Ministère de l'Enseignement Supérieur et de la Recherche Scientifique – Algérie
Université 20 Août 1955 – Skikda
Faculté de Technologie
Département de Génie des Procédés
Réf : D012126010D

Thèse

Présentée en vue de l'obtention du diplôme de

Doctorat – LMD

Modélisation avancée des performances probabilistes des systèmes instrumentés de sécurité

Option : Hygiène et Sécurité Industrielle

Réalisé par :

Nabil BOUDJOGHRA

Soutenue publiquement : Le 29/04/2026

Devant le jury :

Président	Pr. Youcef ZENNIR	Université du 20 Août 1955 – Skikda
Rapporteur de thèse	Pr. Fares INNAL	Université du 20 Août 1955 – Skikda
Examinateur	Dr. Malika KHELFAOUI	Université du 20 Août 1955 – Skikda
Examinateur	Dr. Amina BENAISSA	Université du 20 Août 1955 – Skikda
Examinateur	Pr. Hamid BENTARZI	Université du M'hamed Bougara – Boumerdès

Année universitaire : 2025/2026

Résumé

La sécurité industrielle vise à maintenir les risques industriels à un niveau tolérable en s'appuyant sur un processus de gestion structuré en trois étapes clés : (1) l'analyse des risques, (2) l'évaluation des risques et (3) la réduction des risques, chacune reposant sur des techniques spécifiques. La réduction des risques intervient lorsque certains risques sont jugés inacceptables à l'issue de l'évaluation. Elle s'appuie sur des barrières de sécurité dont la performance détermine leur capacité à atteindre le niveau de risque cible (risque tolérable). Cette thèse se concentre sur un type spécifique de barrières de sécurité : les Systèmes Instrumentés de Sécurité (SIS), en mettant l'accent sur leur performance probabiliste. La norme IEC 61508 propose une approche orientée performance, permettant de concevoir un SIS avec un niveau de sécurité (SIL atteint ou achevé) conforme aux exigences de sécurité requises (SIL requis). La détermination de la performance probabiliste de SIS peut être menée de plusieurs manières, notamment via des modèles mathématiques. Cependant, la capacité des modèles existants à couvrir tous les cas et leur précision restent incertaines, ce qui justifie une analyse approfondie. Dans ce contexte, nous développerons de nouvelles formules de PFH basées sur la loi binomiale, en supposant que le procédé surveillé s'arrête immédiatement après la détection d'une défaillance dangereuse du SIS. Par ailleurs, de nouvelles formules pour le PFD_{avg} seront établies en tenant compte de la stratégie de tests échelonnés.

Mots-clés : sécurité industrielle, sécurité fonctionnelle, gestion des risques industriels, systèmes instrumentés de sécurité (SIS), modélisation des PFD et PFH, loi binomiale, tests échelonnés.

Abstract

Industrial safety aims to maintain industrial risks at a tolerable level by relying on a management process structured in three key steps: (1) risk analysis, (2) risk assessment and (3) risk reduction, each based on specific techniques. Risk reduction occurs when certain risks are deemed unacceptable at the end of the assessment. It is based on safety barriers whose performance determines their ability to achieve the target risk level (tolerable risk). This thesis focuses on a specific type of safety barriers: Safety Instrumented Systems (SIS), with an emphasis on their probabilistic performance. The IEC 61508 standard proposes a performance-oriented approach, allowing to design a SIS with a safety level (SIL reached or completed) compliant with the required safety requirements (required SIL). The determination of the probabilistic performance of SIS can be carried out in several ways, in particular via mathematical models. However, the ability of the existing models to cover all cases and their accuracy remain uncertain, which warrants further analysis. In this context, we will develop new PFH formulas based on the binomial distribution, assuming that the monitored process stops immediately after the detection of a dangerous failure of the SIS. Furthermore, new formulas for the PFD_{avg} will be established, taking into account the staggered testing strategy.

Keywords: industrial risks, industrial safety, functional safety, industrial risk management, safety instrumented systems (SIS), PFD and PFH modeling, Binomial law, staggered test.

ملخص

تهدف السلامة الصناعية إلى الحفاظ على المخاطر الصناعية عند مستوى مقبول من خلال الاعتماد على عملية إدارة منظمة في ثلاث خطوات رئيسية: (1) تحليل المخاطر، (2) تقييم المخاطر و(3) الحد من المخاطر، كل منها يعتمد على تقنيات محددة. يحدث الحد من المخاطر عندما يتم اعتبار بعض المخاطر غير مقبولة في نهاية التقييم. ويستند ذلك إلى حواجز السلامة التي يحدد أداؤها قدرتها على تحقيق مستوى المخاطر المستهدف (المخاطر المقبولة). تركز هذه الأطروحة على نوع معين

من حواجز السلامة: أنظمة السلامة الآلية (SIS)، مع التركيز على أدائها الاحتمالي. يقترح معيار IEC 61508 نهجًا موجهًا نحو الأداء، مما يسمح بتصميم أنظمة السلامة الآلية بمستوى أمان (SIL المحقق أو المُنجز) متوافق مع متطلبات السلامة المطلوبة (SIL المطلوبة). يمكن إجراء تحديد الأداء الاحتمالي لأنظمة السلامة الآلية بعدة طرق، وخاصة من خلال النماذج الرياضية. ومع ذلك، تظل قدرة هذه النماذج الموجودة على تغطية جميع الحالات ودقتها غير مؤكدة، مما يستدعي المزيد من التحليل. في هذا السياق، سنطوّر صيغًا جديدة لـ PFH استنادًا إلى التوزيع الثنائي، بافتراض توقف العملية المُراقَبة فور اكتشاف أي عطل. علاوةً على ذلك، سيتم وضع صيغ جديدة لـ PFD_{avg} ، مع مراعاة استراتيجية الاختبارات المتدرجة.

الكلمات المفتاحية: السلامة الصناعية، السلامة الوظيفية، إدارة المخاطر الصناعية، أنظمة السلامة الآلية(SIS)، نمذجة PFD وPFH, قانون ذو الحدين، الاختبارات المتدرجة.

Remerciements

Alhamdulillah,

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce travail de thèse.

Tout d'abord, je remercie chaleureusement monsieur **INNAL Fares**, mon directeur de recherche, pour son encadrement précieux, sa disponibilité et ses conseils éclairés tout au long de ce parcours. Sa rigueur scientifique, son soutien constant et sa confiance en mes capacités ont été des moteurs essentiels pour mener à bien ce projet.

Je souhaite également remercier les membres du jury, [**Youcef ZENNIR, Malika KHELFAOUI, Amina BENAISSA, Hamid BENTARZI**], pour avoir accepté d'évaluer ce travail et pour leurs remarques constructives qui ont enrichi ma réflexion.

Bien que tous n'aient pas été cités ici, je garde une pensée reconnaissante pour celles et ceux qui, par leur présence discrète ou leurs conseils, ont contribué à l'aboutissement de cette aventure intellectuelle et humaine.

Dédicace

À mes parents,

Pour leur amour inconditionnel, leur soutien sans faille et leurs sacrifices silencieux qui ont rendu ce parcours possible.

À ma fiancée,

Pour sa patience infinie et son amour qui m'ont porté tout au long de ce parcours.

À mes amis,

Pour leurs mots réconfortants, leurs conseils et les moments partagés qui m'ont aidé à traverser ce parcours.

À tous ceux qui croient en moi,

Cette thèse est dédiée à vous.

Table des matières

Résumé ..... **I**

Remerciement ..... **III**

Abréviations, acronymes ..... **IV**

Liste des figures ..... **XI**

Liste des tableaux ..... **XIII**

Introduction générale **1**

Chapitre 1. La gestion des risques industriels et ses techniques

1.1. Introduction **4**

1.2. Risque et sécurité industrielle : concepts clés **4**

1.2.1. Risque industriel 4

1.2.2. Sécurité industrielle 5

1.2.2.1. Sécurité fonctionnelle 5

1.3. Processus de gestion des risques industriels et ses techniques **6**

1.3.1. Étapes du processus de gestion des risques 8

1.3.1.1. Analyse des risques 9

1.3.1.1.1. Analyse qualitative des risques 9

1.3.1.1.2. Analyse quantitative des risques 10

1.3.1.2. Évaluation des risques 11

1.3.1.3. Réduction des risques 12

1.3.1.3.1. Barrières de sécurité 12

1.3.1.3.1.1. Classification 12

1.3.1.3.1.2. Performance 14

1.3.1.3.1.3. Défense en profondeur 17

1.3.1.3.1.4. Système instrumenté de sécurité (SIS) 18

1.3.1.3.1.4.1. Fonction (SIF) 20

1.3.1.3.1.4.2. Performance (SIL) 20

1.3.2. Techniques utilisées à chaque étape du processus de gestion des risques 21

1.3.2.1. Techniques d'analyse des risques 22

1.3.2.1.1. HAZOP (Hazard and Operability Study) 22

1.3.2.1.2. LOPA (Layer of Protection Analysis) ……...23
1.3.2.1.3. ALOHA (Areal Locations of Hazardous Atmospheres) ……25
1.3.2.2. Techniques d'évaluation des risques ……..…26
1.3.2.2.1. ALARP (As Low As Reasonably Practicable) ……..…26
1.3.2.2.2. Matrice des risques ……....27
1.3.2.3. Techniques de réduction des risques ……28
1.3.2.3.1. Technique de la norme IEC 61508 ……..…28
1.3.2.3.1.1. Allocation de la performance requise du SIS (SIL requis) …….29
1.3.2.3.1.2. Détermination de la performance réelle du SIS (SIL réel) ……..29
1.3.2.3.1.3. Validation du SIS ……..…...29
1.3.2.3.1.4. Re-conception du SIS ……..……30
1.3.2.3.1.5. Maintien du SIS dans le temps ……..……..30
1.4. Conclusion ……...….30

Chapitre 2. Application industrielle : mise en œuvre du processus de gestion des risques industriels

2.1. Introduction ……..…32
2.2. Description de l'étude de cas : « Sphère de stockage de butane 305-TK-002 » 32
2.3. Processus de gestion du risque de BLEVE lié à la sphère …….....35
2.3.1. Analyse qualitative du risque de BLEVE à l'aide de HAZOP ……..35
2.3.2. Analyse quantitative du risque de BLEVE à l'aide de LOPA et ALOHA …….....37
2.3.3. Évaluation du risque de BLEVE à l'aide de la matrice des risques ..……40
2.3.4. Réduction du risque de BLEVE à l'aide de l'IEC 61508 ……..43
2.4. Conclusion ……....46

Chapitre 3. L'approche probabiliste dans l'évaluation de la performance des systèmes de sécurité

3.1. Introduction ……...……..…49
3.2. Attributs de la performance probabiliste des systèmes de sécurité …...……49
3.2.1. Fiabilité et disponibilité ……..……..49
3.2.2. Maintenabilité ……...52
3.3. Tests périodiques (essai périodique) ……..53
3.3.1. Tests parfaits et tests imparfaits ……53
3.3.2. Test complet et test partiel ……..……..…54

3.3.3. Test simultané et test échelonné ……..……...…54
3.4. Paramètres de la performance probabiliste des systèmes de sécurité ……....54
3.4.1. Durées caractéristiques …….....55
3.4.2. Taux caractéristiques ……....56
3.4.2.1. Taux de défaillance $\lambda(t)$ ……53
3.4.2.1.1. Définitions ……..56
3.4.2.1.2. Taux de défaillance selon la norme IEC 61508 ……..58
3.4.2.2. Taux de réparation $\mu(t)$ ……61
3.5. Bases de données génériques liés à la fiabilité, la disponibilité et à la maintenabilité des systèmes ……..…62
3.5.1. Bases de données pour la sûreté de fonctionnement ……62
3.5.2. Restrictions liées à l'utilisation des bases de données ……..64
3.5.3. Certaines formules utilisées dans le cadre du retour d'expérience ……...65
3.6. Formules analytiques pour l'évaluation de la performance des SIS ……..69
3.6.1. Formules de IEC 61508 (Ed. 2010) ……..…69
3.6.2. Approche SINTEF ……71
3.7. Conclusion ……...72

Chapitre 4. Développement d'une formulation analytique du PFH fondée sur l'approche binomiale

4.1. Introduction ……75
4.2. Nouvelle formulation de la PFH fondée sur une approche binomiale……75
4.2.1. Approche générique ……..…75
4.2.2. Formules du $\mathrm{PFH}_{\mathrm{KOON}}^{\mathrm{ind}}$……76
4.2.2.1. Formulation générique ……...76
4.2.2.2. Formules du $\mathrm{PFH}^{\mathrm{ind}}$ pour les architectures standards……...77
4.2.2.3. Résultats numériques …… 77
4.2.3. Formule de la $\mathrm{PFH}_{\mathrm{KooN}}^{\mathrm{CCF}}$……78
4.2.3.1. Contribution générique des CCFs ……..…78
4.2.3.2. Formules de la $\mathrm{PFH}_{\mathrm{KooN}}^{\mathrm{CCF}}$ pour les architectures standards ……80
4.2.3.3. Résultats numériques…….....81
4.2.4. Formules PFH globales ……83
4.2.4.1. Formules PFH pour les architectures standards ……83

4.2.4.2. Comparaison numérique ……...85
4.3. Conclusion ……91

Chapitre 5. Développement d'une formulation analytique du PFD_{avg} avec tests échelonnés

5.1. Introduction 93
5.2. Stratégie de tests échelonnés 93
5.3. Etablissement de la PFD_{avg} des architectures usuelles 95
5.3.1. Architecture 1oo2 95
5.3.2. Architecture 2oo2 98
5.3.3. Architecture 1oo3 99
5.3.4. Architecture 2oo3 101
5.4. Généralisation des formules PFD_{avg} 103
5.4.1. Cas général des architectures KooN 103
5.4.2. Cas spécifiques des architectures NooN et 1ooN 105
5.4.3. Prise en compte des CCF 106
5.5. Comparaison des résultats relatifs à la PFD_{avg} 107
5.6. Conclusion 109

Conclusion générale 110

Annexes 112

Annexe A : Modélisation des effets des phénomènes dangereux avec le logiciel PHAST …113
Annexe B : Calcul automatique de la performance des SIS avec le logiciel GRIF 121

Bibliographie 124

Abréviations, acronymes

AdD Arbre des Défaillances

ALARP As Low As Raisonably Practicable (aussi faible que raisonnablement possible)

ALOHA Areal Locations of Hazardous Atmospheres

ARAMIS Advanced Risk Assessment Methodology for Industrial Systems (Méthodologie avancée d'évaluation des risques pour les systèmes industriels).

API American Petroleum Institute

ARIA Analyse Recherche et Information sur les Accidents

ASTM American Society for Testing and Materials

BARPI Bureau d'Analyse des Risques et Pollutions Industriels

BLEVE Boiling Liquid Expanding Vapor Explosions

BPCS Basic Process Control System

BPM Barrier Performance Management (gestion de la performance des barrières)

BS British Standard

CCF Common Cause Failure **(**défaillance de cause commune)

CEI Commission Electrotechnique Internationale (International Electrotechnical Commission)

CAMEO Computer-Aided Management of Emergency Operations

COSO ERM Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management.

