 61508 (Eq. 2.13) sont plus élevés que les précédents. Pour les cas de DC = 0.9 et 0.99, les résultats liés à la formule de la CEI 61508 induisent un SIL2 (voir tableau 1.1), alors que les autres approches conduisent à un SIL3. En dépit de cet écart, la CEI 61508 fournit une formule *PFH* qui reste conservative et ne sous-estime pas le SIL de la configuration 2oo2.

En conclusion, pour ces deux premières configurations, la norme CEI 61508 propose des formules analytiques acceptables produisant des résultats conservatives par rapport aux résultats précis provenant des modèles MMP et MA.

2.4.2. Configurations 1oo2, 2oo3 et 1oo3

Afin de procéder à une comparaison efficace entre les différentes approches, nous considérons seulement la contribution des défaillances indépendantes : $\beta = 2\ \beta_D = 0$. En fait, le terme commun ($\beta\ \lambda_{DU}$: défaillances de cause communes) entre les formules de la CEI 61508 et les nouvelles formules pourrait avoir une contribution majeure aux résultats de la *PFH* et donc masquerait les éventuels écarts. Les résultats obtenus pour ces configurations sont respectivement présentés dans les tableaux 2.3, 2.4 et 2.5.

Tableau 2.3 : Résultats de la *PFH* pour la configuration 1oo2 sans DCC

DC	Approches			
	CEI 61508 : Eq. (2.16)	**MMP**	**MA**	**NF : Eq. (2.22)**
0	1.099E-7	1.075E-7	1.064E-7	1.099 E-7
0.6	1.768E-8	4.357E-8	4.348E-8	4.406E-8
0.9	1.135E-9	1.096E-8	1.099E-8	1.103E-8
0.99	1.495E-11	1.099E-9	1.102E-9	1.103E-9

Tableau 2.4 : Résultats de la *PFH* pour la configuration 2oo3 sans DCC

DC	Approches			
	CEI 61508 : Eq. (2.24)	**MMP**	**MA**	**NF : Eq. (2.28)**
0	3.297E-7	3.178E-7	3.124E-7	3.297E-7
0.6	5.304E-8	1.299E-7	1.293E-7	1.322E-7
0.9	3.405E-9	3.285E-7	3.289E-7	3.308E-7
0.99	4.485E-11	3.295E-9	3.307E-9	3.309E-9

Tableau 2.5 : Résultats de la *PFH* pour la configuration 1oo3 sans DCC

DC	Approches			
	CEI 61508 : Eq. (2.29)	**MMP**	**MA**	**NF : Eq. (2.34)**
0	2.419E-9	2.326E-9	2.276E-9	2.419E-9
0.6	1.570E-10	3.818E-10	3.808E-10	3.912E-10
0.9	2.622E-12	2.508E-11	2.523E-11	2.547E-11
0.99	5.068E-15	3.699E-13	3.724E-13	3.739E-13

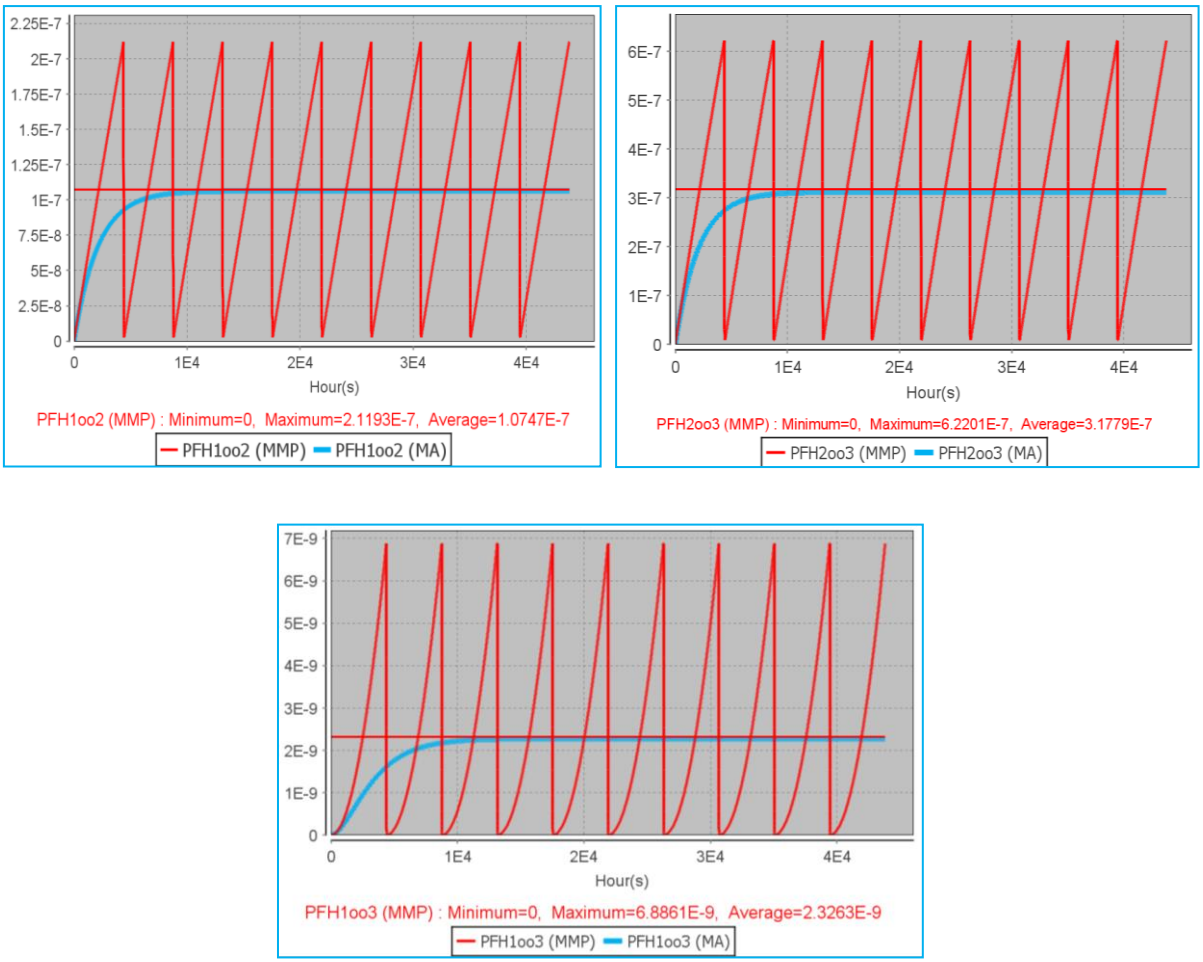

Figure 2.22 : Courbes relatives aux PFH_{1oo2} PFH_{2oo3} et PFH_{1oo3} (DC = 0)

L'examen des tableaux 2.3, 2.4 et 2.5 montre que les résultats obtenus à l'aide des approches MMP, MA et des nouvelles formules sont très proches. Notons que les résultats calculés à partir des nouvelles formules sont très légèrement conservatives comparés aux valeurs numériques issues de l'approche markovienne. Par ailleurs, les formules de la CEI 61508, qui sont formellement fausses comme nous l'avons déjà montré à la section 2.3, induisent des résultats inférieurs à ceux fournis par les autres approches. Par conséquent, les formules de la CEI 61508 pourraient conduire à des SIL sous-estimés, ce qui est dangereux. Il convient de noter que les résultats obtenus ne tiennent pas compte de la contribution des DCC. Leur considération, pourrait réduire les divergences constatées. Toutefois, même avec la prise en compte des DCC, la possibilité d'aboutir à des SIL erronés via l'usage des formules de la CEI 61508 reste toujours envisageable.

2.5. Conclusion

Les systèmes instrumentés de sécurité constituent une barrière de sécurité vitale pour prévenir ou maitriser l'occurrence des événements dangereux. L'objectif principal de ce travail était de vérifier la validité des formules analytiques relatives à la *PFH* fournie par la norme internationale CEI 61508. Cette mesure fiabiliste, rappelons-le, représente la fréquence moyenne de défaillance d'un système fonctionnant en forte demande ou en demande continue. Ces formules tiennent compte de la possibilité de mise en état de repli de sécurité de l'*EUC* consécutive à la détection d'une défaillance dangereuse au niveau du SIS. Pour cette fin, les configurations *KooN* basiques traitées dans cette norme ont été modélisées à l'aide de modèles markoviens multi-phases et approchés. De nouvelles formules de la *PFH* ont été dérivées à partir des modèles approchés. L'examen de ces formules a montré que les formules de la CEI 61508 ne sont valables que pour le cas où le nombre de défaillances DD entraînant un arrêt d'urgence automatique N-K+1 = 1 (configurations : 1oo1 et 2oo2). Cette remarque pourrait être généralisée aux systèmes *NooN*. Pour N-K+1 ≠ 1, les nouvelles formules contiennent des termes supplémentaires par rapport aux formules de la CEI 61508. Ainsi, ces dernières formules induisent des résultats de *PFH* sous-estimés ce qui est dangereux d'un point de vue sécuritaire. Ce fait a été confirmé par de différentes comparaisons numériques.

Chapitre 3

Etude comparative des formulations analytiques relatives à la PFH et nouvelles généralisations

3.1. Introduction

Après avoir procédé au deuxième chapitre à une vérification approfondie des formules analytiques de la *PFH* fournies par la deuxième édition de la CEI 61508, via les graphes de Markov, l'objet de ce troisième chapitre est l'élargissement de l'éventail de la précédente étude comparative. Pour ce faire, ce chapitre est consacré à l'étude des différentes expressions analytiques relatives à la *PFH* des architectures *KooN* retrouvées dans la littérature. Plus précisément, les formules *PFH* considérées sont celles données dans les deux éditions de la norme CEI 61508 (première et deuxième éditions) [CEI 61508, 2002 ; CEI 61508, 2010], le manuel PDS [PDS, 2010] et les nouvelles formules développées au chapitre précédent.

Le reste de ce chapitre est organisé comme suit. Nous commençons d'abord par présenter les différents ensembles de formules *PFH* considérées. Les paramètres utilisés et leurs hypothèses sous-jacentes sont mis en évidence. Nous conduisons ensuite une étude comparative des résultats numériques qu'elles produisent en se référant aux valeurs numériques dérivées des modèles de Markov multi-phases et approchées considérés comme références dans le présent document. Puis, afin de consolider cette comparaison numérique, nous faisons un ultime recours à un autre type de modèles comportementaux des configurations *KooN* : Réseaux de Petri (RdP) animés par simulation de Monte Carlo. En effet, nous développons des modèles *RdP* pour l'ensemble des configurations étudiées et comparons les résultats qu'ils induisent à ceux précédemment retrouvés. Par ailleurs, des généralisations pour chaque ensemble de formules *PFH* sont proposées. Ces généralisations permettent le calcul de la *PFH* d'une architecture *KooN* quelconque. Finalement, la dernière partie de ce chapitre est dédiée à une étude détaillée de la configuration 2oo3 en termes de résultats numériques. Les conclusions obtenues sont confirmées à travers le traitement d'un système réel. Ce focus sur l'architecture 2oo3 était motivé par l'usage intensif de cette architecture dans l'industrie.

3.2. Différentes formules analytiques relatives à la *PFH*

Malgré le pouvoir de modélisation et la précision de calcul des méthodes relevant du domaine de la sûreté de fonctionnement des systèmes (arbres de défaillances, chaines de Markov, …), les spécialistes de la sécurité industrielle, pour une large part, préfèrent toujours utiliser des formules simplifiées, en particulier si elles sont fournies par des normes internationales ou des référentiels industriels. Cette section regroupe trois séries de formules bien connues de *PFH* ainsi que les formules nouvellement développées.

3.2.1. Formules de la *PFH* fournies par la CEI 61508 (1ère édition)

Le tableau 3.1 regroupe les formules présentées dans la partie 6 de la CEI 61508 (1ère édition) pour le calcul de la *PFH* des configurations *KooN* de base (1oo1, 1oo2, 2oo2, 1oo3, 2oo3). Il convient de noter qu'afin de considérer la capacité d'arrêt d'urgence automatique de l'*EUC* suite à la détection d'une défaillance dangereuse du SIS, les formules du tableau 3.1 diffèrent sommairement de celles de la CEI 61508. En effet, nous les avons légèrement corrigées en supprimant la contribution des défaillances de cause commune détectées: $\beta_D \lambda_{DD}$.

Tableau 3.1 : Formules de *PFH* fournies par la CEI 61508 (1ère éd.)

KooN	***PFH***
1oo1	λ_{DU}
1oo2	$2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} + \beta\lambda_{DU}$
1oo3	$6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^3 t_{CE} t_{GE} + \beta\lambda_{DU}$
2oo2	$2\lambda_{DU}$
2oo3	$6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} + \beta\lambda_{DU}$

Avec :

- La CEI 61508 ne considère pas les DCC pour les configurations *NooN*.
- $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}\ MTTR$
- $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}\ MTTR$
- $MTTR$ (Mean Time To Restoration) : temps moyen de réparation pour les défaillances dangereuses détectées (DD) et non détectées (DU).
- T_1: Intervalle de de tests périodiques. Les tests permettent de révéler des défaillances dangereuses non détectées.
- L'architecture 1oo3 n'est pas abordée dans la première édition de la CEI 61508. La formule correspondante est dérivée sur la base de la généralisation donnée dans [Innal, 2008].

Nous donnons ci-après une généralisation qui néglige la contribution des défaillances dangereuses DCC : non prise en compte du terme $\beta_D \lambda_{DD}$. Bien entendu, cette simple généralisation peut incorporer des séquences contenant *N*-*K*+1 défaillances DD. Néanmoins,

comme la probabilité de ces dernières séquences peut être numériquement négligée devant celles des autres séquences, la généralisation suivante reste valide.

$$PFH_{KooN} = A_{N-K+1}^{N}[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^{N-K} \cdot [f_1(\beta_D)\lambda_{DD} + f_2(\beta)\lambda_{DU}] \prod_{i=1}^{N-K} MDT_i + f_3(\beta)\lambda_{DU} \quad (3.1)$$

Avec :

$A_{N-K+1}^{N} = \frac{N!}{(K-1)!}$

$MDT_i = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{i+1} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

$f_1(\beta_D) = \begin{cases} (1-\beta_D) & \text{pour } N \neq K \\ 0 & \text{pour } N = K \end{cases}$

$f_2(\beta) = \begin{cases} (1-\beta) & \text{pour } N \neq K \\ 1 & \text{pour } N = K \end{cases}$

$f_3(\beta) = \begin{cases} \beta & \text{pour } N \neq K \\ 0 & \text{pour } N = K \end{cases}$

3.2.2. Formules de la *PFH* fournies par la CEI 61508 (2ème édition)

Dans cette deuxième édition, les formules de la *PFH* ont été complètement révisées. Comme indiqué précédemment, cette révision prend en compte l'hypothèse selon laquelle le SIS) l'*EUC* dans un état sûr dès la détection d'une défaillance dans l'un des N–K+1 canaux. Cette hypothèse reste évidemment valable pour les DCC : le terme $\beta_D\lambda_{DD}$ n'est plus incorporé dans les formules révisées. Ces formules sont regroupées dans le tableau 3.2.

Tableau 3.2 : Formules de *PFH* fournies par la CEI 61508 (2ème éd.)

KooN	***PFH***
1oo1	λ_{DU}
1oo2	$2\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$
1oo3	$6\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)^2(1-\beta)\lambda_{DU}t_{CE}t_{GE} + \beta\lambda_{DU}$
2oo2	$2\lambda_{DU}$
2oo3	$6\big((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$

Avec :

- La CEI 61508 ne considère pas les DCC pour les configurations *NooN*.
- $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

- $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}\ MTTR$

- *MRT* (*Mean Repair Time*) : temps moyen de réparation pour les défaillances dangereuses non détectées (DU). En introduisant le paramètre *MRT*, la CEI 61508 fait une distinction entre le temps de réparation pour les défaillances DD et DU. Cependant, tout calcul effectue dans la CEI 61508 suppose que *MRT* = *MTTR*.

La lecture du tableau 3.2 nous permet d'établir la généralisation donnée ci-dessous.

$$PFH_{KooN} = A^N_{N-K+1}[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^{N-K} \cdot f_2(\beta)\lambda_{DU} \prod_{i=1}^{N-K} MDT_i + f_3(\beta)\lambda_{DU} \quad (3.2)$$

3.2.3. Formules de la *PFH* fournies dans le manuel PDS

Les différentes expressions de la *PFH* présentées par le manuel PDS [Hauge *et al.*, 2010] sont données au tableau 3.3.

Tableau 3.3 : Formules *PFH* fournies par le manuel PDS

KooN	***PFH***
1oo1	λ_{DU}
1oo2	$(\lambda_{DU}\ \tau)^2/\tau + \beta\ \lambda_{DU}$
1oo3	$(\lambda_{DU}\ \tau)^3/\tau + C_{1oo3}\ .\ \beta\ \lambda_{DU}$
2oo2	$2\lambda_{DU}$
2oo3	$3\ (\lambda_{DU}\ \tau)^2/\tau + C_{2oo3}\ .\ \beta\ \lambda_{DU}$

Avec :

- $M = K$.
- $\tau = T_1$: Intervalle de tests périodiques.
- La contribution des défaillances dangereuses détectées n'est pas prise en compte. Cela signifie que le SIS met l'*EUC* dans un état sûr dès la détection d'une défaillance dans un canal.
- Le temps de réparation pour les défaillances dangereuses non détectées est ignoré (négligé devant τ).
- Contrairement à la CEI 61508, la contribution des DCC est incluse à l'aide du modèle du facteur bêta généralisé [Hokstad et Corneliussen, 2004 ; Hokstad *et al.*, 2006], où le

facteur C_{MooN} est introduit. Les valeurs typiques pour ce facteur sont données dans le tableau 3.4.

- Les DCC pour les configurations *NooN* ne sont pas considérees.

Tableau 3.4 : Valeurs typiques du facteur C_{MooN}

MooN	**N=2**	**N=3**	**N=4**	**N=5**	**N=6**	**N=7**	**N=8**
M=1	1.0	0.5	0.3	0.21	0.17	0.15	0.15
M=2		2.0	1.1	0.7	0.4	0.27	0.15
M=3			2.9	1.8	1.1	0.8	0.6
M=4				3.7	2.4	1.6	1.1
M=5					4.3	3.0	2.1
M=6						4.8	3.5
M=7							5.3

La généralisation suivante est proposée dans le manuel PDS:

$$PFH_{KooN} = \begin{cases} \dfrac{N!}{(N-M+1)!\ (M-1)!}\ [(\lambda_{DU}\,\tau)^{N-M+1}/\tau] \ +\ C_{MooN}\,.\beta\lambda_{DU} & \text{pour } N \neq M \\ N\lambda_{DU} & \text{pour } N = K \end{cases} \tag{3.3}$$

3.2.4. Formules de la *PFH* nouvellement développées

Les formules dérivées dans le deuxième chapitre sont regroupées dans le tableau 3.5. Rappelons que ces formules ont été développées, en se basant sur des modèles markoviens approchés, afin de vérifier la validité de celles données dans la CEI 61508 (2ème éd.).

Tableau 3.5 : Nouvelles formules *PFH*

KooN	***PFH***
1oo1	λ_{DU}
1oo2	$2\big((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\big)t_{CE1}\lambda_{DU}+\beta\lambda_{DU}+$ $2(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)\lambda_{DD}$
1oo3	$6\big((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\big)t_{CE1}t_{GE1}\lambda_{DU}+\beta\lambda_{DU}+$ $6\big((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\big)(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)t_{GE1}\lambda_{DD}+$ $3\left((1-\beta_D)\lambda_{DD}\,MTTR+(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)\right)\beta\lambda_{DU}$ $+3(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)\beta_D\lambda_{DD}$
2oo2	$(2-\beta)\lambda_{DU}$
2oo3	$6\big((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\big)t_{CE1}(1-\beta)\lambda_{DU}+\beta\lambda_{DU}+$ $6(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)(1-\beta_D)\lambda_{DD}+$ $3\left((1-\beta_D)\lambda_{DD}\,MTTR+(1-\beta)\lambda_{DU}\left(\frac{T1}{2}+MRT\right)\right)\beta\lambda_{DU}$

Avec :

- La contribution des DCC à la *PFH* est traitée à l'aide du modèle du facteur bêta.
- Les DCC pour les configurations *NooN* sont prises en compte.
- $t_{CE1}=\frac{(1-\beta)\lambda_{DU}}{\lambda_D^{ind}}\left(\frac{T_1}{2}+MRT\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D^{ind}}\,MTTR$
- $t_{GE1}=\frac{(1-\beta)\lambda_{DU}}{\lambda_D^{ind}}\left(\frac{T_1}{3}+MRT\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D^{ind}}\,MTTR$
- $\lambda_D^{ind}=(1-\beta)\lambda_{DU}+(1-\beta_D)\lambda_{DD}$

Afin d'étendre les développements donnés au tableau 3.5 au cas général des configurations *KooN*, nous proposons la généralisation donnée par l'équation (3.4).

$$PFH_{KooN} = A_{N-K+1}^{N}[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^{N-K} \cdot f_1(\beta)\lambda_{DU} \prod_{i=1}^{N-K} MDT_i$$
$$+ A_{N-K+1}^{N}\,(1-\beta)\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^{N-K-1} \cdot$$
$$f_2(\beta_D)\lambda_{DD} \prod_{i=2}^{N-K} MDT_i$$
$$+ f_3(\beta)\lambda_{DU} + N(1-\beta_D)\lambda_{DD}\, MTTR\, f_4(\beta)\lambda_{DU}$$
$$+ N(1-\beta)\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)[f_4(\beta)\lambda_{DU} + f_5(\beta_D)\lambda_{DD}] \qquad (3.4)$$

Avec :

$$MDT_i = \frac{(1-\beta)\lambda_{DU}}{\lambda_D^{ind}}\left(\frac{T_1}{i+1} + MRT\right) + \frac{(1-\beta_D)\lambda_{DD}}{\lambda_D^{ind}}\, MTTR$$

$$\lambda_D^{ind} = (1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD}$$

$$f_1(\beta) = \begin{cases} (1-\beta) & \text{pour } K > 1 \\ 1 & \text{pour } K = 1 \end{cases}$$

$$f_2(\beta_D) = \begin{cases} (1-\beta_D) & \text{pour } K > 1 \text{ et } K \neq N \\ 1 & \text{pour } K = 1 \text{ et } K \neq N \\ 0 & \text{pour } K = N \end{cases}$$

$$f_3(\beta) = \begin{cases} \beta & \text{pour } N > 1 \\ 0 & \text{pour } N = 1 \end{cases}$$

$$f_4(\beta) = \begin{cases} \beta & \text{pour } N > 2 \text{ et } K \neq N \\ 0 & \text{pour } N \leq 2 \text{ ou } N = K \end{cases}$$

$$f_5(\beta_D) = \begin{cases} \beta_D & \text{pour } N > 2 \text{ et } K = 1 \\ 0 & \text{pour } N \leq 2 \text{ ou } K > 1 \end{cases}$$

L'inspection des deux généralisations liées aux formules présentées dans la CEI 61508 (2ème éd.) (Eq. (3.2)) et à celles nouvellement établies (Eq. (3.4)), permet de constater les divergences suivantes :

- Dans l'équation (3.2), les termes MDT_i sont calculées en utilisant des taux de défaillances indépendantes : $(1-\beta)\lambda_{DU}$ et $(1-\beta_D)\lambda_{DD}$ au lieu de λ_{DU} et λ_{DD}. Cette modification est justifiée car il s'agit bien des séquences de défaillances indépendantes. Toutefois, ce changement aurait un impact minime sur les résultats numériques.
- Pour la quantité $f_1(\beta)\lambda_{DU}$: la définition de la fonction $f_1(\beta)$ permet de prendre en compte le fait que le dernier événement d'une séquence de défaillance (finissant par une défaillance DU) dans une architecture 1ooN se caractérise par un taux λ_{DU} et non pas $(1-\beta)\lambda_{DU}$, car un seul canal reste en marche avant l'occurrence d'une telle défaillance.

- Le deuxième terme de la sommation dans l'équation (3.4) représente les séquences de défaillances indépendantes non prises en compte dans les formules de la deuxième édition de la CEI 61508 (Eq. (3.2)).
- Les deux derniers termes de la sommation dans l'équation (3.4) représentent les séquences de défaillances débutant par une défaillance DD ou DU indépendante et terminant par une défaillance de cause commune (détectée ou non détectée). Cette quantité n'est également pas prise en compte par la CEI 61508.
- Les différentes quantités qui manquent à l'appel dans le cadre de la CEI 61508 (2ème éd.) engendrent des résultats sous-estimes. Ce fait nous l'avons déjà souligné au chapitre précédent.

3.3. Modélisation des configurations *KooN* via les réseaux de Petri (RdP) stochastiques

Les réseaux de Petri (RdP), en particulier grâce à leur formalisme graphique et aux outils mathématiques sous-jacents, sont couramment utilisés dans la modélisation et l'évaluation de performance des systèmes complexes actuels. Plus précisément, les RdP offrent un outil adéquat et puissant pour modéliser des systèmes complexes en termes de concurrence (parallélisme), d'aspects séquentiels, de synchronisation, de partage de ressources et d'exclusion mutuelle (situations conflictuelles).

L'objet de cette section est de construire des modèles RdP pour les configurations *KooN* considérées, en prenant en compte la capacité d'arrêt automatique d'urgence, afin de permettre une comparaison numérique réfléchie des différents ensembles de formules *PFH*.

3.3.1. Principes de base relatifs aux RdP

Les RdP ont été développés par Carl Adam Petri lors de son travail doctoral sur la communication avec les automates. Dans la suite, la présentation des RdP est délibérément limitée aux concepts nécessaires utilisés dans le cadre de ce manuscrit. Une description détaillée de ce formalisme est donnée dans [David et Alla, 2010]. Un RdP est une notation graphique avec une structure mathématique sous-jacente adaptée à la modélisation de systèmes événementiels (systèmes à événements discrets) [Gu et Bahri 2002; Sachdeva *et al.*, 2008]. Il peut être identifié comme un type particulier de graphe orienté qui contient deux parties [CEI 61508, 2010 ; Blume *et al.*, 2007] :

- Partie statique comprenant trois objets :
  - *Les Places*, représentées par des cercles ou des ovales dans la représentation graphique, sont des états des composants du système.
  - *Les transitions,* dessinées sous forme de barres, correspondant à des événements potentiels modifiant l'état d'un réseau de Petri. Des délais peuvent être attribués aux transitions (par exemple, le temps requis pour exécuter une tâche donnée).
  - *Les arcs orientés* relient des places à des transitions (*arcs amont*) et des transitions à des places (*arcs aval*). Les arcs sont pondérés avec un nombre positif. Par exemple, le poids d'un arc amont peut indiquer les ressources nécessaires pour réaliser une action donnée, tandis que celui d'un arc aval peut indiquer la quantité résultant de cette action. Ce poids est égal à un s'il n'est pas explicitement mentionné sur le graphe.

- Partie dynamique:
  - *Jetons* représentés par de petits points solides. Chaque place peut potentiellement contenir aucun ou un nombre positif de jetons. La distribution des jetons à certaines places est appelée *marquage*. Les jetons traversent les transitions lorsque des événements se produisent. Un jeton peut, par exemple, représenter la présence ou l'absence d'une ressource.
  - *Prédicats ou gardes* : toute formule qui peut être vraie ou fausse, permettant la *validation* des transitions. Il est à noter qu'une transition est *valide* (*franchissable, sensibilisée*) lorsque toutes ses places d'entrée contiennent au moins le nombre de jetons requis par chaque arc amont (indiqué par son poids) et que tous les prédicats sont «vrais».
  - *Assertions*, toute équation mettant à jour certaines variables lorsqu'une transition est déclenchée ou *franchie*. Une transition est franchie si elle est valide et que le délai requis est écoulé (durée entre la validation et le franchissement). Ce délai peut être déterministe ou stochastique (délai aléatoire, par exemple exponentiel négatif). Si ce délai est nul, la validation coïncide avec le franchissement.
  - Lors du franchissement d'une transition, ses places d'entrée perdent autant de jetons que spécifiés par les poids des arcs amont respectifs, ses places de sortie gagnent autant de jetons que spécifiés par les poids des arcs aval respectifs et les assertions sont mises à jour.

Dans le cas où des transitions déterministes et stochastiques sont impliquées, les RdP ne peuvent pas être résolus facilement à l'aide d'approches analytiques. Cela dit, la simulation de Monte Carlo est généralement utilisée [Zio, 2013]. Son idée principale est d'utiliser des nombres aléatoires pour animer un modèle comportemental du système réel et donc de produire un large échantillon à partir duquel des statistiques sont obtenues (moyenne, variance et intervalle de confiance).

La figure 3.1 montre un RdP relatif au comportement d'un composant réparable. Il possède quatre places $\{P_1, P_2, P_3, P_4\}$ et trois transitions $\{T_1, T_2, T_3\}$. Initialement (à $t = 0$), le marquage du RdP peut être représenté par le vecteur $M_0 = [1, 0, 0, 3]$, ce qui signifie qu'il existe initialement un jeton dans P_1, pas de jetons dans P_2 et P_3 et trois jetons dans P_4. Les places P_1, P_2 et P_3 correspondent aux états possibles du composant et représentent respectivement les états de marche, en attente de réparation et en réparation. P_4 est une place auxiliaire qui modélise la disponibilité de l'équipe de réparation (quatre réparateurs sont disponibles). Les transitions T_1, T_2 et T_3 modélisent les événements se produisant sur le composant, respectivement : défaillance, début de réparation et fin de réparation. De plus, les transitions T_1 et T_3 possèdent des délais stochastiques définis par $d_1 = f(\lambda)$ et $d_3 = g(\mu)$, respectivement. Nous considérons par exemple que f et g sont des fonctions exponentielles négatives *:* λ_C et μ_C se rapportent respectivement aux taux de défaillance et de réparation. La transition T_2 est déterministe ($d_2 = 0$: transition instantanée). Initialement, seule la transition T_1 est valide, car le poids de son arc amont (reliant P_1 à T_1) est égal au marquage de P_1 (nombre de jetons = 1). T_1 est franchie (tirée) dès que son délai d_1 est écoulé. d_1 est un délai stochastique obtenue par échantillonnage de Monte Carlo en utilisant la transformation inverse de la fonction f: $d_1 = -(1/\lambda) \cdot \ln(R)$, où R est une variable aléatoire uniformément répartie sur [0, 1]. Le tir de T_1 entraîne la suppression du jeton de P_1, l'ajout d'un jeton dans P_2 et donner l'assertion «working = false». Le composant atteint un état de défaillance et attend la réparation. Par conséquent, la transition T_2 est activée si les pièces de rechange sont disponibles (garde: Spare parts = true). La variable Spare parts (pièces de rechange) peut être mise à jour en fonction de l'évolution d'un RdP supplémentaires liés, par exemple, à d'autres composants et à la chaîne d'approvisionnement en pièces de rechange. La réparation du composant implique deux réparateurs : le poids de l'arc amont reliant P_4 à T_2 est égal à 2. Ainsi, le tir de T_2 a pour effet de retirer le jeton de la place P_2 et deux jetons de la place P_4 et un jeton apparaît à la place P_3. Et ainsi de suite tant que le tir de la prochaine transition valide appartient à la période d'observation.