CPFCC China Petroleum & Fuel Chemical Corporation

CSU Critical Safety Unavailability

DC Diagnostic Coverage (Couverture du Diagnostic)

DCC Défaillance de Cause Commune

DCS Distributed Control System (Système de contrôle distribué)

E/E/EP Electrique / Electronique / Electronique Programmable

EFFECTS Emergency, Fire & Failure Event Consequence and Threat Simulation

EN European Norm (Norme Européenne)

ER Evénement Redouté

ESD Emergency Shutdown System

EUC Equipment Under Control (équipement à protéger)

FLACS FLame ACceleration Simulator

GRIF Graphiques Interactifs pour la Fiabilité

HAZOP HAZard and Operability study (Analyse de risque et d'exploitation)

IEC	International Electrotechnical Comission
ILO	International Labour Organization (Organisation internationale du Travail)
IPL	Independent Protection Layer (Couche de protection indépendante)
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)
MOV	Motor Operated Valve (vanne motorisée)
MTBF	Mean Time Between Failure (durée moyenne entre défaillances consécutives)
MTTF	Mean Time To (first) Failure (durée moyenne de fonctionnement avant la Première défaillance)
MTTR	Mean Time To Repair (durée moyenne de réparation)
MUT	Mean Up Time (durée moyenne de fonctionnement après réparation)
NC	Niveau de Confiance
NF	Norme Française
OHSAS	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)
PHAST	Process Hazard Analysis Software Tool
PI	Pressure Indicator (Indicateur de pression)
PLC	Programmable Logic Controller (Automate Programmable)
PSV	Pressure Safety Valve (soupape de sécurité à pression)
PST	Partial Stroke Test (Test de Course Partielle)
PT	Pressure Transmitter (Transmetteur de pression)
QRA	Quantitative Risk Assessment (évaluation quantitative des risques)
RA2K	Raffinerie de Skikda
RFF	Risk Reduction Factor (facteur de réduction du risque)
ROV	Remotely Operated Valve (vanne commandée à distance)
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).
VCE	Vapor Cloud Explosions

Liste des figures

Figure 1.1 : Processus de gestion des risques et techniques associées 7
Figure 1.2 : Espace du risque 13
Figure 1.3 : Classification des barrières de sécurité. 14
Figure 1.4 : Configuration basique d'un SIS 18
Figure 1.5 : Configuration redondante d'un SIS 19
Figure 1.6 : Phases de l'étude HAZOP. 23
Figure 1.7 : Analyse des couches de protection (LOPA). 24
Figure 1.8 : Modèle ALARP 27
Figure 1.9 : Matrice des risques 28
Figure 1.10 : Technique de réduction du risque de la norme IEC 61508. 29
Figure 2.1 : Sphère de stockage de butane 305-TK-002 32
Figure 2.2 : Processus de gestion du risque de BLEVE 36
Figure 2.3 : Développement de scénario de BLEVE 36
Figure 2.4 : Rapport de donnes et de résultats liées au phénomène de BLEVE 39
Figure 2.5 : Distances d'effets thermiques liées au phénomène de BLEVE 39
Figure 2.6 : Graphique PFD et SIL du SIS 45
Figure 3.1 : Evolution de la fiabilité et de la défiabilité en fonction du temps. 50
Figure 3.2 : Evolution de disponibilité et d'indisponibilité en fonction du temps. 51
Figure 3.3 : Evolution de maintenabilité en fonction du temps 52
Figure 3.4 : Interconnexion des FDMS selon le diagramme de Venn 53
Figure 3.5 : Durées liées à la fiabilité, la disponibilité et à la maintenabilité des systèmes 56
Figure 3.6 : Variation du taux de défaillance dans pour les équipements électroniques …. 57
Figure 3.7 : Variation du taux de défaillance pour les équipements mécanique…. 57
Figure 4.1 : Evolution de la PFH^{ind} selon DC et β pour différentes architectures KooN 78
Figure 4.2 : Evolution de la PFH_{KooN}^{CCF} en fonction de DC et β 82
Figure 4.3 : Différence relative entre les formules proposées et de celles de la CEI 61508 87
Figure 4.4 : Différence relative entre les résultats des formules proposées et de celles de la CEI 61508 (CCFs) 88
Figure 4.5 : *PFH* relative à l'architecture 2oo3 90
Figure 5.1 : Chronologie des tests échelonnés dans une architecture constituée de n éléments 93
Figure 5.2 : Evolution de la PFD d'un seul canal en fonction du temps (λ_{DU}=1E-5/h ; T_1= 8760 et θ_1=4380) 94

Figure 5.3 : Evolution de la PFD_{avg} d'un seul canal en fonction du temps (λ_{DU}=1E-5/h ; T_1= 8760) 94

Figure 5.4 : Evolution de la PFD de chacun des deux canaux 95

Figure 5.5 : Variation de la PFD_{1oo2}^{avg} en fonction de θ_1.....97

Figure 5.6 : PFD_{1oo2}^{avg} sans et avec stratégie de tests échelonnés 98

Figure 5.7 : PFD_{2oo2}^{avg} sans et avec stratégie de tests échelonnés.....99

Figure 5.8 : Evolution de la PFD de chacun des trois canaux 100

Figure 5.9 : PFD_{1oo3}^{avg} sans et avec stratégie de tests échelonnés 101

Figure 5.10 : PFD_{2oo3}^{avg} sans et avec stratégie de tests échelonnés 102

Figure 5.11 : Evolution de PFD_{avg} selon DC et β pour différentes architectures KooN 109

Figure A.1 : Développement du scénario de flash fire ……..…113

Figure A.2 : Développement du scénario de UVCE ……..113

Figure A.3 : Développement du scénario de feux de chalumeau ……...114

Figure A.4 : Développement du scénario de feu de nappe ……....114

Figure A.5 : Développement du scénario de Boil-Over ……..92

Figure A.6 : Développement du scénario d'explosion d'un réservoir atmosphérique à toit fixe.....115

Figure B.1 : Interface du logiciel GRIF-module SIL 121

Figure B.2 : Résultats du logiciel GRIF-module SIL 124

Liste des tableaux

Tableau 1.1 : Référentiels de gestion des risques industriels 8
Tableau 1.2 : Niveaux de SIL en fonction de PFD_{avg} et PFH 21
Tableau 2.1 : Données techniques de la sphère 305-TK-002 33
Tableau 2.2 : Caractéristiques du butane 33
Tableau 2.3 : Etude HAZOP pour « pression élevée dans la sphère » 37
Tableau 2.4 : Résultats de la méthode LOPA 38
Tableau 2.5 : Seuils des effets thermiques sur la vie humaine 40
Tableau 2.6 : Seuils des effets thermiques sur les équipements 40
Tableau 2.7 : Echelle des probabilités d'occurrences annuelles 41
Tableau 2.8 : Échelle des gravités sur les personnes 41
Tableau 2.9 : Échelle des gravités sur les biens. 41
Tableau 2.10 : Matrice des risques 42
Tableau 2.11: Niveaux de risque 42
Tableau 2.12 : Caractéristiques du SIS proposé 43
Tableau 2.13 : Amélioration de performance du SIS proposé 46
Tableau 3.1 : Différences entre tests parfaits et tests imparfaits 54
Tableau 3.2 : Différences entre tests complets et tests partiels 54
Tableau 3.3 : Différences entre tests simultanés et tests test échelonnés 54
Tableau 3.4 : Facteurs Influençant μ(t) 62
Tableau 3.5 : Bases de données de fiabilité 63
Tableau 3.6 : Formules analytiques relatives aux PFD_{moy} des architectures KooN selon la CEI 61508-6 70
Tableau 3.7 : Formules analytiques relatives aux *PFH* des architectures KooN selon la CEI 61508-6 70
Tableau 3.8 : Formules analytiques simplifiées relatives aux PFD_{moy} des architectures KooN selon SINTEF 71
Tableau 3.9 : Exemple de valeurs du facteur C_{MooN} 72
Tableau 3.10 : Formules analytiques simplifiées relatives aux *PFH* des architectures KooN selon SINTEF 72
Tableau 4.1 : Formules de la PFH_{KooN}^{ind} pour les architectures usuell 77
Tableau 4.2 : Résultats de la *PFH* (h^{-1}) sans CCF 78
Tableau 4.3 : Formules de la PFH_{KooN}^{CCF} pour les architectures standards 81
Tableau 4.4 : Résultats de la PFH_{KooN}^{CCF} (h^{-1}) 81

Tableau 4.5 : Formules de *PFH* proposées ……..83

Tableau 4.6 : Formules de *PFH* fournies par la CEI 61508 (Ed. 2010) ……..83

Tableau 4.7 : Formules de PFH présentées dans la référence …… 84

Tableau 4.8 : Comparaisons des *PFH* individuelles ……...86

Tableau 4.9 : Comparaisons des *PFH* CCFs ……...87

Tableau 4.10 : Comparaisons des *PFH* globales …….....89

Tableau 5.1. Probabilités de défaillance des différents canaux 100

Tableau 5.2 : Formules PFD_{avg} pour certaines architectures KooN (K ≠ 1, N) 104

Tableau 5.3 : Valeurs de $\sum_{j=0}^{N} \frac{c(N,j)}{j+1}$.....105

Tableau 5.4 : Formules PFD_{avg} pour certaines architectures 1ooN 106

Tableau 5.5 : Formules PFD_{avg} de certaines architectures classiques incluant les CCFs 106

Tableau 5.6 : Comparaisons des résultats PFD_{avg} 108

Tableau A.1 : Tableau de Kinsella …….118

Tableau A.2 : Comportement des produits vis-à-vis des phénomènes de boil over classique et boil over couche mince …….119

Tableau A.3 : Calculs des distances d'effets liées au phénomène de BLEVE ……..120

Introduction générale

1. Problématique

La maîtrise des risques industriels constitue aujourd'hui un enjeu majeur pour les installations à risques, en particulier dans le secteur pétrolier et gazier où la complexité des procédés, la présence de substances dangereuses et les conditions opératoires sévères renforcent la nécessité d'une gestion rigoureuse de la sécurité. Ces installations peuvent générer des phénomènes dangereux (incendie, explosion, rejets toxiques) aux conséquences dévastatrices sur les personnes, les biens et l'environnement.

L'objectif n'est pas l'élimination absolue des risques, matérielle impossible, mais de garantir qu'ils sont ramenés et maintenus à des niveaux acceptables ou tolérables par la société et la réglementation. Pour y parvenir, une démarche appropriée de gestion des risques permet d'identifier les mesures de maîtrise (barrières de sécurité) et d'évaluer leur performance, s'appuyant sur des normes de référence comme l'ISO 31000 [1] et l'IEC 61508 [2].

Au sein de ces barrières, les systèmes instrumentés de sécurité (SIS) occupent une place capitale. Ils garantissent le fonctionnement sûr en surveillant en continu les paramètres opératoires clés et en ramenant le procédé dans un état de sécurité lors d'événements dangereux. La norme IEC 61508 [2] encadre leur conception et leur exploitation à travers le concept de niveau d'intégrité de sécurité (SIL : *Safety Integrity Level*), établissant une relation directe entre la réduction du risque recherchée et les exigences de performance du SIS.

La sécurité fonctionnelle repose directement sur la capacité de ces systèmes à fonctionner exactement au moment opportun. Quantifier leur performance est donc un besoin fondamental, caractérisé par deux mesures principales selon leur mode de sollicitation :

- *La probabilité moyenne de défaillance dangereuse à la demande (PFD_{avg}),* pour les systèmes à faible demande.
- *La fréquence moyenne des défaillances dangereuses (PFH),* pour les systèmes à forte demande ou continu.

Dans le cadre de cette thèse, l'accent est mis sur deux limites majeures de la littérature actuelle :

1. *Une considération inadéquate ou incomplète de l'arrêt immédiat du procédé* (*shutdown*) après la détection d'une défaillance dangereuse au sein du SIS, conduisant à des résultats non conservatifs (optimistes) et dangereux lors de l'évaluation du PFH.
2. *La non-considération de l'impact des stratégies de test complexes,* plus particulièrement des tests échelonnés ou décalés (*staggered tests*), sur le calcul de la $\mathrm{PFD}_{\mathrm{avg}}$. L'absence de formulation analytique générale pour ces configurations ne permet pas d'évaluer de manière optimale le gain réel qu'ils apportent sur la réduction de la $\mathrm{PFD}_{\mathrm{avg}}$.

2. Objectifs

Pour pallier ces limites, cette thèse vise à contribuer à l'amélioration et au renforcement de la modélisation probabiliste de la performance des SIS à travers les objectifs spécifiques suivants :

1. *Étude et intégration du cadre global de gestion des risques* **:** Mettre en œuvre le processus de management de la sécurité industrielle en l'appliquant de manière concrète à un cas d'étude réel de la raffinerie RA2K.
2. *Développement de nouvelles formulations pour le PFH* **:** Proposer de nouvelles expressions analytiques basées sur la loi binomiale, permettant d'intégrer rigoureusement l'hypothèse de l'arrêt automatique et immédiat du procédé surveillé suite à la détection d'une défaillance dangereuse.
3. *Optimisation du calcul de la PFD_{avg} sous tests échelonnés* **:** Développer de nouvelles expressions de la $\mathrm{PFD}_{\mathrm{avg}}$ spécifiquement adaptées aux architectures KooN soumises à des stratégies de tests échelonnés ou décalés, afin de combler le manque de formulations analytiques générales dans ce domaine.

3. Organisation du mémoire

Afin d'atteindre ces objectifs, le manuscrit est structuré en cinq chapitres complémentaires :

Le premier chapitre traite des concepts fondamentaux liés au risque et à la sécurité industrielle dans les industries pétrolières et gazières, du processus de gestion des risques et des techniques associées. Il met en lumière l'intégration de la norme IEC 61508 [2] dans le cadre de la norme IEC 31010 [3] au cours de la phase finale du processus de gestion des risques.

Le deuxième chapitre illustre une application pratique du cadre méthodologique développé dans le chapitre précédent, à travers une étude de cas portant sur un réservoir de stockage de butane à la raffinerie RA2K.

Dans le troisième chapitre, nous entamons l'étude de l'approche probabiliste pour l'évaluation de la performance des systèmes de sécurité. Cette approche permet de modéliser des événements tels que les défaillances et les réparations, afin d'estimer les performances des systèmes dans des conditions réelles. Elle s'appuie sur des outils statistiques et mathématiques, tels que l'estimation empirique, les lois de probabilité ainsi que des méthodes d'analyse comme les arbres de défaillances (AdD) [4], pour évaluer des indicateurs clés tels que la fiabilité, la disponibilité et la maintenabilité.

Le quatrième chapitre est consacré aux formules de PFH pour l'évaluation des SIS, ce chapitre présente une généralisation du PFH fondée sur une approche binomiale, permettant une modélisation plus souple et précise des architectures redondantes.

Le cinquième chapitre traite de la modélisation probabiliste des SIS, en se focalisant sur le calcul de la PFD_{avg} pour des architectures KooN soumises à des tests échelonnés ou décalés. Cette stratégie de tests à l'avantage de réduire la PFD_{avg}, par rapport aux tests simultanés. Notons qu'une formulation analytique générale tenant compte de ce type de test est inexistante.

En somme, cette recherche vise à renforcer l'exactitude, la flexibilité et la pertinence des outils de calcul utilisés pour la sécurité fonctionnelle, tout en proposant une démarche intégrée allant de la gestion globale des risques à l'évaluation fine de la performance des SIS.

Chapitre 1

La gestion des risques industriels et ses techniques

1.1. Introduction

Ce chapitre explore la gestion des risques dans les environnements industriels, en particulier dans les industries pétrolières et gazières, où des machines complexes, des matériaux dangereux et des opérations sous haute pression représentent des risques importants pour la sécurité des personnes, des équipements et de l'environnement. Nous commençons par passer en revue les concepts fondamentaux liés au risque et à la sécurité industrielle, suivis d'une présentation du processus de gestion des risques et des techniques qui y sont associées.

Ce chapitre met en évidence l'intégration de la technique de la norme IEC 61508 dans le cadre de l'IEC 31010, plus particulièrement lors de la phase finale du processus de gestion des risques.

1.2. Risque et sécurité industrielle : concepts clés

En replaçant la gestion des risques dans le contexte industriel général qui l'a établie, nous proposons tout d'abord de passer en revue les principaux concepts liés au risque et à la sécurité industrielle.

1.2.1. Risque industriel

Le concept de risque possède un grand nombre d'acceptions que ce soit dans le langage courant ou dans les références techniques. Néanmoins, dans le contexte industriel, on trouve un consensus clair sur la définition du risque, qui vise à associer deux entités à partir desquelles il est plus généralement défini : probabilité et conséquence.

On préfère ici retenir les définitions suivantes :

- « *Le risque est la combinaison de la probabilité de survenue d'un événement dangereux et de la gravité de ses conséquences* » [4].
- « *Le risque est défini comme la combinaison de la probabilité d'occurrence d'un accident industriel et de la gravité de ses conséquences sur les personnes, l'environnement et les biens* » [5].
- « *Le risque est la combinaison de la probabilité d'un événement et de ses conséquences* » [6].

Mathématiquement, le risque est souvent représenté par l'équation suivante [7] :

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

Où,

- *P* : possibilité d'occurrence : mesure de la possibilité (probabilité ou fréquence) qu'un événement dangereux ou un accident se produise,
- *G* : gravité des conséquences : mesure de l'importance (l'ampleur et l'impact) des conséquences potentielles d'un événement dangereux ou d'un accident sur les personnes, les biens et l'environnement,
- × : symbole de multiplication qui caractérise (matérialise) le terme de « combinaison » mentionnée dans la définition précédente du concept de « risque ».

En conséquence, un risque se caractérise selon deux paramètres : probabilité d'occurrence et gravité des conséquences. Ce couple de valeurs permet d'estimer un niveau de risque.

1.2.2. Sécurité industrielle

La définition de la sécurité industrielle fait référence à la définition de la sécurité globale sauf qu'elle concerne les risques rencontrés en milieu industriel (risques industriels).

- « *La sécurité est l'absence de risque intolérable* » [8].
- « *La sécurité est l'état dans lequel le risque de dommages corporels ou matériels est limité à un niveau acceptable* » [9].

Dans un sens large, *La* sécurité industrielle est définie de la manière suivante : « *La sécurité industrielle est l'ensemble des dispositions techniques, des moyens humains et des mesures organisationnelles appliqués aux installations et activités industrielles, visant à réduire le risque à un niveau acceptable en prévenant les accidents ou en atténuant leurs conséquences ; par extension, état résultant de ces dispositions* » [10, 11]. Il s'agit d'une discipline qui garantit l'intégrité physique et la santé des travailleurs, l'intégrité des biens et de l'environnement, tout en contribuant à l'augmentation de la productivité, de l'efficacité et de la rentabilité des entreprises manufacturières.

1.2.2.1. Sécurité fonctionnelle

La norme internationale IEC 61508, souvent considérée comme la référence pour la sécurité fonctionnelle, la définit ainsi : « *sous-ensemble de la sécurité industrielle 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* » [12].

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 » [12]. 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.

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 lui-même.

Les systèmes électriques, électroniques et électroniques programmables (E/E/PE) relatifs à la sécurité sont tout simplement les systèmes instrumentés de sécurité (SIS), objet principal de cette thèse.

1.3. Processus de gestion des risques industriels et ses techniques

La gestion des risques est définie comme l'ensemble des activités coordonnées visant à réduire le risque à un niveau jugé tolérable ou acceptable, correspondant au niveau cible de sécurité, dans un délai et un contexte donné [13, 14].

La gestion des risques est présentée comme un processus itératif qui comprend différentes phases dont la séquence et les techniques utilisées dans chaque phase sont décrites dans la Figure 1.1. Ce processus est celui défini par la norme CEI 31010 : 2019, laquelle s'inscrit dans le cadre général de l'ISO 31000 : 2018, en mettant l'accent sur les techniques de gestion des risques. Il convient de noter qu'il existe plusieurs cadres génériques et spécifiques/sectoriels définissant la structure générale d'un système de gestion des risques industriels. Les principaux d'entre eux sont récapitulés dans le Tableau 1.1. Il importe de signaler qu'une entreprise industrielle moderne ne s'appuie pas sur un seul référentiel, mais sur un écosystème de cadres, lequel peut être aligné sur les principes de l'ISO 31000 pour une cohérence globale. Par exemple, une entreprise industrielle peut utiliser l'ISO 31000 pour structurer son système global de management des risques, puis appliquer des normes plus spécifiques (comme l'IEC 61511) pour des risques particuliers.

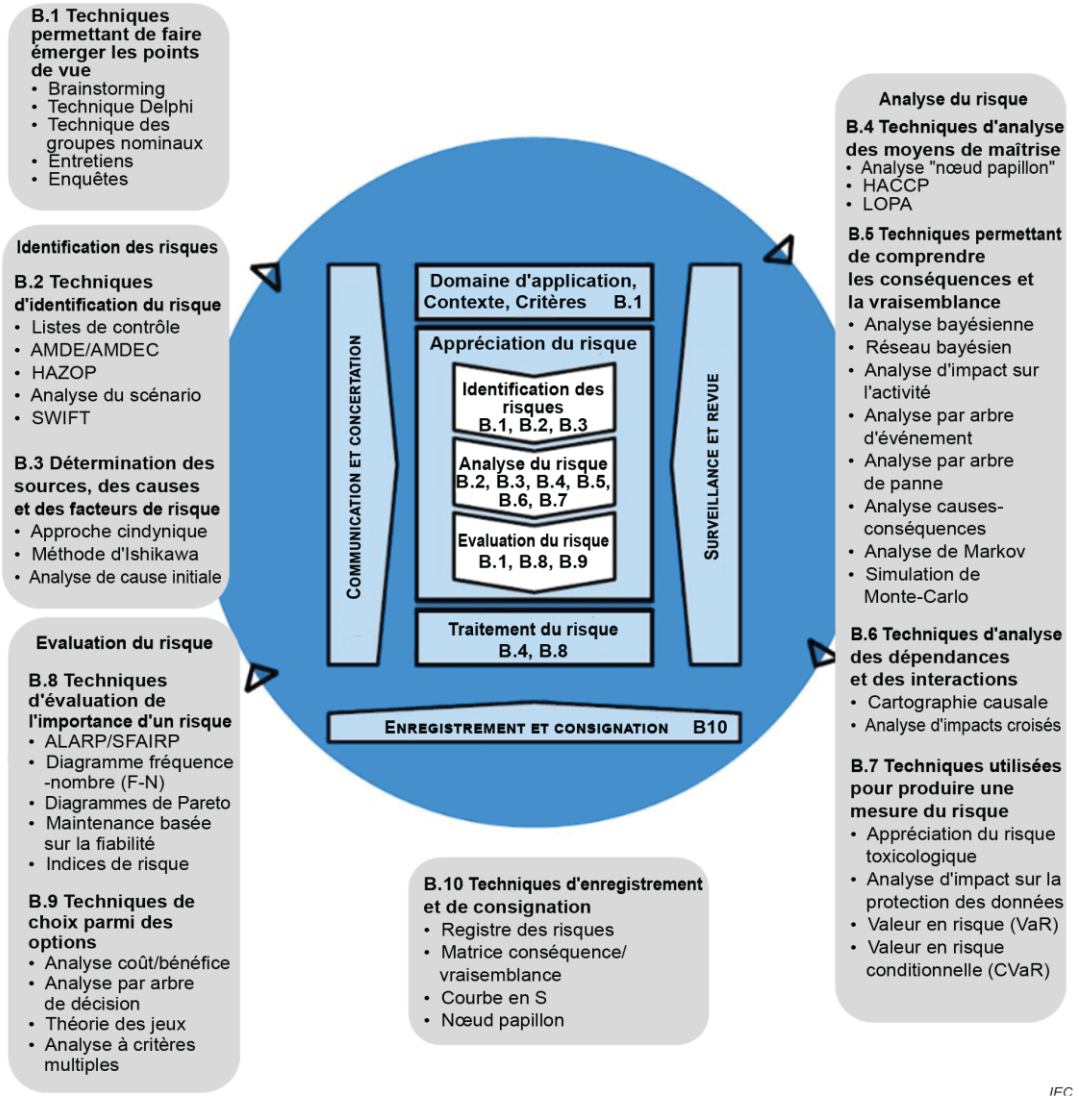


Figure 1.1 : Processus de gestion des risques et techniques associées [15]

Tableau 1.1 : Référentiels de gestion des risques industriels

Référentiel / Norme	Domaine d'application	Objectifs principaux
ISO 31000 : 2018	Générique (tous secteurs)	Définir un cadre générique de management des risques. C'est la norme générique et internationale de référence pour le management des risques, adaptable à tous types d'organisations.
CEI 31010 : 2019	Industrie (complément ISO 31000)	Détailler les méthodes et techniques d'évaluation des risques. Approche méthodologique, outils pratiques pour l'industrie (très utilisées en ingénierie et industries à risques).
ISO 45001 : 2018	Santé et sécurité au travail en milieu industriel	Prévenir les accidents et améliorer les conditions de travail. Centrée sur la protection des travailleurs dans l'industrie.
ISO 14001 : 2015	Management environnemental industriel	Identifier, évaluer et réduire les risques environnementaux. Approche cycle de vie, réduction des impacts industriels
ISO 9001 : 2015	Qualité industrielle	Intégrer l'approche par les risques dans le management de la qualité. Amélioration continue, maîtrise des processus industriels.
IEC 61508 : 2010	Sécurité fonctionnelle des systèmes industriels (les processus automatisés)	Assurer la fiabilité et la sécurité des systèmes électriques/électroniques. Référentiel clé pour les industries à haut risque (pétrochimie, énergie, transport).
CCPS	Sécurité des procédés (générique)	C'est un cadre complet et détaillé, considéré comme une référence mondiale pour la sécurité des procédés « process safety »
API	Sécurité des procédés pétroliers et gaziers	Fournit un cadre pour le suivi des indicateurs de performance en sécurité des procédés
Directive SEVESO III	Industrie à risques majeurs	Prévention des accidents majeurs. Ce n'est pas une norme volontaire mais une obligation réglementaire pour les sites industriels détenteurs de quantités importantes de substances dangereuses.

1.3.1. Étapes du processus de gestion des risques

Le processus de gestion des risques, illustré à la Figure 1.1, peut être structuré en trois phases principales : analyse des risques, évaluation des risques et réduction des risques.

1.3.1.1. Analyse des risques

L'analyse des risques est définie dans le Guide ISO/CEI 51 [ISO, 1999] comme : « *l'utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque* » [16].

A partir de la définition du risque vue précédemment, l'activité d'analyse de risques consiste logiquement à répondre aux trois questions suivantes [17] :

1. Qu'est-ce-qui peut conduire à des situations dangereuses ?
2. Quelles sont les chances pour que ces situations se produisent ?
3. Si elles se produisent, à quelles conséquences doit-on s'attendre ?

La première question revient à rechercher les scénarios (*Si*) pouvant conduire à un accident. Ensuite, l'analyse de risques va estimer la possibilité d'apparition de chaque scénario *Si* à partir d'une mesure d'occurrence (dans une approche probabiliste, il s'agira de la probabilité *Pi* associée à *Si*). La troisième question s'attache à décrire et à estimer les conséquences *Ci* liées au scénario *Si*.

Ainsi, l'activité d'analyse de risques consiste à évaluer le risque *R* défini par l'ensemble des triplets [18] : $R = < Si, Pi, Ci >$.

Si le risque est une notion intrinsèque, son analyse dépend en revanche de la qualité des données introduites. On peut ainsi associer à cette analyse un attribut qui représente la qualité de la connaissance que l'on a de la prévision du risque [19]. Pour améliorer cette qualité, il faut améliorer la qualité de chacun des membres des triplets : la connaissance précise des scénarios, l'estimation de leur probabilité d'apparition et l'estimation des conséquences. Dans ce contexte, on distingue deux différents types d'analyse des risques : l'analyse qualitative des risques et l'analyse quantitative des risques.

1.3.1.1.1. Analyse qualitative des risques

L'analyse qualitative du risque s'appuie sur une approche déterministe (déclarative) dans l'identification des scénarios d'accident et l'estimation de leur probabilité d'occurrence et de leur gravité des conséquences. Cette approche repose sur des données historiques des accidents passés survenus sur des installations similaires, qui sont fournies dans des bases de données d'accidents (comme ARIA [20] et USCSB [21]). Ou sur l'expression explicite des jugements d'experts ou des parties prenantes, basés sur leur expérience, leurs connaissances, ou des critères spécifiques définis au préalable. Elle prend généralement les scénarios les plus

défavorables (les pires cas raisonnablement envisageables) comme référence. Cette approche est souvent utilisée lorsque les données quantitatives ne sont pas disponibles ou difficiles à obtenir. Il convient de noter que l'analyse qualitative fournit une base de données pour l'analyse quantitative.

1.3.1.1.2. Analyse quantitative des risques

Analyse quantitative du risque (QRA : *quantitative risk assessment*) est une approche formelle et systématique permettant d'estimer la probabilité et les conséquences d'événements et d'exprimer les résultats de manière quantitative en tant que risque pour les personnes, l'environnement ou l'entreprise [22]. Cette analyse est une forme d'analyse détaillée qui essaye de traduire le mieux possible par le calcul, le risque pour les personnes, les biens et l'environnement, en fonction de sa fréquence d'occurrence et de la gravité des conséquences [23]. En conséquent, les deux paramètres de risque sont estimés comme suit [24, 25] :

- *L'estimation de l'occurrence* d'un accident sert à quantifier la probabilité ou la fréquence, tout dépend de l'approche suivie :
  - L'approche statistique (ou fréquentielle) : repose sur l'analyse des données historiques et empiriques relatives à des événements similaires, c'est-à-dire l'observation des défaillances qui se sont déjà produites (observations réelles), et suppose que le passé est représentatif du futur, où elle utilise les fréquences observées pour estimer la probabilité d'occurrence future. En effet, elle se base sur la fréquence d'occurrence des événements dans un grand nombre d'essais ou d'observations. Cette approche considère que la probabilité d'un événement est la limite de sa fréquence relative lorsque le nombre d'essais tend vers l'infini. Egalement, elle exprime la fréquence ou le taux comme le nombre d'occurrences d'un événement par unité de temps.
  - L'approche analytique (ou probabiliste) : repose sur des modèles (mathématiques ou de simulation) basés sur les paramètres du système. Ces modèles comprennent les lois de probabilité, les méthodes d'analyses telles que l'arbre de défaillance, les simulations Monte Carlo ou les méthodes bayésiennes, et intègrent des informations comme les probabilités de défaillance des composants individuels, les scénarios combinatoires conduisant à l'événement dangereux, les incertitudes et les facteurs aléatoires impliqués. Cette approche vise à calculer la probabilité qu'un accident survienne sur une période définie. Le résultat est exprimé par un chiffre [sic] entre 0 et 1, 0 indiquant une impossibilité et 1 indiquant une certitude

absolue [26]. Elle est particulièrement utile pour les systèmes nouveaux ou les systèmes où les événements rares, incertains ou complexes sont prépondérants. Dans ces systèmes, les données historiques sont insuffisantes ou inexistantes.

- *L'estimation des conséquences* d'un accident sert à quantifier les impacts potentiels des événements accidentels, notamment sur les personnes, l'environnement et les biens. Cette estimation suit généralement une approche séquentielle et méthodique qui repose sur des données scientifiques, des normes internationales (comme celles de l'ISO ou de l'AIChE), des modèles mathématiques (Shield (voir annexe B), Gaussian plume, Heskestad, AEGL, probit), et des outils logiciels spécialisés pour la simulation des risques (ex. PHAST (voir annexe B), ALOHA, FLACS, in:Flux ou EFFECTS).

La combinaison des deux types d'analyses est souvent utilisée pour tirer parti des forces de chacune. Une analyse qualitative (déterministe) peut poser les bases d'une évaluation rapide et claire, tandis qu'une analyse quantitative (probabiliste) affine l'évaluation pour mieux gérer les incertitudes et prioriser les actions de réduction des risques.

1.3.1.2. Évaluation des risques

L'évaluation des risques désigne une procédure fondée sur l'analyse du risque pour déterminer si le risque tolérable a été dépassé [27]. Elle revient à comparer le niveau de risque estimé à celui jugé acceptable ou tolérable par l'entreprise/organisme concerné [28]. Les critères d'acceptabilité du risque doivent résulter d'un consensus entre les différents partenaires impliqués dans la démarche de gestion des risques. Ces critères sont fonction du contexte de l'établissement concerné, sa fonction et des objectifs poursuivis dans la gestion des risques.

A ce propos, la définition du risque tolérable donnée dans la référence [27] laisse transparaître la difficulté de retenir des critères objectifs et forfaitaires pour l'acceptation du risque : « *Risque accepté dans un certain contexte et fondé sur les valeurs admises par la société* ». La norme EN 61508-5 en son annexe A (§ A2) indique « *la détermination du risque tolérable pour un événement dangereux a pour but d'établir ce qui est jugé raisonnable eu égard à la fréquence (ou probabilité) de l'événement dangereux et à ses conséquences spécifiques* » [30]. La définition de critères d'acceptabilité du risque est une étape-clé et délicate dans le processus de gestion de celui-ci dans la mesure où elle va motiver la nécessité de considérer de nouvelles mesures de réduction des risques.

En fonction de l'évaluation du risque, deux scénarios sont possibles. Si le niveau de risque est considéré comme acceptable ou tolérable, le processus s'achève avec la mise en place d'une

surveillance continue du risque. En revanche, si le risque est jugé inacceptable, il est nécessaire de poursuivre le processus en initiant la phase de réduction du risque.

1.3.1.3. Réduction des risques

La réduction nécessaire du risque est la réduction qui doit être réalisée pour se conformer au risque tolérable (niveau de sécurité cible du procédé) pour une situation donnée [30]. Pour réduire un risque, il faut réduire au moins un de ses paramètres (sa fréquence d'occurrence et/ou sa gravité) [31]. Pour y parvenir, des barrières de sécurité sont utilisées.

1.3.1.3.1. Barrières de sécurité

Le terme « *barrière de sécurité* », ainsi que des termes similaires tels que « *couche de protection* », « *élément critique pour la sécurité* », « *élément important pour la sécurité* » et « *système de sécurité* », sont fréquemment utilisés dans les réglementations, les normes et la littérature scientifique. Toutefois, une revue de la littérature montre qu'il n'existe pas de définition universelle et communément acceptée de ces termes dans la littérature. Nous préférons conserver ici les définitions suivantes :

- « *Les barrières de sécurité sont des moyens physiques et/ou non physiques prévus pour prévenir, contrôler ou atténuer les événements indésirables ou les accidents.* » [32].
- « *Une barrière de sécurité est toute solution ou système opérationnel, organisationnel ou technique qui minimise la probabilité que des événements indésirables se produisent et limite les conséquences de tels événements* » [33].