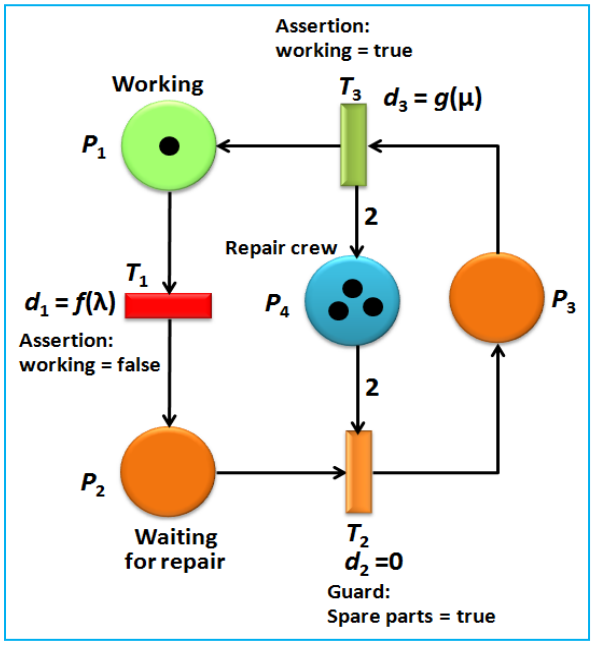

Figure 3.1 : RdP d'un composant réparable

3.3.2. RdP des configurations *KooN*

La définition de chacune des architectures est donnée au niveau du deuxième chapitre. Nous nous limitons donc à la présentation directe des différents RdP correspondants. Notons que tous les RdP suivants ont été saisis à l'aide du logiciel GRIF [GRIF, 2018]. Quelques explications relatives à la syntaxe utilisée sont données ci-dessous :

- **# *i*** : le marquage de la place *i*.
- **!** : introduit une liste des assertions qui se mettent à jour lors du tire des transitions.
- **?** : spécifie une liste des gardes qui doivent être vérifiées pour que la transition soit activée.
- **drc d**: loi de Dirac pour le délai **d** (délai déterministe).
- **exp x**: transition avec un délai stochastique suivant une fonction exponentielle négative ayant le paramètre **x**.
- **@ (*k*) (e_1, e_2,…, e_n)** est une logique de type *k* parmi *n* (e_i sont des expressions booléennes).
- Les informations mentionnées au niveau d'une transition donnée sont données dans l'ordre suivant: numéro, nom, loi caractérisant le délai de tir, gardes et assertions.

3.3.2.1. Configuration 1oo1

La figure 3.2 donne le RdP relatif à cette première configuration. Le canal (C) est initialement opérationnel (# 1 = 1). A partir de cet état, il peut subir soit une défaillance DD (transition N°1 pour atteindre la place 2), soit une défaillance DU (transition N°2 pour atteindre la place 3). Suite à une défaillance DD, le canal passe immédiatement à l'état d'arrêt

d'urgence (place 4), car le délai relatif à la transition N°3 est nul (drc 0). Suite à une panne DU, la place 3 reste marquée jusqu'à l'occurrence du prochain test périodique (? PT= true). Une fois cette condition vérifiée, l'état d'arrêt d'urgence est immédiatement atteint et le canal retrouve son état initial après une durée moyenne égale à 1/MSD=MTTRsd. Les tests périodiques sont modélisés à l'aide du RdP situé à droite.

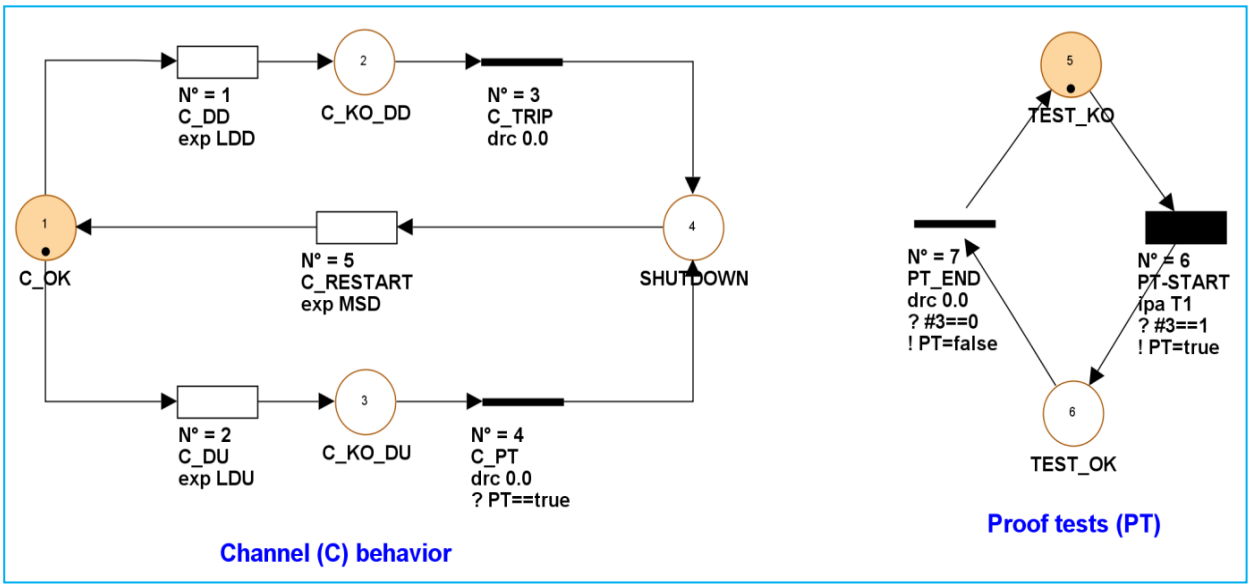

Figure 3.2 : RdP relatif à la configuration 1oo1

3.3.2.2. Configuration 2oo2

La figure 3.3 donne le RdP relatif à la configuration 2oo2. Les deux canaux (C1 et C2) sont initialement opérationnels (# 1 = 1 ; # 5 = 1). Chaque canal a quatre possibilités de défaillance : défaillance DD indépendante (transition C1_DD, pour le canal 1), défaillance DU indépendante (transition C1_DU, pour le canal 1), défaillance DD de cause commune (transition C1_CCFDD, pour le canal 1) et une défaillance DU de cause commune (transition C1_CCFDU, pour le canal 1). Suite à au moins une défaillance DD dans l'un des canaux, le système passe immédiatement à l'état d'arrêt d'urgence (place 12), car la garde ? # 2 = 1 or # 6= 1 sur la transition S_SHUTDOWN est vérifiée. Le système retrouve ensuite son état initial (# 1 = 1 ; # 5 = 1) après une durée moyenne égale à 1/MSD=MTTRsd. Aussi, le système tombe en panne (transition S_FAILURE) si au moins l'un des canaux subit une défaillance DU : ? # 3 = 1 or # 7= 1. Suite à une panne DU dans un canal, la place correspondante (place 3 ou place 7) reste marquée jusqu'à soit l'occurrence du prochain test périodique (? PT= true), soit un arrêt d'urgence automatique provoqué par une défaillance DD de l'autre canal (? TRIP= true). Il convient de noter que chaque composant peut être mis en attente (Standby)

suite à un arrêt d'urgence de l'EUC (? TRIP= true). Dans cet état, le canal ne peut pas tomber en panne.

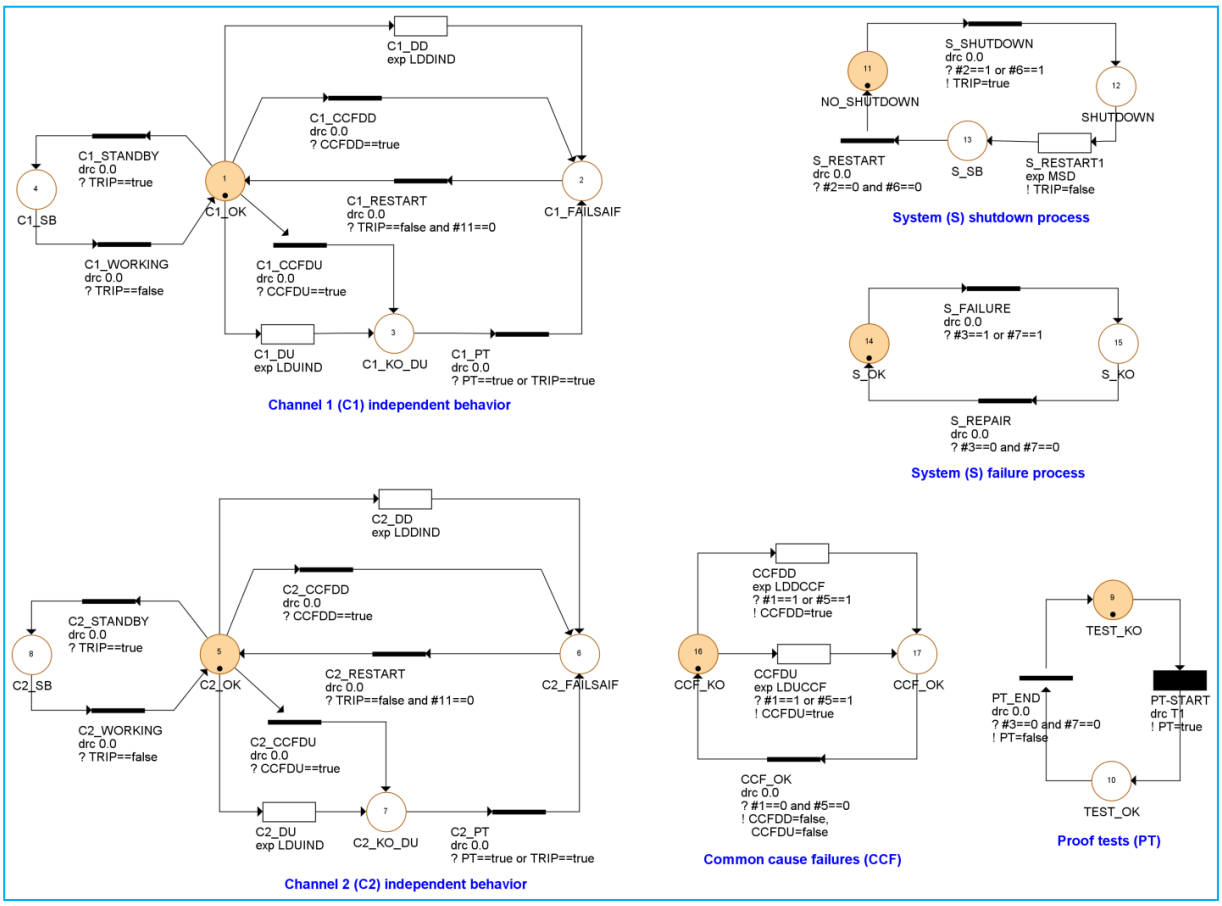

Figure 3.3 : RdP relatif à la configuration 2oo2

3.3.2.3. Configuration 1oo2

Les deux principaux RdP de la figure 3.4 représentent le comportement de chaque canal pouvant avoir trois états possible (fonctionnement initial, défaillance DD et défaillance DD). Les défaillances DD et DU de chaque canal peuvent se produire indépendamment ou à la suite d'événements CCF. Ces derniers événements sont pris en compte via un RdP auxiliaire contenant les places 9 et 10. Les défaillances DU sont révélés par des tests périodiques (? PT = true), modélisés par le RdP contenant les places 7 et 8. De plus, un arrêt automatique d'urgence de l'EUC est produit lorsque les deux canaux rencontrent une défaillance DD. Cette condition est caractérisée à l'aide de la garde ? # 3 == 1 and # 5 == 1, où les places 3 et 5 représentent respectivement une défaillance DD des premier et deuxième canaux. L'arrêt d'urgence se produit (!TRIP = true) instantanément puisque le délai relatif à la transition correspondante (S_SHUTDOWN) est nul (drc 0). Après un tel arrêt, le système 1oo2 retrouve son état initial après une durée moyenne égale à 1/MSD. Par ailleurs, cette architecture

devient indisponible si les deux canaux ne sont pas opérationnels et l'EUC n'est pas en état d'arrêt d'urgence: ?(# 1 == 0 and # 4 == 0) and TRIP == false (garde sur la transition S_FAILURE). Le système 1oo2 redevient opérationnel dès que l'un des canaux retrouve son état initial : ?(# 1 == 1 or # 4 == 1) (garde sur la transition S_REPAIR).

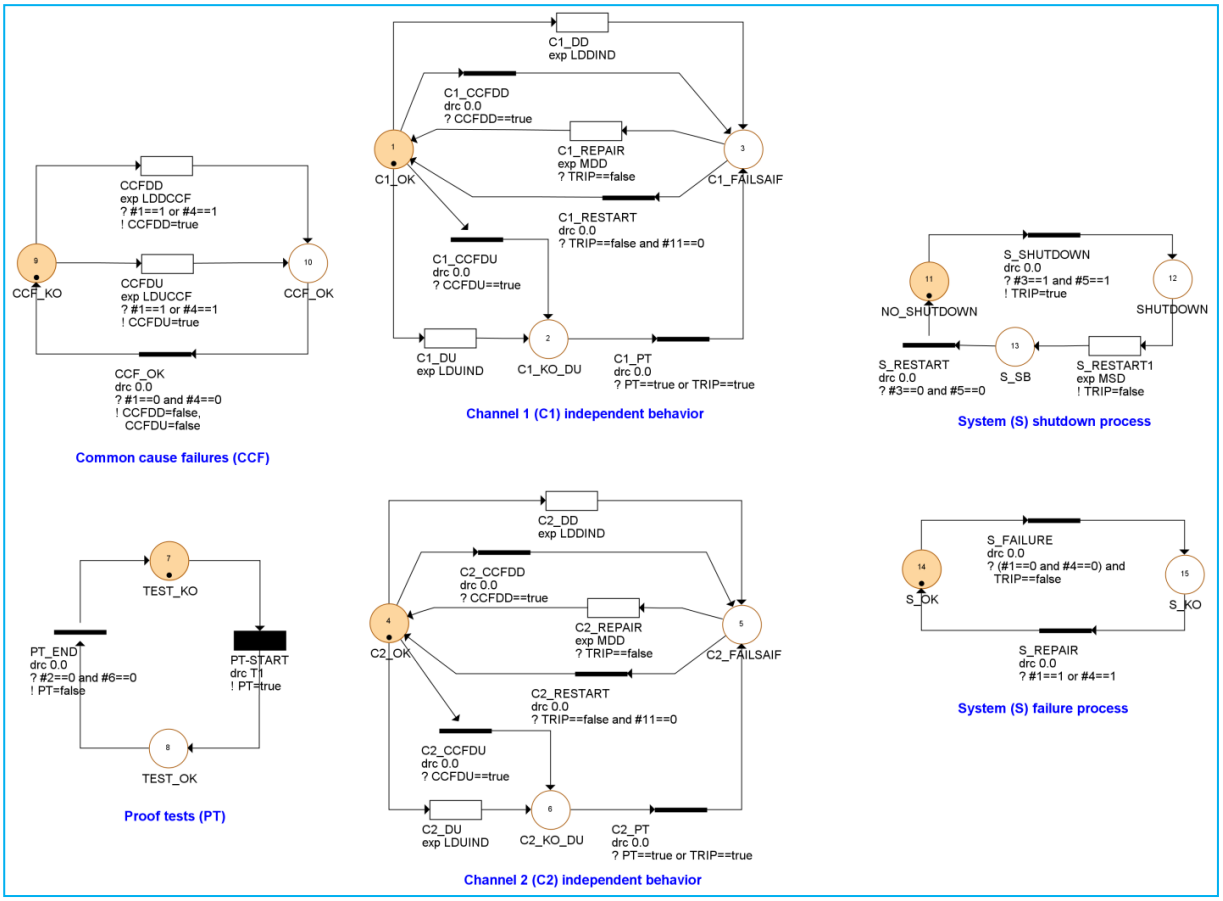

Figure 3.4 : RdP relatif à la configuration 1oo2

3.3.2.4. Configuration 2oo3

Les trois principaux RdP de la figure 3.5 représentent le comportement de chaque canal pouvant avoir quatre états possibles (fonctionnement initial, défaillance DD, défaillance DD et Standby). Notez que les défaillances DD et DU de chaque canal peuvent se produire indépendamment ou à la suite d'événements CCF. Ces derniers événements sont pris en compte via un RdP dédié (contenant les places 12 et 13). Les défaillances DU sont révélés par des tests périodiques (? PT = true), modélisés par le RdP contenant les places 10 et 11. De plus, un arrêt automatique d'urgence de l'EUC est réalisé chaque fois que deux canaux rencontrent une défaillance DD. Cette condition est caractérisée à l'aide de la garde ? @ (2) (# 2 == 1, # 5 == 1, # 8 == 1), où les places 2, 5 et 8 représentent une défaillance DD du premier, deuxième et troisième canal, respectivement. L'arrêt d'urgence se produit (!TRIP = true)

instantanément puisque le délai relatif à la transition correspondante (S_SHUTDOWN) est nul (drc 0). Après un tel arrêt, le système 2oo3 retrouve son état initial après une durée moyenne égale à 1/MSD. Par ailleurs, cette architecture devient indisponible si au moins deux canaux ne sont pas opérationnels et l'EUC n'est pas en état d'arrêt d'urgence: ? @ (2) (# 1 == 0, # 4 == 0, # 7 == 0) and TRIP == false (garde sur la transition S_FAILURE). Le système 2oo3 retrouve un état de fonctionnement dès que deux canaux deviennent opérationnels.

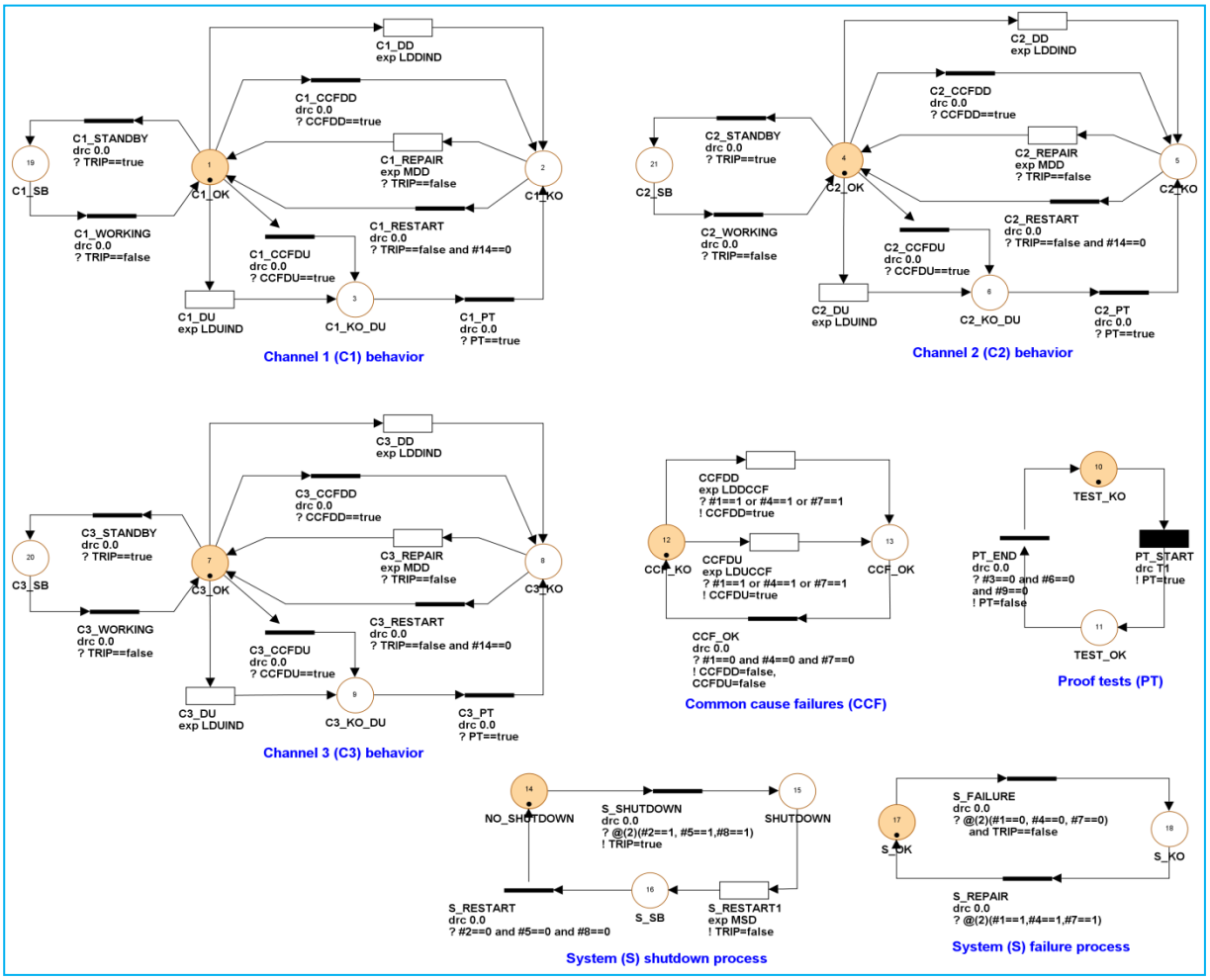

Figure 3.5 : RdP relatif à la configuration 2oo3

3.3.2.5. Configuration 1oo3

Les trois principaux RdP de la figure 3.6 représentent le comportement de chaque canal pouvant avoir trois états possibles (fonctionnement initial, défaillance DD et défaillance DD). Les défaillances DD et DU de chaque canal peuvent se produire indépendamment ou à la suite d'événements CCF. Les défaillances DU sont révélés par des tests périodiques (? PT = true). De plus, un arrêt automatique d'urgence de l'EUC est produit lorsque les trois canaux rencontrent une défaillance DD. Cette condition est caractérisée via la garde ? # 2 == 1 and #

5 == 1 and # 8 == 1 sur la transition S_SHUTDOWN. Après un tel arrêt, le système 1oo3 retrouve son état initial après une durée moyenne égale à 1/MSD. Par ailleurs, cette architecture devient indisponible si les trois canaux ne sont pas opérationnels et l'EUC n'est pas en état d'arrêt d'urgence: ?(# 1 == 0 and # 4 == 0 and # 7 == 0) and TRIP == false (garde sur la transition S_FAILURE). Le système 1oo3 redevient opérationnel dès que l'un des canaux retrouve son état initial : ?(# 1 == 1 or # 4 == 1 or # 7 == 1) (garde sur la transition S_REPAIR).

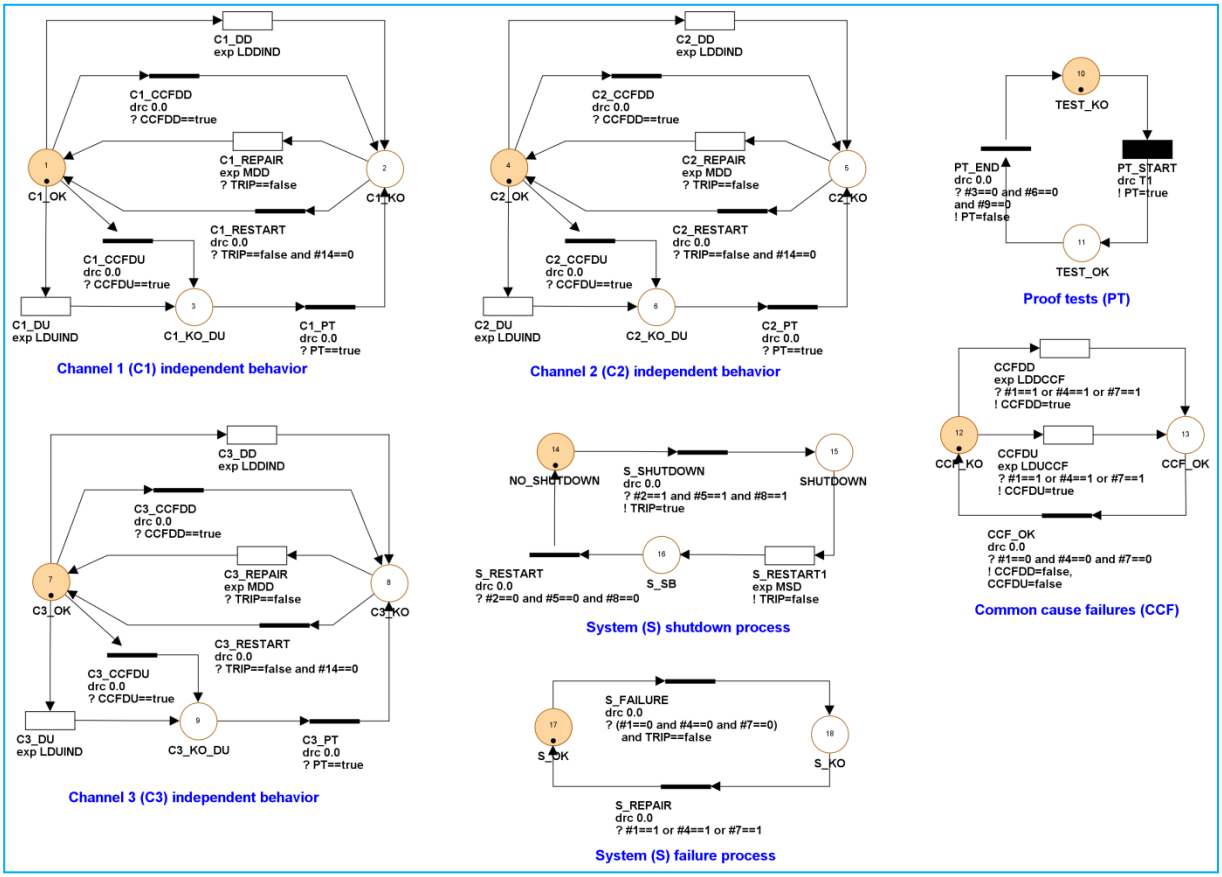

Figure 3.6 : RdP relatif à la configuration 1oo3

3.4. Comparaison des résultats des différentes séries de formules

Afin d'examiner les différents ensembles de formules *PFH*, une comparaison numérique des résultats qu'ils induisent est effectuée. En outre, les résultats dérivés des modèle de Markov multi-phases, développés au chapitre précédent, et RdP sont présentés. Cela aide à conclure concernant l'exactitude et la validité de chaque série de formules de la *PFH*. Les calculs ont été effectués en utilisant le jeu de paramètres suivants : λ_D = 2.5E–5h^{-1}; *MTTR* = *MRT* = 8 *h*; T_1 = 8760 *h*. Différentes valeurs pour les facteurs *DC*, β et β_D ont été

utilisées. Les résultats obtenus sont présentés au tableau 3.6. Les *PFH* moyennes sont calcules sur une période d'observation de 5 ans.

L'examen du tableau 3.6 montre que les résultats de la *PFH* pour la configuration 1oo1 produits par les différentes formules analytiques sont identiques et légèrement conservatifs par rapport à ceux dérivés des modèles markovien multi-phases (MMP) et RdP correspondants. Ces deux derniers modèles représentent le plus fidèlement possible le comportement des configurations *KooN* et fournissent des résultats presque identiques pour l'ensemble des configurations *KooN*. Pour la configuration 2oo2, cet aspect conservatif est toujours maintenu. Cependant, les nouvelles formules développées donnent des résultats légèrement inférieurs à ceux des trois premières séries de formules. Cela est dû au fait que les nouvelles formules incorporent le terme (2-β), alors que les autres formules négligent raisonnablement le facteur β devant 1. De plus, les écarts entre les valeurs numériques fournies par les nouvelles formules et celles des modèles de Markov et RdP diminuent lorsque les valeurs de *DC* augmentent (voir figure 3.7). Cette dernière remarque est toujours applicable pour les autres configurations *KooN* étudiées (1oo2, 1oo3 et 2oo3). Globalement, les formules analytiques utilisées fournissent des résultats valides pour les configurations 1oo1 et 2oo2. Cette conclusion pourrait être généralisée aux configurations *NooN*.

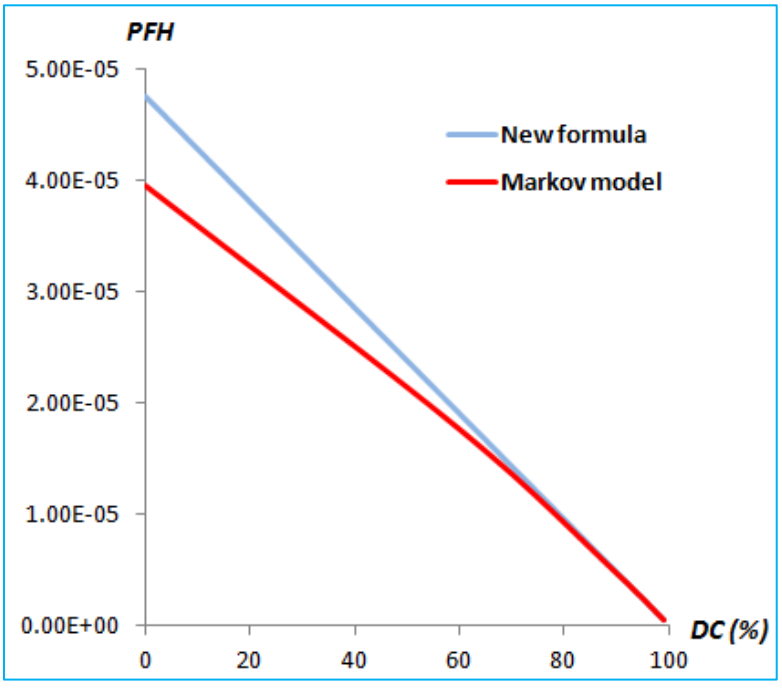

Figure 3.7 : *PFH* relatif à la configuration 2oo2 en fonction de *DC* (β=0.1)

Tableau 3.6 : Résultats relatifs à la *PFH* (h^{-1})

KooN	*DC* (%)	*β* (%)	Séries de formules et modèles *PFH*					
			CEI 61508 (1ère éd.)	**CEI 61508 (2ème éd.)**	**PDS**	**NF**	**MMP**	**RdP**
1oo1	0		2.50E-5	2.50E-5	2.50E-5	2.50E-5	2.24E-5	2.24E-5
	60		1.00E-5	1.00E-5	1.00E-5	1.00E-5	9.57E-6	9.58E-6
	90		2.50E-6	2.50E-6	2.50E-6	2.50E-6	2.47E-6	2.47E-6
	99		2.50E-7	2.50E-7	2.50E-7	2.50E-7	2.50E-7	2.48E-7
1oo2	0	10	6.94E-6	6.94E-6	7.98E-6	7.44E-6	6.05E-6	6.05E-6
		20	8.51E-6	8.51E-6	1.05E-5	9.39E-6	7.72E-6	7.70E-6
	60	10	2.90E-6	1.74E-6	1.88E-6	2.98E-6	2.74E-6	2.73E-6
		20	3.63E-6	2.61E-6	2.88E-6	3.76E-6	3.47E-6	3.47E-6
	90	10	7.48E-7	2.97E-7	3.05E-7	7.45E-7	7.28E-7	7.25E-7
		20	9.42E-7	5.40E-7	5.55E-7	9.40E-7	9.20E-7	9.15E-7
	99	10	8.34E-8	2.56E-8	2.55E-8	7.45E-8	7.42E-8	7.52E-8
		20	1.02E-7	5.05E-8	5.05E-8	9.40E-8	9.37E-8	9.32E-8
1oo3	0	10	3.38E-6	3.38E-6	2.45E-6	4.22E-6	3.11E-6	3.11E-6
		20	5.62E-6	5.62E-6	3.70E-6	7.09E-6	5.35E-6	5.34E-6
	60	10	1.16E-6	1.06E-6	5.77E-7	1.36E-6	1.21E-6	1.21E-6
		20	2.12E-6	2.05E-6	1.08E-6	2.49E-6	2.22E-6	2.22E-6
	90	10	2.61E-7	2.51E-7	1.26E-7	3.01E-7	2.91E-7	2.91E-7
		20	5.09E-7	5.01E-7	2.51E-7	5.81E-7	5.64E-7	5.62E-7
	99	10	2.52E-8	2.50E-8	1.25E-8	2.89E-8	2.88E-8	2.86E-8
		20	5.01E-8	5.00E-8	2.50E-8	5.68E-8	5.66E-8	5.61E-8
2oo2	0	10	5.00E-5	5.00E-5	5.00E-5	4.75E-5	3.88E-5	3.88E-5
		20	5.00E-5	5.00E-5	5.00E-5	4.50E-5	3.72E-5	3.71E-5
	60	10	2.00E-5	2.00E-5	2.00E-5	1.90E-5	1.75E-5	1.75E-5
		20	2.00E-5	2.00E-5	2.00E-5	1.80E-5	1.67E-5	1.67E-5
	90	10	5.00E-6	5.00E-6	5.00E-6	4.75E-6	4.65E-6	4.67E-6
		20	5.00E-6	5.00E-6	5.00E-6	4.50E-6	4.41E-6	4.42E-6
	99	10	5.00E-7	5.00E-7	5.00E-7	4.75E-7	4.74E-7	4.76E-7
		20	5.00E-7	5.00E-7	5.00E-7	4.50E-7	4.49E-7	4.52E-7
2oo3	0	10	1.58E-5	1.58E-5	2.14E-5	1.66E-5	1.19E-5	1.19E-5
		20	1.55E-5	1.55E-5	2.64E-5	1.68E-5	1.25E-5	1.25E-5
	60	10	6.71E-6	3.21E-6	4.63E-6	6.63E-6	5.78E-6	5.80E-6
		20	6.88E-6	3.82E-6	6.63E-6	6.74E-6	5.94E-6	5.96E-6
	90	10	1.74E-6	3.92E-7	6.64E-7	1.66E-6	1.60E-6	1.60E-6
		20	1.82E-6	6.19E-7	1.16E-6	1.69E-6	1.63E-6	1.63E-6
	99	10	2.00E-7	2.67E-8	5.16E-8	1.66E-7	1.65E-7	1.65E-7
		20	2.07E-7	5.14E-8	1.02E-7	1.69E-7	1.67E-7	1.67E-7

Voyons maintenant les valeurs de la *PFH* pour le cas où $N \neq K$. Les résultats obtenues pour les configurations 1oo2 et 2oo3 présentent presque la même tendance. En fait, sauf pour $DC = 0$ (1oo2 et 2oo3) et pour $DC = 0.6$ et $\beta = 0.2$ (2oo3), les résultats induits par les formules de la CEI 61508 (2ème éd.) et du manuel PDS sont inférieurs à ceux obtenus avec les autres approches, y compris les modèles de Markov et RdP (Figure 3.8). Ils pourraient donc conduire à une surestimation des SIL, ce qui est dangereux du point de vue de la sécurité. Par

exemple, le SIL atteint par la configuration 2oo3 (DC = 0.99 et β = 0.1) selon ces deux approches optimistes est SIL3, tandis que les autres approches aboutissent à un SIL2 (voir tableau 1.1). La CEI 61508 (1ère éd.) et les nouvelles formules présentent des valeurs de *PFH* toujours supérieures à celles correspondant aux modèles markoviens et RdP (pour les deux configurations). De plus, lorsque la valeur de DC augmente, les résultats des nouvelles formules se rapprochent de ceux des modèles markoviens et RdP et restent inférieurs à ceux de la CEI 61508 (1ère éd.) (Figure 3.8). Il est à noter que ces derniers résultats peuvent conduire à une sous-estimation du SIL. Par exemple, le SIL réalisable selon la configuration 1oo2 (DC = 0.99 et β = 0.2) obtenu par l'approche CEI 61508 (1ère éd.) est SIL2, tandis que les autres approches donnent un SIL3. Cela n'affecterait pas la sécurité des équipements protégés, mais pourrait entraîner des dépenses supplémentaires inutiles.

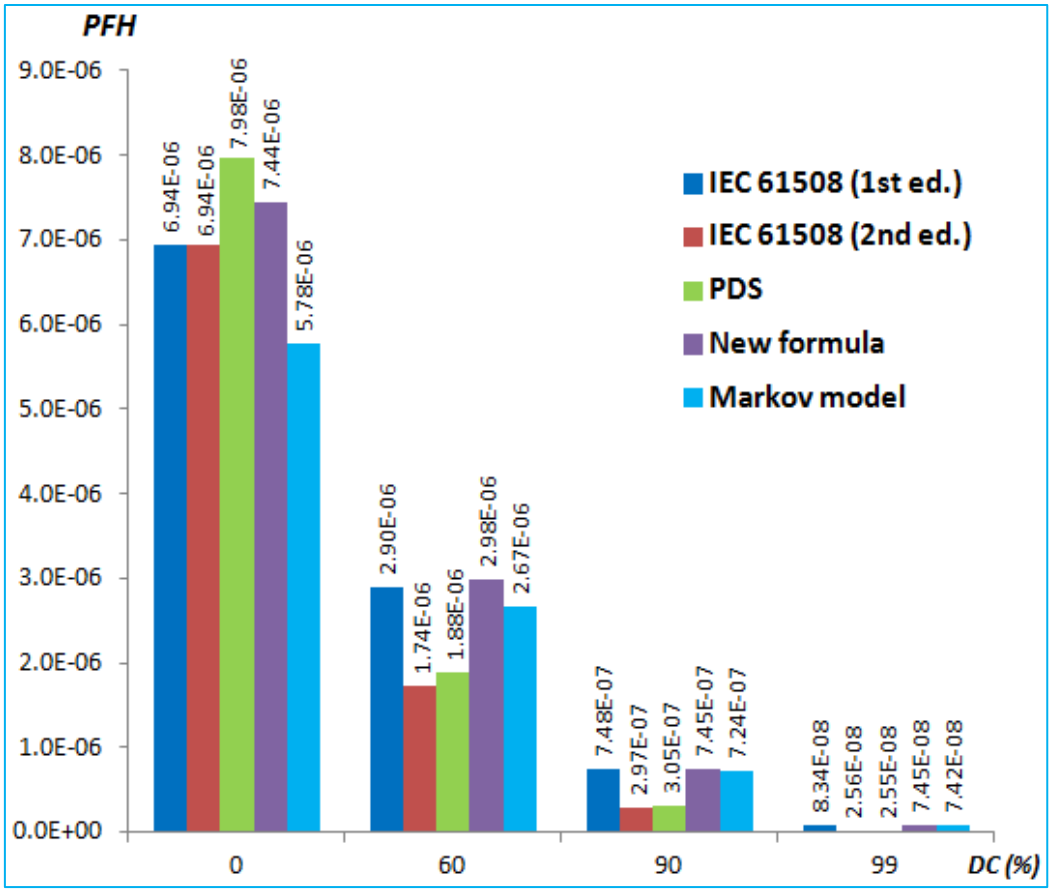

Figure 3.8 : *PFH* relatif à la configuration 1oo2 (β=0.1)

Pour la configuration 1oo3 (figure 3.9), les expressions du manuel PDS ont toujours les valeurs de la *PFH* les plus basses. Cela peut s'expliquer par la faible valeur du facteur C_{1oo3} (0.5) utilisé pour les défaillances de causes commune (DCC). Les nouvelles formules fournissent les valeurs les plus élevées et qui se rapprochent le plus de celles des modèles

markoviens et RdP avec l'augmentation de *DC*. Les formules CEI 61508 (1ère et 2ème éd.) Présentent des valeurs de *PFH* inférieures à celles associées aux modèles markoviens et RdP et, bien entendu, aux nouvelles formules. Il convient de noter que l'aspect non conservatif de la CEI 61508 (1ère éd.) est révélé pour la première fois. Cet aspect s'explique par la non prise en compte des séquences de défaillances initiées par une défaillance indépendante et terminées par une DCC (deux derniers termes de l'équation (3.4)).

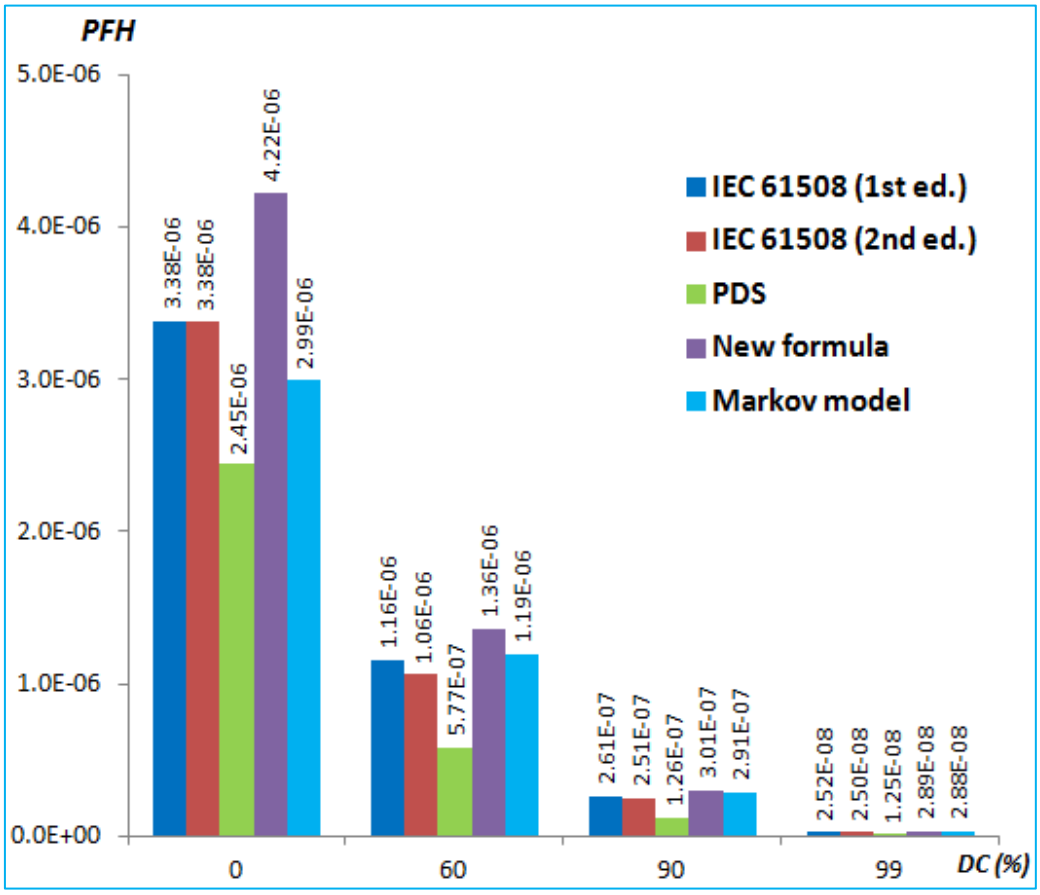

Figure 3.9 : *PFH* relatif à la configuration 1oo3 (β=0.1).

Un deuxième ensemble de résultats est fourni en ignorant la contribution des *DCC* : $\beta = \beta_D = 0$. En fait, le terme commun ($\beta\lambda_{DU}$) entre les formules de la CEI 61508 et celles nouvellement développées peut contribuer majoritairement aux résultats *PFH* et masquer ainsi les divergences possibles. Les résultats obtenus pour les configurations sélectionnées sont présentés dans le tableau 3.7.

Tableau 3.7 : Résultats de la *PFH* (h^{-1}) sans DCC

KooN	*DC* (%)	Séries de formules et modèles *PFH*				
		CEI 61508 (1ère éd.)	**CEI 61508 (2ème éd.)**	**PDS**	**NF**	**MMP**
1oo1	0	2.50E-5	2.50E-5	2.50E-5	2.50E-5	2.47E-5
	60	1.00E-5	1.00E-5	1.00E-5	1.00E-5	9.58E-6
	90	2.50E-6	2.50E-6	2.50E-6	2.50E-6	2.47E-6
	99	2.50E-7	2.50E-7	2.50E-7	2.50E-7	2.47E-7
1oo2	0	5.49E-6	5.49E-6	5.48E-6	5.49E-6	4.08E-6
	60	2.20E-6	8.80E-7	8.76E-7	2.20E-6	1.94E-6
	90	5.58E-7	5.58E-8	5.48E-8	5.49E-7	5.32E-7
	99	6.48E-8	6.48E-10	5.48E-10	5.49E-8	5.47E-8
1oo3	0	1.20E-6	1.20E-6	1.20E-6	1.20E-6	7.03E-7
	60	1.94E-7	7.76E-8	7.67E-8	1.94E-7	1.53E-7
	90	1.25E-8	1.25E-9	1.20E-9	1.24E-8	1.16E-8
	99	1.81E-10	1.80E-12	1.20E-12	1.53E-10	1.52E-10
2oo2	0	5.00E-5	5.00E-5	5.00E-5	5.00E-5	4.12E-5
	60	2.00E-5	2.00E-5	2.00E-5	2.00E-5	1.85E-5
	90	5.00E-6	5.00E-6	5.00E-6	5.00E-6	4.90E-6
	99	5.00E-7	5.00E-7	5.00E-7	5.00E-7	4.98E-7
2oo3	0	1.65E-5	1.65E-5	1.64E-5	1.65E-5	1.03E-5
	60	6.60E-6	2.64E-6	2.63E-6	6.59E-6	5.37E-6
	90	1.67E-6	1.67E-7	1.64E-7	1.65E-6	1.56E-6
	99	1.94E-7	1.94E-9	1.64E-9	1.65E-7	1.64E-7

Presque les mêmes conclusions tirées précédemment concernant les résultats numériques relatifs à la *PFH*, mais de manière encore plus apparente, peuvent être tirées lorsque les *DCC* ne sont pas comptabilisés. Il est à noter que, dans ce cas, les formules de la *PFH* de la CEI 61508 (1ère éd.) restent conservatives par rapport aux modèles markoviens et RdP pour toutes les configurations étudiées (même pour l'architecture 1oo3).

Enfin, nous mettons l'accent sur le fait que les expressions de la *PFH* nouvellement développées sont, dans tous les cas (avec et sans DCC) et pour l'ensemble des configurations

étudiées, les seules formules qui produisent des résultats conservatifs par rapport aux modèles markoviens et RdP respectifs.

3.5. Etude détaillée de l'architecture 2oo3

L'usage courant de cette architecture nous a incités à l'investiguer davantage en considérant un éventail plus large de données de fiabilité exploitées. Cette partie est scindée en deux volets. Le premier volet est dévolu à une comparaison poussée des résultats obtenus de différentes approches. Le deuxième volet, quant à lui, concerne l'étude d'un cas concret : une architecture de contrôle *i*-TMR (independent Triple Modular Redundancy).

3.5.1. Comparaison des résultats numériques

Le but de cette section est de corroborer les conclusions précédentes relatives à la vérification numérique de la cohérence de la formule *PFH* de la configuration 2oo3 fournie dans la norme CEI 61508. Les résultats numériques sont obtenus en utilisant les différentes approches suivantes : CEI 61508 (deuxième édition), nouvelle formule (NF), modèles markoviens multi-phases (MMP), modèles markoviens approchés (MA) et l'approche RdP. Les calculs ont été effectués pour plusieurs valeurs typiques de λ_D (2.5E-6 h^{-1}; 5E-6 h^{-1}; 2.5E-5 h^{-1}), T_1 (4380 *h*; 8760 *h*; 17520 *h*), DC (0; 0.6; 0.9; 0.99), et β (0.1; 0.2). Dans tous les cas, on suppose que MTTR = MRT = 8 *h*; $MTTR_{SD}$ = 24 *h*; $\beta = 2\,\beta_D$. Les valeurs de la *PFH* sont calculées sur une période d'observation de 10 ans (87600 *h*). Pour l'approche RdP, 1E+6 histoires (itérations) ont été réalisées. Les résultats obtenus sont rassemblés dans le tableau 3.8.

L'examen de ce tableau montre que les résultats de la *PFH* obtenus en utilisant les approches MMP et RdP sont presque identiques. Cette similitude était attendue puisque ces approches modélisent le comportement exact du système 2oo3. Par conséquent, leurs résultats sont considérés comme valeurs de référence.

L'approche MA induit des résultats de *PFH* proches des résultats de référence avec un aspect légèrement non conservatif pour DC = 0 et 0.6. Cet aspect n'est pas systématiquement observé pour les deux autres valeurs de DC.

Les différences les plus importantes, si elles existent, sont principalement observées pour la valeur la plus élevée de λ_D (i.e. 2.5E-6 h^{-1}). De plus, la figure 3.10 montre le fait que les valeurs de la *PFH* en régime permanent obtenues à partir de l'approche MA se rapprochent des valeurs de la *PFH* moyennes obtenues à partir du modèle MMP. Il est à noter que les résultats de l'approche MA ne sont valables qu'en régime stationnaire.

Note : dans les figures suivantes, les approches MA, MMP et RdP sont respectivement désignées CMC (Classical Markov Chain), MPMC (multi-phase Markov Chain) et PN (Petri nets).

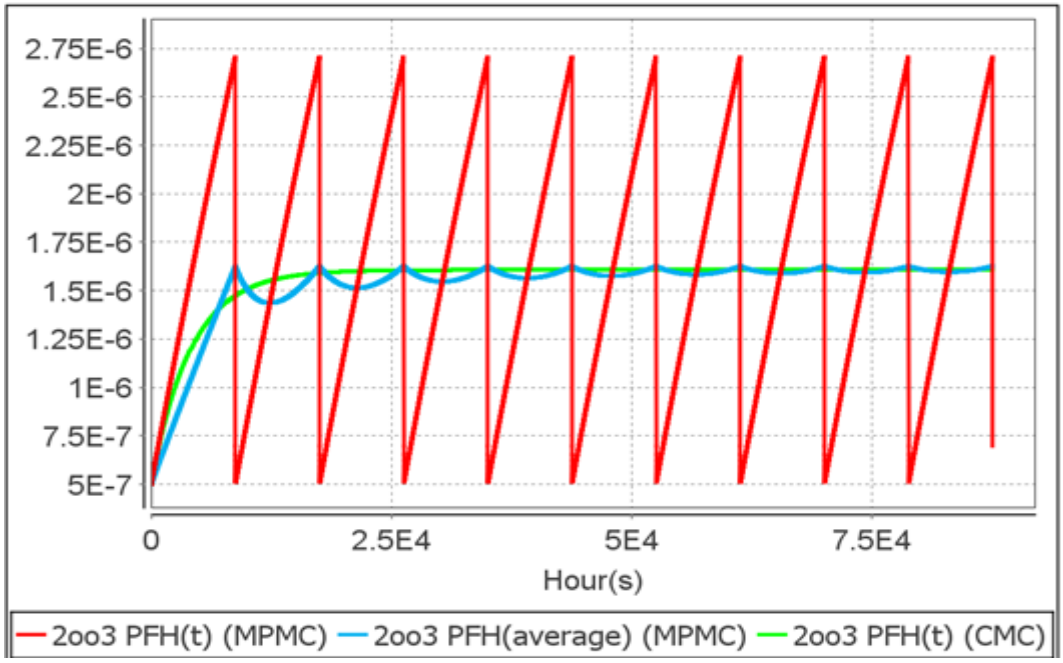

Figure 3.10 : Résultats de la *PFH* obtenus avec MMP et MA pour λ_D = 2.5E-5 h^{-1}, *DC* = 0.9, β = 0.2 et T_1 = 8760 *h*.

La formule de la CEI 61508 fournit des résultats acceptables uniquement dans le cas de DC = 0. En effet, pour DC = 0, le taux de défaillance dangereuse détectée λ_{DD} est nul et donc la capacité d'arrêt n'a pas d'importance. Pour les autres valeurs de DC, la formule de la CEI 61508 produit des résultats sous-estimés de la *PFH*, ce qui est dangereux du point de vue de la sécurité. Le SIL atteint dans le cas où λ_D= 2.5E-5 h^{-1}; T_1 = 8760 *h*; DC = 0.99 et β = 0.1 selon la formule de la CEI 61508 est le SIL3 (*PFH* = 2.67E–8), tandis que les autres approches conduisent à un SIL2 (tableau 1.1). Plus généralement, l'inspection du tableau 3.8 montre que la formule de la CEI 61508 surestime le SIL pour tous les cas où λ_D = 2.5E-5 h^{-1}, β = 0.2, DC = 0.9 et 0.99. Cette surestimation est également observée lorsque β = 0.1 pour les combinaisons suivantes : DC = 0.9 et 0.99, λ_D = 2.5E-5 h^{-1} et 5E-6 h^{-1}, T_1 = 8760 *h* et 17520 *h*.

Tableau 3.8 : Résultats de la *PFH* (h^{-1})

DC (%)	β (%)	λ_D (h^{-1})	T_1=4380 h					T_1=8760 h					T_1=17520 h				
			CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP	CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP	CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP
0	10	2.50E-6	3.17E–7	3.20E–7	3.15E–7	3.15E–7	3.16E–7	3.83E–7	3.91E–7	3.76E–7	3.78E-7	3.78E–7	5.16E–7	5.31E–7	4.90E–7	4.98E–7	4.98E–7
		5.00E-6	7.67E–7	7.82E–7	7.53E–7	7.57E–7	7.55E–7	1.03E–6	1.06E–6	9.81E–7	9.96E-7	9.98E–7	1.56E–6	1.62E–6	1.37E–6	1.42E–6	1.43E–6
		2.50E-5	9.17E–6	9.54E–6	7.73E–6	8.09E–6	8.09E–6	1.58E–5	1.66E–5	1.10E–5	1.19E–5	1.19E–5	2.91E–5	3.06E–5	1.44E–5	1.61E–5	1.61E–5
	20	2.50E-6	5.53E–7	5.6E–7	5.51E–7	5.51E–7	5.51E–7	6.05E–7	6.18E–7	5.99E–7	6.01E–7	6.01E–7	7.10E–7	7.37E–7	6.89E–7	6.95E–7	6.91E–7
		5.00E-6	1.21E–6	1.24E–6	1.20E–6	1.20E–6	1.20E–6	1.42E–6	1.47E–6	1.38E–6	1.39E–6	1.39E–6	1.84E–6	1.95E–6	1.69E–6	1.73E–6	1.73E–6
		2.50E-5	1.03E–5	1.1E–5	9.13E–6	9.41E–6	9.41E–6	1.55E–5	1.68E–5	1.17E–5	1.25E–5	1.25E–5	2.60E–5	2.87E–5	1.45E–5	1.58E–5	1.58E–5
60	10	2.50E-6	1.11E–7	1.28E–7	1.27E–7	1.27E–7	1.27E–7	1.22E–7	1.56E–7	1.54E–7	1.54E–7	1.54E–7	1.44E–7	2.13E–7	2.06E–7	2.07E–7	2.07E–7
		5.00E-6	2.44E–7	3.13E–7	3.08E–7	3.09E–7	3.07E–7	2.88E–7	4.25E–7	4.11E–7	4.14E–7	4.15E–7	3.76E–7	6.50E–7	6.06E–7	6.16E–7	6.17E–7
		2.50E-5	2.11E–6	3.83E–6	3.49E–6	3.57E–6	3.58E–6	3.21E–6	6.63E–6	5.52E–6	5.79E–6	5.80E–6	5.41E–6	1.23E–5	8.59E–6	9.34E–6	9.37E–6
	20	2.50E-6	2.09E–7	2.24E–7	2.22E–7	2.22E–7	2.22E–7	2.18E–7	2.47E–7	2.44E–7	2.44E–7	2.45E–7	2.36E–7	2.95E–7	2.87E–7	2.88E–7	2.87E–7
		5.00E-6	4.36E–7	4.95E–7	4.88E–7	4.89E–7	4.89E–7	4.73E–7	5.9E–7	5.74E–7	5.76E–7	5.77E–7	5.45E–7	7.80E–7	7.33E–7	7.42E–7	7.41E–7
		2.50E-5	2.91E–6	4.38E–6	4.05E–6	4.11E–6	4.11E–6	3.82E–6	6.74E–6	5.73E–6	5.94E–6	5.96E–6	5.62E–6	1.15E–5	8.30E–6	8.90E–6	8.90E–6

Tableau 3.8 : Résultats de la *PFH* (suite)

DC (%)	β (%)	λ_D (h^{-1})	T_1=4380 h					T_1=8760 h					T_1=17520 h				
			CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP	CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP	CEI 61508 Eq. (2.24)	NF Eq. (2.28)	MA	MMP	RdP
90	10	2.5E-6	2.57E–8	3.21E–8	3.20E–8	3.20E–8	3.19E–8	2.64E–8	3.91E–8	3.89E–8	3.89E–8	3.88E–8	2.78E–8	5.31E–8	5.27E–8	5.27E–8	5.29E–8
		5E-6	5.29E–8	7.83E–8	7.80E–8	7.79E–8	7.79E–8	5.57E–8	1.06E–7	1.05E–7	1.06E–7	1.06E–7	6.13E–8	1.63E–7	1.59E–7	1.60E–7	1.60E–7
		2.5E-5	3.22E–7	9.57E–7	9.33E–7	9.37E–7	9.36E–7	3.92E–7	1.66E–6	1.58E–6	1.60E–6	1.60E–6	5.32E–7	3.06E–6	2.76E–6	2.84E–6	2.86E–6
	20	2.5E-6	5.06E–8	5.6E–8	5.59E–8	5.59E–8	5.58E–8	5.12E–8	6.19E–8	6.17E–8	6.17E–8	6.18E–8	5.24E–8	7.37E–8	7.31E–8	7.32E–8	7.34E–8
		5E-6	1.02E–7	1.23E–7	1.23E–7	1.23E–7	1.24E–7	1.05E–7	1.47E–7	1.46E–7	1.47E–7	1.47E–7	1.09E–7	1.95E–7	1.91E–7	1.92E–7	1.94E–7
		2.5E-5	5.61E–7	1.1E–6	1.07E–6	1.07E–6	1.07E–6	6.19E–7	1.69E–6	1.61E–6	1.63E–6	1.63E–6	7.36E–7	2.87E–6	2.59E–6	2.66E–6	2.70E–6
99	10	2.5E-6	2.51E–9	3.21E–9	3.21E–9	3.20E–9	3.25E–9	2.52E–9	3.91E–9	3.91E–9	3.91E–9	3.92E–9	2.53E–9	5.31E–9	5.31E–9	5.31E–9	5.43E–9
		5E-6	5.04E–9	7.83E–9	7.82E–9	7.82E–9	7.85E–9	5.07E–9	1.06E–8	1.06E–8	1.06E–8	1.07E–8	5.12E–9	1.63E–8	1.62E–8	1.62E–8	1.62E–8
		2.5E-5	2.59E–8	9.57E–8	9.53E–8	9.51E–8	9.51E–8	2.67E–8	1.66E–7	1.64E–7	1.65E–7	1.65E–7	2.81E–8	3.06E–7	3.00E–7	3.02E–7	3.04E–7
	20	2.5E-6	5E–9	5.60E–9	5.60E–9	5.59E–9	5.63E–9	5.01E–9	6.19E–9	6.18E–9	6.18E–9	6.22E–9	5.03E–9	7.37E–9	7.36E–9	7.36E–9	7.39E–9
		5E-6	1E–8	1.24E–8	1.24E–8	1.24E–8	1.24E–8	1.01E–8	1.47E–8	1.47E–8	1.47E–8	1.47E–8	1.01E–8	1.95E–8	1.94E–8	1.94E–8	1.95E–8
		2.5E-5	5.08E–8	1.09E–7	1.09E–7	1.09E–7	1.09E–7	5.14E–8	1.69E–7	1.67E–7	1.67E–7	1.69E–7	5.26E–8	2.87E–7	2.79E–7	2.81E–7	2.86E–7

Selon le tableau 3.8, les résultats de la formule de la CEI 61508 deviennent inférieurs aux autres approches avec l'augmentation de l'un des paramètres suivants : le taux de défaillance dangereuse λ_D, la couverture de diagnostic DC et l'intervalle des tests périodiques T_1 (figures 3.11-3.13).

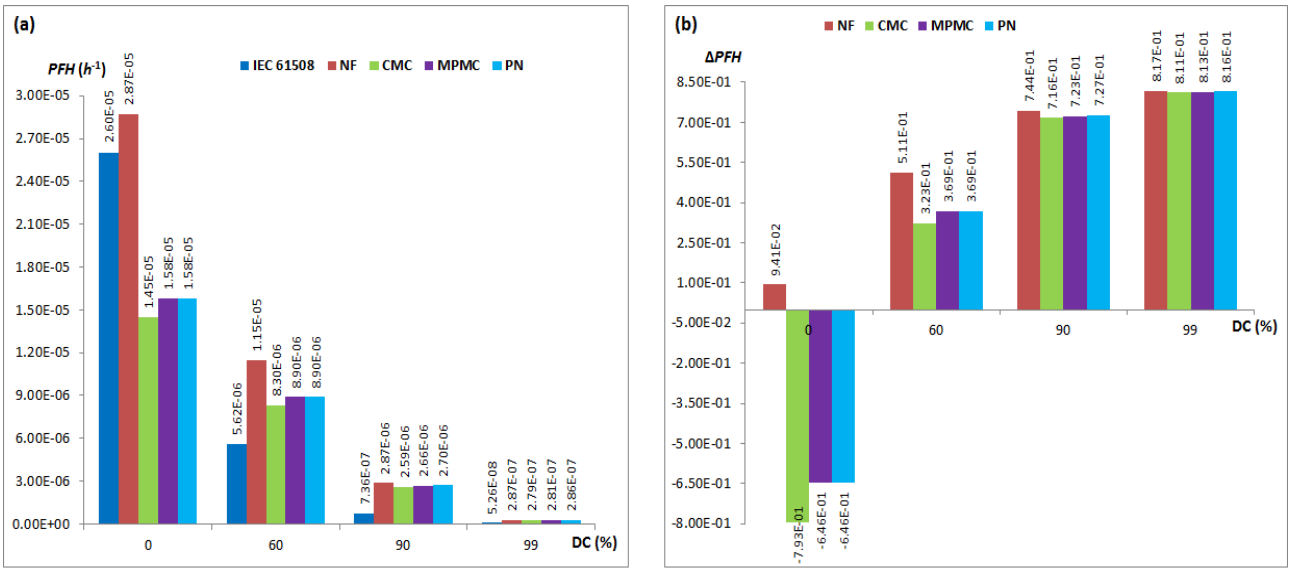

Figure 3.11 : Impact de l'augmentation de *DC* sur (a) les valeurs de la *PFH* et (b) la différence relative à la *PFH* de la CEI 61508 pour λ_D = 2.5E-5 h^{-1}, β = 0.2 et T_1 = 17520 *h*.