1.3.1.3.1.1. Classification

Les barrières de sécurité peuvent être classées selon leurs fonctions et leur nature comme suit :

- ***Classification des fonctions de barrière*** *:* Il est courant de classer les fonctions de barrière comme étant la prévention, le contrôle et l'atténuation [34, 35, 36]. Certain auteur décrit seulement deux fonctions principales des barrières de sécurité : la prévention et la protection [37]. Les barrières de prévention sont conçues pour arrêter ou empêcher qu'un événement indésirable ne se produise en premier lieu. Ils fonctionnent en réduisant la probabilité qu'un accident se produise. Les barrières de protection, en revanche, visent à minimiser ou à atténuer les conséquences une fois qu'un événement indésirable s'est produit. Ils se concentrent sur la réduction de la gravité des dommages causés aux personnes, aux biens ou à l'environnement. Innal [38] illustre cette catégorisation dans la Figure 1.2.

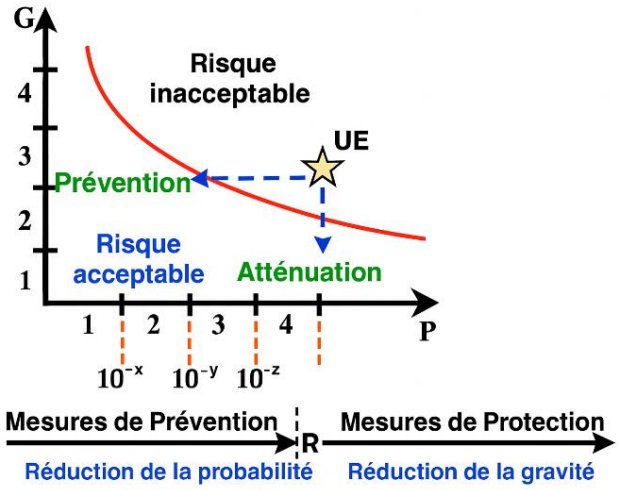


Figure 1.2 : Espace du risque [38]

- ***Classification des types de barrière :*** une catégorisation couramment utilisée consiste à distinguer les barrières physiques et non physiques [39, 40, 41].

  Dans la norme CEI : 61511, les mesures de réduction des risques sont classées comme suit : systèmes instrumentés de sécurité (SIS), autres systèmes technologiques liés à la sécurité et installations externes de réduction des risques. Un SIS est spécifiquement un système E/E/EP (électrique, électronique et électronique programmable), par exemple, un système d'arrêt d'urgence, un système de détection d'incendie et de gaz. D'autres systèmes liés à la sécurité technologique utilisent des technologies autres que E/E/EP, par exemple les soupapes de décharge et les disques de rupture. Les dispositifs de réduction des risques externes sont des mesures visant à réduire le risque qui sont séparées et distinctes du SIS ou d'autres systèmes liés à la sécurité technologique, par exemple les systèmes de drainage et les pares-feux.

  Plusieurs auteurs font la distinction entre les barrières passives et actives [42, 43, 44]. Les barrières passives sont des éléments physiques ou de conception qui ne nécessitent aucune action, énergie ou activation pour remplir leur fonction de protection. Ils fonctionnent par leur simple présence et ne dépendent pas de systèmes opérationnels ni d'intervention humaine. Parmi les exemples, on trouve les murs coupe-feu, les digues de confinement et les écrans anti-explosion. En revanche, les barrières actives nécessitent une certaine forme d'activation, d'énergie ou d'intervention pour remplir leur fonction de protection. Elles doivent passer d'un état à un autre en réponse à une variation d'une grandeur mesurable du processus (par exemple, la température ou la pression) ou à un signal provenant d'une autre source (comme un bouton-poussoir ou un interrupteur). Une couche de protection active comprend généralement un capteur,

un processus de prise de décision et une action. Parmi les exemples, on trouve les systèmes de sprinklers, les systèmes d'arrêt d'urgence et les alarmes.

Une méthode recommandée pour classer les systèmes de barrières est illustrée dans la Figure 1.3.

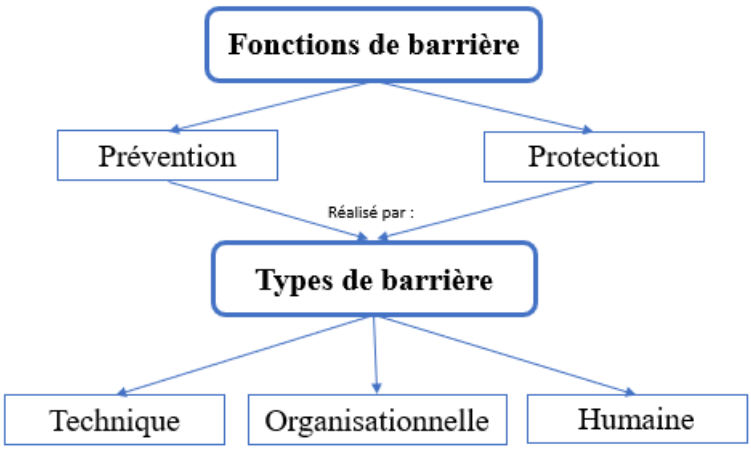


Figure 1.3 : Classification des barrières de sécurité

1.3.1.3.1.2. Performance

L'analyse des performances attendues des barrières est essentielle à la réduction des risques. En effet, la réduction des risques est directement proportionnelle à la performance des barrières de sécurité. Sur la base de l'expérience acquise dans le cadre de plusieurs projets et de la synthèse de la littérature examinée, on a recommandé que les attributs suivants soient pris en compte pour caractériser la performance des barrières de sécurité :

- Fiabilité/disponibilité
- Fonctionnalité/efficacité
- Temps de réponse
- Robustesse
- Indépendance
- Maintenabilité

Pour certains types de barrières, tous les attributs ne sont pas pertinents ou nécessaires pour décrire les performances de la barrière.

- La fiabilité/disponibilité de la barrière est la capacité d'une barrière de sécurité à exécuter une fonction de sécurité *lorsque cela est nécessaire, ou à la demande* dans toutes les conditions énoncées [45, 46].

La fiabilité/disponibilité de la barrière peut être exprimée comme la probabilité de ne pas échouer (sur demande) à exécuter une fonction. La fiabilité/disponibilité des barrières de sécurité correspond au niveau d'intégrité de sécurité (SIL) exigé par la norme IEC 61511 pour les SIS et au niveau de confiance (NC) pour tous les types de barrières de sécurité comme décrit dans le projet ARAMIS [47]. La méthode PDS [48] se concentre également sur diverses mesures de perte de sécurité ou d'indisponibilité de sécurité pour une fonction de sécurité (probabilité de non-fonctionnement à la demande) et utilise le terme d'indisponibilité critique de sécurité (CSU) pour quantifier la perte totale de sécurité.

La fiabilité est l'attribut le plus important pour caractériser la performance d'une barrière de sécurité.

- La fonctionnalité/efficacité d'une barrière est la capacité d'une barrière de sécurité à exécuter une fonction de sécurité pendant une durée, *dans un mode non dégradé* et dans des conditions spécifiées [49, 50].

  Cet attribut correspond aux exigences de fonction de sécurité (fonctionnalité) exigées par la CEI : 61511 et à l'effectivité des barrières de sécurité telles que décrites dans le projet ARAMIS.

  La fonctionnalité/efficacité est mesurée par la façon dont la barrière atteint son objectif. Elle est soit un pourcentage, soit une probabilité de performance de la fonction de sécurité définie. Le degré « possible » de réalisation peut être exprimé de manière probabiliste comme la probabilité d'exécution réussie de la fonction spécifiée ou le pourcentage d'exécution réussie. Par exemple, si la fonction est de pomper de l'eau, une exigence fonctionnelle peut être que le débit d'eau soit 100 l/min. Si la pompe donne un débit de 80 l/m on dit que sa fonctionnalité/efficacité est de 80% en termes de pourcentage ou 0.8 en termes de probabilité.

  La différence entre fonctionnalité/efficacité et fiabilité/disponibilité d'une barrière peut être illustrée par l'exemple d'un système ESD. La fonction de la barrière est de bloquer le flux. La fonctionnalité d'une vanne ESD qui se ferme sans fuite interne peut être de 100 %. Une fuite interne à travers la vanne réduit son efficacité, mais la fiabilité, exprimée par la probabilité de fermeture de la vanne à la demande, n'est pas influencée par la fuite interne.

- Le temps de réponse d'une barrière de sécurité correspond à la durée écoulée *entre le moment où une déviation survient*, laquelle aurait dû activer une barrière de sécurité, *et l'accomplissement de la fonction* spécifiée de cette barrière [51, 52].

Le temps de réponse peut être défini de manière légèrement différente selon les types de fonctions de barrière. Cela peut être illustré par la différence entre un système ESD et un système de déluge. Le temps de réponse d'un système ESD correspond au temps nécessaire à la fermeture de la vanne ESD, moment où la fonction « arrêt du flux » est accomplie. En revanche, pour un système de déluge, le temps de réponse correspond au temps nécessaire à la délivrance de la quantité d'eau spécifiée (et non au temps nécessaire à l'extinction de l'incendie).

- La robustesse d'une barrière est sa capacité *à résister à des charges d'accident* données et à *fonctionner comme spécifié* lors des séquences d'accident. Cet attribut est pertinent pour les systèmes de barrières passives et actives, et il peut être nécessaire d'évaluer la robustesse pour plusieurs types de scénarios d'accident [53, 54].

- Une barrière de sécurité est qualifiée IPL (*Independent Protection Layer*), si son fonctionnement *ne dépend pas du fonctionnement des autres IPLs* d'une part, et *de l'événement initiateur*, d'autre part [55, 56].

  Cette propriété d'indépendance permettra à une barrière de remplir sa fonction de sécurité indépendamment de toute cause ou défaillance commune.

- La maintenabilité est la capacité d'une barrière de sécurité à être maintenu ou restauré dans un état opérationnel, dans des conditions données d'utilisation, avec des procédures, des ressources et dans un délai prédéterminé [57, 58]. Elle traduit la facilité, la rapidité et l'efficacité avec lesquelles une barrière peut être inspectée, réparée ou remise en service. Notons que *la testabilité* est généralement considérée comme un sous-attribut de la maintenabilité).

La fonction spécifiée d'une barrière de sécurité doit être énoncée comme une exigence fonctionnelle (exigence déterministe). Une exigence fonctionnelle est une spécification des critères de performance liés à une fonction [59]. Les exigences fonctionnelles relatives aux performances des barrières de sécurité peuvent exister dans des réglementations, des normes, des codes de conception, etc., ou sous forme d'exigences tenant compte des risques et basées sur des évaluations des risques utilisant des critères d'acceptation des risques [60].

Il faut noter que de nombreuses normes, guides et outils de gestion ont été développés afin de garantir la performance des barrières de sécurité. Ces référentiels visent à encadrer les bonnes pratiques pour la conception, l'installation, l'évaluation, ainsi que la maintenance de ces barrières dans divers contextes industriels. Parmi les normes les plus couramment utilisées, on retrouve : IEC 61508, IEC 61511, API RP 754, ISO 31000. En complément de ces normes,

plusieurs guides techniques et méthodologies sont largement utilisés : Guides de l'Energy Institute (EI), Outils de gestion des performances des barrières (BPM Tools), Bowtie XP.

- ***Évolution des performances des barrières de sécurité dans le temps*** — Quelle que soit la barrière de sécurité, qu'elle soit technique, organisationnelle ou humaine, ses performances sont susceptibles de se dégrader dans le temps, notamment en cas d'absence ou d'inefficacité de maintenance, de formations et de mise à jour. Le maintien des performances de ces barrières techniques dans le temps doit être assuré par la mise en œuvre d'une maintenance et d'une inspection appropriées, y compris des tests de fonctionnement périodiques. Quant aux barrières humaines ou barrières nécessitant des interventions humaines, le maintien de leurs performances est assuré en agissant sur le facteur humain par des sensibilisations et des formations en matière de maintenance et de sécurité industrielle. La motivation et l'état physique et moral doivent être pris en considération.

  La performance « de conception » signifie que la barrière est censée être aussi efficace qu'au moment de son installation, tandis que la performance « opérationnelle » inclut l'influence du système de gestion de la sécurité [61]. Cette valeur peut être inférieure à celle « de conception » si certains problèmes sont identifiés lors de l'audit du système de gestion de la sécurité. La performance réelle d'une barrière peut être inférieure à la performance spécifiée en raison des contraintes de conception, de dégradations, de conditions opérationnelles, etc.

1.3.1.3.1.3. Défense en profondeur

Le concept de défense en profondeur (*defence-in-depth*) constitue la base de la discussion sur les barrières de sécurité.

- Reason [62] décrit la défense en profondeur comme des « couches successives de protection ».
- Le concept de la « défense en profondeur » consiste en la combinaison de plusieurs barrières de sécurité pour arrêter la progression d'une séquence accidentelle » [63].
- La défense en profondeur est une stratégie de sécurité qui repose sur la mise en place de plusieurs couches de protection afin de ralentir ou de contrer une menace.

Plusieurs modèles ont été développés pour expliquer la défense en profondeur, parmi lesquels on retrouve :

- Le modèle linéaire (aussi appelé modèle séquentiel) : ce modèle considère que les incidents se produisent comme une séquence d'événements en cascade. Chaque couche de défense agit comme une barrière indépendante, et si une barrière échoue, la suivante

prend le relais. C'est comparable à une série de murs successifs : si un intrus franchit le premier mur, il doit encore faire face aux suivants. Les défenses sont disposées de manière séquentielle, chacune ayant un rôle spécifique et distinct. Par exemple le modèle du fromage suisse proposé par James Reason [64] illustre bien cette approche.

- Le modèle non linéaire : ce modèle reconnaît que les incidents peuvent survenir de manière plus complexe et interconnectée. Il prend en compte les interactions entre différentes composantes du système et reconnaît que les défaillances peuvent se produire simultanément ou s'influencer mutuellement (notamment dans les systèmes modernes, marqués par leur complexité et leur dynamique). Les barrières de défense ne sont pas simplement disposées en série mais forment un réseau interconnecté où chaque élément peut avoir des impacts multiples et variés sur les autres. Par exemple, le modèle FRAM (*Functional Resonance Analysis Method*) [65] illustre bien cette approche.

Par la suite, s'agissant du modèle linéaire ou non linéaire d'un accident, la modélisation et la simulation du comportement d'une barrière de sécurité dans une séquence accidentelle permettent l'évaluation de la performance de la défense en profondeur. En littérature, de nombreuses techniques ont été proposées pour mettre en œuvre l'évaluation des performances de la défense en profondeur, telles que l'analyse des couches de protection (LOPA) [66] et l'arbre d'événements (ADE) [67] lorsque l'on considère le modèle linéaire, ainsi que l'arbre de défaillance (ADD) [68] et la simulation de Monte Carlo [69] dans le cas d'un modèle non-linéaire.

1.3.1.3.1.4. Système instrumenté de sécurité (SIS)

Un SIS est une barrière technique de sécurité composée d'éléments de détection (entrée), d'un solveur logique et d'actionneurs (éléments finaux) [70]. Les figures 1.4 et 1.5 illustrent la composition typique d'un SIS.