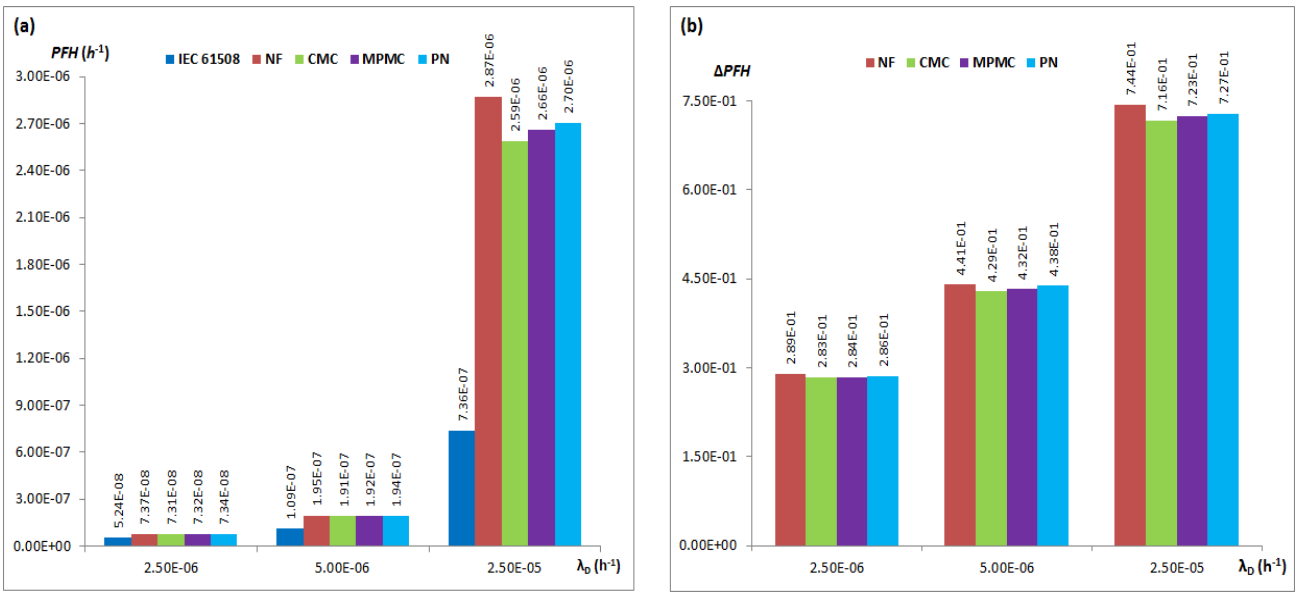

Figure 3.12 : Impact de l'augmentation de λ_D sur (a) les valeurs de la *PFH* et (b) la différence relative à la *PFH* de la CEI 61508 pour *DC* = 0.9, β = 0.2 et T_1 = 17520 *h*.

La figure 3.11(a) montre les résultats de la *PFH* avec différentes valeurs de DC pour λ_D = 2.5E-5 h^{-1}, T_1 = 17520 h et β = 0.2. De plus, la figure 3.11(b) illustre la différence entre les résultats relatifs à la *PFH* de la norme CEI 61508 et ceux liés aux autres approches : $\Delta PFH = \frac{PFH_x - PFH_{IEC\,61508}}{PFH_x}$, x représente toute autre approche utilisée. On peut voir que plus le DC est important, plus la différence relative à la *PFH* est importante. On peut également remarquer à partir de la figure 3.11(a) que la *PFH* diminue avec l'augmentation du DC en raison de la réparation rapide des défaillances détectées et des arrêts automatiques déclenchés par ces défaillances.

La figure 3.12(a) montre la variation de la *PFH* avec l'augmentation du paramètre λ_D pour DC = 0.9, T_1 = 17520 h et β = 0.2. Elle montre clairement l'augmentation de la *PFH* avec celle du paramètre λ_D. La différence relative entre les résultats de la *PFH* donnés par la formule de la CEI 61508 et les autres approches augmente avec l'augmentation du taux de défaillance dangereuse λ_D (figure 3.12(b)). Cela signifie que l'aspect non conservatif de la formule de la CEI 61508 devient plus sévère lorsque λ_D augmente. Ces dernières conclusions sont toujours valables en ce qui concerne la variation de l'intervalle de test périodique T_1, comme le montre la figure 3.13. En effet, avec l'augmentation de T_1, les valeurs de la *PFH* augmentent (figure 3.13(a)). De plus, la sous-estimation de la *PFH* par la formule de la CEI 61508 devient plus significative avec l'augmentation de T_1, comme on peut le voir à partir de la variation de la différence relative à la *PFH* (figure 3.13(b)).

Enfin, la nouvelle formule développée (NF) donne les résultats de la *PFH* les plus conservatifs dans tous les cas, qui se rapprochent de ceux dérivés des approches MA, MMP et RdP lorsque DC augmente, comme le montre la figure 3.14. Précisément, la figure 3.14(a) montre que la différence entre les valeurs de la *PFH* données par la nouvelle formule et celles dérivées des trois autres approches diminue lorsque DC augmente. Pour plus de détails, la différence relative associée $\left(\Delta PFH = \frac{PFH_{NF} - PFH_x}{PFH_{NF}}\right)$ est donnée sur la figure 3.14(b).

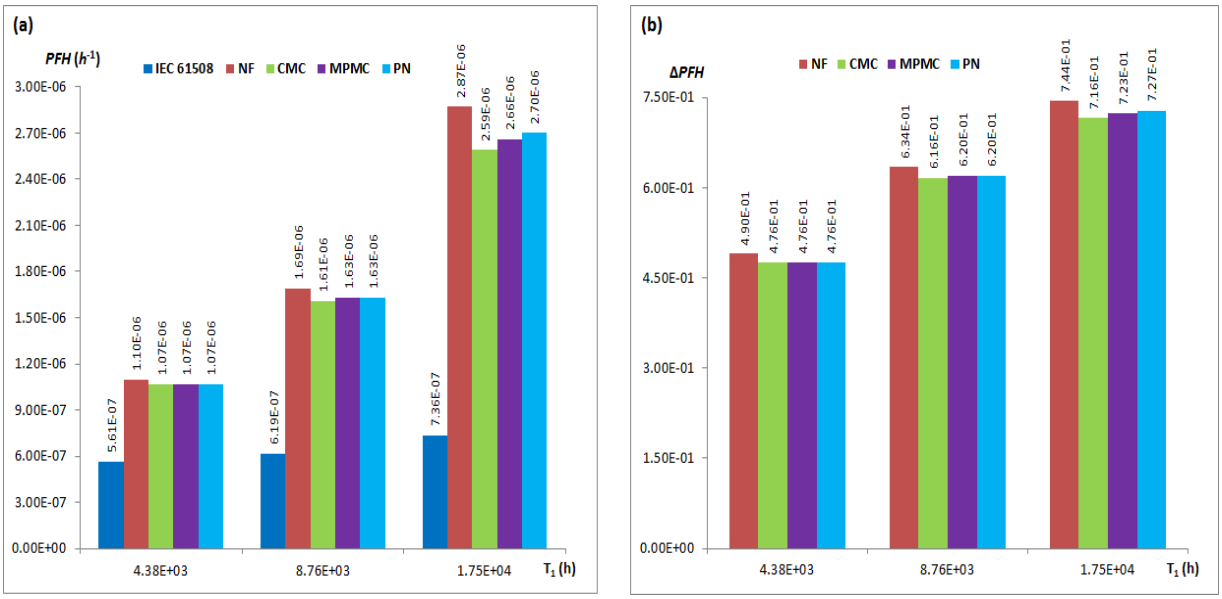

Figure 3.13 : Impact de l'augmentation de T_1 sur (a) les valeurs de la *PFH* et (b) la différence relative à la *PFH* de la CEI 61508 pour λ_D = 2.5E-5 h^{-1}, DC = 0.9 et β = 0.2.

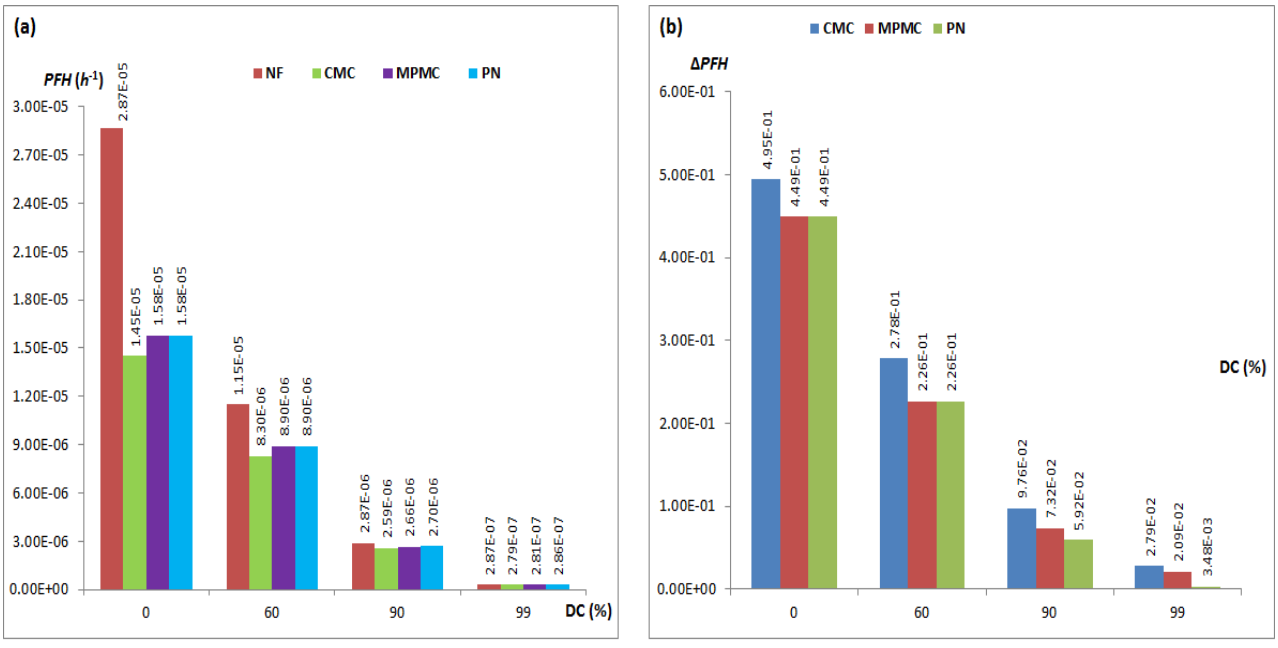

Figure 3.14 : Impact de l'augmentation du *DC* sur (a) les valeurs de la *PFH* et (b) la différence relative à la *PFH* de NF pour λ_D = 2.5E-5 h^{-1}, β = 0.2 et T_1 = 17520 h.

3.5.2. Etude de cas : i-TMR PLC

3.5.2.1. Description du système

Le système considéré est un Contrôleur Logique Programmable Triplex indépendant : i-TMR PLC (*independent Triple Modular Redundancy Programmable Logic Controller*). Il se compose de trois ensembles d'unité logique (PLC) indépendantes et d'un dispositif de vote générant une valeur de sortie finale (figure 3.15) [Son et al.2018]. Chaque ensemble de PLC est constitué des modules suivants : entrée/sortie analogique (AI/AO), entrée/sortie numérique (DI/DO), processeur (PRO), communication critique de sécurité (SCC : Safety Critical Communication), communication sur l'état de sécurité (SSC : Safety Status Communication), bus de fond de panier (BUS) et un module d'alimentation électrique (PWR : Power).

Les valeurs du procédé surveillé en provenance des capteurs, qui peuvent être une valeur numérique ou analogique, sont transmises à l'entrée analogique/numérique (AI/DI). Après le conditionnement du signal, les sorties sont envoyées au module PRO via le BUS. Le résultat généré par PRO est transmis à la sortie analogique / numérique AO / DO via le BUS. Enfin, le dispositif de vote exécute une logique de vote majoritaire (2oo3) pour les valeurs numériques ou sélectionne la valeur médiane pour les valeurs analogiques. La valeur générée est ensuite utilisée pour agir sur les éléments finaux tels qu'une vanne de régulation. Comme les modules de chaque PLC sont configurés en série, la défaillance de l'un d'eux entraîne la défaillance du PLC correspondant. De plus, la défaillance de deux PLC ou la défaillance du dispositif de vote entraînerait la défaillance du système i-TMR. Cela dit, les PLC sont agencés en architecture 2oo3 et le dispositif de vote est considéré comme une architecture simplex (1oo1). Selon la capacité d'arrêt automatique, la détection d'une défaillance dangereuse dans deux PLC ou dans le dispositif de vote met le procédé contrôlé dans un état de repli (shutdown).

3.5.2.2. Calcul de la *PFH*

Les taux de défaillance de chaque module sont regroupés dans le tableau 3.9 [Son et *al.*, 2018]. De plus, nous considérons les données suivantes pour chaque module : DC = 0.9, $\beta = 2$ $\beta_D = 5$ %. MTTR = MRT= 8 h, $MTTR_{SD}$ = 72 h et trois valeurs pour l'intervalle de test périodique T_1 (4380 h ; 8760 h; 17520 h). Il est à noter que le taux de défaillance dangereuse total pour chaque PLC (λ_D^{PLC}) est obtenu en additionnant les taux de défaillance de ses modules constitutifs. En conséquence et sur la base du tableau 3.9 ; $\lambda_D^{PLC} = 5.61E-5\ h^{-1}$. Les résultats de la *PFH* pour l'ensemble des PLC obtenus en utilisant les différentes approches sont donnés au tableau 3.10.

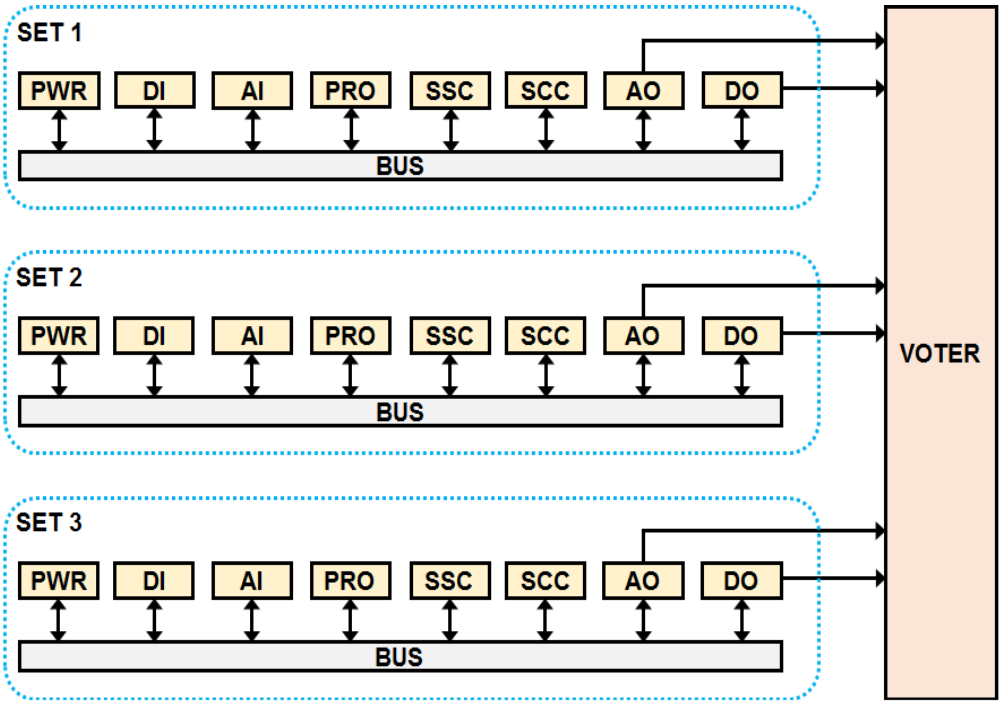

Figure 3.15 : Schéma fonctionnel du PLC i-TMR [Son et *al.*, 2018].

Tableau 3.9 : Taux des défaillances des modules

Modules	λ_D (h^{-1})
Analog Input (AI)	4.49E–6
Digital Input (DI)	7.72E–6
Processor (PRO)	7.78E–6
Analog Output (AO)	5.83E–6
Digital Output (DO)	6.11E–6
Backplane BUS (BUS)	8.40E–6
Safety Critical Communication (SCC)	6.88E–6
Safety Status Communication (SSC)	3.44E–6
Power (PWR)	5.44E–6
Voter	6.23E–6

Tableau 3.10 : Résultats de la *PFH* (h^{-1}) pour le système i-TMR PLC

Systèmes	T_1 **(h)**	**Approches**				
		CEI 61508 Eq. (2.24)	**NF Eq. (2.28)**	**MA**	**MMP**	**RdP**
PLC (2oo3)	4380	6.77E–7	4.14E–6	3.89E–6	3.95E–6	3.96E–6
	8760	1.06E–6	7.97E–6	7.07E–6	7.32E–6	7.32E–6
	17520	1.82E–6	1.56E–5	1.24E–5	1.32E–5	1.33E–5
Voter (1oo1)	6.23E–7 (Eq. (2.12))					
i-TMR PLC	4380	1.30E–6	4.76E–6	4.51E–6	4.57E–6	4.58E–6
	8760	1.68E–6	8.59E–6	7.69E–6	7.94E–6	7.94E–6
	17520	2.44E–6	1.62E–5	1.30E–5	1.38E–5	1.39E–5

L'examen du tableau 3.10 indique que les valeurs de la *PFH* fournies par les approches MMP et RdP sont presque identiques pour l'ensemble des PLC. L'approche MA donne des résultats de *PFH* proches mais légèrement optimistes par rapport à ceux donnés par les approches MMP et RdP. La formule de la CEI 61508 a induit les résultats de *PFH* les plus bas qui surestime donc le SIL des PLC, en particulier pour T_1 = 4380 *h* et 17520 *h*. La nouvelle formule (NF) fournit des valeurs de *PFH* conservatives par rapport à celles données par les autres approches, tout en aboutissant au même SIL obtenu à partir des approches MA, MMP et RdP. La *PFH* associé au i-TMR PLC (en incluant le dispositif de vote) est obtenue en additionnant les *PFH* liées au ensemble des PLC et au dispositif de vote. Ce dernier étant constitué d'un seul canal (configuration 1oo1), sa *PFH* est simplement égale à son taux de défaillance dangereuse non détectée (équation 2.12) : $PFH_{Voter} = \lambda_{DU}^{Voter} = DC \cdot \lambda_{D}^{Voter} =$ 6.23E–7 h^{-1}.

Les conclusions énoncées pour les ensembles du PLC sont toujours valables pour le système global i-TMR PLC et sont conformes à celles soulignées dans la section 3.5.1. Il convient de noter que la *PFH* dérivée des approches MA, MMP et RdP et NF, pour T_1 = 17520 *h*, ne correspond à aucun SIL (voir tableau 1.1). Par conséquent, cet intervalle de test ne doit pas être appliqué dans le cadre du i-TMR PLC considéré pour les applications critiques de sécurité en mode de fonctionnement élevé ou continu.

3.6. Conclusion

Ce chapitre a été consacré à une étude comparative entre différentes séries de formules concernant la *PFH* de cinq configurations *KooN* couramment utilisées : 1oo1, 2oo2, 1oo2, 2oo3 et 1oo3. Quatre séries de formules *PFH* ont été prises en compte : expressions analytiques données dans la norme CEI 61508 (première et deuxième éditions), celles fournies dans le manuel PDS et les formules développées au cours du deuxième chapitre. Leurs hypothèses sous-jacentes, lorsqu'elles sont disponibles, sont également présentées.

Par ailleurs, nous avons développé des modèles RdP pour chacune des architectures précédentes. Cette nouvelle modélisation a permis de confirmer la validité des modèles markoviens donnés au deuxième chapitre.

Différentes valeurs numériques relatives aux séries de formules étudiées ont été comparées à celles dérivées des modèles markoviens multi-phases et RdP. Pour les configurations 1oo1 et 2oo2, toutes les expressions analytiques ont donné des résultats presque identiques. Cela pourrait être généralisé à toutes les architectures *NooN*. Pour les configurations 1oo2 et 2oo3, les expressions analytiques fournies dans la CEI 61508 (1ère éd.) et celles récemment développées présentaient les meilleures performances en induisant des résultats conservatifs, mais proches de celles dérivées des modèles de Markov et RdP. En ce qui concerne la configuration 1oo3, seules les nouvelles formules ont fourni des résultats conservatifs et acceptables. Ceci peut être généralisé pour les architectures avec une redondance plus élevée (1oo4, 2oo4,…) : $N - K + 1 > 2$.

Finalement, nous avons réalisé une étude détaillée de la configuration 2oo3. Cette dernière a absolument confirmé les résultats précédents. Plus précisément, la réduction des valeurs de *PFH* de la formule CEI 61508 par rapport aux autres approches est davantage favorisée par l'augmentation du taux de défaillance dangereuse (λ_D), de la couverture de diagnostique (DC) et de l'intervalle des tests périodique T_1. Certaines de ces constatations ont été corroborées par un exemple illustratif : un Contrôleur Logique Programmable Triplex indépendant (i-TMR PLC).

L'implication pratique de ces conclusions est qu'un SIL surestimé conduirait à la validation erronée de la fonction de sécurité attribuée au SIS par rapport aux spécifications d'exigence de sécurité déterminées lors de l'étude d'allocation des SIL. Par conséquent, nous réitérons notre suggestion d'utiliser les nouvelles formules *PFH*, car elles sont plus précises et donc plus sûres.

Chapitre 4

Inclusion des tests partiels et imparfaits dans l'évaluation de la PFD_{avg}

4.1. Introduction

Les deux précédents chapitres étaient exclusivement dédiés aux SIS opérant en mode sollicitation élevée ou en fonctionnement continu. A contrario, ce quatrième et dernier chapitre est dévolu aux SIS ayant un mode de fonctionnement à faible sollicitation, c'est-à-dire, la fonction de sécurité n'est activée que sur sollicitation et moins d'une fois par an. La mesure de défaillance cible pertinente pour ce mode de fonctionnement est spécifiée, rappelons-le, en termes de probabilité moyenne de défaillance dangereuse de la fonction de sécurité sur sollicitation (PFD_{avg}). Comme nous l'avons déjà mentionné au premier chapitre, la PFD_{avg} correspond à l'indisponibilité moyenne du SIS évaluée sur une période donnée.

A l'instar de la mesure *PFH*, la norme CEI 61508 donne une liste des paramètres à prendre en compte pour l'évaluation de la PFD_{avg} : l'architecture du système (KooN), le taux de défaillances dangereuses (λ_D), proportion des défaillances de causes communes (β), couverture des tests de diagnostic réalisés automatiquement en ligne (DC), intervalles de tests périodiques, différents temps de réparation, etc.

Au cours de ce dernier chapitre, nous donnons une attention particulière aux tests périodiques qui sont mis en œuvre pour révéler les défaillances dangereuses cachées : non détectées par les tests en ligne et les tests automatiques de diagnostic. En effet, nous allons mettre l'accent sur l'efficacité des tests périodiques par la considération des *tests partiels* et des *tests imparfaits*. Cette considération pourrait contribuer à un accroissement significatif de la PFD_{avg}.

Le reste du présent chapitre est organisé comme suit. Un court rappel relatif aux principes de tests est d'abord présenté. Puis, les tests partiels et les tests imparfaits sont explicités avec suffisamment de détail. Ensuite, nous traitons la modélisation des tests partiels et des tests imparfaits à l'aide de modèles holistiques notamment les arbres des défaillances (AdD) et les chaines de Markov. Enfin, les conclusions nécessaires sont déduites.

4.2. Principes relatives aux tests

Dans ce qui suit, nous tenons à expliquer les termes et les notions nécessaires utilisés dans la suite de ce manuscrit.

4.2.1. Tests périodiques

Le terme test périodique est parfois utilisé de manière interchangeable avec test fonctionnel. Alors que certains auteurs les voient comme identiques [ISA-TR84.00.03, 2002], d'autres les voient comme différents [CEI 61508, 2010] et certains utilisent même les deux termes ensemble : test périodique fonctionnel [OLF-070, 2004]. Notons que le terme « essai fonctionnel » tel qu'utilisé dans les parties 2, 3 et 7 de la [CEI 61508, 2010] porte une signification différente. Ce dernier est réalisé dans le but de : « *révéler les défaillances pendant les phases de spécification et de conception. Eviter les défaillances lors de la réalisation et de l'intégration du logiciel et du matériel* » [CEI 61508-7, 2010].

Par ailleurs, il convient d'indiquer que dans la deuxième édition de la CEI 61508, la désignation « test périodique » utilisée dans sa première édition est remplacée par « *essai périodique* ». Aussi, elle indique qu'il existe un synonyme : « *test d'épreuve* » comme traduction directe des termes anglo-saxons « *proof test* » utilisés dans la version anglaise de la CEI 61508. Dans le cadre de cette thèse, nous maintenons l'ancienne dénomination « *test périodique* » du fait de son usage très répandu, surtout au sein de la communauté scientifique.

L'objectif des tests périodiques est de révéler les défaillances non détectées par les tests en ligne ou de diagnostic. En effet, la CEI 61508 dans sa 4ème partie [CEI 61508-4, 2010] définit le test périodique comme : *« essai périodique destiné à détecter les défaillances dangereuses cachées d'un système relatif à la sécurité de telle sorte que, si nécessaire, une réparation puisse rétablir le système dans une condition « comme neuf » ou dans une condition aussi proche que possible de celle-ci »*. Dans cette définition, seules les défaillances dangereuses sont citées, mais les défaillances sûres peuvent également être révélées par les tests périodiques.

Les tests périodiques peuvent contribuer à atteindre et à améliorer le SIL sans apporter de modifications à la conception du système de sécurité [Torres-Echeverria, 2009]. Les principes, les pratiques et procédures de tests périodiques avec des exemples sont expliqués dans le document [HSE-UK, 2002]. Il contient le contenu et le format des procédures des tests périodiques, planification et ordonnancement, registres des tests, compétences requises, connaissance des risques et gestion du changement. L'étude HSE-UK justifie, à juste titre, qu'il existe un conflit entre la nécessité de tests périodiques et l'exigence de minimiser les temps

d'arrêt induits par ces tests. En effet, les tests périodiques demandent des ressources en termes d'heures de travail, d'équipement et de coordination. Ils perturbent souvent la production et conduisent à son arrêt [Jin et Rausand, 2014]. Ils sont donc réalisés *hors ligne* car leur mise en œuvre nécessite l'arrêt du système contrôlé (EUC).

Malgré le fait que l'étude HSE-UK précise que le test de *bout en bout* est la pratique idéale, elle admet également que les *tests* (*périodique*) *partiels* sont une pratique nécessaire dans les situations où des tests de bout en bout ne sont pas forcément convenables ou possibles. Cet avantage attribué aux tests partiels est imputable au fait que ces derniers ne requirent pas l'arrêt de l'EUC (réalisés *en ligne*). Ils permettent donc d'améliorer la performance de la fonction de sécurité sans perturber le fonctionnement de l'EUC.

Nous signalons, *in fine*, l'importance de la fréquence des tests périodiques, caractérisée par l'intervalle entre deux tests consécutifs (T_1 selon la nomenclature de la CEI 61508). Notons que des différentes fréquences de tests peuvent être utilisées pour les différents constituants du SIS. Aussi, la valeur de la PFD_{avg}^{max} pourrait être utilisée pour déterminer les fréquences optimales des tests périodiques.

4.2.2. Tests parfaits et tests imparfaits

L'efficacité de l'essai périodique dépend à la fois de sa couverture des défaillances et de l'efficacité de la réparation [CEI 61508-4, 2010]. Dans ce contexte, un *test périodique parfait* rend compte de la capacité du test périodique à révéler et à traiter toutes les défaillances non détectées de l'élément objet du test. A ce titre, les hypothèses associées à un test parfait sont :

- Le test est réalisé dans des conditions similaires à la situation de sollicitation réelle.
- Le test périodique doit révéler toutes les défaillances cachées et les défaillances d'éléments qui pourraient conduire à de telles défaillances.
- Les défaillances révélées sont réparées et tous les canaux doivent être dans un état aussi bon que neuf après réparation.

Dans la pratique, il n'est pas facile de détecter 100 % des défaillances dangereuses cachées pour des systèmes autres que les SIS de faible complexité [CEI 61508-4, 2010]. En effet, certains facteurs peuvent affecter le test ou le test peut ne pas couvrir tous les aspects spécifiés, ce qui peut conduire à la non détection de certaines défaillances cachées. Ainsi, un *test périodique imparfait* ne rétablirait pas une fonction de sécurité dans un état « *aussi bon que neuf* » et donc l'indisponibilité (PFD_{avg}) augmenterait [CEI 61511-2, 2016].

Bukowski et Van Beurden ont classé les tests imparfaits en deux catégories : *incomplets* et *incorrects* [Bukowski et Van Beurden, 2009] :

- L'*exhaustivité* du test périodique est définie ici comme la *probabilité* que toutes les défaillances dangereuses soient révélées/vérifiées lors d'un test périodique qui est fonction du composant et des tests exécutés. Sur la base de cette définition, un test *périodique incomplet* (*partiel*) a donc une relation avec la *limitation du test lui-même*.
- L'*exactitude* du test périodique indique la *probabilité* que le test réel soit correctement exécuté par l'équipe de test comme spécifié et que toutes les défaillances existantes sont révélées, réparées et aucun nouveau problème est introduit pendant le test. Celle-ci est donc vue comme une fonction des capacités de maintenance et de culture sur un site spécifique. Un *test périodique incorrect* a une relation avec *les limites de ceux qui* effectuent le test.

Des études ont montré que l'exhaustivité des tests a un impact plus important sur la PFD_{avg} que l'exactitude des tests [Brissaud *et al.*, 2012; Bukowski et Van Beurden, 2009].

4.2.3. Sources d'imperfection des tests périodiques

Comme nous l'avons implicitement mentionné précédemment, l'imperfection des tests peut être engendrée par une situation où les conditions et les procédures de test ne sont pas exactement les mêmes que les conditions de la sollicitation réelle de la fonction de sécurité. [Rolén, 2007] a attribué les sources de l'imperfection des tests à cinq facteurs principaux, notamment les méthodes, le matériel, les machines, le milieu et la main-d'œuvre. Ces attributs avec leurs caractéristiques individuelles sont illustrés à la figure 4.1.

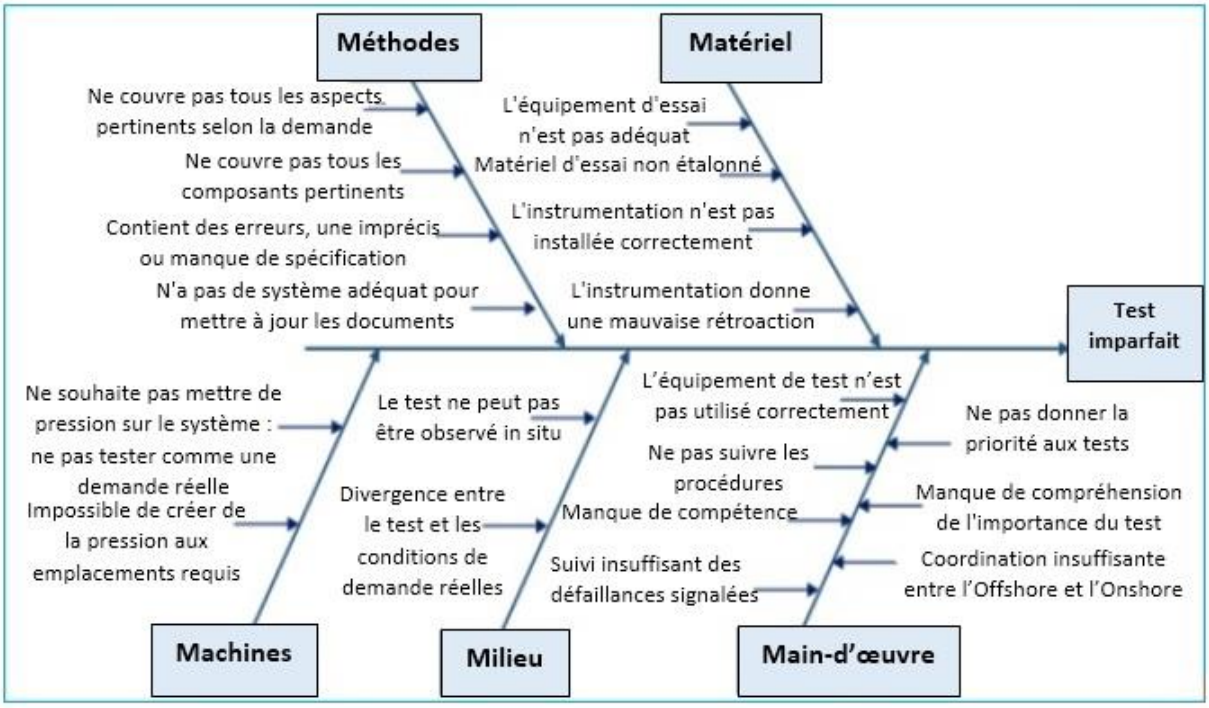

Figure 4.1 : Diagramme d'Ishikawa relatif aux sources d'imperfection des tests [Rolén, 2007]

[Hauge et *al.*, 2013] donnent des exemples typiques montrant comment certaines conditions de test peuvent ne pas révéler toutes les défaillances cachées. Citons à titre illustratif les suivants :

- *Transmetteurs mis en mode test et signaux injectés :* le mode test se substitue au mode de fonctionnement d'origine des transmetteurs et l'injection de signaux (généralement avec des transmetteurs smart/fieldbus) peut être différente de la situation réelle et ne révèle donc pas tous les modes de défaillance.
- *Transmetteurs de pression (PT) testés à partir du manifold :* le test consiste à introduire la pression d'une source externe pour voir si le PT détecte et réagit en conséquence (figure 4.2). Cela signifie que les lignes d'impulsion ne sont pas testées. Dans une situation réelle, il peut y avoir un blocage où les changements de pression sont présents. Ceci rend les tests non parfaits à 100 % car les facteurs environnants ne sont pas inclus dans la procédure de test comme indiqué par le cercle rouge sur la figure 4.2.
- Une autre illustration typique d'un test imparfait des transmetteurs de pression est que les tests sont normalement effectués après l'isolement des transmetteurs du procédé surveillé, car la mise sous pression d'une canalisation à la pression de déclenchement peut conduire à une situation dangereuse. Dans ce contexte, les défaillances qui peuvent

être causées par une contamination des conduites de détection de pression peuvent ne pas être révélées par le test [Jin et *al.*, 2013].

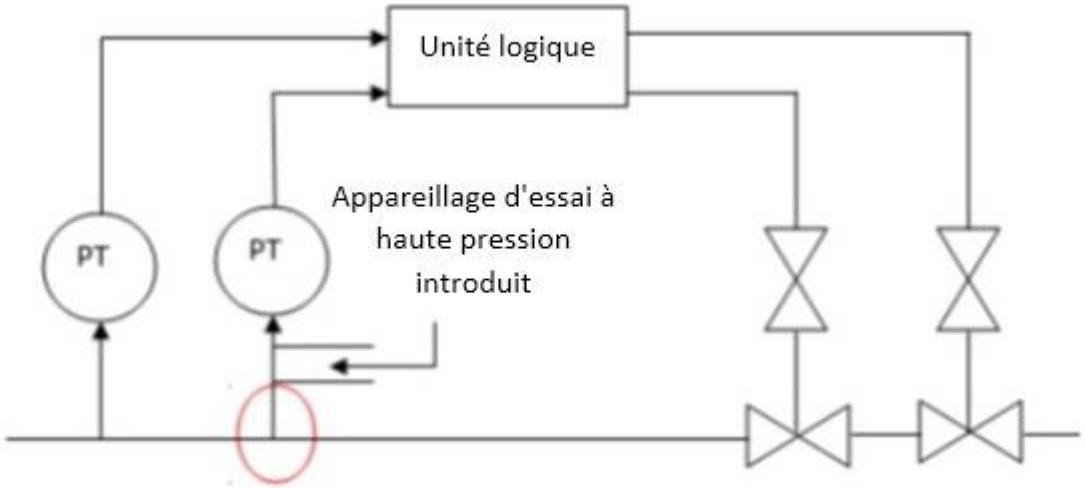

Figure 4.2 : Illustration du test du transmetteur de pression

- *Equipement non testé en position normale :* un exemple de ceci est le test périodique des détecteurs feu/gaz. L'introduction de gaz ou de fumées doit être organisée de manière à atteindre la hauteur où ces détecteurs sont installés. L'utilisation des fumées de gaz qui ne possèdent pas forcément les mêmes caractéristiques que celles utilisées en situation réelle présente une limitation du test. Aussi, la position ou le contact établit avec les détecteurs en raison de l'appareil de test est un autre facteur pouvant réduire l'efficacité du test. Il pourrait également y avoir un changement ou une modification de la disposition existante, peut-être l'installation de tuyaux et de brides dans la pièce ou dans la zone, qui empêche le fonctionnement réel des détecteurs.

4.2.4. Test complet et test partiel

Le *test périodique complet* est un test effectué à des intervalles spécifiques destiné à révéler et à traiter tous les modes de défaillances cachées de l'équipement ou du composant testé. Dans la plupart des cas, ces tests nécessitent l'arrêt du système surveillé (EUC) qui entraîne des arrêts de production. Un *test périodique partiel* est un test effectué à des intervalles spécifiques, plus courts que ceux des tests complets, conçu pour révéler et traiter certains modes de défaillances cachées sans perturber significativement l'EUC. Il est en général planifié est mis en œuvre pour permettre l'extension des périodes des tests complets, permettant ainsi de réduire les pertes de production tout en maintenant l'intégrité du système.

En outre, selon [HSE-UK, 2002], il existe deux catégories de tests partiels, à savoir :

- Test des composants du système à de différents moments et fréquences, ce que l'on appelle test échelonné. Dans ce cas de figure, l'aspect partiel n'est pas lié à la proportion des défaillances détectées par le test, mais plutôt au nombre de composants testés.
- Test des sous-ensembles de fonctions de composants individuels sous forme de simulation de mesure ou la course partielle des soupapes. Dans le cadre de ce travail de recherche, seule cette deuxième catégorie est concernée.

Pour faire le lien avec la répartition précédente des tests en termes de tests parfait et imparfait, les tests périodiques complet et partiel peuvent être imparfaits s'ils ne révèlent pas et ne traitent pas adéquatement les modes de défaillances pour lesquels ils ont été conçus. A ce titre, nous réfutons l'argument d'exhaustivité comme cause d'imperfection des tests, tel que avancé par [Bukowski et Van Beurden, 2009]. Seule donc l'exactitude du test au regard de son intention pourrait conduire à son imperfection.

4.2.5. Test de course partielle

Le test de course partielle (PST : *partial stroke testing*), exemple typique des tests partiels, est une technique communément utilisée pour détecter certains modes de défaillances d'une vanne d'arrêt d'urgence sans avoir à la fermer complètement. En effet, un PST peut détecter le mode de défaillance « *vanne bloquée en position ou ouverte* » en fermant partiellement la vanne, 15 % de fermeture par exemple, en ligne et donc sans arrêter l'EUC. Cela va de soi, avec ce test, il n'est pas possible de détecter un mode de défaillance comme « *fermeture incomplète de la vanne* ».

Les PST sont des compléments plutôt qu'un moyen d'éliminer le besoin pour les tests périodiques complets [Summers et Zachary, 2000 ; Nuis, 2005]. Ils présentent les mérites et limites données au tableau 4.1, légèrement adapté de [Lundteigen et Rausand, 2007].

Il existe un certain nombre de techniques différentes disponibles pour les PST. La figure 4.4 montre comment ce test est effectué sur une vanne d'arrêt d'urgence en utilisant deux méthodes : PST intégré, activé manuellement à partir du solveur logique du SIS, et l'usage d'un package PST du fournisseur. Avec le package PST, le test peut être déclenché manuellement ou automatiquement.

Tableau 4.1 : Avantages et inconvénients des PST

Avantages	Inconvinients
Réduction des perturbations opérationnelles par l'extension de l'intervalle des tests complets : les coûts d'exploitation et de maintenance peuvent être réduits car moins d'heures de travail et moins d'arrêts programmés de production sont nécessaires.	Système plus complexe en raison de matériel et de logiciels supplémentaires.
Augmentation de la disponibilité de la fonction de securité (des vannes): reduction de la PFD_{avg} (voir figure 4.3)	Usure accrue due à un fonctionnement plus fréquent.
Réduction de la probabilité de collage des joints en raison d'un fonctionnement plus fréquent de la vanne.	Augmentation potentielle des déclenchements intempestifs entraînant ainsi un arrêt de l'EUC : la vanne peut continuer vers la position de sécurité au lieu de revenir à la position initiale.
Réduction de l'usure de la zone du siège de la vanne puisque elle est moins fréquemment amenée en position fermée (extension de l'intervalle des tests complets).	Non approprié pour certains systèmes qui sont sensibles aux perturbations.

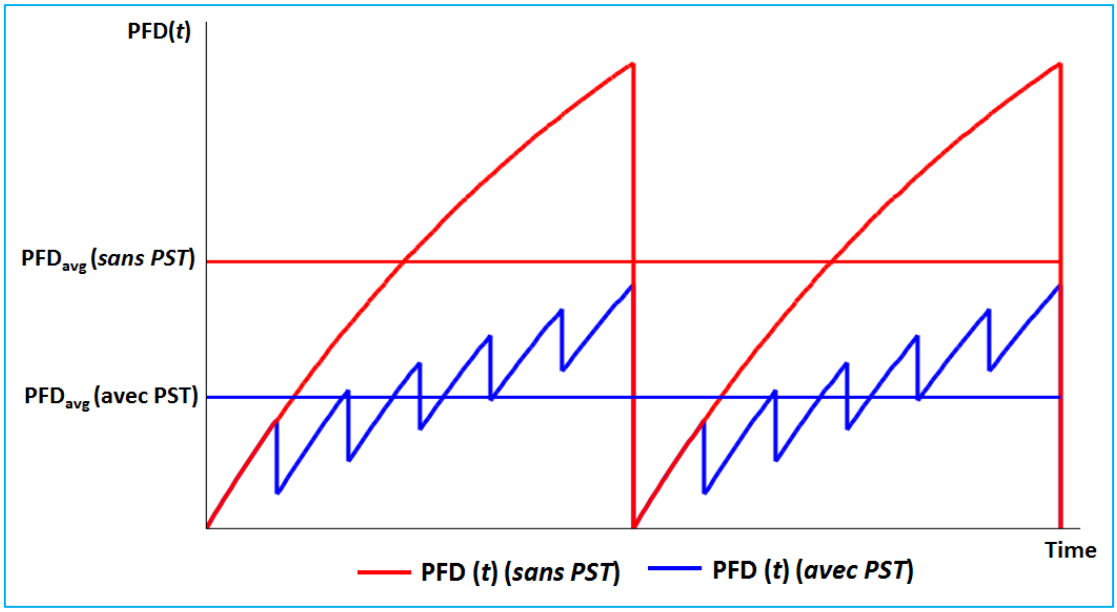

Figure 4.3 : Impact des PST sur la PFD_{avg}

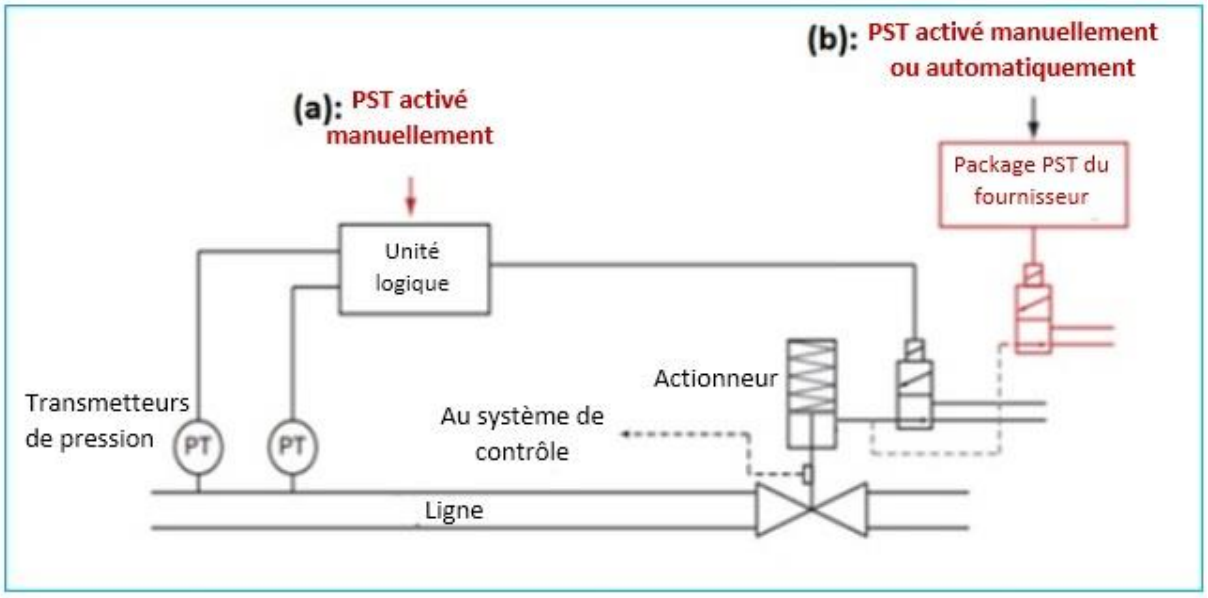

Figure 4.4 : Configurations PST : (a) intégré au SIS et (b) via un package PST supplémentaire [Lundteigen et Rausand, 2008]

4.3. Nouvelle taxonomie des défaillances

Rappelons que les modes de défaillances des SIS se répartissent en défaillances dangereuses (D) et défaillances sûres (S), selon leurs effets sur la fonction de sécurité. A son tour, une défaillance dangereuse peut être détectées par les tests automatiques de diagnostic (défaillances DD) ou non détectées par ces mêmes tests (défaillances DU). Les différents taux de défaillances relatifs à cette répartition sont donnés au deuxième chapitre (équation (2.3) et figure 2.3). Afin de rendre compte des tests périodiques partiels (par exemple, tests de course partielle sur les vannes) et de l'imperfection des tests périodiques complets, une nouvelle répartition s'impose. Dans le cadre de cette thèse, nous adoptons les hypothèses suivantes :

- Les tests périodiques partiels sont considérés comme parfaits : ils détectent les modes de défaillances DU, pour lesquels ils sont conçus, et permettent la restauration des composants testés dans une condition « comme neuf ».
- La proportion des défaillances DU révélées par un test partiel est sa couverture, désignée par la lettre grecque θ. La détermination de θ est hors du cadre de cette thèse. A ce titre, une approche détaillée de la détermination de ce facteur, dans le cas des tests de course partielle des vannes (PST), est fournie dans [Lundteigen et Rausand, 2008].
- Les défaillances DU détectées par un test partiel (DU_{PT}) sont réparées dans un délai moyen noté MRT_{PT}. L'indice « PT » désigne « test partiel (partial test) ».

- Les défaillances DU résiduelles, qui ne sont pas révélées par les tests partiels, restent toujours cachées. Une partie de ces défaillances est révélée par le prochain test périodique complet (DU_{FT}). Elle dépend de sa couverture, notée PCT (*proof test coverage*) dans la CEI 61508. L'indice « FT » désigne « test complet (full test) ».
- La réparation des défaillances DU_{FT} est supposée parfaite : un état « aussi bon que neuf » est atteint pour le ou les éléments défectueux. La durée de réparation moyenne correspondante est notée MRT_{FT}. Du fait que le test périodique complet s'effectue en général hors ligne, la MRT_{FT} peut être négligée.
- Les défaillances DU non révélées par les tests périodiques complets (DU_{ND}) restent toujours cachées. L'indice « ND » indique « non détectées ».
- Les tests partiels et complets sont supposés périodiques. Les tests partiels sont répartis d'une manière uniforme sur l'intervalle de tests complets (T_1) : effectués chaque période égale à $T_{PT} = T_1/m$, ou m est un nombre entier.
- Lorsque les instants d'un test partiel et d'un test complet coïncident, le test partiel est considéré comme inclut dans le test complet. De ce fait, les défaillances révélées par le test partiel sont également entièrement révélées par le test complet.
- Les durées nécessaires pour la réalisation des tests partiels et complets sont supposées nulles.
- Dans le cadre architecture redondante, il existe des défaillances de causes communes (DCC) pour chacun des modes de défaillances identifiés : DU_{PT}, DU_{FT} et DU_{ND}. En mettant à profit le model du facteur β (équation (2.2)), les proportions correspondantes sont respectivement $\beta_{PT}, \beta_{FT,}$ et β_{ND}.

La figure 4.5 fournie la nouvelle classification des défaillances de même que les taux de défaillances associés, compte tenu des différentes hypothèses précédentes et de la section 2.2.2 du deuxième chapitre.

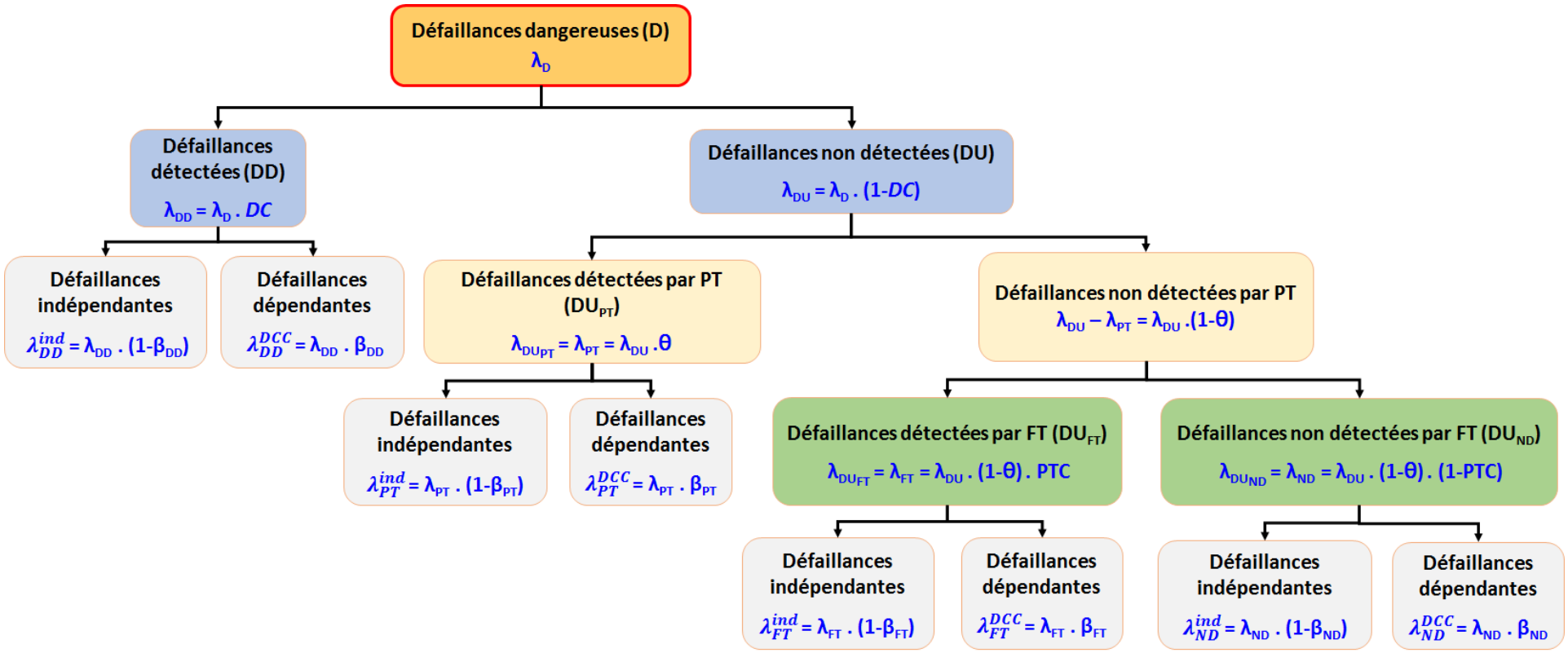

Figure 4.5 : Nouvelle classification des défaillances considérant les tests partiels et les tests complets imparfaits

4.4. Formulations relatives à la PFD_{avg} incluant les tests partiels

Dans cette section, plusieurs formules relatives à la PFD_{avg} sont regroupées. Ces formules tiennent compte des tests partiels et des tests complets supposés parfaits (PTC = 100 %), c'est-à-dire, toutes les défaillances dangereuses sont révélées et correctement traitées à l'issue du test périodique complet. La courbe typique de la $PFD(t)$, dans ce cas de figure, est représentée à la figure 4.6. Notons que les formules PFD_{avg} qui ne traitent pas les tests partiels, telles que celles fournies dans la partie 6 de la CEI 61508, ne sont pas abordées, car elles sont assez connues et largement étudiées [Innal, 2008 ; Oliveira et Ibrahimovitch, 2010 ; Jin *et al.*, 2013 ; Guaninian, 2014 ; Innal *et al.*, 2015 ; Chebila et Innal, 2015]. Précisons que *les formules suivantes sont toutes récrites conformément à la terminologie utilisée dans cette thèse*. Nous attirons l'attention sur le fait que la capacité de mise à l'arrêt automatique de l'EUC, suite à une détection d'une défaillance dangereuse dans le SIS, ne s'applique pas dans le cadre de la PFD_{avg}.

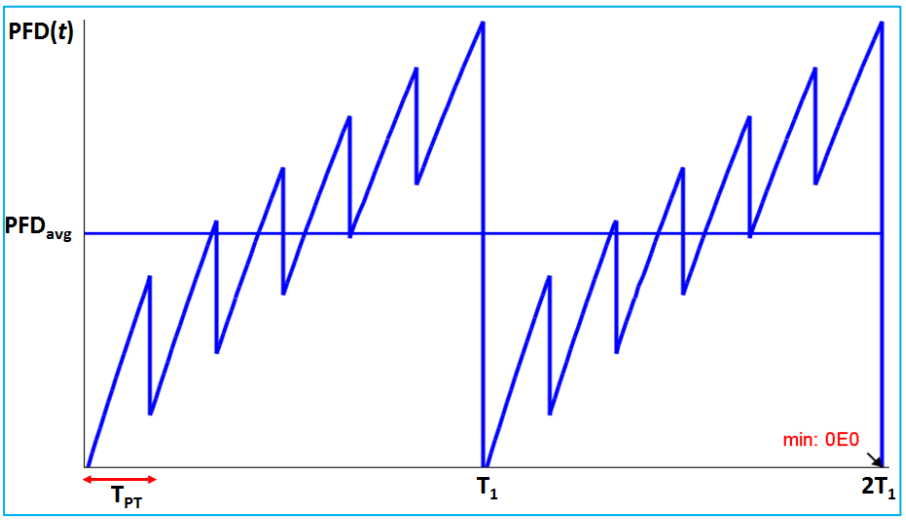

Figure 4.6 : Courbe typique de la $PFD(t)$ pour tests partiels et complets parfaits

4.4.1. Formules d'Oliveira [Oliveira, 2009]

En s'inspirant du schéma général des formules de la CEI 61508, Oliveira propose deux expressions différentes pour le calcul de la PFD_{avg} avec considération des tests de course partielle. La lecture prudente du document [Oliveira, 2009] ne nous a pas satisfaits quant à l'exactitude de l'approche adoptée. Nous pensons que les formules développées sont plutôt erronées. Elles correspondent aux formules (4.1) et (4.2) données dans ce qui suit. Nous constatons que les différentes partitions de défaillances (DD, DU_{PT}, DU_{FT}) sont incluses, ainsi

que les différentes durées de réparation associées. Par ailleurs, Oliveira attribue le même facteur de cause commune pour les modes DU_{PT} et DU_{FT} : $\beta_{PT} = \beta_{FT} = \beta$.

$$PFD_{avg(1)}^{KooN} = \frac{N!}{(K-1)!\ (N-K)!}\left[(1-\beta)\,\lambda_{DU} + (1-\beta_D)\,\lambda_{DD}\right]^{N-K+1} \cdot \left(T_{CE\_PST}\right)^{N-K} \cdot T_{KooN\_PST}$$
$$+\ \beta\,\lambda_{FT}\left(\frac{T_1}{2} + MRT\right) + \beta\,\lambda_{PT}\left(\frac{T_{PT}}{2} + MRT_{PT}\right) + \beta_D\,\lambda_{DD} MTTR \qquad (4.1)$$

$$PFD_{avg(2)}^{KooN} = \frac{N!}{(K-1)!\ (N-K+1)!}\left[(1-\beta)\,\lambda_{DU} + (1-\beta_D)\,\lambda_{DD}\right]^{N-K+1} \cdot (T_1)^{N-K} \cdot T_{KooN\_PST}$$
$$+\ \beta\,\lambda_{FT}\left(\frac{T_1}{2} + MRT\right) + \beta\,\lambda_{PT}\left(\frac{T_{PT}}{2} + MRT_{PT}\right) + \beta_D\,\lambda_{DD} MTTR \qquad (4.2)$$

Avec :

$$\begin{cases} T_{CE_{PST}} = \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR + \frac{\lambda_{PT}}{\lambda_D} \cdot \left(\frac{T_{PT}}{2} + MRT_{PT}\right) + \frac{\lambda_{FT}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MRT\right) \\ T_{KooN_{PST}} = \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR + \frac{\lambda_{PT}}{\lambda_D} \cdot \left(\frac{T_{PT}}{N-K+2} + MRT_{PT}\right) + \frac{\lambda_{FT}}{\lambda_D} \cdot \left(\frac{T_1}{N-K+2} + MRT\right) \end{cases} \qquad (4.3)$$

4.4.2. Formule de Brissaud [Brissaud et *al.*, 2012]

Dans le cadre de cette étude, les auteurs ont étudié l'impact de la distribution des tests partiels, durant un intervalle de test périodique complet, sur la PFD_{avg}. Nous reportons ci-après la formule établie dans le cas d'une distribution périodique.

$$PFD_{avg}^{KooN} = 1 - \sum_{x=K}^{N}\left[S(K,N,x) \cdot \frac{1-e^{-x\cdot\lambda_{DU}\cdot T_{PT}}}{x\cdot\lambda_{DU}\cdot T_{PT}} \cdot \frac{1}{m}\sum_{i=1}^{m}\left[e^{-x\cdot(1-\theta)\cdot\lambda_{DU}\cdot(i-1)\cdot T_{PT}}\right]\right] \qquad (4.4)$$

Avec : $T_{PT} = T_1/m$. En outre, la quantité $S(K,N,x)$ est donnée par la relation suivante :

$$S(K,N,x) = \sum_{l=K}^{x}\binom{N}{x}\cdot\binom{x}{l}\cdot(-1)^{x-l}, \quad \text{où } \binom{n}{p} = \frac{n!}{(n-p)!\,p!} \qquad (4.5)$$

Au sein de la formule (4.4), les défaillances DD ne sont pas considérées. De plus, les différentes durées de réparation relatives aux défaillances DU_{PT} et DU_{FT} sont négligées. En effet, les auteurs assument que pendant les opérations de tests et de maintenance des mesures sont mises en œuvre afin de maintenir l'EUC en sécurité. Finalement, notons que la contribution des défaillances de causes communes (DCC) n'est également pas incluse.

4.4.3. Formule de Jin [Jin et Rausand, 2014]

La formule développée au cours de ce travail est donnée ci-après. Une fois de plus, seul le cas d'une distribution périodique des tests partiels nous intéresse.

$$PFD_{avg}^{KooN} = \frac{1}{m}\sum_{i=1}^{m}\sum_{j=0}^{N-K}\binom{N}{j}\left((i-1)\,(1-\beta_{FT})\lambda_{FT}\cdot T_{PT}\right)^{j}\cdot \frac{(N-j)!([(1-\beta_{PT})\,\lambda_{PT}+(1-\beta_{FT})\,\lambda_{FT}]\cdot T_{PT})^{N-j-K+1}}{(N-j-K+2)!(K-1)!} + \frac{1}{m}\sum_{i=1}^{m}\sum_{j=N-K+1}^{N}\binom{N}{j}\left((i-1)(1-\beta_{FT})\,\lambda_{FT}\cdot T_{PT}\right)^{j} + \frac{\beta_{PT}\,\lambda_{PT}\cdot T_{PT}}{2} + \frac{\beta_{FT}\,\lambda_{FT}\cdot T_{1}}{2} \quad (4.6)$$

A l'image de l'équation (4.4), la formule (4.6) ne rend pas compte des défaillances DD et des différentes durées de réparation. Toutefois, les défaillances DCC y sont intégrées (les deux derniers termes de l'égalité (4.6)).