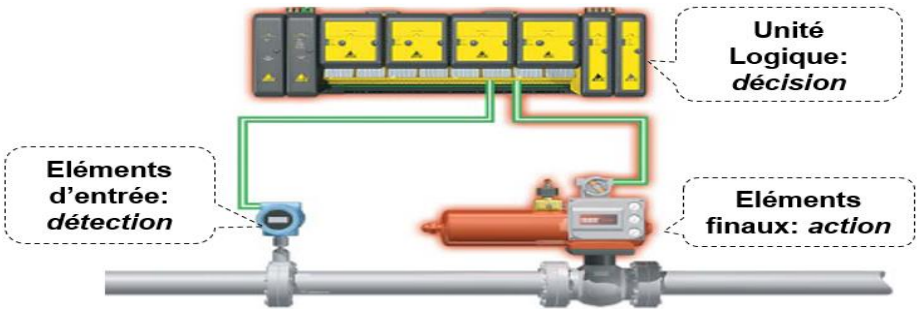


Figure 1.4 : Configuration basique d'un SIS

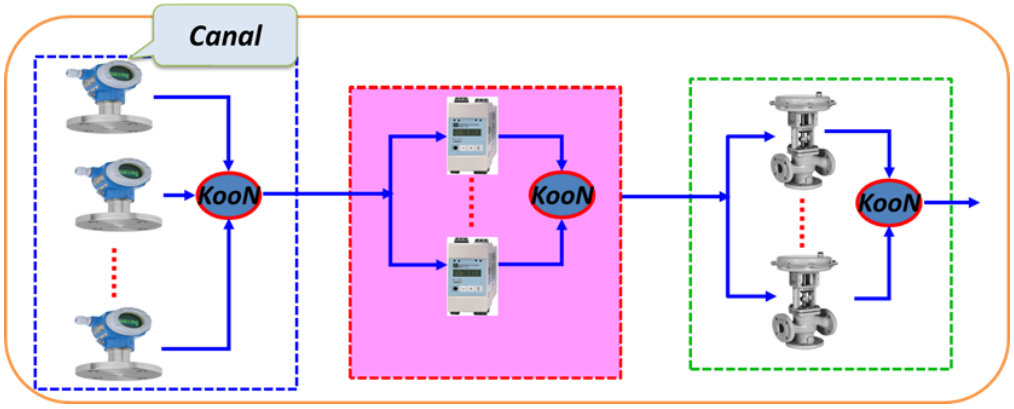


Figure 1.5 : Configuration redondante d'un SIS

Dans une boucle SIS, l'information suit un cheminement organisé en trois étapes principales :

1. ***Acquisition de l'information (capteurs/détecteurs) :*** la boucle commence par des capteurs placés dans l'installation.
   - Leur rôle est de surveiller en permanence des paramètres critiques du procédé : pression, température, débit, niveau, présence de flamme ou de gaz dangereux.
   - Ces capteurs traduisent la grandeur mesurée en un signal électrique (analogiques : une variation continue de tension (ex: 0-10 V) ou de courant (4-20 mA), binaires (TOR : la présence ou l'absence d'une tension (ex: 24 V)) ou numérique (capteur intelligent : HART)), optique ou radio (onde électromagnétique).
   - Le signal est envoyé via câble en cuivre ou fibre optique ou radio (onde électromagnétique) directement à l'automate (point-à-point) ou via un réseau de communication industriel (PROFIBUS, Ethernet/IP) de types câble en cuivre ou fibre optique ou radio.
2. ***Traitement et décision (automate) :*** les signaux envoyés par les capteurs arrivent ensuite à un automate (le « cerveau » du SIS).
   - Cet automate compare les valeurs mesurées avec des seuils de sécurité prédéfinis.
   - Il applique une *logique de décision* programmée, par exemple à l'aide d'une matrice cause–effet ou de langages fonctionnels tels que le FBD (Function Block Diagram). (Exemple : *si deux détecteurs de gaz voisins sont en alarme, alors déclencher la fermeture des vannes de la zone*.)
   - Si une condition dangereuse est confirmée, l'automate envoie immédiatement un ordre d'action.
3. ***Exécution de l'action (actionneurs)*** **:** l'ordre de l'automate est transmis à un ou plusieurs actionneurs, c'est-à-dire les éléments qui agissent physiquement sur l'installation.

- Exemple : une vanne de sécurité se ferme pour isoler une ligne, un compresseur est arrêté, un brûleur est coupé, des alarmes sonores/visuelles sont déclenchées.
- L'objectif est toujours de *mettre l'installation dans un état sûr* en un minimum de temps.

Les principaux types de SIS retrouvés dans l'industrie pétrolière et gazière sont : le système feux et gaz (FGS), le système d'arrêt d'urgence (ESD) et Système de commande et de régulation du procédé (BPCS).

1.3.1.3.1.4.1. Fonction (SIF)

- *Fonction de sécurité* : fonction destinée à atteindre ou à maintenir un état de sécurité, par rapport à un événement dangereux spécifique [71].
- *Fonction Instrumenté de sécurité :* est une *action automatique* réalisée par le SIS pour atteindre ou maintenir un état sûr pour un procédé industriel face à des conditions de fonctionnement spécifiques et dangereuses [72].

La fonction principale du SIS dans l'industrie pétrolière et gazière est de détecter les situations dangereuses (haute pression, fuite de gaz, etc.) pouvant conduire à un accident (incendie, explosion, etc.), puis de mettre en œuvre un ensemble de réactions nécessaires à la sécurité de l'Equipement Sous Contrôle (EUC).

1.3.1.3.1.4.2. Performance (SIL)

La performance probabiliste du SIS (disponibilité du SIS) correspond à la mesure de sa capacité à accomplir sa fonction (SIF). L'évaluation de la performance du SIS fait l'objet principal de cette section. Selon la norme IEC61508, l'évaluation de la disponibilité du SIS revient à évaluer l'indisponibilité du SIS (probabilité de défaillance) puis à déduire le niveau d'intégrité de sécurité (SIL). La norme CEI 61508 spécifie deux mesures de la non-disponibilité, en fonction de la fréquence à laquelle le SIS est sollicité pour répondre à des événements dangereux : la probabilité moyenne de défaillance dangereuse à la demande (PFD_{avg}) et la fréquence moyenne de défaillance dangereuse (PFH). La première mesure est adaptée aux SIS sollicités 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 correspondance entre les niveaux SIL, les indicateurs ci-dessus est présentée dans le Tableau 1.2.

Tableau 1.2 : Niveaux de SIL en fonction de PFD_{avg} et PFH [73]

SIL	PFD_{avg}	PFH $(h)^{-1}$
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

La quantification des deux mesures précédentes (PFD_{avg} et PFH) nécessite la prise en compte de plusieurs paramètres : les taux de défaillances ($\lambda = \lambda_D + \lambda_S$), la couverture de diagnostic (DC), intervalles et type de tests périodiques (complets et partiels) (T), le temps de réparation (MTTR), et les défaillances de cause commune (CCFs : Common Cause Failures), tout en prenant en compte l'architecture ou configuration du système (nombre d'éléments utilisés et leur logique de vote, KooN : K-sur-N). Ces paramètres peuvent être fournis par le fabricant (tels qu'Emerson, Schneider Electric, Yokogawa, Honeywell ou Siemens) ou issues de bases de données génériques, notamment le PDS Data Handbook et l'Exida SERH.

Pour réaliser ces calculs, la norme CEI 61511 fournit des formules analytiques simplifiées qui sont valables sous certaines hypothèses [74]. De plus, plusieurs formules simplifiées peuvent être trouvées dans la littérature [75–77]. Il convient de noter que ces calculs peuvent également être effectués en utilisant des méthodes quantitatives classiques, telles que l'analyse par arbre de défaillance, les chaînes de Markov et les réseaux de Petri [78], ainsi qu'en utilisant des logiciels de calcul automatique tels que GRIF (GRaphical Interface for reliability Forecasting) [79], IMS SIS (Integrity Management Solutions of Safety Instremented System), exSILentia, SILver, SIS-TECH SOLVER, SILCalc, etc.

1.3.2. Techniques utilisées à chaque étape du processus de gestion des risques

La gestion des risques peut être réalisée de plusieurs manières, selon la qualité des informations et des données collectées sur le système. Il est préférable de choisir des techniques de gestion des risques adaptées à l'entreprise et à ses activités. Dans ce contexte, de nombreuses techniques de gestion des risques ont été développées. Chaque étape du processus de gestion des risques a ses techniques spécifiques ; nous allons présenter HAZOP pour l'étape d'analyse qualitative du risque, LOPA et ALOHA pour l'étape d'analyse quantitative du risque, ALARP et la matrice des risques pour l'étape d'évaluation du risque, et IEC 61508 pour l'étape de réduction du risque. Le choix de ces méthodes est approprié pour notre étude de cas. La combinaison de ces techniques construit une approche bien structurée et efficace, notamment pour l'industrie du pétrole et gaz.

1.3.2.1. Techniques d'analyse des risques

1.3.2.1.1. HAZOP (Hazard and Operability Study)

La méthode HAZOP (*Hazard and operability study*) a été développée par la société Imperial Chemical Industries (ICI) au début des années 1960. Elle a depuis été adaptée dans différents secteurs d'activité. Considérant de manière systématique les dérives des paramètres d'une installation en vue d'en identifier les causes et les conséquences, cette méthode est particulièrement utile pour l'examen de systèmes thermo-hydrauliques, pour lesquels des paramètres comme le débit, la température, la pression, le niveau, la concentration sont particulièrement importants pour la sécurité de l'installation. On s'intéresse à l'influence des déviations par rapport aux valeurs nominales des divers paramètres physiques régissant le procédé [80].

Une caractéristique fondamentale de la méthode est sa mise en œuvre en équipe pluridisciplinaire sous la direction d'un animateur. Pour stimuler le « processus de réflexion créative » des mots clés, représentant des déviations par rapport aux valeurs nominales, sont utilisés : plus, moins, pas, etc. Les déviations de chaque paramètre d'intérêt (pression, température, débit, etc.) sont passées en revue l'une après l'autre afin de mettre en évidence leurs causes, leurs conséquences, les moyens de détection et les actions correctrices (automatiques ou manuelles) nécessaires lorsqu'une déviation dangereuse a été détectée [80].

Les phases de l'étude HAZOP sont présentées dans l'organigramme de la Figure 1.6.

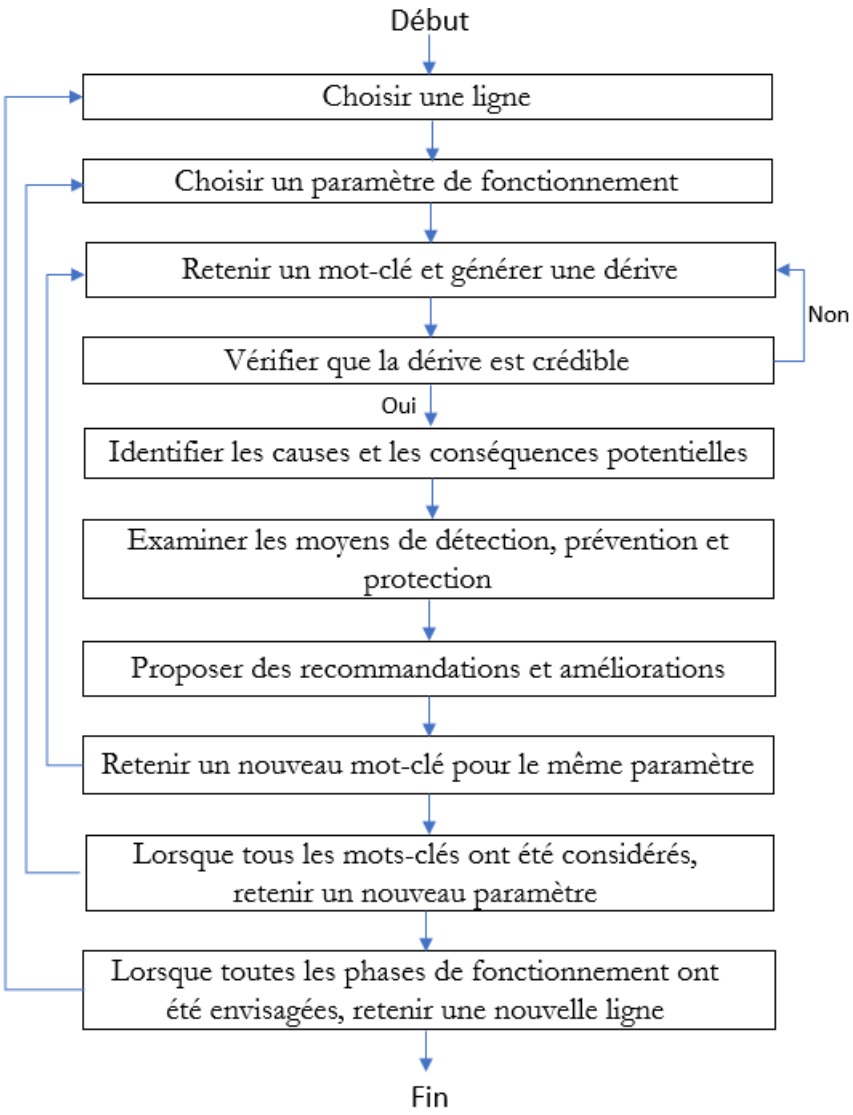


Figure 1.6 : Phases de l'étude HAZOP

1.3.2.2. LOPA (Layer of Protection Analysis)

L'analyse des couches de protection (LOPA) est une méthode quantitative (semi-quantitative) couramment utilisée en analyse des risques dans les industries de procédés. Elle permet d'estimer la fréquence d'occurrence des accidents potentiels. La méthode s'appuie sur les données issues de l'analyse qualitative des risques (généralement l'étude HAZOP) et prend en compte chaque risque identifié en documentant les événements initiateurs et les couches de protection indépendantes (IPLs) qui peuvent empêcher le scénario de se produire et de s'aggraver (voir Figure 1.7) [81].

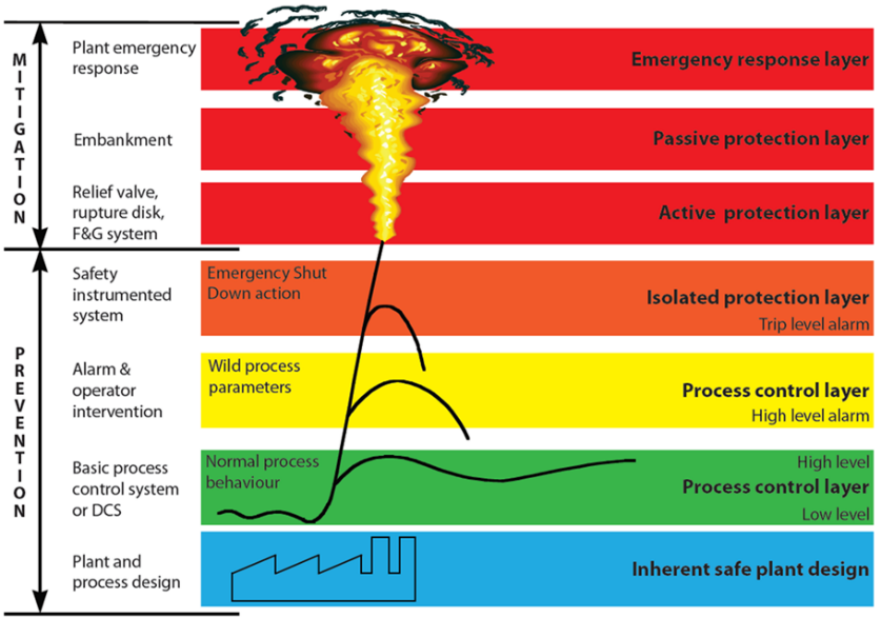


Figure 1.7 : Analyse des couches de protection (LOPA) [82]

Son principe est d'estimer la fréquence des accidents (événements d'impact) à travers la quantification des fréquences des événements initiateurs, et des probabilités de défaillance à la demande de chaque couche de protection.

La fréquence du scénario d'accident est obtenue en multipliant la fréquence de l'événement initiateur par les probabilités moyennes de défaillance à la demande (PFD_{avg}) de chaque IPL s'opposant à ce même événement [83].

$$f^c = f^{IE} \times \prod_i PFD_{avg}^i \qquad (1.2)$$

Où,

- f^c: fréquence d'occurrence d'accident,
- f^{IE}: fréquence d'occurrence de l'événement initiateur,
- PFD_{avg}^i : probabilité moyenne de défaillance sur demande de la barrière i.

Il convient de soulever un point important concernant les limites de la LOPA par rapport à l'analyse par arbre de défaillance (AdD) dans l'analyse de fréquence des accidents :

- Limites de LOPA :
  - Utilise des valeurs de probabilité génériques qui ne tiennent pas compte des détails spécifiques du système.
  - Traite les couches de protection comme indépendantes, ce qui peut ne pas refléter la réalité.

- Ne pas pouvoir modéliser les interactions complexes entre les composants.

- Avantages de l'AdD :
  - Modélise certaines interactions et dépendances des composants.
  - Prend en compte des taux de défaillance et des délais de réparation spécifiques.
  - Permet l'analyse de la redondance et des défaillances de cause commune.
  - Fournit des calculs de probabilité plus précis grâce à la logique booléenne.
  - Permet l'analyse de sensibilité de différentes combinaisons de défaillances.

1.3.2.3. ALOHA (Areal Locations of Hazardous Atmospheres)

Le logiciel ALOHA (Areal Locations of Hazardous Atmospheres) est le programme de modélisation des risques de la suite logicielle CAMEO® (Computer-Aided Management of Emergency Operations), largement utilisée pour la planification et la réponse aux urgences chimiques. ALOHA permet de saisir des informations sur un rejet chimique réel ou potentiel, puis de générer des estimations des zones de menace pour différents types de risques. ALOHA peut modéliser le BLEVE (Boiling Liquid Expanding Vapor Explosions), le VCE (Vapor Cloud Explosions), les feux de jet, les feux en nappe, les nuages de gaz toxiques et les nuages de gaz inflammables. Les estimations des zones de menace sont affichées sur une grille dans ALOHA et peuvent également être cartographiées dans MARPLOT® (Mapping Application for Response, Planning, and Local Operational Tasks), ArcMap d'Esri, Google Earth et Google Maps. La zone de menace rouge représente le niveau de gravité le plus élevé, tandis que les zones orange et jaune représentent les zones de gravité décroissante [84].