4.4.4. Formule de Chebila [Chebila et Innal, 2015]

Afin de s'affranchir de certaines limites qui entachent les deux formulations précédentes, Chebila et Innal ont développé une expression donnant la PFD_{avg} améliorée (équation (4.7)). En effet, elle considère les défaillances DD et la durée de réparation sous-jacente. Néanmoins, les durées de réparation relatives aux modes DU_{PT} et DU_{FT} ne sont pas prises en compte. La formule (4.7) peut être améliorée davantage par l'ajout de ces durées aux niveaux des contributions de causes communes (deux dernier termes de la formule).

$$PFD_{avg}^{KooN} = \frac{\binom{N}{N-K+1}}{(N-K+2)\cdot[(1-\beta_{PT})\,\lambda_{PT}+(1-\beta_{FT})\,\lambda_{FT}]\cdot m\cdot T_{PT}}\cdot\sum_{j=0}^{m-1}\left(\left[\frac{(1-\beta_D)\lambda_{DD}}{(1-\beta_D)\lambda_{DD}+\mu_{DD}}+\{[(1-\beta_{PT})\,\lambda_{PT}+(1-\beta_{FT})\,\lambda_{FT}]+(1-\beta_{FT})\,\lambda_{FT}\cdot j\}\cdot T_{PT}\right]^{N-K+2}-\left[\frac{(1-\beta_D)\lambda_{DD}}{(1-\beta_D)\lambda_{DD}+\mu_{DD}}+(1-\beta_{FT})\,\lambda_{FT}\cdot j\cdot T_{ST}\right]^{N-K+2}\right)+\frac{\beta_D\lambda_{DD}}{\beta_D\lambda_{DD}+\mu_{DD}}+\beta_{PT}\lambda_{PT}\cdot\frac{T_{PT}}{2}+\beta_{FT}\lambda_{FT}\cdot\frac{T_1}{2} \quad (4.7)$$

4.4.5. Formules de Innal [Innal et *al.*, 2016]

Ce travail présente une approche intéressante fondée sur les chaines de Markov multi-phases et une structure arborescente des différentes séquences de défaillance dangereuses. Elle a permis d'établir une formule PFD_{avg} générique qui tient compte de tous les modes de

défaillances et de leurs durées de réparation respectives. Cette formule est présentée ci-dessous. S1, S2 et S3 indiquent des séquences de défaillances commençant par une défaillance DU_{PT}, une défaillance DU_{FT} et une défaillance DD, respectivement.

$$PFD_{avg}^{KooN} = PFD_{avg}^{S1} + PFD_{avg}^{S2} + PFD_{avg}^{S3} + PFD_{avg}^{DCC} \quad (4.8)$$

Avec :

$$\begin{cases} PFD_{S1}^{avg} = \dfrac{N!}{(K-1)!} \cdot (1-\beta_{PT})\lambda_{PT} \cdot \left((1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT}\right)^{h} \cdot \\ \quad \prod_{i=1}^{h+1}\left(\dfrac{T_{PT}}{i+1} + MRT_{PT}\right) \cdot \left[\left((1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT}\right) \cdot \left(\dfrac{T_{PT}}{N-K+2} + MRT_{PT}\right) + (1-\beta_{D})\lambda_{DD} MTTR\right]^{j} \\ PFD_{S2}^{avg} = \dfrac{N!}{(K-1)!} \cdot \left\{ \begin{array}{c} C_1 + \left((1-\beta_{FT})\lambda_{FT}\right)^{N-K} \cdot \prod_{p=1}^{N-K}\left(\dfrac{T_1}{p+1} + MRT_{FT}\right) \cdot \\ \left[(1-\beta_{FT})\lambda_{FT} \cdot \left(\dfrac{T_1}{N-K+2} + MRT_{FT}\right) + j \cdot \left(\dfrac{(1-\beta_{PT})\lambda_{PT}}{\mu_5} + \lambda_{DD}\, MTTR\right)\right] \end{array} \right\} \\ PFD_{S3}^{avg} = \begin{cases} N \cdot (1-\beta_{D})\lambda_{DD} \cdot MTTR, & if N = K \\ 0, if N > K \end{cases} \\ PFD_{avg}^{DCC} = \beta_{FT}\, \lambda_{FT}\left(\dfrac{T_1}{2} + MRT_{FT}\right) + \beta_{PT}\lambda_{PT}\left(\dfrac{T_{PT}}{2} + MRT_{PT}\right) + \beta_{D}\, \lambda_{DD} MTTR \end{cases} \quad (4.9)$$

Où :

$$C_1 = \begin{cases} \sum_{g=1}^{N-K-1}\left((1-\beta_{FT})\lambda_{FT}\right)^{g} \cdot \prod_{l=1}^{g}\left(\frac{T_1}{l+1} + MRT_{FT}\right) \cdot \frac{(1-\beta_{PT})\lambda_{PT}}{\mu_5} \cdot \left((1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT}\right)^{s} \cdot \\ \qquad \prod_{x=1}^{s}\left(\frac{T_{PT}}{x+2} + MRT_{PT}\right) \cdot \\ \left[\left((1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT}\right) \cdot \left(\frac{T_{PT}}{N-K+2-g} + MRT_{PT}\right) + (1-\beta_{D})\lambda_{DD} \cdot MTTR\right], \quad if\ N > K+1 \\ 0, \ if \ N \le K+1 \end{cases} \quad (4.10)$$

$$\begin{cases} h = \max(0, \quad N-K-1) \\ j = \begin{cases} 1, & if\ N > K \\ 0, & if\ N = K \end{cases} \\ s = \max\ (0, \ N-K-1-g) \\ \mu_5 = \left(MRT_{PT} + \dfrac{(3m-1)\cdot T_{PT}}{6m}\right)^{-1} \end{cases}$$

Une forme simplifiée de l'équation (4.8) peut être obtenue si la contribution des défaillances DD est négligée et si les tests partiels sont fréquents, de tel sort que $1/\mu_5 \approx T_{PT}/2+MRT_{PT}$. Cette PFD_{avg} simplifiée est donnée par la formule (4.11).

$$PFD_{KooN}^{avg} = \frac{N!}{(K-1)!} \cdot \sum_{g=0}^{N-K+1} \left((1-\beta_{FT})\lambda_{FT}\right)^{g} \cdot \prod_{l=1}^{g} \left(\frac{T_1}{l+1} + MRT\right) \cdot \left((1-\beta_{PT})\lambda_{PT}\right)^{f_1} \cdot \left(\left(1-\beta_{PT}\right)\lambda_{PT} + \left(1-\beta_{FT}\right)\lambda_{FT}\right)^{(N-K+1-g-f_1)} \cdot \prod_{x=1}^{N-K+1-g} \left(\frac{T_{PT}}{x+1} + MRT_{PT}\right) \quad (4.11)$$

Où : $f_1 = \begin{cases} 1, & if\ g < N-K+1 \\ 0, & if\ g = N-K+1 \end{cases}$

Finalement, concernant la même étude [Innal et *al.*, 2016], une autre formule générique est proposée (équation (4.12)), en se basant sur la structure générale des formules fournies dans la CEI 61508. Cette formule peut être vue comme une rectification partielle de celle développée par Oliveira (formule (4.1)). Cependant, comme démontré dans [Innal et *al.*, 2016], elle reste tout de même formellement erronée.

$$PFD_{KooN}^{avg} = \frac{N!}{(K-1)!} \cdot \left[(1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT} + (1-\beta_D)\,\lambda_{DD}\right]^{N-K+1} \cdot \prod_{i=1}^{N-K+1} MDT_{1ooi} + \beta_{FT}\,\lambda_{FT}\left(\frac{T_1}{2} + MRT_{FT}\right) + \beta_{PT}\lambda_{PT}\left(\frac{T_{PT}}{2} + MRT_{PT}\right) + \beta_D\,\lambda_{DD} MTTR \quad (4.12)$$

Avec :

$$MDT_{1ooi} = \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR + \frac{\lambda_{PT}}{\lambda_D} \cdot \left(\frac{T_{PT}}{i+1} + MRT_{PT}\right) + \frac{\lambda_{FT}}{\lambda_D} \cdot \left(\frac{T_1}{i+1} + MRT\right) \quad (4.13)$$

4.4.6. Comparaison numérique

Nous allons maintenant procéder à une comparaison numérique des résultats issus de certaines formules précédentes pour les architectures *KooN* usuelles. Les formules (4.4), (4.6) et (4.7) ne sont pas prises en compte. En effet, une comparaison des résultats fournis par les équations (4.4) et (4.6) a été effectuée dans [Jin et Rausand, 2014]. De plus, les résultats induits par les équations (4.6) et (4.7) ont été examinés d'une manière détaillée dans [Chebila et Innal, 2015]. Ces trois formules donnent des PFD_{avg} très proches. Rappelons que ces formules négligent les temps de réparations des défaillances DU. Dans ce qui suit, seules les expressions incluant ces temps de réparation sont utilisées. Aussi, seule la contribution des défaillances indépendantes est considérée dans cette comparaison. Cette option permet une comparaison effective entre les précédentes formules. En effet, les défaillances de causes communes (DCC),

possédant à très peu près la même expression mathématique, peuvent masquer les différences potentielles. Le jeu de paramètres utilisés à cette fin est le suivant : λ = 1E–6/*h* ; DC = 0.6 ; θ = 0.6 ; $\beta_D = \beta_{PT} = \beta_{FT} = 0$; *MTTR* = MRT_{FT} = MRT_{PT} = 8 *h* ; T_1= 17520 *h*. De plus, différents intervalles de tests partiels sont utilisés. Rappelons qu'à ce stade, l'imperfection des tests périodiques complets n'est encore pas considérée. L'ensemble des résultats obtenus est regroupé au tableau 4.2.

Tableau 4.2 : Différents résultats numériques

KooN	T_{PT}	**Séries de formules PFD_{avg}**				
		[Oleveira, 2oo9]		**[Innal et al., 2016]**		
		Eq. (4.1)	**Eq. (4.2)**	**Eq. (4.8)**	**Eq. (4.11)**	**Eq. (4.12)**
1oo1	4380	1.935E-03	1.935E-03	1.935E-03	1.935E-03	1.935E-03
	2190	1.672E-03	1.672E-03	1.672E-03	1.672E-03	1.672E-03
	1460	1.585E-03	1.585E-03	1.585E-03	1.585E-03	1.585E-03
	730	1.497E-03	1.497E-03	1.497E-03	1.497E-03	1.497E-03
1oo2	4380	5.004E-06	2.265E-05	4.620E-06	4.723E-06	5.004E-06
	2190	3.738E-06	1.958E-05	3.510E-06	3.523E-06	3.738E-06
	1460	3.357E-06	1.856E-05	3.194E-06	3.192E-06	3.357E-06
	730	2.997E-06	1.753E-05	2.905E-06	2.894E-06	2.997E-06
1oo3	4380	1.092E-08	2.982E-07	1.262E-08	1.311E-08	1.458E-08
	2190	7.050E-09	2.579E-07	8.313E-09	8.376E-09	9.422E-09
	1460	6.001E-09	2.445E-07	7.250E-09	7.251E-09	8.021E-09
	730	5.061E-09	2.310E-07	6.345E-09	6.315E-09	6.766E-09
2oo2	4380	3.870E-03	3.870E-03	3.870E-03	3.870E-03	3.870E-03
	2190	3.345E-03	3.345E-03	3.344E-03	3.344E-03	3.345E-03
	1460	3.170E-03	3.170E-03	3.170E-03	3.170E-03	3.170E-03
	730	2.994E-03	2.994E-03	2.994E-03	2.994E-03	2.994E-03
2oo3	4380	1.501E-05	6.795E-05	1.386E-05	1.417E-05	1.501E-05
	2190	1.121E-05	5.874E-05	1.053E-05	1.057E-05	1.121E-05
	1460	1.007E-05	5.567E-05	9.582E-06	9.577E-06	1.007E-05
	730	8.990E-06	5.260E-05	8.716E-06	8.683E-06	8.990E-06

L'examen du tableau 4.2 montre que les différentes formules donnent des résultats identiques pour les configurations 1oo1 et 2oo2. Ce constat peut être généralisé pour toute configuration *NooN*. De plus, les formules (4.1) et (4.12) fournissent des valeurs similaires pour les architectures 1oo2 et 2oo3. Ceci peut également être généralisé pour les architectures (N-1)ooN. Pour des redondances plus élevées, la formule (4.2) induit des valeurs trop conservatifs, tandis que la formule (4.1) donne les valeurs les plus optimistes. Ces conclusions nous permettent de corroborer le fait que les relations données par Oliveira sont incorrectes dans le cas général. Les relations (4.8) et (4.11) donnent des résultats proches, l'équation (4.8) étant légèrement conservative lorsque le test partiel T_{PT} diminue (la réciproque est vraie). Nous

pouvons finalement noter que les résultats de l'équation (4.12) peuvent être vus comme une majoration acceptable de ceux obtenus en utilisant les autres équations (à l'exception de (4.2)). Cependant, elle reste formellement fausse (voir Innal et *al*., 2016 pour plus de détail).

4.5. Inclusion de l'imperfection des tests périodiques complets dans la PFD_{avg}

Un SIS doit être testé régulièrement pour découvrir toute défaillance cachée potentielle. Dans l'estimation de PFD_{avg}, les tests périodiques complets sont généralement supposés être parfaits : le SIS est rétabli dans un état « comme neuf » à l'issue du test. Cette supposition n'est nécessairement pas vérifiée en réalité. En fait, comme nous l'avions déjà évoqué, en raison d'éventuelles divergences entre le fonctionnement réel du SIS et les conditions de test (ou autres facteurs), certaines défaillances peuvent rester non révélés après le test et/ou ne sont pas réparées (traitées) comme voulu.

4.5.1. Approches existantes

L'imperfection des tests est généralement traitée en utilisant trois approches distinctes :

- ***Approche de la CEI 61508* :** considération de la couverture des tests complets aux niveaux des taux de défaillances DU (*PTC*). Ceci induit la répartition de la figure 4.5 : une proportion DU_{FT} ayant le taux λ_{FT} et une proportion DU_{ND} possédant le taux λ_{ND}.
- ***Approche implémentée dans le logiciel GRIF* :** considération de l'efficacité du test comme la probabilité de détection des défaillances DU lors d'un test donné (σ). La différence avec la première approche est qu'au moment du test soit la totalité des défaillances sont détectées et correctement réparées (avec une probabilité σ), soit ces mêmes défaillances ne sont pas détectées (selon une probabilité 1-σ) (voir figure 4.7). La prise en compte de cette option dans le logiciel GRIF est réalisée via un modèle markovien multi-phases.
- ***Approche PDS* :** ajout d'une probabilité constante relative aux défaillances indépendantes du test (P_{TIF}). Les défaillances indépendantes du test (*TIF : test independent failures*) sont des défaillances ne pouvant pas être révélées par les tests périodiques complets ou même par les tests de diagnostic (non *détectables* par les tests). Seule une vraie sollicitation sur la fonction de sécurité peut les révéler. Selon le manuel PDS [PDS, 2006], P_{TIF} représente la probabilité qu'un seul élément, qui vient juste d'être testé, de faillir à la sollicitation indépendamment de l'intervalle des tests

périodiques complets. Certaines valeurs génériques de P_{TIF}, basées sur jugements d'experts, sont données dans [Hauge et Onshus, 2006]. L'usage de P_{TIF} est plus approprié que ceux des *PTC* et σ lorsqu'il s'agit des défaillances systématiques de conception de matériels ou de logiciels. Rappelons que la maitrise de ce genre de défaillances dans la CEI 61508 ne requière pas le calcul de la PFD_{avg}. Il convient de signaler que le manuel PDS suggère également l'usage de l'approche CEI 61508 comme alternative.

Bien entendu, les trois approches précédentes induisent des PFD_{avg} différentes, tel que schématisé dans la figure 4.8 (pour un seul composant).

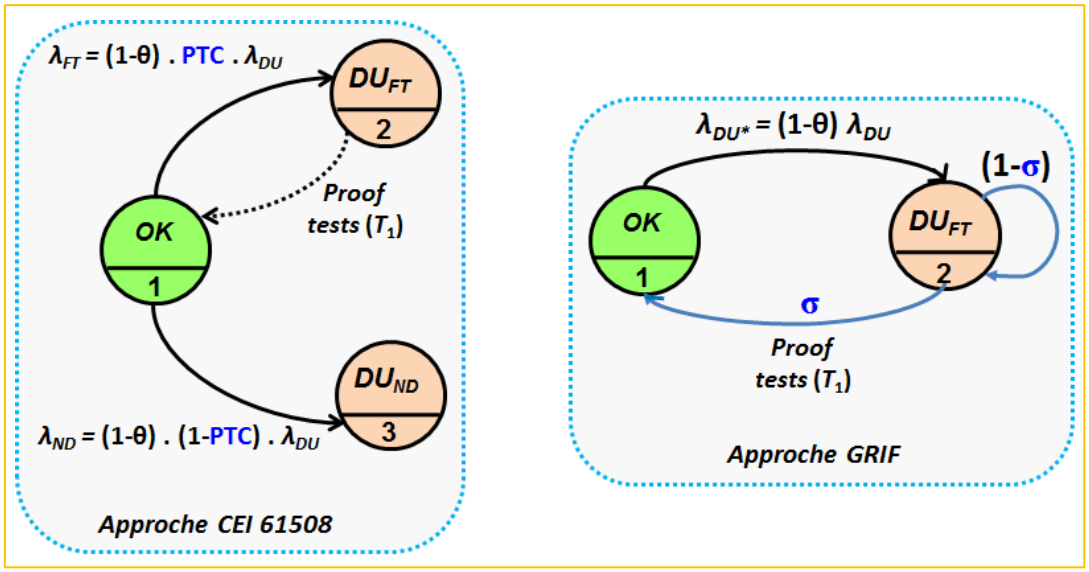

Figure 4.7 : Approches CEI 61508 et GRIF pour la considération de l'efficacité des tests

L'examen de la figure 4.8 montre que dans le cadre de l'approche CEI 61508, basée sur PTC, il n'existe pas de régime stationnaire pour la quantité $PFD_{avg}(t)$. Ceci implique que la PFD_{avg} correspondante continue d'augmenter en fonction du temps et ne possède donc pas de valeur limite. Cette augmentation est attribuée aux défaillances DU_{ND}. Cette approche conduirait donc à des PFD_{avg} pessimistes. Pour les deux autres approches, il existe un comportement stationnaire qui se traduit par l'existence d'une valeur limite de la PFD_{avg}. Il convient de signaler que ce comportement stationnaire est atteint plus rapidement dans le cas de l'approche PDS que celui de l'approche GRIF. Nous avons vérifié numériquement que plus les valeurs de σ sont faibles, plus l'atteinte du régime stationnaire est lente.

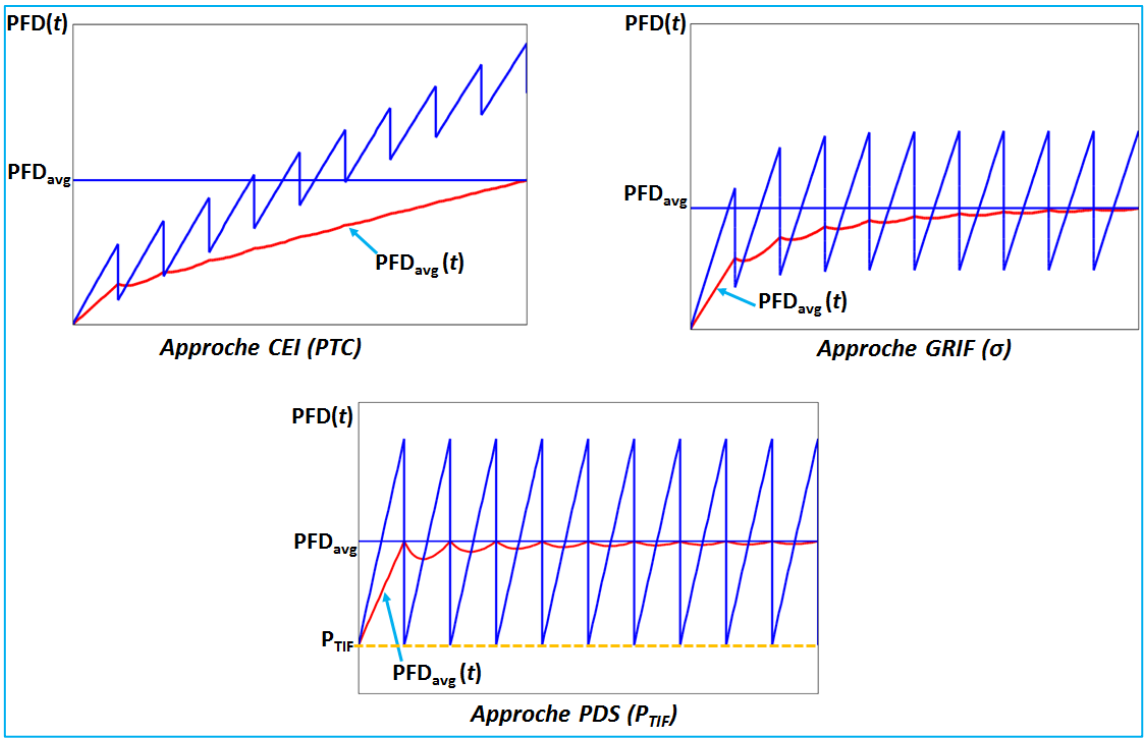

Figure 4.8 : Evolution de la PFD(t) et $PFD_{avg}(t)$ selon les approches CEI 61508, GRIF et PDS

4.5.2. Formulations relatives à la PFD_{avg} incluant l'imperfection des tests complets

Nous reportons dans ce qui suit les formules PFD_{avg} qui tiennent compte de la contribution de l'imperfection (ou l'efficacité) des tests périodiques complets. Ces formules ne sont pas nombreuses et n'incluent pas l'apport des tests partiels. Par ailleurs, les approches CEI 61508 et PDS ont été suivies pour l'établissement de ces formules.

4.5.2.1. Formule fournie dans la CEI 61508-6

Seule la formule correspondant à l'architecture 1oo2 est fournie dans la CEI 61508, voir équation (4.14). Bien entendu, le paramètre PTC est mis en œuvre. Selon la CEI 61508, les défaillances DU qui ne sont pas révélées par les tests périodiques complets (DU_{ND}) peuvent être mises en évidence par d'autres moyens tels qu'une sollicitation réelle sur la fonction de sécurité ou pendant la révision complète de l'équipement. Si les défaillances ne sont pas détectées via ces moyens, il convient de supposer qu'elles demeureront pendant toute la durée de vie de l'équipement.

$$PFD_{avg}^{1oo2} = 2\,[(1-\beta)\,\lambda_{DU} + (1-\beta_D)\,\lambda_{DD}]^2 \cdot T_{CE} \cdot T_{GE} + \beta_D\,\lambda_{DD} MTTR + \beta\,\lambda_{DU} \cdot PTC\left(\frac{T_1}{2} + MRT\right) + \beta\,\lambda_{DU} \cdot (1-PTC)\left(\frac{T_2}{2} + MRT\right) \quad (4.14)$$

Avec :

$$\begin{cases} T_{CE} = \dfrac{PTC\ \lambda_{DU}}{\lambda_D} \cdot \left(\dfrac{T_1}{2} + MRT\right) + \dfrac{(1-PTC)\,\lambda_{DU}}{\lambda_D} \cdot \left(\dfrac{T_2}{2} + MRT\right) + \dfrac{\lambda_{DD}}{\lambda_D} \cdot MTTR \\ T_{CG} = \dfrac{PTC\ \lambda_{DU}}{\lambda_D} \cdot \left(\dfrac{T_1}{3} + MRT\right) + \dfrac{(1-PTC)\,\lambda_{DU}}{\lambda_D} \cdot \left(\dfrac{T_2}{3} + MRT\right) + \dfrac{\lambda_{DD}}{\lambda_D} \cdot MTTR \\ T_2 : \text{durée moyenne entre sollicitations sur la fonction de sécurité.} \end{cases}$$

Un simple examen de cette formule nous permet de constater que les durées moyennes de réparation ainsi que les proportions de défaillances DCC relatives aux défaillances DU_{FT} et DU_{ND} sont égales : $MRT_{FT} = MRT_{ND} = MRT;\ \beta_{FT} = \beta_{ND} = \beta$. Notons que dans le cadre de ce travail doctoral, la durée T_2 peut également représente la durée de vie de l'équipent.

Une simple généralisation de la formule (4.14) peut être opérée. Nous proposons l'expression (4.15). Toutefois, au même titre de la relation (4.14), elle est formellement erronée.

$$PFD_{KooN}^{avg} = \frac{N!}{(K-1)!} \cdot [(1-\beta)\,\lambda_{DU} + (1-\beta_D)\,\lambda_{DD}]^{N-K+1} \cdot \prod_{i=1}^{N-K+1} MDT_{1ooi}$$

$$+ \beta_D\,\lambda_{DD} MTTR\ + \beta\,\lambda_{DU} \cdot PTC\left(\frac{T_1}{2} + MRT\right) + \beta\,\lambda_{DU} \cdot (1-PTC)\left(\frac{T_2}{2} + MRT\right) \quad (4.15)$$

Avec :

$$MDT_{1ooi} = \frac{PTC\ \lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{i+1} + MRT\right) + \frac{(1-PTC)\,\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_2}{i+1} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

4.5.2.2. Formules fournie dans le manuel PDS [Haugue et *al.*, 2013]

Ce document propose des formules fondées sur les concepts P_{TIF} et PTC séparément. Nous les donnons dans ce qui suit.

- ***Formules fondées sur le concept P_{TIF}*** : la contribution des défaillances indépendantes du test (TIF) pour les architectures *KooN* est donnée au tableau 4.3. Bien évidemment, les PFD_{avg} globaux doivent être calculées par l'ajout des autres contributions non dues aux TIF (formules CEI 61508, PDS…). Les valeurs de C_{KooN} sont celles données au tableau 3.4 (chapitre 3).

Tableau 4.3 : Contribution des défaillances TIF à la PFD_{avg} [Haugue et *al.*, 2013]

KooN	Formules
1oo1	P_{TIF}
1oo2	$\beta \cdot P_{TIF}$
KooN (k < N)	$C_{KooN} \cdot \beta \cdot P_{TIF}$
NooN	$N \cdot P_{TIF}$

- ***Formules fondées sur le concept PTC***: selon le manuel PDS, une alternative à l'approche précédente est l'usage du PTC introduit dans la CEI 61508. A ce titre, deux généralisations simplifiées des architectures *KooN* sont proposées. Elles sont les suivantes :

$$PFD_{KooN}^{avg} \approx \begin{cases} PTC\left(N \cdot \lambda_{DU} \cdot \frac{T_1}{2}\right) + (1 - PTC)\left(N \cdot \lambda_{DU} \cdot \frac{T_2}{2}\right) & K = N \\ PTC\left(C_{KooN} \cdot \beta \cdot \lambda_{DU} \cdot \frac{T_1}{2}\right) + (1 - PTC)\left(C_{KooN} \cdot \beta \cdot \lambda_{DU} \cdot \frac{T_2}{2}\right), & K \neq N \end{cases} \quad (4.16)$$

Pour le cas $K \neq N$, seules les défaillances DCC sont tenues en compte dans la PFD_{avg}. Afin d'améliorer la formulation (4.16), les auteurs du manuel PDS propose deux formules étendues pour les architectures 1oo2 et 2oo3, en considérant différentes combinaisons de défaillances (voir équations (4.17) et (4.18)). Pour une redondance élevée, la dernière formule de l'équation (4.16) est largement suffisante.

$$PFD_{1oo2}^{avg} = \beta\lambda_{DU} \cdot PTC \cdot \frac{T_1}{2} + \beta\lambda_{DU} \cdot (1 - PTC) \cdot \frac{T_2}{2} + \frac{(PTC \cdot \lambda_{DU} \cdot T_1)^2}{3} + \frac{\left((1-PTC) \cdot \lambda_{DU} \cdot T_2\right)^2}{3} + 2 \cdot \left((1 - PTC)\lambda_{DU} \cdot \frac{T_2}{2}\right) \cdot \left(PTC \cdot \lambda_{DU} \cdot \frac{T_1}{2}\right) \quad (4.17)$$

$$PFD_{2oo3}^{avg} = 2 \cdot \beta\lambda_{DU} \cdot PTC \cdot \frac{T_1}{2} + 2 \cdot \beta\lambda_{DU} \cdot (1 - PTC) \cdot \frac{T_2}{2} + (PTC \cdot \lambda_{DU} \cdot T_1)^2 + \left((1 - PTC) \cdot \lambda_{DU} \cdot T_2\right)^2 + 3 \cdot \left((1 - PTC)\lambda_{DU} \cdot \frac{T_2}{2}\right) \cdot \left(PTC \cdot \beta\lambda_{DU} \cdot \frac{T_1}{2}\right) \quad (4.18)$$

Les différentes durées de réparation ne sont pas considérées. Aussi, dans les défaillances indépendantes le facteur β (le même pour les défaillances DU_{FT} et DU_{ND}) est négligé devant le 1 : $(1 - \beta) \approx 1$. Toutes ces inconvénients peuvent être très facilement corrigés dans les formules précédentes. En outre, la contribution des défaillances DD peut également être considérée telle que définie dans le manuelle PDS.

4.5.3. Nouvelle proposition de formule PFD_{avg} incluant les tests partiels et l'imperfection des tests complets

Dans l'ensemble des formules mentionnées dans le cadre des tests périodiques complets imparfaits, aucune d'elles combine les tests partiels et l'imperfection dans les tests complets. Pour y remédier, nous proposons dans ce qui suit une expression générique inédite permettant l'estimation de la PFD_{avg} des architectures *KooN*. Pour ce faire, nous assumons que les durées de réparations des défaillances DU_{PT}, DU_{FT} et DU_{ND} sont négligeables devant leurs intervalles de tests respectives. Par ailleurs, seules les approches fournies dans des documents reconnus sont exploitées, en l'occurrence l'approche CEI 61508 (PTC) et l'approche PDS (P_{TIF}).

En mettant à profit une approche similaire à celle utilisée dans la référence [Chebila et Innal, 2015], nous avons réalisé les développements suivants.

4.5.3.1. Formulation de la $PFD(t)$

L'indisponibilité instantanée d'une architecture *KooN* imputables aux défaillances indépendantes peut être calculée en utilisant la loi binomiale :

$$PFD_{KooN}^{ind}(t) = \sum_{i=N-K+1}^{N} \binom{N}{i} [q_{ind}(t)]^i . [1 - q_{ind}(t)]^{N-i} \quad (4.19)$$

Où $q_{ind}(t)$ représente l'indisponibilité instantanée d'un seul canal.