L'approche du logiciel ALOHA dans l'estimation des conséquences d'un scénario d'accident est la suivante :

1. Identification des phénomènes dangereux : il s'agit de recenser les événements pouvant provoquer des conséquences graves. Par exemple, une fuite de gaz inflammable, une explosion, un incendie ou une émission toxique.
2. Caractérisation du scénario accidentel : cela inclut la description des conditions dans lesquelles le phénomène dangereux pourrait se produire, telles que :
   - Les propriétés physico-chimiques du produit impliqué.
   - Les conditions de rejet (débit, durée, conditions de pression/température, instantané, continu…).
   - Les paramètres environnementaux (vent, température, humidité).
   - Les caractéristiques de l'installation (volume de stockage, pression).

3. Modélisation physique : utiliser des modèles mathématiques ou des outils de simulation pour prédire les effets physiques du phénomène, comme :
    - Les surpressions générées par une explosion.
    - Les flux thermiques produits par un incendie.
    - Les concentrations atteintes dans le cas d'une dispersion toxique.
4. Détermination des zones d'effets :
    - Utilisation des seuils réglementaires (létalité, effets irréversibles...)
    - Cartographie des zones d'impact
    - Calcul des distances d'effets
5. Evaluation des effets sur les cibles : étudier les conséquences pour les populations, les équipements, ou l'environnement à partir des données d'impact. Cela inclut :
    - Les courbes de vulnérabilité ou relations dose-effet.
    - Les seuils réglementaires pour la santé et la sécurité.

1.3.2.2. Techniques d'évaluation des risques

1.3.2.2.1. ALARP (As Low As Reasonably Practicable)

Le principe ALARP « As Low As Reasonably Practicable » reconnaît qu'il existe trois grandes catégories de risques [85] (voir Figure 1.8):

1. ***Risque acceptable*** : le niveau de risque est considéré comme négligeable et ne nécessite pas d'actions supplémentaires.
2. ***Risque tolérable*** : nous préférerions ne pas courir le risque, mais il est tolérable compte tenu des avantages obtenus en l'acceptant. Le risque est tolérable si le coût nécessaire à l'investissement de la mesure proposée (recommandation) est supérieur au coût de la perte potentielle. Le coût en inconvénients ou en argent est mis en balance avec l'ampleur du risque et un compromis est accepté (analyse coût-bénéfice).
3. ***Risque inacceptable*** : le niveau de risque est si élevé que nous ne sommes pas prêts à le tolérer. Les pertes dépassent de loin tous les avantages possibles de la situation.

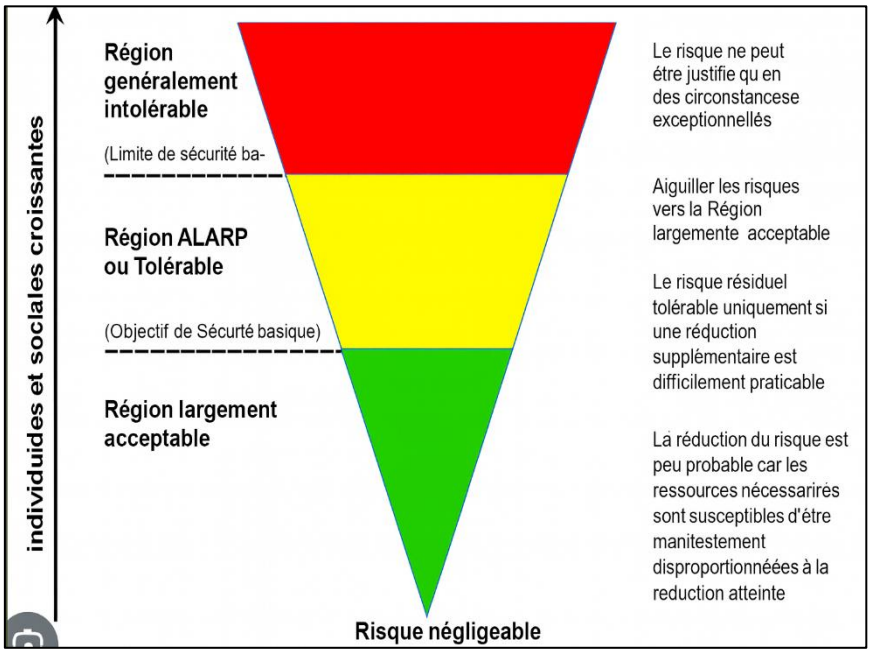


Figure 1.8 : Modèle ALARP [86].

L'un des aspects difficiles de la mise en œuvre du principe ALARP consiste à définir les trois niveaux de risque. Ce principe guide essentiellement l'ingénieur concepteur et le spécialiste de la sécurité dans la définition des objectifs de risque tolérable pour une situation dangereuse. Il s'agit de la première étape de l'établissement d'une norme de performance pour tout système de sécurité.

1.3.2.2.2. Matrice des risques

La matrice des risques est un outil d'analyse qui évalue la gravité d'un risque par rapport à la probabilité qu'il se réalise [87]. Elle met en avant le degré d'impact de chaque risque (déterminer les niveaux de risque). Les matrices de risques ont toutes la même structure de base. Il s'agit généralement de grilles de 5 x 5 qui indiquent la probabilité que les risques se produisent sur l'axe Y et la gravité de leurs conséquences sur l'axe X. Chaque axe suit une échelle allant de très faible, à très élevé. Les risques auxquels l'entreprise pourrait être confrontée sont placés dans la matrice des risques en fonction de leur position sur cette échelle. Cela permet de déterminer les niveaux de risque : *Probabilité* × *Conséquence* = *Niveau de risque*.

Si le risque est élevé sur l'échelle de probabilité et élevé sur l'échelle de conséquence, le niveau de risque peut être défini comme très élevé. Inversement, si le risque est faible sur l'échelle de probabilité et faible sur l'échelle des conséquences, le niveau de risque sera très faible. Dans une matrice des risques, les niveaux de risque sont mis en évidence par un système

de codes de couleur. Un risque dont le niveau de risque global est faible est indiqué par un code couleur vert. S'il est moyen, il est représenté en jaune ou en orange. Un risque globalement élevé est représenté en rouge. Ce système de feux tricolores permet de comprendre rapidement en un coup d'œil les niveaux de risque.

Malgré cette structure de base, les matrices de risques peuvent varier considérablement en fonction de l'entreprise et de la manière dont elles sont utilisées. En effet, la matrice des risques est établie selon le principe ALARP.

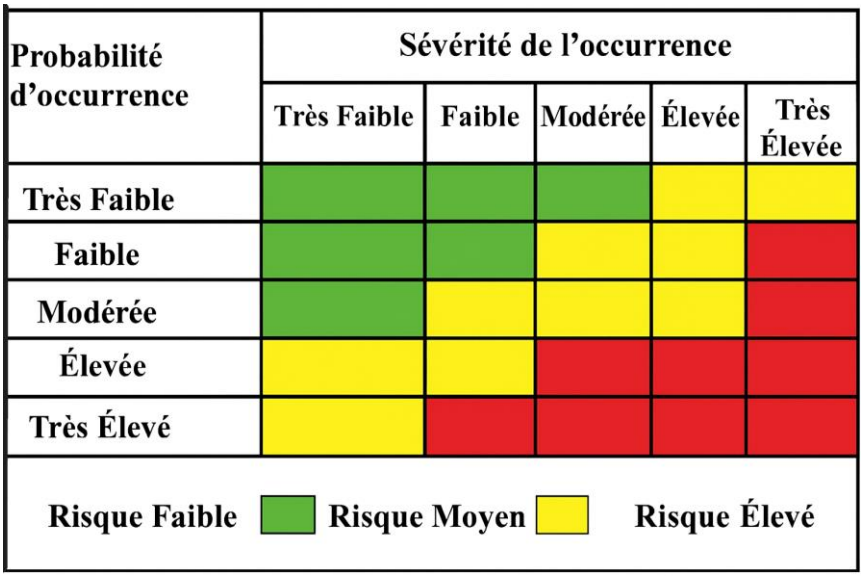


Figure 1.9 : Matrice des risques

1.3.2.3. Techniques de réduction des risques

1.3.2.3.1. Technique de la norme IEC 61508

Les techniques de réduction des risques consistent à optimiser les performances des barrières de sécurité existantes ou à en ajouter de nouvelles. Pour être efficaces, ces techniques ne doivent pas être aléatoires : elles doivent être conçues méthodiquement afin de répondre aux exigences de sécurité (niveau de risque tolérable). La norme IEC 61508 a été élaborée comme une norme axée sur la performance, dans le but d'encadrer la conception et le fonctionnement des SIS afin de garantir leur capacité à réduire les risques associés au processus protégé à un niveau tolérable défini.

La norme CEI 61508 fournit une technique structurée, reposant sur l'analyse et l'évaluation des risques, pour déterminer le niveau de fiabilité requis pour les SIS afin de maîtriser ces risques. Elle vise à concevoir et à exploiter les SIS avec une fiabilité répondant à ces exigences [88]. Le schéma de la technique IEC 61508 est présenté à la Figure 1.10.

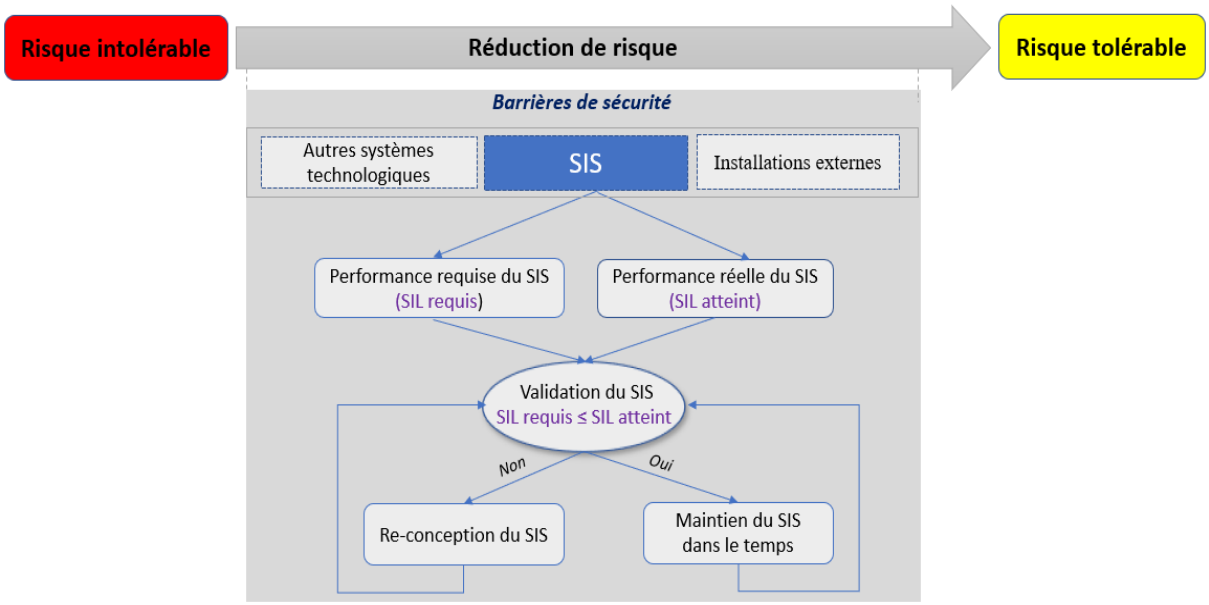


Figure 1.10 : Technique de réduction du risque de la norme IEC 61508

Cette norme laisse à l'utilisateur le soin de réaliser son analyse et évaluation de risque et lui offre les moyens de réduire ce risque.

1.3.2.3.1.1. Allocation de la performance requise du SIS (SIL requis)

Il s'agit du niveau de fiabilité minimale que le SIS doit atteindre pour remplir sa fonction de réduction des risques avec une confiance satisfaisante, et ainsi maintenir le risque à un niveau tolérable. La norme IEC 61511 décrit plusieurs méthodes d'allocation du SIL requis [89, 90]. Certaines sont de type qualitatif (le graphe de risque, la grille de criticité, etc.) basées sur la combinaison de plusieurs paramètres de risque, et d'autres sont quantitatives (LOPA) consistant à quantifier la PFD_{avg} ou la PFH requises, puis à déterminer le SIL correspondant en se référant au Tableau 1.2.

1.3.2.3.1.2. Détermination de la performance réelle du SIS (SIL atteint ou achevé)

Il s'agit de la fiabilité réelle du SIS (conçu ou existant) dans l'exécution de sa fonction. Plusieurs méthodes de détermination de ce SIL sont présentées dans le paragraphe (1.3.1.3.1.4.2).

1.3.2.3.1.3.Validation du SIS

Cela consiste à comparer le SIL atteint au SIL requis. Si le SIL atteint est inférieur au SIL requis, le SIS doit être reconçu de manière que le SIL atteint soit égal ou supérieur au SIL requis. Si le SIL atteint est supérieur ou égal au SIL requis, on considère que ce SIS satisfait aux exigences de sécurité qui lui sont associées, et il convient alors de le maintenir dans le temps.

1.3.2.3.1.4. Re-conception du SIS

Pour améliorer la fiabilité de SIS pour que (SIL atteint ≥ SIL requis), des modifications doit être porter sur le SIS qui peuvent inclurent :

- Le choix des éléments constitutifs du SIS.
- Architecture du system (nombre d'éléments utilisés et leur logique de vote).
- La maintenance des éléments constitutifs du SIS (stratégie des tests périodique, stratégie de réparation, etc.).

Il convient de noter que ces modifications influent sur les paramètres liés à la fiabilité du SIS : λ, DC, T, MTTR, CCFs.

1.3.2.3.1.5. Maintien du SIS dans le temps

Un programme rigoureux de maintenance de SIS (stratégie des tests périodique, stratégie de réparation, etc.) est nécessaire pour maintenir le SIL du SIS dans le temps. Ce programme doit faire partie du plan de management de la sécurité fonctionnelle.

1.4. Conclusion

L'objectif de ce chapitre était de présenter le processus de gestion des risques industriels et ses techniques associées, en mettant en évidence la complémentarité entre les normes IEC 31010 et IEC 61511. L'intégration des référentiels ISO 31000 et IEC 61508 apparaît non seulement possible, mais également complémentaire dans le cadre du management des risques industriels. L'ISO 31000, en tant que norme générique, fournit les fondements et les techniques méthodologiques nécessaires à l'identification, l'analyse et l'évaluation des risques. Cette approche permet de distinguer les risques acceptables de ceux qui demeurent intolérables. Pour ces derniers, l'apport de l'IEC 61508 se révèle déterminant. En effet, cette norme propose des prescriptions techniques précises pour la réduction des risques résiduels, notamment à travers la mise en œuvre de systèmes instrumentés de sécurité et la détermination du niveau d'intégrité requis (SIL requis). Dès lors, l'articulation de ces deux référentiels offre une démarche cohérente, allant de l'évaluation globale des risques à leur réduction effective par des moyens techniques adaptés. Cette démarche structurée constitue une base solide pour la phase d'application pratique qui sera développée dans le chapitre suivant, dédiée à l'étude de cas portant sur un système réel de gestion des risques industriels.

Chapitre 2

Application industrielle : mise en œuvre du processus de gestion des risques industriels

2.1. Introduction

Ce chapitre illustre une application pratique du cadre méthodologique développé dans le chapitre précédent, à travers une étude de cas portant sur un réservoir de stockage de butane à la raffinerie RA2K. Il met particulièrement l'accent sur la mise en œuvre de la technique prescrite par la norme IEC 61508, utilisée dans la phase finale du processus de gestion des risques que nous proposons.

2.2. Description de l'étude de cas : « Sphère de stockage de butane 305-TK-002 »

Avant chaque élaboration d'une analyse de risque, il est d'abord nécessaire de décrire les différentes dimensions (processus, système de contrôle, système de sécurité, etc.) liées au système à étudier. Dans cette étude, le système concerné est une sphère de stockage de butane (cf. Figure 2.1) appartenant à la section de stockage de butane d'une raffinerie de condensats (RA2K) située à Skikda-Algérie.