La contribution des défaillances de causes commune (DCC) est donnée par la simple relation suivante :

$$PFD_{KooN}^{DCC}(t) = q_{DCC}(t) \quad (4.20)$$

L'indisponibilité globale est donc :

$$PFD_{KooN}(t) = PFD_{KooN}^{ind}(t) + PFD_{KooN}^{DCC}(t) - PFD_{KooN}^{ind}(t) \cdot PFD_{KooN}^{DCC}(t) \quad (4.21)$$

Comme nous l'avons d'ores et déjà mentionné, plusieurs contributions forment les quantités $q_{ind}(t)$ et $q_{DCC}(t)$. Plus précisément, les défaillances DD, DU_{PT}, DU_{FT}, DU_{ND} et TIF sont retenues dans le cadre de cette étude. Ces défaillances sont supposées indépendantes les unes des autres. Nous pouvons désormais écrire :

$$q(t) = pr(DD \cup DU_{PT} \cup DU_{FT} \cup DU_{ND} \cup TIF) \quad (4.22)$$

$q(t)$ peut être $q_{ind}(t)$ ou $q_{DCC}(t)$. Par disjonction des événements précédents, nous obtenons :

$$q(t) = pr(DD) + pr(DU_{PT}) \cdot pr(\overline{DD}) + pr(DU_{FT}) \cdot pr(\overline{DU_{PT}}) \cdot pr(\overline{DD}) + pr(DU_{ND}) \cdot pr(\overline{DU_{FT}}) \cdot pr(\overline{DU_{PT}}) \cdot pr(\overline{DD}) + pr(TIF) \cdot pr(\overline{DU_{ND}}) \cdot pr(\overline{DU_{FT}}) \cdot pr(\overline{DU_{PT}}) \quad (4.23)$$

Où $\bar{X}$ représente le complément de l'événement X : $pr(\bar{X}) = 1 - pr(X)$.

Les lois de défaillances associées aux différents événements sont données ci-après. Il est important de signaler que dans les formules suivantes il convient d'utiliser les taux de défaillances indépendantes dans $q_{ind}(t)$ et de causes commune dans $q_{DCC}(t)$. Cette remarque reste valide pour les probabilités dues aux TIF.

- ***Défaillances DD*** : défaillances détectée immédiatement après leur apparition et ensuite réparées selon un taux constant μ =1/MTTR. La probabilité de défaillance correspondante est très connue :

$$pr(DD) = q_{DD}(t) = \frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}} \cdot \left[1 - e^{-(\lambda_{DD}+\mu_{DD})\cdot t}\right] \quad (4.24)$$

- ***Défaillances DU_{PT}*** : défaillances détectée lors des tests partiels et instantanément réparées (MRT_{PT} = 0). La durée des tests est également considérée comme nulle. La contribution de ces défaillances à la probabilité de défaillance du canal est donnée par la relation (4.25) :

$$pr(DU_{PT}) = q_{PT}(t) = 1 - e^{-\lambda_{PT}\cdot\left[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\right]} \quad (4.25)$$

Où $Int(x)$ donne la partie entière de x.

- ***Défaillances DU_{FT}*** : défaillances détectée lors des tests complets et instantanément réparées (MRT = 0). Encore une fois, la durée des tests négligée. La probabilité correspondante est donnée par la relation (4.26) :

$$pr(DU_{FT}) = q_{FT}(t) = 1 - e^{-\lambda_{FT}\cdot\left[t - Int\left(\frac{t}{T_1}\right).T_1\right]} \quad (4.26)$$

- ***Défaillances DU_{ND}*** : défaillances non détectables par les tests partiels et complets. Seule une révision complète du canal pourrait les mettre en lumière. Par conséquent, elles sont modélisées via une loi exponentielle :

$$pr(DU_{ND}) = q_{ND}(t) = 1 - e^{-\lambda_{ND}\cdot t} \quad (4.27)$$

- ***Défaillances TIF*** : défaillances non détectables par les tests partiels et complets. Comme indiqué précédemment, elles sont caractérisées par une probabilité constante :

$$pr(TIF) = q_{TIF}(t) = P_{TIF} \quad (4.28)$$

L'insertion des formules (4.24) jusqu'à (4.27) dans celle donnée par l'équation (4.23) permet de calculer la *PFD*(*t*) exacte d'une architecture *KooN* donnée via l'équation (4.21), compte tenu des hypothèses annoncées.

4.5.3.2. Formulation de la PFD_{avg}

Une estimation directe de PFD_{avg} peut simplement être obtenue numériquement en calculant la *PFD*(*t*) pour suffisamment d'instants *t* et d'en calculer ensuite la moyenne arithmétique. La période d'observation est prise égale à [0, T_2] :

$$PFD_{avg}^{KooN}(0, T_2) = \frac{\Delta t}{T_2} \cdot \sum_{t=0:\,\Delta t:\,T_2} PFD_{KooN}(t) \quad (4.29)$$

Où Δt représente le pas de calcul tel que le nombre des évaluations = $\frac{T_2}{\Delta t}$. L'idéal est de prendre $\Delta t = 1$.

Du fait que les formules simplifiées sont toujours privilégiées par les analystes, nous proposons dans ce qui suit une formule générique inédite permettant d'estimer d'une manière approchée la PFD_{avg} des architectures *KooN*.

Si $pr(X)$ est très faible, ce qui est généralement le cas dans le cadre des SIS, alors : $pr(\bar{X}) = 1 - pr(X) \approx 1$. Par voie de conséquence, l'équation (4.21) se simplifie comme suit :

$$PFD_{KooN}(t) \approx PFD_{KooN}^{ind}(t) + PFD_{KooN}^{DCC}(t) \approx \binom{N}{N-K+1}[q_{ind}(t)]^{N-K+1} + q_{DCC}(t) \quad (4.30)$$

Avec :

$$q(t) \approx q_{DD}(t) + q_{PT}(t) + q_{FT}(t) + q_{ND}(t) + P_{TIF} \quad (4.31)$$

Par ailleurs, comme les taux de défaillances sont faibles, $q_{DD}(t)$ atteint rapidement le régime stationnaire et $\lambda \cdot t \ll 1$. Dans ces conditions, nous pouvons écrire :

$$\begin{cases} q_{DD}(t) \approx q_{DD}(\infty) = \frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}} \approx \lambda_{DD} \cdot MTTR \\ q_{PT}(t) = \lambda_{PT}.\left[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\right] \\ q_{FT}(t) = \lambda_{FT}.\left[t - Int\left(\frac{t}{T_1}\right).T_1\right] \\ q_{ND}(t) = \lambda_{ND}.t \end{cases} \quad (4.32)$$

Cela dit, l'équation (4.30) peut être mise sous la forme suivante :

$$PFD_{KooN}(t) \approx \binom{N}{N-K+1} \cdot \Big((1-\beta_D)\lambda_{DD} \cdot MTTR + (1-\beta_{TIF})P_{TIF} + (1-\beta_{PT})\lambda_{PT}.\Big[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\Big] + (1-\beta_{FT})\lambda_{FT}.\left[t - Int\left(\frac{t}{T_1}\right).T_1\right] + (1-\beta_{ND})\lambda_{ND}.t\Big)^{N-K+1} + \beta_D\,\lambda_{DD} \cdot MTTR + \beta_{TIF}P_{TIF} + \beta_{PT}\,\lambda_{PT}.\left[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\right] + \beta_{FT}\,\lambda_{FT}.\left[t - Int\left(\frac{t}{T_1}\right).T_1\right] + \beta_{ND}\,\lambda_{ND}.t \quad (4.33)$$

La moyenne de cette quantité sur la période [0, T_2] peut être calculée d'une manière précise selon l'équation (4.29). Dans le but de dériver une formule générique simplifiée, nous procédant ainsi :

$$PFD_{avg}^{KooN} = \frac{1}{T_2} \cdot \int_0^{T_2} PFD_{KooN}(t)\,\mathrm{d}t$$

$$\approx \frac{\binom{N}{N-K+1}}{T_2} \int_0^{T_2} \Big((1-\beta_D)\lambda_{DD} \cdot MTTR + (1-\beta_{TIF})P_{TIF} + (1-\beta_{PT})\lambda_{PT}.\Big[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\Big] + (1-\beta_{FT})\lambda_{FT}.\left[t - Int\left(\frac{t}{T_1}\right).T_1\right] + (1-\beta_{ND})\lambda_{ND}.t\Big)^{N-K+1}\,\mathrm{d}t + \frac{1}{T_2}\int_0^{T_2}\Big(\beta_D\,\lambda_{DD} \cdot MTTR + \beta_{TIF} \cdot P_{TIF} + \beta_{PT}\,\lambda_{PT}.\Big[t - Int\left(\frac{t}{T_{PT}}\right).T_{PT}\Big] + \beta_{FT}\,\lambda_{FT}.\Big[t - Int\left(\frac{t}{T_1}\right).T_1\Big] + \beta_{ND}\,\lambda_{ND}.t\Big)\,\mathrm{d}t \quad (4.34)$$

Le second intégral correspond à la contribution des DCC. Il en résulte la somme suivante :

$$PFD_{avg(DCC)}^{KooN} = \beta_D\,\lambda_{DD} \cdot MTTR + \beta_{TIF}\,P_{TIF} + \beta_{PT}\,\lambda_{PT}\frac{T_{PT}}{2} + \beta_{FT}\,\lambda_{FT}\frac{T_1}{2} + \beta_{ND}\,\lambda_{ND}\frac{T_2}{2} \quad (4.35)$$

Cette contribution peut être améliorée par l'ajout des temps de réparations respectifs aux défaillances DU_{PT} et DU_{FT} :

$$PFD_{avg(DCC)}^{KooN} = \beta_D\,\lambda_{DD}\cdot MTTR + \beta_{TIF}\,P_{TIF} + \beta_{PT}\,\lambda_{PT}\left(\frac{T_{PT}}{2} + MRT_{PT}\right) + \beta_{FT}\,\lambda_{FT}\left(\frac{T_1}{2} + MRT\right) + \beta_{ND}\,\lambda_{ND}\,\frac{T_2}{2} \quad (4.36)$$

Le premier intégral correspond aux défaillances indépendantes. Son calcul nécessite un peu d'aménagement pour se passer de la fonction *Int*(). En effet, si l'on suppose que les tests périodiques complets sont uniformément distribués sur la durée T_2 : $T_2 = n\cdot T_1 = n\cdot(m\cdot T_{PT})$, cet intégral peut être réécrit autrement en réinitialisant les *t* aux moments des tests (voir figure 4.9 et la relation (4.37)).

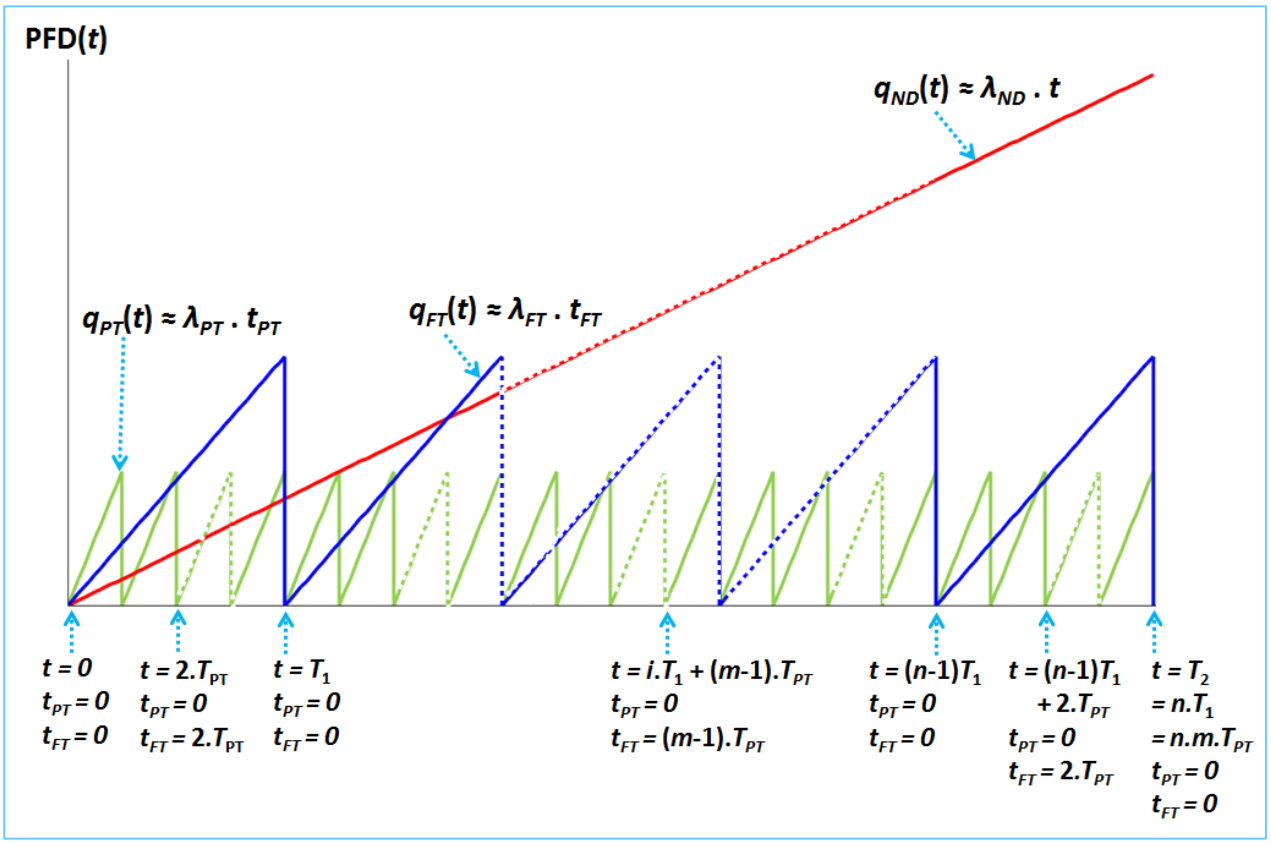

Figure 4.9 : Evolution de $q_{PT}(t)$, $q_{FT}(t)$ et $q_{ND}(t)$ en fonction du temps

$$PFD_{avg(ind)}^{KooN} = \frac{\binom{N}{N-K+1}}{n\cdot m\cdot T_{PT}}\cdot\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(\int_0^{T_{PT}}\left(\left(1-\beta_D\right)\lambda_{DD}\cdot MTTR + \left(1-\beta_{TIF}\right)P_{TIF} + \left(1-\beta_{PT}\right)\lambda_{PT}.t + \left(1-\beta_{FT}\right)\lambda_{FT}.(t+j\cdot T_{PT}) + \left(1-\beta_{ND}\right)\lambda_{ND}.(t+j\cdot T_{PT}+i\cdot m\cdot T_{PT})\right)^{N-K+1}\mathrm{d}t\right)$$

$$= \frac{\binom{N}{N-K+1}}{n \cdot m \cdot T_{PT}} \cdot \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left(\int_0^{T_{PT}} \left\{ \left(1-\beta_D\right)\lambda_{DD} \cdot MTTR + \left(1-\beta_{TIF}\right) P_{TIF} + \lambda_{DU}^{ind} \cdot t + \left(\left(1-\beta_{FT}\right)\lambda_{FT} + \left(1-\beta_{ND}\right)\lambda_{ND} \right) \cdot j \cdot T_{PT} + \left(1-\beta_{ND}\right)\lambda_{ND} \cdot i \cdot m \cdot T_{PT} \right\}^{N-K+1} \mathrm{d}t \right) \quad (4.37)$$

Avec :

$$\lambda_{DU}^{ind} = (1-\beta_{PT})\lambda_{PT} + (1-\beta_{FT})\lambda_{FT} + (1-\beta_{ND})\lambda_{ND}$$

La solution de cet intégral nous permet d'obtenir l'approximation suivante :

$$PFD_{avg(ind)}^{KooN} \approx \frac{\binom{N}{N-K+1}}{n \cdot m \cdot T_{PT} \cdot \lambda_{DU}^{ind} \cdot (N-K+2)} \cdot \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left(\left\{ \left(1-\beta_D\right)\lambda_{DD} \cdot MTTR + \left(1-\beta_{TIF}\right) P_{TIF} + \left(\lambda_{DU}^{ind} + \left(\left(1-\beta_{FT}\right)\lambda_{FT} + \left(1-\beta_{ND}\right)\lambda_{ND} \right) \cdot j + \left(1-\beta_{ND}\right)\lambda_{ND} \cdot i \cdot m \right) \cdot T_{PT} \right\}^{N-K+2} - \left\{ \left(1-\beta_D\right)\lambda_{DD} \cdot MTTR + \left(1-\beta_{TIF}\right) P_{TIF} + \left(\left(\left(1-\beta_{FT}\right)\lambda_{FT} + \left(1-\beta_{ND}\right)\lambda_{ND} \right) \cdot j + \left(1-\beta_{ND}\right)\lambda_{ND} \cdot i \cdot m \right) \cdot T_{PT} \right\}^{N-K+2} \right) \quad (4.38)$$

Finalement, la formule donnant la PFD_{avg} globale s'obtient en sommant les quantités fournies par les relations (4.38) et (4.36) :

$$PFD_{avg}^{KooN} \approx \frac{\binom{N}{N-K+1}}{n \cdot m \cdot T_{PT} \cdot \lambda_{DU}^{ind} \cdot (N-K+2)} \cdot \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \left(\left\{ (1-\beta_D)\lambda_{DD} \cdot MTTR + (1-\beta_{TIF}) P_{TIF} + \left(\lambda_{DU}^{ind} + \left((1-\beta_{FT})\lambda_{FT} + (1-\beta_{ND})\lambda_{ND} \right) \cdot j + (1-\beta_{ND})\lambda_{ND} \cdot i \cdot m \right) \cdot T_{PT} \right\}^{N-K+2} - \left\{ (1-\beta_D)\lambda_{DD} \cdot MTTR + (1-\beta_{TIF}) P_{TIF} + \left(\left((1-\beta_{FT})\lambda_{FT} + (1-\beta_{ND})\lambda_{ND} \right) \cdot j + (1-\beta_{ND})\lambda_{ND} \cdot i \cdot m \right) \cdot T_{PT} \right\}^{N-K+2} \right) + \beta_D \lambda_{DD} \cdot MTTR + \beta_{TIF} P_{TIF} + \beta_{PT} \lambda_{PT} \left(\frac{T_{PT}}{2} + MRT_{PT} \right) + \beta_{FT} \lambda_{FT} \left(\frac{T_1}{2} + MRT \right) + \beta_{ND} \lambda_{ND} \frac{T_2}{2} \quad (4.39)$$

4.6. Modélisation holistique

Une manière plus directe d'obtenir la PFD_{avg} d'une architecture *KooN* usuelle est de recourir aux modèles de sûreté de fonctionnement tels que l'arbre des défaillances (AdD), les chaines de Markov et les réseaux de Petri. Cette dernière option n'est pas investie dans la suite de ce chapitre. Par ailleurs, du fait de l'inconvénient majeurs des chaines de Markov qui est l'explosion combinatoire des états, il est n'est pas pratique, car très difficile, de développer des modèles markoviens pour les architectures possédant une redondance élevée. Cela dit, l'usage de cette approche dans ce qui suit est partiel. En effet, il consiste dans la modélisation des comportements individuels relative à certains modes de défaillances du même composant (canal). L'intégration des modèles markoviens développés au sein de l'AdD construit fournit permet un outil de calcul puisant : AdD basé sur les chaines de Markov. Ce type d'approche est disponible dans le logiciel GRIF.

Le formalisme des AdD présente une alternative intéressante aux formules simplifiées. Toutefois, sa mise en œuvre requiert la disponibilité et la maitrise d'outils logiciels dédiés. L'approche AdD permet facilement de tenir compte des différentes partitions de défaillances définies précédemment (voir figure 4.10). Cependant, le calcul de la PFD_{avg} nécessite la connaissance des probabilités instantanées attachées à ses différents événements de base. Si l'on considère les hypothèses précédentes relatives à la non considération des durées de réparations des défaillances DU, les lois données par les relations (4.24) jusqu'à (4.28) sont suffisante. A contrario, l'utilisateur de l'AdD se retrouve dépourvu car à ce jour il n'existe pas une loi spécifique dédiée aux composants testés périodiquement qui tient compte du taux de réparation et de l'efficacité du test σ. Cela concerne les événements DU_{PT} et DU_{FT} indépendantes et de causes communes. Il serait donc nécessaire de modéliser le comportement de chacun de ces modes de défaillances d'une manière convenable. Ceci peut être accompli à l'aide des chaines de Markov multi-phases, comme montré sur la figure 4.10. Notons que les chaines de Markov classiques relatives aux défaillances DD et DU_{ND} ne sont pas nécessaires du fait que les lois donnant leurs probabilités instantanées sont archiconnues (relations (4.24) et (4.27), respectivement). Pour les défaillances DU_{FT}, les probabilités des états au début de chaque nouvelle période entre tests $P(b_{i+1})$ sont calculées à partir de celles obtenues à la fin de la période précédente $P(e_i)$ comme suit (voir chapitre 2, équation (2.6)) :

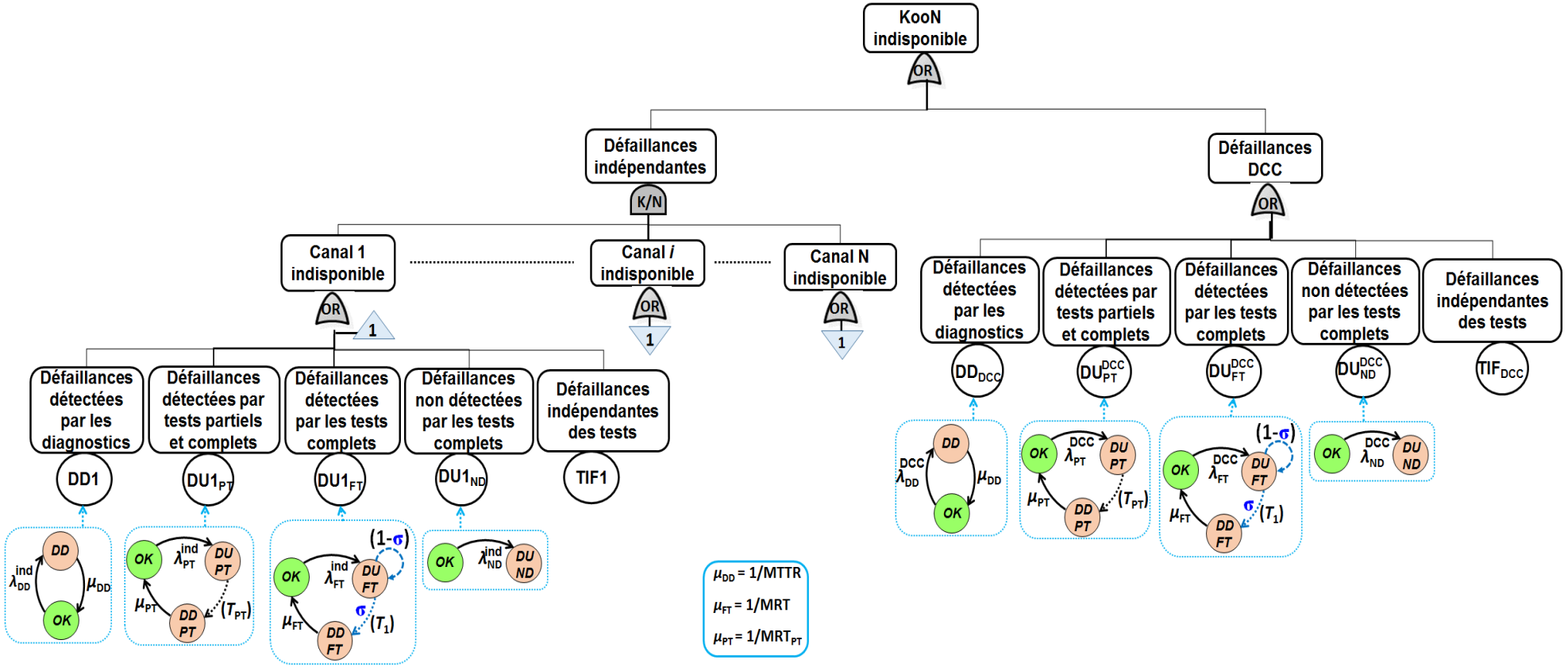

Figure 4.10 : AdD relatif à une architecture *KooN* incluant des chaines de Markov pour les événements de base de chaque canal

$$\begin{bmatrix} P_{(OK)}(b_{i+1}) \\ P_{(DU)}(b_{i+1}) \\ P_{(DD)}(b_{i+1}) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & (1-\sigma) \\ 0 & 1 & \sigma \end{bmatrix} \begin{bmatrix} P_{(OK)}(e_i) \\ P_{(DU)}(e_i) \\ P_{(DD)}(e_i) \end{bmatrix} \Rightarrow \begin{cases} P_{(OK)}(b_{i+1}) = P_{(OK)}(e_i) \\ P_{(DU)}(b_{i+1}) = (1-\sigma) \cdot P_{(DU)}(e_i) \\ P_{(DD)}(b_{i+1}) = P_{(DD)}(e_i) + \sigma \cdot P_{(DU)}(e_i) \end{cases} \quad (4.40)$$

L'équation (4.40) permet de considérer les approches CEI 61508 et GRIF dans le traitement de l'imperfection des tests périodiques complets. Cette considération peut être conjointe ou séparée. En effet, si l'approche CEI est CEI 61508, il suffit de mettre σ =1. Dans le cas contraire (adoption de l'approche GRIF), où une valeur spécifique (entre 0 et 1) est attribuée à σ, il suffit de mettre PTC =1 : $\lambda_{FT} = PTC \cdot \lambda_{DU} = \lambda_{DU}$; $\lambda_{ND} = (1 - PTC) \cdot \lambda_{DU} = 0$. Pour considerer les deux approches simultanément, il suffit d'attribuer aux PTC et σ des valeurs différentes de 0 et 1. Par ailleurs, dans le cas des tests partiels (défaillances DU_{PT}), σ est prise égale à 1.

L'écriture de l'équation (4.40) sous le logiciel GRIF est donnée à la figure suivante. Les états 1, 2 et 3 (figure 4.11) correspondent respectivement aux états *OK*, *DU* et *DD* (équation (4.40)).

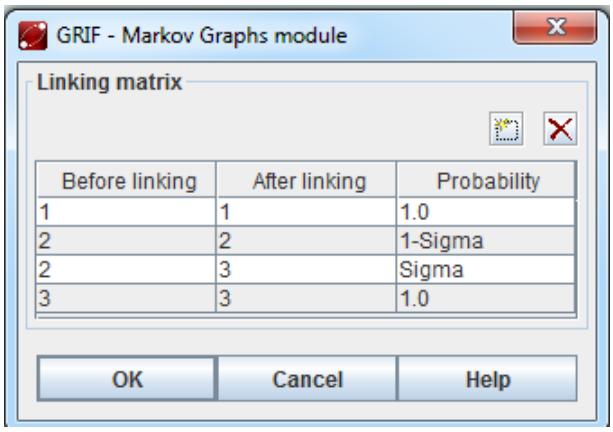

Figure 4.11 : Ecriture de la matrice d'enchainement dans le logiciel GRIF

Une autre manière d'intégrer les chaines de Markov à l'AdD est l'élaboration d'un modèle markovien multi-phases pour un canal entier incluant l'ensemble des modes de défaillances, à l'exception des défaillances TIF (probabilité constante). Cette façon de faire permet de réduire la taille de l'AdD final. Le modèle AdD correspondant est présenté à la figure 4.12.

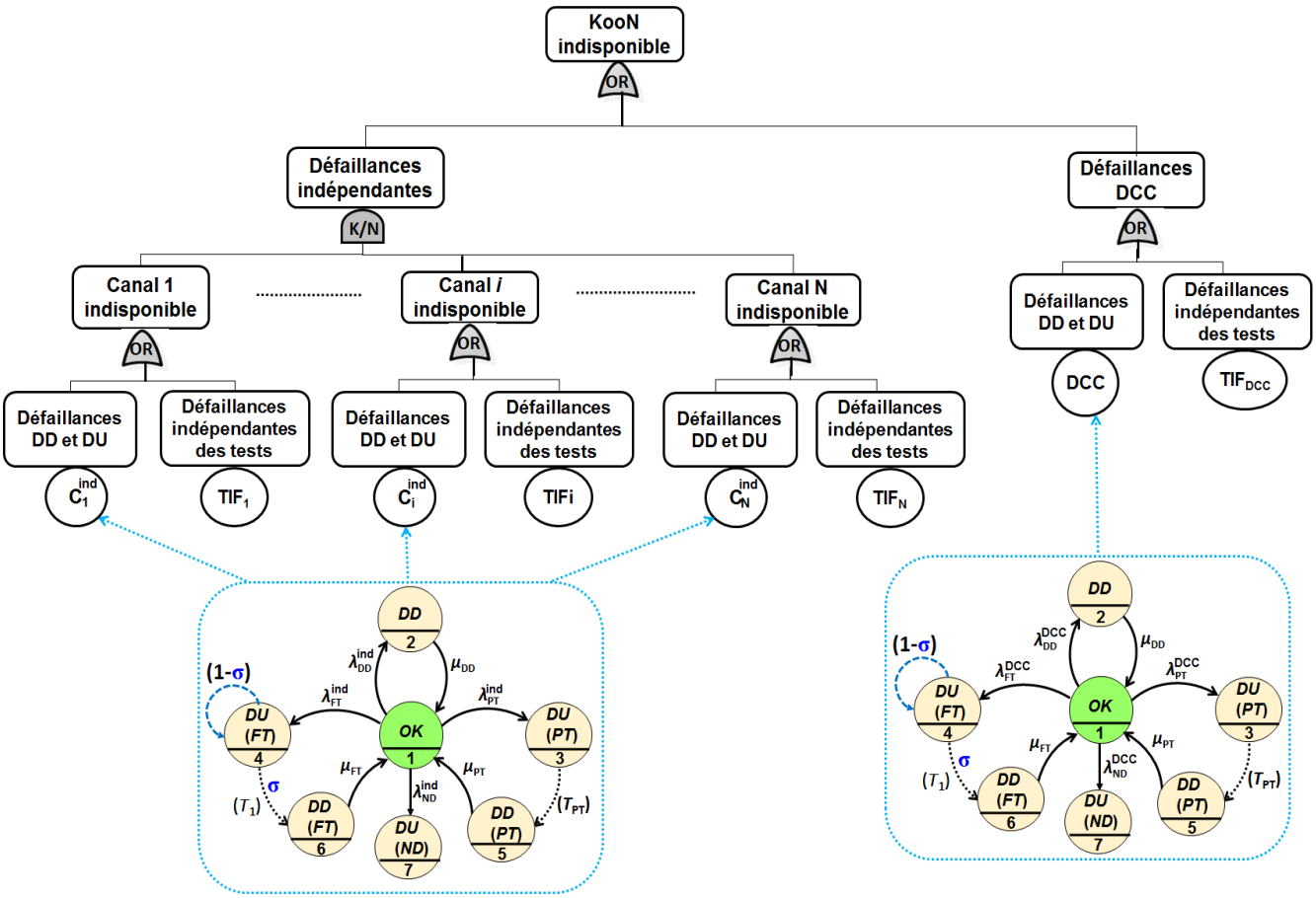

Figure 4.12 : AdD relatif à une architecture *KooN* incluant des chaines de Markov d'un canal entier (sauf TIF)

Néanmoins, le calcul de la $PFD(t)$ avec cette option est compliqué comparé à l'option précédente. Ceci est imputable à l'existence de deux périodes de tests différentes dans le même modèle markovien (T_1 et T_{PT}). Afin de s'affranchir de cet inconvénient, nous proposons la procédure suivante. Elle consiste à créer deux matrices d'enchainement relatives aux modèle markovien de la figure 4.12. Elles sont présentées sous format GRIF à la figure 4.13. Pour pouvoir enchainer les phases du modèle markovien en fonction de ces deux matrices, il est ensuite nécessaire de créer un autre tableau. La dimension de ce tableau change en fonction du nombre de périodes T_{PT} incluses dans l'intervalle T_1, c'est-à-dire, en fonction de m (voir tableau 4.4). Si l'on considère un canal testé partiellement chaque 3 mois (T_{PT} = 2190 h) et testé entièrement chaque an (T_1 = 8760 h), le tableau 4.4 devient celui représenté à la figure 4.14 (sous format GRIF).