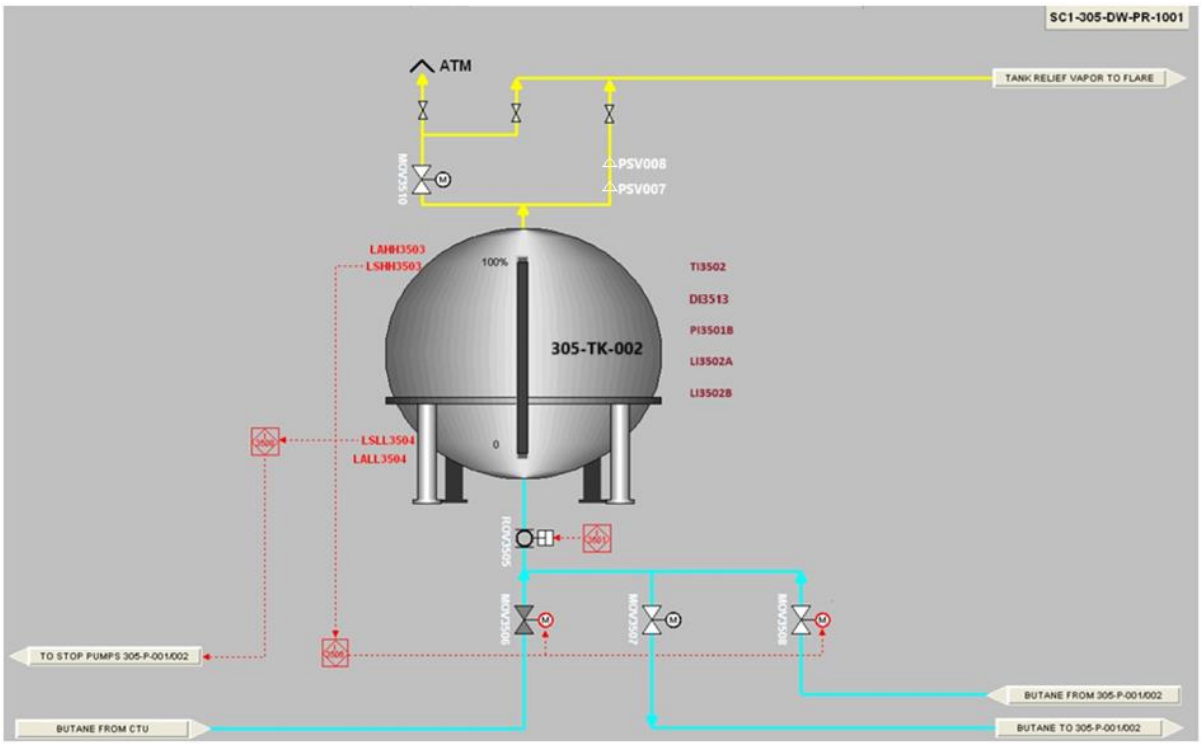


Figure 2.1 : Sphère de stockage de butane 305-TK-002

Les données techniques de cette sphère et les caractéristiques de butane sont présentées dans les Tableaux 2.1 et 2.2 [91].

Tableau 2.1 : Données techniques de la sphère 305-TK-002

Nom de tag	305-TK-002
Conçu par	The petrochemical equipment factory of CPFCC
Pression de conception	8,71 Bar
Température de conception	65 C°
Capacité	1767 m^3
Fluide de service	Butane
Poids total à vide	184900 Kg
Pression de test d'épreuve	13,1 Bar
Matériau	ASTM A516 Gr 70 Acier au carbone pour récipients sous pression selon la norme ASTM, Grade 70

Tableau 2.2 : Caractéristiques du butane

Formule chimique	C_4H_{10}
Point Eclair	<-50 °C
Temp. Auto Inflammation	287 °C
Limite Inferieure d'explosivité LIE	1,8 %
Limite Supérieure d'explosivité LSE	8,8 %
Temp ébullition	0 °C
Tension Vapeur	1.7 à 15°C
Etiquetage	
Phrase de risque	H220, H280 H220 : Gaz extrêmement inflammable. H280 : Contient un gaz sous pression ; peut exploser sous l'effet de la chaleur.

La sphère est équipée de lignes, des vannes, des pompes, un système de contrôle et de sécurité pour la réception, le stockage et l'expédition de butane.

- ***Procédé***

La sphère 305-TK-002 reçoit le butane en provenance de l'unité de topping de condensat (CTU) par une ligne d'entrée équipée de la vanne motorisée MOV3506. La sortie de la sphère est connectée au collecteur d'aspiration des pompes d'expédition de butane (305-P-001/002) via la vanne MOV3507. Le collecteur de décharge des pompes (305-P-001/002) envoie le butane vers le système de comptage pour transfert (*custody transfer metering*) ou le recycle vers les réservoirs via la vanne MOV3508 lorsque le débit dans le collecteur chute en dessous

d'une limite prédéfinie. De plus, les pompes peuvent assurer une circulation de butane de réservoir à réservoir à travers un autre collecteur de décharge [92].

- ***Système de contrôle et de sécurité***

Le réservoir est équipé d'un système de contrôle et de sécurité qui permet de mesurer le niveau, la pression et la température, ainsi que de maîtriser toute déviation de ces paramètres pouvant entraîner des accidents. Plus de détails concernant les fonctionnalités de ce système sont donnés dans ce qui suit.

Un indicateur de pression (PI3501B) est installé au sommet de la sphère. Il est relié au système de contrôle distribué (DCS) via un transmetteur de pression (PT3501B), afin de transmettre l'indication de pression de la sphère. Lorsque la pression du réservoir dépasse la limite haute prédéfinie, une pré-alarme est déclenchée afin d'alerter les opérateurs. Le côté vapeur de la sphère est équipé de deux soupapes de sécurité (PSV007 et PSV008), réglées à des pressions de décharge de 0,87 MPa(g) et 0,915 MPa(g), respectivement. De plus, une vanne motorisée (MOV3510) est installée sur la sphère, qui peut être ouverte manuellement par l'opérateur en cas d'urgence, soit via un bouton-poussoir sur site, soit à distance depuis le DCS, afin de relâcher la pression du réservoir. La sortie de la vanne MOV3510 est reliée à la torche, ainsi qu'à un évent permettant d'évacuer la surpression vers l'atmosphère à un emplacement sécurisé. Ce dispositif assure que, même en cas de défaillance de la torche, la pression dans la sphère puisse être relâchée en toute sécurité [92].

Deux indicateurs de niveau de butane (LI3502A et LI3502B) sont installés au sommet de la sphère. Ils sont connectés au DCS via deux transmetteurs (LT3502A et LT3502B), permettant la surveillance du niveau de butane aussi bien localement qu'en salle de contrôle (salle DCS). Deux switches de niveau de butane (LSLL3504 et LSHH3503) sont installés respectivement en bas et en haut de la sphère. Ils sont connectés au DCS pour contrôler les niveaux très bas et très hauts de butane dans la sphère. Lorsque le niveau du réservoir descend en dessous de la limite basse prédéfinie, une pré-alarme est déclenchée pour alerter les opérateurs. Si le niveau descend en dessous de la limite très basse prédéfinie, le système DCS enverra un signal d'interdiction pour fermer toutes les pompes en opération (305-P-001/002) et activera une alarme. Lorsque le niveau du réservoir dépasse la limite haute, une pré-alarme sera déclenchée pour alerter les opérateurs. Si le niveau dépasse la limite très haute, le système DCS enverra des signaux d'interdiction pour fermer toutes les vannes motorisées d'entrée du réservoir (MOV3506 et MOV3508) et activera une alarme [92].

La soupape d'urgence (ROV3505) est installée à l'entrée (respectivement à la sortie) de la sphère. En appuyant sur le bouton poussoir PB-3501 du DCS ou sur le bouton poussoir local PB3501A situé dans le secteur du parc de stockage, la ROV3505 se ferme et les pompes (305-P-001/002) sont arrêtées, isolant ainsi la sphère de la réception (respectivement du transfert) de liquide. Cette soupape sert de dispositif ESD (soupape de fermeture d'urgence) pour isoler la sphère, protégeant ainsi le réservoir contre le sur-remplissage et le vidange, et protégeant également la pompe contre les dommages en cas de fonctionnement à sec.

De plus, un thermomètre à points multiples (TI3502) est installé pour l'indication de la température dans la sphère. Le signal de température est transmis au DCS via un transmetteur (TT3502) [92].

2.3. Processus de gestion du risque de BLEVE lié à la sphère

Afin de maîtriser le risque de BLEVE associé à la sphère 305-TK-002, un processus de gestion du risque structuré en quatre étapes successives sera mis en œuvre, comme illustré dans le diagramme de la Figure 2.2 [93, 94].

2.3.1. Analyse qualitative du risque BLEVE à l'aide de l'HAZOP

- ***Description du phénomène de BLEVE***

BLEVE (*Boiling Liquid Expanding Vapour Explosion*) est un type d'explosion provoqué par une augmentation brutale de la pression à l'intérieur d'un réservoir, à la suite d'un dégagement de vapeur par un liquide inflammable en ébullition (vaporisation non contrôlée). La forte pression du gaz exercée sur le réservoir (P gaz >> P atmosphère) provoque la rupture du réservoir et la détente très rapide de gaz dans l'atmosphère en feu (boule de feu à effet thermique), ce qui conduit au phénomène d'ébullition-explosion [95]. Le scénario du BLEVE est illustré dans la Figure 2.3.

Etape 1 : Analyse qualitative du risque

Objectif : Identifier les événements dangereux ou les enchaînements d'événements dangereux (scénarios) pouvant conduire à un risque BLEVE

Description de risque BLEVE	Identification des scénarios de risque BLEVE par la méthode HAZOP

↓

Etape 2 : Analyse quantitative du risque

Objectif : Quantifier le risque BLEVE en termes de probabilité et gravité

Quantification de la fréquence d'occurrence de risque BLEVE par la méthode LOPA	Quantification de la gravité des conséquences de risque BLEVE par logiciel ALOHA

↓

Etape 3 : Évaluation du risque

Objectif : Vérifier l'acceptabilité du risque BLEVE

Comparaison de niveau de risque quantifié (estimé) à un niveau jugé tolérable par l'entreprise RA2K en utilisant la matrice des risques de RA2K

↓

Etape 4 : Réduction du risque

Objectif : Réduire le niveau de risque à un niveau tolérable

Détermination de la performance que le SIS doit avoir (SIL requis) pour réduire le risque BLEVE au niveau tolérable prédéterminé en utilisant la méthode LOPA	Détermination de la performance réelle de SIS proposé (SIL réelle) en utilisant les formules PFD de la normes IEC61508 et logiciel GRIF, puis la vérification de sa capacité d'atteindre la réduction de risque requise	Optimisation de la performance réelle de SIS (SIL réelle) pour plus de sécurité

Figure 2.2 : Processus de gestion du risque de BLEVE

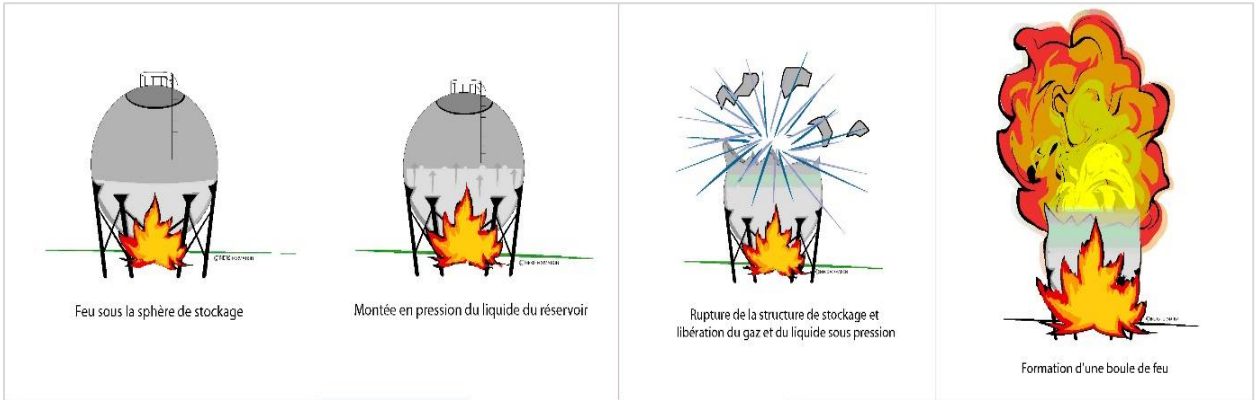


Figure 2.3 : Développement du scénario de BLEVE

Il faut noter qu'il y'a un type spécifique de BLEVE provoqué par une augmentation brutale de la pression à l'intérieur d'un réservoir sans ébullition de produit contenant dans le réservoir. La forte pression du gaz exercée sur le réservoir (P gaz >> P atmosphère) provoque la rupture du réservoir et la détente très rapide de gaz dans l'atmosphère sans feu (onde de pression à effet de souffle), c'est le BLEVE froid.

- ***Identification des scénarios du risque de BLEVE***

L'usage de l'HAZOP a permis d'identifier les scénarios de BLEVE potentiels associés à la sphère 305-TK-002. Un extrait de l'HAZOP relatif à la déviation « pression élevée dans la sphère » est donné au Tableau 2.3.

Tableau 2.3 : Etude HAZOP pour « pression élevée dans la sphère »

Déviation		**Causes**	**Conséquences**	**Actions et moyens de sécurité**	**Recommandations**
Paramètre	**Mot-clé**				
Pression	Haute	- Une agression thermique (feu de torche, feu de nappe)	- BLEVE chaud	- Dépressurisation par PSVs (PSV3509A et PSV3509B) et MOV3510 - Refroidissement par système de Déluge - Isolation thermique et résistance des matériaux de la sphère	- Automatisation de la dépressurisation de la sphère en intégrant le capteur (PI 3501B), le PLC et la vanne (MOV 3510) dans une boucle (SIS) - Installation d'un disque de rupture
		- Le sur remplissage du réservoir	- BLEVE froid	- Coupure d'alimentation par MOV3506 et MOV3508 (interlock 3506) - Isolation de la sphère par ROV3505 (interlock 3501) - Résistance des matériaux de la sphère (acier carbone)	- La rigueur dans l'application du programme d'inspection et de test de la résistance des matériaux de la sphère
		- Défaillance mécanique (choc, corrosion, fatigue)		- Dépressurisation par PSVs (PSV3509A et PSV3509B) et MOV3510 - Résistance des matériaux de la sphère (acier carbone)	

Dans ce qui suit, on va aborder le scénario BLEVE le plus courant, à savoir le BLEVE chaud.

2.3.2. Analyse quantitative du risque BLEVE à l'aide de LOPA et ALOHA

Comme évoqué précédemment, l'analyse quantitative du risque sert à estimer le niveau de risque en quantifiant ses deux paramètres : la probabilité d'occurrence et la gravité des conséquences.

- ***Quantification de la fréquence d'occurrence du risque de BLEVE à l'aide de LOPA***

Pour la quantification de la fréquence d'accident (BLEVE), la méthode LOPA requiert les données numériques relatives aux fréquences des causes initiatrices et aux probabilités de défaillance des couches de protection qui interviennent pour empêcher le développement de cette cause initiatrice. A cet effet, des valeurs génériques sont généralement disponibles dans la littérature [96, 97, 98]. Pour l'étude de cas considérée, nous nous référons à l'Eq. (1.2) et au référence [95] pour calculer la fréquence de l'accident BLEVE. Les résultats obtenus sont présentés dans le Tableau 2.4.

Tableau 2.4 : Résultats de la méthode LOPA

Eléments LOPA	**Description**	**Fréquence** (an^{-1})	**PFD**
Evènement initiateur	Feu à proximité de la sphère : l'agression thermique de la sphère par un feu de torche ou de nappe, etc. provoque une augmentation de la pression à l'intérieur de la sphère et une fragilisation du matériau constituant la sphère	10^{-1}	/
Couches de protection	Conception : la forme sphérique permet la diminution de la pression de la sphère en distribuant la pression à l'intérieur de la sphère au long du paroi de la sphère. Ainsi que le matériau constituant de la sphère qui lui permet de résister à la pression interne de la sphère et aux effets thermiques du feu	/	10^{-1}
	Alarme + action de l'opérateur : l'opérateur, averti par l'alarme PAH-3501B, ouvre la MOV3510 pour dépressuriser la sphère		10^{-1}
	PSVs : les deux soupapes de sécurité de pression (PSV3509A et PSV3509B) permettent de dépressuriser la sphère		2×10^{-2}
	Système déluge : système de refroidissement de la sphère pour abaisser de température de la sphère en cas de feu		10^{-1}
Accident	BLEVE	2×10^{-6}	/

- ***Quantification de la gravité des conséquences du risque de BLEVE à l'aide de ALOHA***

Afin de quantifier l'ampleur des conséquences, nous présentons ci-après les zones d'effets liés aux scenario BLEVE, obtenues à l'aide du logiciel ALOHA. Les données de calcul et les résultats sont présentés respectivement dans les Figures 2.4 et 2.5. Par ailleurs, les seuils des effets thermiques sur la vie humaine et sur les équipements sont respectivement présentés dans les Tableaux 2.5 et 2.6.