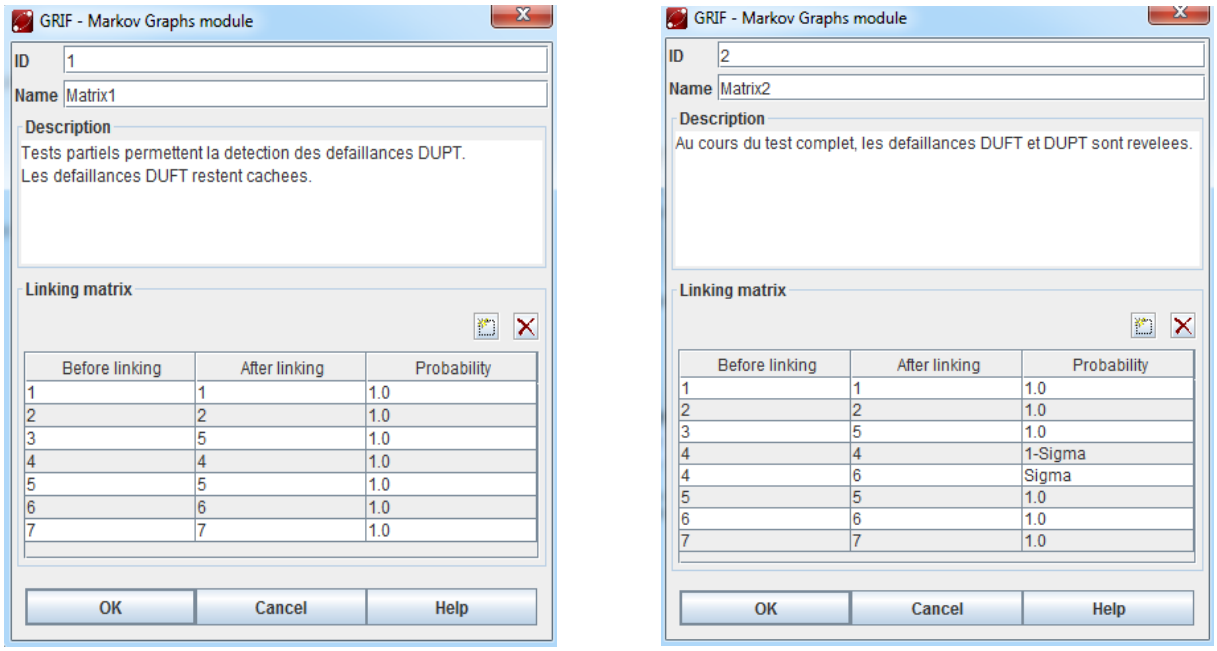

Figure 4.13 : Matrices d'enchainements : (Matrix1) détection des défaillances DU_{PT}, (Matrix2) détection des défaillances DU_{FT} et DU_{PT}.

Tableau 4.4 : Enchainement des phases du modèle markovien de la figure 4.12.

Phase N°	**Graph**	**Duration**	**Next phase**	**Linking Matrix**
1	Modele de Markov de la figure 4.12	T_{PT}	2	Matrix1
2	Modele de Markov de la figure 4.12	T_{PT}	3	Matrix1
...	...	...	...	...
m -1	Modele de Markov de la figure 4.12	T_{PT}	m	Matrix1
m	Modele de Markov de la figure 4.12	T_{PT}	1	Matrix2

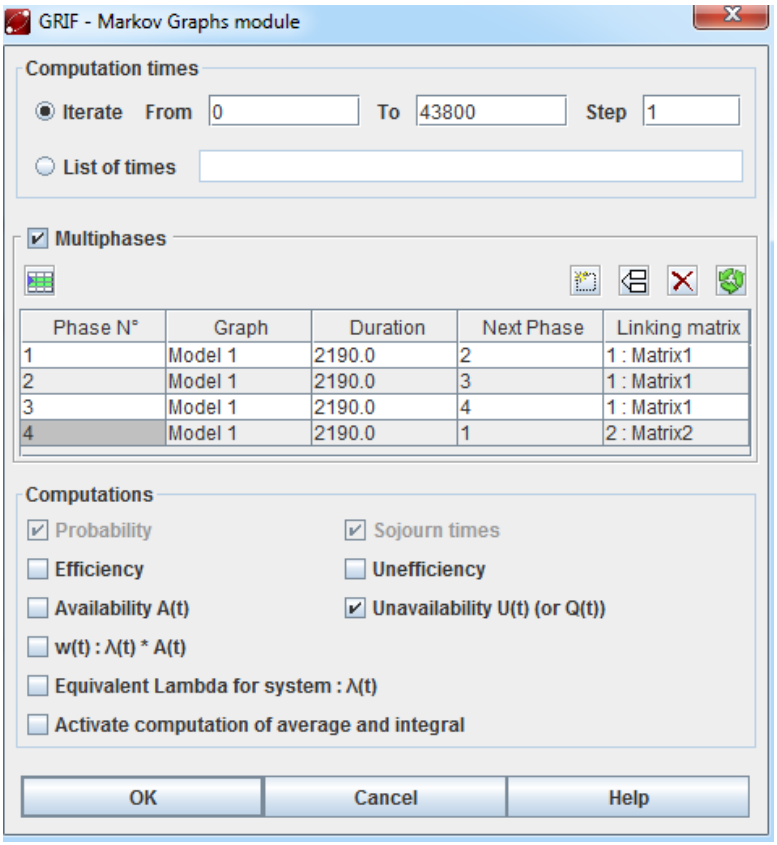

Figure 4.14 : Enchainement des phases pour m = 8760/2190 = 4.

4.7. Vérification numérique

Dans cette section, nous allons procéder à une comparaison des résultats de la PFD_{avg} de certaines architectures *KooN* fournies par la formule analytique simplifiée développée dans ce document (relation (4.39)) et par le modèle holistique proposé à la figure 4.10. Notons que les deux modèles holistiques proposés donnent les mêmes valeurs de la PFD_{avg}. Par ailleurs, l'équation (4.29) produit les mêmes résultats que ces deux modèles holistiques, si les durées de réparation des défaillances DU sont négligées. C'est ainsi que le deuxième modèle holistique et l'équation (4.29) ne sont pas retenus dans ce qui suit. Les résultats obtenus sont regroupés au tableau 4.5. Les données d'entrée utilisées sont les suivantes : λ_D = 1E–6/h ; DC = 0.6 ; θ = 0.6 ; PTC = {0.5 ; 0.7} ; σ = {0.5 ; 0.7}; P_{TIF} = 5E-3 ; $\beta_D = \beta_{PT} = \beta_{FT}$ = 0 ; $MTTR$ = 8 h ; MRT_{FT} = MRT_{PT} =0 ; T_1 = 17520 h ; T_2 = 87600 h. De plus, plusieurs intervalles de tests partiels ont été considérés : T_{PT} = {730 h ; 1460 h ; 2190 h ; 4380 h}. Notons que les approches de traitement de l'imperfection des tests complets ne sont pas considérées simultanément dans cette étude comparative. Avec l'approche CEI 61508 (PTC), la valeur 1 est affectée à σ. La réciproque est

vraie si l'approche GRIF (σ) est retenue. Rappelons que dans certaines situations réelles, à notre avis, les deux approches peuvent être prises conjointement.

Tableau 4.5 : Résultats PFD_{avg} avec prise en compte de l'imperfection des tests complets

KooN	***T_{PT}***	**Approches**					
		Eq. (4.39)		**AdD basé sur les chaines de Markov : Modèle 1 (Fig. 4.10)**			
		PTC		**PTC**		**σ**	
		0.7	**0.5**	**0.7**	**0.5**	**0.7**	**0.5**
1oo1	4380	8.614E-03	9.735E-03	8.588E-03	9.698E-03	7.771E-03	8.621E-03
	2190	8.351E-03	9.472E-03	8.328E-03	9.438E-03	7.511E-03	8.360E-03
	1460	8.264E-03	9.385E-03	8.241E-03	9.351E-03	7.424E-03	8.273E-03
	730	8.176E-03	9.297E-03	8.154E-03	9.264E-03	7.337E-03	8.186E-03
1oo2	4380	7.648E-05	9.957E-05	7.601E-05	9.876E-05	6.145E-05	7.607E-05
	2190	7.186E-05	9.436E-05	7.144E-05	9.363E-05	5.731E-05	7.149E-05
	1460	7.038E-05	9.268E-05	6.998E-05	9.197E-05	5.598E-05	7.001E-05
	730	6.892E-05	9.103E-05	6.853E-05	9.034E-05	5.468E-05	6.856E-05
1oo3	4380	6.982E-07	1.063E-06	6.914E-07	1.049E-06	4.939E-07	6.852E-07
	2190	6.356E-07	9.817E-07	6.298E-07	9.696E-07	4.438E-07	6.236E-07
	1460	6.162E-07	9.563E-07	6.107E-07	9.446E-07	4.284E-07	6.044E-07
	730	5.974E-07	9.316E-07	5.922E-07	9.204E-07	4.135E-07	5.859E-07
2oo2	4380	1.723E-02	1.947E-02	1.710E-02	1.930E-02	1.548E-02	1.716E-02
	2190	1.670E-02	1.894E-02	1.658E-02	1.878E-02	1.496E-02	1.665E-02
	1460	1.653E-02	1.877E-02	1.641E-02	1.861E-02	1.479E-02	1.648E-02
	730	1.635E-02	1.859E-02	1.624E-02	1.844E-02	1.462E-02	1.630E-02
2oo3	4380	2.295E-04	2.987E-04	2.266E-04	2.942E-04	1.834E-04	2.268E-04
	2190	2.156E-04	2.831E-04	2.131E-04	2.789E-04	1.710E-04	2.132E-04
	1460	2.111E-04	2.780E-04	2.087E-04	2.740E-04	1.671E-04	2.088E-04
	730	2.068E-04	2.731E-04	2.044E-04	2.692E-04	1.632E-04	2.045E-04

L'inspection de ce dernier tableau montre que, pour les mêmes valeurs de PTC et σ, l'approche CEI 61508 fondée sur l'usage du PTC donne des valeurs numériques pessimistes comparées à celles dérivée de l'approche basée sur l'efficacité du test σ. Par ailleurs, la formule que nous avons proposée produit des valeurs de PFD_{avg} très proches de celles obtenues via le modèle holistique de la figure 4.10. Un léger aspect conservatif est observé concernant la formule nouvellement développée. Ceci nous conduit à valider mutuellement cette formule et le modèle AdD proposé. Il convient également de signaler que la réduction de l'intervalle de test partiel ne permet pas une diminution manifeste de la PFD_{avg} pour le jeu de paramètres utilisé. A ce titre, la figure 4.15 présente l'évolution de PFD_{avg} de l'architecture 2oo3 en

fonction de la variation de T_{PT} (l'approche CEI 61508 est exploitée avec PTC = 0.7). Il est clair que la réduction de T_{PT} de 17520 *h* (T_1) jusqu'à 1 *h* ne réduit pas significativement cette PFD_{avg}. D'autres voies d'amélioration s'imposent alors. Nous nous investiguerons pas davantage ces voies car elles sortent du cadre de recherche de cette thèse.

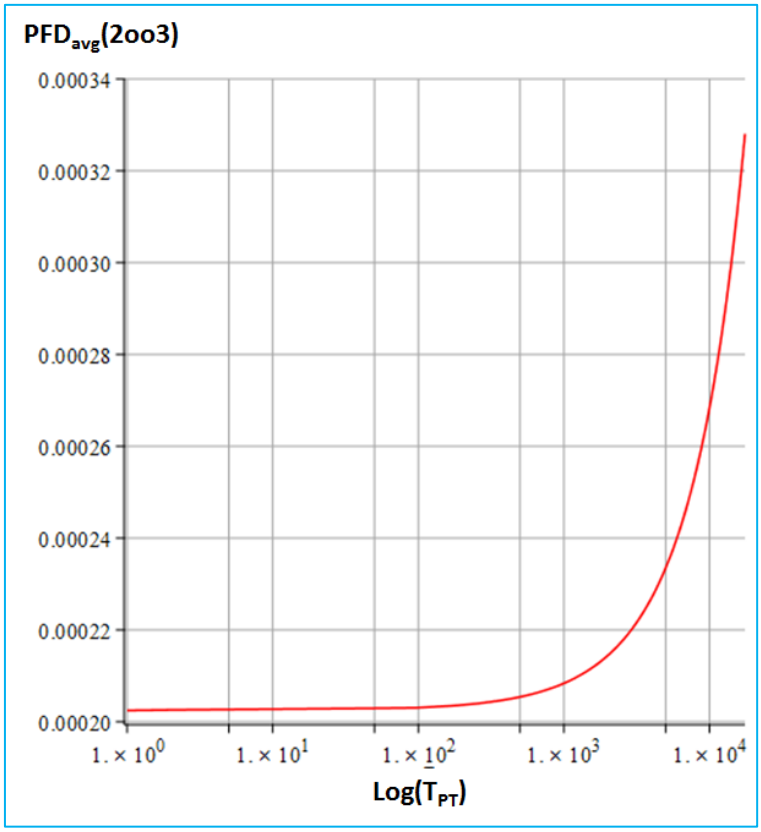

Figure 4.15 : Evolution de la PFD_{avg}^{2oo3} en fonction de T_{PT}.

4.8. Conclusion

Au cours de ce dernier chapitre, nous avons d'abord discuté les définitions relatives aux tests partiels et imparfaits. Puis, nous avons élaboré une nouvelle taxonomie des défaillances dangereuses lorsque ces tests existent simultanément. Ensuite, une revue de littérature des différentes formules mathématiques existantes liées à la PFD_{avg}, qui considèrent les tests partiels et/ou les tests imparfaits, a été conduite. A ce titre, si la prise en compte des tests partiels est largement étudiée, nous n'avions trouvé aucune formule qui considère en même temps les contributions des tests partiels et imparfaits. Il convient de noter que trois approches de traitement de l'imperfection des tests ont été remarquées et discutées : approche CEI (basée sur l'usage du facteur PTC), approche PDS (caractérisée par une probabilité constante P_{TIF}) et l'approche implémentée dans le logiciel GRIF (usage d'une probabilité σ caractérisant l'efficacité du test). Pour remédier à la non disponibilité de formules qui tiennent compte de l'imperfection des tests complets, nous avons proposé une expression inédite permettant de calculer la PFD_{avg} de n'importe quelle configuration *KooN*. Nous avons également proposé deux modèles holistiques équivalents fondés sur la combinaison des arbres de défaillances (AdD) et les chaines de Markov. Finalement, une comparaison des valeurs de PFD_{avg} obtenues via la modélisation holistique et la formule proposée a été effectuée. A cette occasion, nous avons pu constater que ces deux approches fournissent des résultats très proches les unes des autres, avec un léger aspect conservatif associé à la formule nouvellement développée. Ces conclusions nous ont permis de la valider.

Conclusion générale et perspectives

De nos jours, dans les installations industrielles qui utilisent des équipements et des activités sophistiqués ainsi que des substances hautement dangereuses, les systèmes instrumentés de sécurité (SIS) constituent une ligne défensive essentielle dans le processus de prévention de la survenue d'événements dangereux et la protection les cibles exposées (les êtres humains, l'environnement et biens).

Le rôle primordial des SIS a attiré notre attention pour les étudier ainsi que leurs indicateurs de performance.

Avant de résumer les résultats de notre travail, nous préférons rappeler ses objectifs brièvement.

Le premier objectif a consisté à mieux comprendre la démarche de la norme CEI 61508, cœur des SIS. Cette compréhension est l'étape clé conduisant à réaliser tous les objectifs.

Le second objectif est de vérifier la cohérence des formules relatives à la PFH fournies dans la CEI 61508 et d'en proposer de nouvelles formulations. L'usage courant de l'architecture 2oo3 nous a incités à l'investiguer davantage en considérant un éventail plus large de données de fiabilité exploitées.

Le troisième et dernier objectif de cette thèse de doctorat a consisté en une étude approfondie des formules relatives à la PFD_{avg} en prenant en compte la contribution des tests imparfaits et partiels. A cette occasion nous avons essayé de proposer une généralisation inédite de ces formules.

Pour tenter de satisfaire à ces trois objectifs, nous avons cherché en premier lieu, dans le chapitre 1, à délimiter clairement les contours de notre thématique de recherche. Pour cela, nous avons souligné tous les termes et les notions de base nécessaires à la compréhension de la norme CEI 61508. La démarche de la norme CEI 61508 a été également fournie en détail. Une étude de cas liée à un réservoir de stockage de butane a été présentée pour mieux illustrer cette démarche.

Avant d'étudier en détail les SIS, il nous a semblé utile d'en mieux connaître la classification des défaillances. Nous avons ainsi proposé, au chapitre 2, un nouvel éclairage et

une définition rigoureuse de la *PFH*. Nous avons également investigué dans ce chapitre les formules analytiques de la CEI 61508 relatives à cette mesure de performance. Nous nous sommes concentrés sur les architectures de base : 1oo1, 2oo2, 1oo2, 2oo3 et 1oo3. La vérification a été faite en utilisant les graphes de Markov.

Au chapitre 3, nous avons présenté une démarche, basée sur les réseaux de Petri des architectures connues. Cette nouvelle modélisation a permis de confirmer la validité des modèles markoviens donnés au deuxième chapitre. Nous avons réalisé une étude détaillée de la configuration 2oo3 qui a absolument confirmé les résultats précédents.

Dans le dernier chapitre, une revue de littérature des différentes formules mathématiques existantes liées à la PFD_{avg}, qui considèrent les tests partiels et/ou les tests imparfaits, a été conduite.

Ce travail, comme toute thèse, n'est pas exhaustif. Il existe d'autres sujets, dans le même contexte, à approfondir. Nous citons deux :

-Le premier est l'indisponibilité des formules traitant la stratégie de tests échelonnés. Les tests échelonnés consistent à tester plusieurs éléments selon un ordre chronologique donné et non en même temps.

-Le deuxième est en relation avec la mesure de fiabilité des SIS relative à l'arrêt du processus dû à ses activations intempestives : STR (Spurious Trip Rate). Une activation intempestive est l'activation de la fonction SIS sans aucune demande réelle du processus protégé, ce qui entraîne une perte de production et est donc économiquement préjudiciable. Il convient de noter que la norme CEI 61508 ne spécifie aucune exigence concernant les activations intempestives.

Finalement, nous espérons que cette contribution doctorale contient des informations importantes en monde industriel.

Bibliographie

Areal Locations of Hazardous Atmospheres (ALOHA) (2006), (U.S. Environmental Protection Agency (EPA)—National Oceanic and Atmospheric Administration (NOAA), téléchargeable sur le site: http://www2.epa.gov.

Birnbaum, Z. W. (1969), On the importance of different components and a multicomponent system. In Multivariable Analysis II. Academic Press, New-York, U.S.A.

Blume, H., Von Sydow, T., Becker, D. et Noll, T.G. (2007), "Application of deterministic and stochastic Petri-Nets for performance modeling of NoC architectures", Journal of Systems Architecture, Vol. 53 No. 8, pp. 466-476.

Brissaud, F., Barros, A. et Berenguer, C. (2012), "Probability of failure on demand of safety systems: impact of partial test distribution", Journal of Risk and Reliability, vol. 226 No. 4, pp. 426-436.

Bukowski, J. V. et Van Beurden, I. (2009), "Impact of proof test effectiveness on safety instrumented system performance", In Reliability and Maintainability Symposium-IEEE. RAMS 2009. Annual, pp. 157–163.

CCPS. (2001), Layer of protection analysis; simplified process assessment, center for chemical process safety of the American institute for chemical Engineers, New York, U.S.A.

CEI 31010. (2019), Management du risque — Techniques d'appréciation du risque.

CEI 61508. (2010), Functional Safety of Electrical/electronic/programmable Electronic Safety-Related Systems (Parties1–7, 2ème Edition), Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61508-2. (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61508-4. (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61508-7. (2010), Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures, Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61511. (2003), Functional Safety-Safety Instrumented Systems for the Process Industry Sector (Parties 1-3, 1ère Edition), janvier 2003-juillet 2003. Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61511. (2016), Functional Safety-Safety Instrumented Systems for the Process Industry Sector (Parties 1-3, 2ème edition), Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61511-1. (2016), Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements, Commission Electrotechnique Internationale, Genève, Suisse.

CEI 61511-2, (2016), Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1:2016, Commission Electrotechnique Internationale, Genève, Suisse.

CEI EN 50126-1. (2019), Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 1: Generic RAMS Process.

Čepin, M. (Janvier 2011), Assessment of Power System Reliability: Methods and Applications, Springer-Verlag Londres, Royaume-Uni.

Charpentier, P. (2002), Architecture d'automatisme en sécurité des machines : Etudes des conditions de conception liées aux défaillances du mode commun, Thèse de DOCTEUR de l'Institut Nationale Polytechnique de LORRAINE – Spécialité Automatique.

Chebila, M. et Innal, F. (2014), "Unification of Common Cause Failures' Parametric Models Using a Generic Markovian Model", Journal of Failure Analysis and Prevention, vol. 14 No. 3, pp.426–434.

Chebila, M. et Innal, F. (2015), "Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH", Journal of Loss Prevention in the Process Industries, vol. 34, pp. 167–176.

David, R. et Alla, H. (2010), Discrete, Continuous and Hybrid Petri Nets, 2nd ed., Springer Publishing Company, Berlin, Allemagne.

Dekkers, R. (2015), Applied System theory, Springer International Publishing, Suisse.

Dowell, A. M. (1998), "Layer of protection analysis for determining safety integrity level", ISA Transactions, Vol. 37, pp. 155-165.

Dutuit Y. et Rauzy A. (2005), "Approximate estimation of system reliability via fault trees". Reliability Engineering and System Safety, Vol. 87 No. 2, pp. 163-172.

Dutuit, Y., Innal, F., Rauzy, A. et Signoret, J.-P. (2008), "Probabilistic assessments in relationship,with safety integrity levels by using fault trees", Reliability Engineering and System Safety, Vol. 93 No. 12, pp. 1867-1876.

Flaus, J.M. (Octobre 2013), Analyse des risques des systèmes de production industriels et de services : Aspects technologiques et humains, Lavoisier, Paris, France.

Goble, W. M. (1998), The use and development of quantitative reliability and safety analysis in new product design, Thèse de doctorat, Eindhoven Université de Technologie, Les Pays-Bas.

GRIF, (2018) "Graphical interface for reliability forecasting software", téléchargeable sur le site: http://grif-workshop.fr/2018/05/nouvelle-version-grif-2018/.

GRIF, (2020)"Graphical interface for reliability forecasting software".

Gu, T. et Bahri, P.A. (2002), “A survey of Petri net applications in batch processes”, Computers in Industry, Vol. 47 No. 1, pp. 99-111.

Hauge, S. et Onshus, T. (2006), Reliability Data for Safety Instrumented Systems: PDS Data.

Hauge, S., Lundteigen, M.A., Hokstad, P. et Håbrekke, S. (2010), “Reliability Prediction Method for Safety Instrumented Systems”, PDS Method Handbook, SINTEF, Norvège.

Hokstad, P. et Rausand, M. (2008), Common cause failure modeling: status and trends, Handbook of performability engineering, Springer.

Hokstad, P. et Corneliussen, K. (2004), “Loss of safety assessment and the IEC 61508 standard”, Reliability Engineering and System Safety, Vol. 83 No. 1, pp. 111–120.

Hokstad, P., Maria, A. et Tomis, P. (2006), “Estimation of common cause factors from systems with different numbers of channels”, IEEE Transactions on Reliability, vol. 55 No. 1, pp. 18–25.

HSE. (2002), Principles for proof testing of safety instrumented systems in the chemical industry.

IEC 60050-192. (2015), International Electrotechnical Vocabulary (IEV) - Part 192: Dependability.

Innal, F. (2008), Contribution à la modélisation des systèmes instrumentés de sécurité et à l’évaluation de leurs performances : Analyse critique de la norme CEI 61508, Thèse de doctorat, Université de Bordeaux.

Innal, F., Cacheux, P.-J., Collas, S., Dutuit, Y., Folleau, C., Signoret, J.-P. et Thomas, P. (2014), “Probability and frequency calculations related to protection layers revisited”, Journal of Loss Prevention Process, Vol. 31, pp. 56-69.

Innal, F., Dutuit, Y. et Chebila, M. (2015), “Safety and operational integrity evaluation and design optimization of safety instrumented systems”, Reliability Engineering and System Safety, Vol. 134, pp. 32-50.

Innal, F., Lundteigen, M.A., Liu, Y. et Barros, A. (2016), “PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models”, Reliability Engineering and System Safety, Vol. 150, pp. 160-170.

ISA-TR84.00.03 (2002). Guidance for testing of process sector safety instrumented functions (SIF) implemented as or within safety instrumented systems (SIS).

ISO 26262 (2007), Functional safety - Engineering Workshop, Organisation internationale de normalisation (ISO).

ISO 31000, (2009), management du risque, Organisation internationale de normalisation (ISO).

ISO 45001 (2018), Systèmes de management de la santé et de la sécurité au travail — Exigences et lignes directrices pour leur utilisation, Organisation internationale de normalisation (ISO).

ISO/CEI Guide 51, (2014), Aspects liés à la sécurité — Principes directeurs pour les inclure dans les normes.

ISO/TR 12489, (2016), Pétrole, pétrochimie et gaz naturel. Modélisation et calcul fiabilistes des systèmes de sécurité.

Jin, H. et Rausand, M. (2014), "Reliability of safety-instrumented systems subject to partial testing and common-cause failures", Reliability Engineering and System Safety, Vol. 121, pp. 146-151.

Jin, H., Lundteigen, M.A. et Rausand M. (2013), "New PFH-formulas for k-out-of-n: F-systems", Reliability Engineering and System Safety, vol. 111 No. 0, pp. 112-118.

Kaplan, S. et Garrick, B.J. (1981), "On The Quantitative Definition of Risk", Risk Analysis Vol. 1 No. 1, pp.11-25.

Le Moigne, J. L. (1984), La théorie du système général – Théorie de la modélisation. PUF, Paris, France.

Lundteigen, M. et Rausand, M. (2007), "The effect of partial stroke testing on the reliability of safety valves", Vol. 3, pp. 2479–2486.

Lundteigen,M. et Rausand,M. (2008), "Partial stroke testing of process shutdown valves: How to determine the test coverage", Journal of Loss Prevention in the Process Industries, Vol. 21 No. 6, pp. 579–588.

Mechri, W., Simon, C., Bicking, F. et BenOthman, K. (2013), "Fuzzy Multiphase Markov Chains to Handle Uncertainties in Safety Systems Performance Assessment", Journal of Loss Prevention in the Process Industries, vol. 26, pp. 594–604.

MIL-STD-882E, (2012), Department of defense standard practice: system safety.

Nuis, W-J. (2005), Partial stroking on fast acting applications, In proceedings from the TÜV Rheinland group's symposium, 09 Juin, Cleveland, OH, U.S.A.

OHSAS 18001, (2007), Occupational Health and Safety Management Certification, British Standards Institute (BSI).

OLF (2004), Norwegian oil and gas association application of IEC 61508 and IEC 61511 in the norwegian petroleumindustry.

Oliveira, L. F. (2009), "PFD of higher-order configurations of sis with partial stroke testing capability", pp. 1919–1928.

Oliveira, L.F. et Abramovitch, R.N. (2010), "Extension of ISA TR84.00.02 PFD equations to KooN architectures", Reliability Engineering and System Safety, Vol. 95 No. 7, pp. 707-715.

Omeiri, H., Innal, F. et Hamaidi, B. (2015), "Safety Integrity Evaluation of a Butane Tank Overpressure Evacuation System According to IEC 61508 Standard", Journal of Failure Analysis and Prevention, vol.15, pp. 892–905.

OREDA (offshore Reliability Data) Handbook (2002), SINTEF, Trondheim, Norvège.

PDS Data Handbook (2010), Reliability Data for Safety Instrumented Systems, SINTEF, Trondheim, Norvège.

Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook, 2006 Edition. SINTEF, Trondheim, Norvège.

Rolén, H. (2007), Partial and imperfect testing of safety instrumented functions, Mémoire de master, NTNU, Norvège.

Sachdeva, A., Kumar, D. et Kumar, P. (2008), "Reliability analysis of pulping system using Petri nets", International Journal of Quality and Reliability Management, Vol. 25 No. 8, pp. 860-877.

Sklet, S. (2006), "Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries", Journal of Hazardous Materials, Vol. 19, pp. 494–506.

SOFREGAZ. (1995), Manuel opératoire-Unité GPL.

Son, K.S., Kim, D.H., Park, G.Y. et Kang, H.G. (2018), "Availability analysis of safety grade multiple redundant controller used in advanced nuclear safety systems", Annals of Nuclear Energy, Vol. 111, pp. 73-81.

Stamatelatos, M. et Dezfuli, S. (Decembre 2011), Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (2ème Edition), NASA Headquarters, Washington, DC.

Stavrianidis, P. et Bhimavarapu, K. (1998), "Safety instrumented functions and safety integrity levels (SIL)", ISA Transactions, Vol. 37 No. 4, pp. 337-351.

Summers, A. E. (1998), "Techniques for assigning a target safety integrity level", ISA Transactions, Vol. 37, pp. 95-104.

Summers, A. E. et Zachary, B. (2000), "Partial-stroke testing of safety block valves", Control Engineering, Vol. 47 No. 12, pp. 87–89.

Torres-Echeverria, A. C. (2009), Modelling and optimization of safety-instrumented systems based on dependability and cost measures. Verlag, Londres, Royaume-Uni.

Zio, E. (2013), The Monte Carlo Simulation Method for System Reliability and Risk Analysis, Springer- Verlag, Londres, Royaume-Uni.