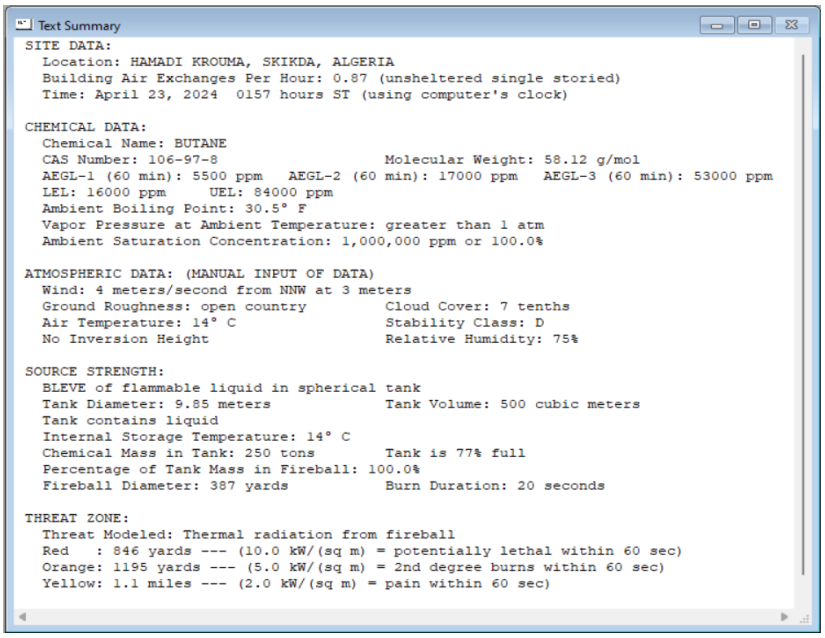


Figure 2.4 : Rapport de donnes et de résultats liées au phénomène de BLEVE

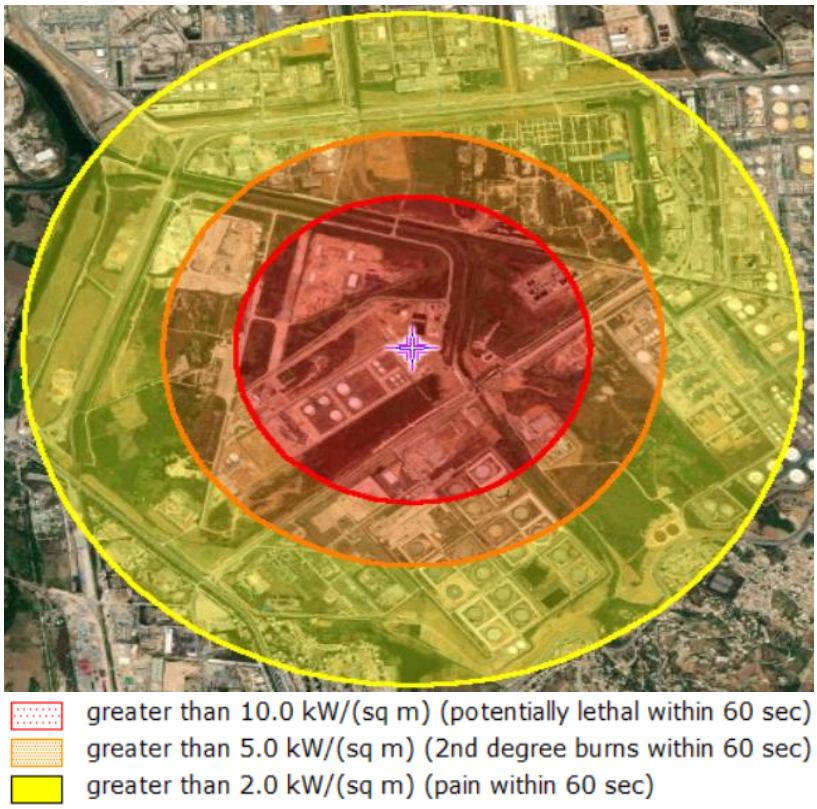


Figure 2.5 : Distances d'effets thermiques liées au phénomène de BLEVE

Tableau 2.5 : Seuils des effets thermiques sur la vie humaine [99]

Seuils	Description	Zone des effets
2.0 kW/m^2	Zones des dangers significatifs, pouvant provoquer des blessures irréversibles (douleurs en une vingtaine de secondes et brûlures au premier degré au bout d'une minute environ)	Délimite la zone des effets irréversibles
5.0 kW/m^2	Zone des dangers graves pour la vie humaine, pouvant conduire à la mort : provoque rapidement des douleurs chez l'homme (en quelques secondes) et des lésions mortelles (pendant plus de 60 secondes). Elle permet donc de déterminer une zone dans laquelle il est impératif de limiter l'implantation de constructions ou d'ouvrages concernant notamment les tiers. Les intervenants (pompiers) munis de vêtements ignifuges ne doivent pas dépasser cette zone.	Délimite la zone des effets létaux
10.0 kW/m^2	Zone des dangers conduisant potentiellement à 100% de décès sans possibilité de fuite ou de secours. Ce seuil permet de déterminer une zone dans laquelle toute présence humaine doit être limitée. Aucun poste fixe ne peut être occupé dans cette zone.	Délimite la zone des effets létaux très significatifs

Tableau 2.6 : Seuils des effets thermiques sur les équipements et structure [99]

Seuils	Description	Zone des effets
35 kW/m^2	Zone des effets dominos pour les équipements sous pression et les structures. Dans une approche prudente, et sans tenir compte de mesures de protection/refroidissement, 100% des infrastructures impactées par le seuil de 35kW/m^2 (5 min) sont considérées comme potentiellement détruites dans l'évaluation de la gravité sur les équipements.	Délimite la zone des effets dominos

Notes :

- Les effets missiles de BLEVE ne sont pas considérés comme quantifiables.
- Le BLEVE chaud ne présente pas un effet de surpression (onde de choc). L'énergie est majoritairement dissipée sous forme thermique (feu), réduisant la contribution de l'expansion physique à la surpression. Cas réels : les études montrent que les dommages dus à un BLEVE chaud proviennent surtout de la chaleur radiative et des projectiles, l'onde de pression restant souvent mineure (sauf cas extrêmes de confinement ou de très haute pression initiale).
- Le butane est un gaz non nocif à l'environnement et l'un des seuls gaz qui n'affecte pas la couche d'ozone.

2.3.3. Evaluation du risque de BLEVE à l'aide de la matrice des risques

Les résultats d'une analyse de risque doivent d'être comparés à des critères de risque afin de définir un plan d'action. Dans le cadre d'une étude de dangers de RA2K [100], ces critères sont définis par une matrice de risque (cf. Tableaux 2.10 et 2.11) et des échelles qui y sont

associées (cf. Tableaux 2.7, 2.8 et 2.9). Il importe de noter que SONATRACH ne possède pas de critères en termes de gravité environnementale pour les risques majeurs.

Tableau 2.7 : Echelle des probabilités d'occurrences annuelles

Probabilité	Description	Fréquence (/an)
E	**Possible mais extrêmement peu probable**. N'est pas impossible au vu des connaissances actuelles mais non rencontré au niveau mondial sur un très grand nombre d'années d'installations	$F < 10^{-6}$
D	**Très improbable**. S'est déjà produit dans ce secteur d'activité mais a fait l'objet de mesures correctives réduisant significativement sa probabilité	$10^{-5} > F > 10^{-6}$
C	**Improbable**. S'est déjà produit dans ce secteur d'activité ou dans ce type d'organisation au niveau mondial, sans que les éventuelles corrections intervenues depuis apportent une garantie de réduction significative de sa probabilité	$10^{-3} > F > 10^{-4}$
B	**Probable**. S'est déjà produit et/ou peut se reproduire pendant la durée de vie de l'installation	$10^{-2} > F > 10^{-3}$
A	**Courant**. S'est produit sur site considéré et/ou peut se produire à plusieurs reprises pendant la durée de vie de l'installation malgré d'éventuelles mesures correctrices	$F > 10^{-2}$

Le niveau de fréquence d'occurrence du BLEVE est évalué en se référant au tableau 2.7. Sa valeur estimée à 2×10^{-6} appartient à l'intervalle $10^{-5} > F > 10^{-6}$. Par conséquent, il est classé dans la catégorie **D** (très improbable).

Tableau 2.8 : Echelle des gravités sur les personnes

Niveau de Gravité	Zone délimitée par le seuil des effets létaux significatif Z3	Zone délimitée par le seuil des effets létaux Z2	Zone délimitée par le seuil des effets irréversibles sur la vie humaine Z1
G5 : Désastreux	Plus de 100 personnes exposées	Plus de 1000 personnes exposées	Plus de 10 000 personnes exposées
G4 : Catastrophique	Entre 10 et 100 personnes exposées	Entre 100 et 1000 personnes exposées	Entre 1 000 et 1 0000 personnes exposées
G3 : Important	Entre 1 et 10 personnes exposées	Entre 10 et 100 personnes exposées	Entre 100 et 1 000 personnes exposées
G2 : Sérieux	Au plus 1 personne exposée	Au plus 10 personnes exposées	Entre 10 et 100 personnes exposées
G1 : Modéré	Aucune personne exposée	Au plus 1 personne exposée	Moins de 10 personnes exposées

Tableau 2.9 : Echelle des gravités sur les biens

Estimation du coût de remplacement	Gravité
C < 200 000€	Modérée
200 000€ < C < 2 M€ (millions d'euros)	Sérieuse
2 M€ < C < 10 M€	Importante
10 M€ < C < 100 M€	Catastrophique
C > 100 M€	Désastreuse

C représente le cout de remplacement des équipements et/ou des bâtiments endommagés dans la distance d'effets de 35 kW/m^2.

Le niveau de gravité du BLEVE est évalué pour les personnes et les biens comme suit :

- *Pour les personnes* : selon l'étude de dangers RA2K qui définit la présence quotidienne de personnel dans les zones Z1, Z2 et Z3, et en se référant au Tableau 2.8, la gravité du BLEVE est classée **G5** (catastrophique).
- *Pour les biens* : d'après les fournisseurs et les experts de l'entreprise RA2K, le coût de remplacement des équipements et/ou des bâtiments endommagés dans la zone d'effet de 35 kW/m², comprenant principalement deux sphères, six bacs de stockage, une sous-station électrique, une torche et une station de traitement des eaux est estimé à 3 millions d'euros. Par conséquent, selon le Tableau 2.9, la gravité du BLEVE est classée comme **G3** (importante).

Tableau 2.10 : Matrice des risques

Fréquence \ Gravité	E	D	C	B	A
G5					
G4					
G3					
G2					
G1					

L'interprétation du niveau de risque est réalisée d'après les définitions suivantes :

Tableau 2.11 : Niveaux de risque

Zones	Classification de risque
	Risque élevé (inacceptable)
	Risque modéré (tolérable)
	Risque faible (acceptable)

Le niveau de risque de BLEVE est évalué à l'aide de la matrice des risques de RA2K pour les personnes et les biens, comme suit :

- *Pour les biens,* le niveau de risque de BLEVE correspond à ***(D/G3)*** et est donc ***tolérable***.

- *Pour les personnes*, le niveau de risque de BLEVE correspond à ***(D/G5)*** et est donc ***inacceptable*** ; il doit être réduit.

2.3.4. Réduction du risque de BLEVE à l'aide de l'approche IEC 61508 - IEC 61511

La norme IEC 61511 fournit une technique de réduction de risque moyennant les barrières de sécurité SIS (cf. la Figure 1.10). Dans notre cas, nous étudions la re-conception du SIS existant afin d'assurer que sa performance est capable de réduire suffisamment la fréquence d'occurrence de risque BLEVE, ramenant ainsi le risque BLEVE à un niveau tolérable.

Le SIS proposé consiste à intégrer le capteur (PI 3501B) avec le PLC et la vanne (MOV 3510) dans une boucle afin d'automatiser la dépressurisation de la sphère en cas de surpression. Ce SIS se présente comme un système d'évacuation d'urgence qui devrait être activé lorsque la pression de la sphère atteint un seuil de 7 bars (il fonctionne à faible demande selon la classification IEC 61508). L'automatisation permet d'améliorer considérablement la réactivité du système en réduisant le temps de réponse par rapport à une intervention manuelle. Elle renforce également la sécurité en limitant la dépendance à l'intervention humaine, ce qui diminue les risques d'erreur ou de retard dans l'activation de la vanne de dépressurisation.

Le SIS proposé est présenté dans le tableau suivant en termes de constituants et des données de fiabilité correspondantes.

Tableau 2.12 : Caractéristiques du SIS proposé

Eléments du SIS	Désignation	Fonction	Données
Capteur	PI 3501B	Détection de surpression excessive dans la sphère (détecter un seuil de 7 bars)	$\lambda_{DD} = 2{,}5 \times 10^{-6}$/h $\lambda_{DU} = 2{,}5 \times 10^{-6}$/h DC =50% T_1= 1 an (8760 heures) MTTR =8 heures
Unité logique	PLC	Traitement du signal émis par le PI 3501B et commande de l'action au MOV3510	$\lambda_{DD} = 0{,}9 \times 10^{-6}$/h $\lambda_{DU} = 0{,}1 \times 10^{-6}$/h DC = 90% T_1=1 an (8760 heures) MTTR = 8 heures
Elément final	MOV 3510	S'ouvre pour dépressuriser la sphère	$\lambda_{DD} = 3 \times 10^{-6}$/h $\lambda_{DU} = 7 \times 10^{-6}$/h DC = 30% T_1= 1 an (8760 heures) MTTR = 24 heures

- ***Détermination de la performance fiabiliste requise de SIS (SIL requis)***

D'abord, nous devons déterminer la performance que le SIS proposé doit avoir pour réduire la fréquence d'occurrence de risque BLEVE au niveau tolérable prédéterminé. En utilisant une formule issue de la méthode LOPA.

$$PFD_{moy}^{SIS} = \frac{F^T}{F^c} \quad (2.1)$$

Avec :

- PFD_{moy}^{SIS} : probabilité moyenne de défaillance dangereuse à la demande (performance requise du SIS),
- F^T : fréquence d'occurrence tolérable de BLEVE prise égale à $9 \times 10^{-7}/an$, en se basant sur la matrice des risques, qui fixe la fréquence tolérable correspondant à un événement dangereux de gravité **G5** à une valeur inférieure à 10^{-6}.
- F^c : la fréquence d'occurrence de BLEVE, calculée précédemment, $2 \times 10^{-6}/an$. Toutefois, la contribution de la barrière (alarme + opérateur action) doit être exclue, car cette dernière partage deux éléments communs avec le système instrumenté de sécurité (PI 3501B et PLC). Ainsi, elle ne satisfait pas la condition d'indépendance exigée par LOPA. Par conséquent, la fréquence devient : $2 \times 10^{-5}/an$.

En appliquant la formule (2.1), on trouve $PFD_{moy}^{SIS} = 4.5 \times 10^{-2}$. Cette valeur correspond à un SIL requis = **SIL 1**.

- ***Détermination de la performance fiabiliste réelle de SIS proposé (SIL atteint)***

La performance probabiliste de la fonction de sécurité, assurée par le SIS proposé, est déterminée par le calcul et la combinaison des performances de ses trois sous-systèmes (S, LS et FE). Cela peut être exprimé par la formule suivante :

$$PFD_{avg}^{SIS} = PFD_{avg}^{S} + PFD_{avg}^{LS} + PFD_{avg}^{FE} \quad (2.2)$$

IEC 61508 fournit des formules analytiques pour l'évaluation de performance de différentes configurations SIS. Dans notre cas, chacun des trois sous-systèmes possède une architecture 1oo1. Par conséquent, la formule analytique utilisée est la suivante :

$$\mathrm{PFD}_{avg}^{1oo1} \approx \frac{\lambda_{\mathrm{DU}} \times \mathrm{T}_1}{2} + \lambda_{\mathrm{DD}} \times \mathrm{MTTR} \quad (2.3)$$

En y insérant les données de fiabilité de chaque sous-système, on obtient :

- $\mathrm{PFD}_{avg}^{S} = \frac{2{,}5\times10^{-6} \times 8760}{2} + 2{,}5 \times 10^{-6} \times 8 = 2.192 \times 10^{-2}$
- $\mathrm{PFD}_{avg}^{LS} = \frac{2{,}5\times10^{-6} \times 8760}{2} + 0{,}9 \times 10^{-6} \times 8 = 4.45 \times 10^{-4}$
- $\mathrm{PFD}_{avg}^{FE} = \frac{7\times10^{-6} \times 8760}{2} + 3 \times 10^{-6} \times 24 = 3.073 \times 10^{-2}$
- $PFD_{avg}^{SIS} \approx 0{,}02192 + 0{,}000445 + 0{,}03073 = 5.31 \times 10^{-2}$

Cette valeur correspond à un **SIL 1**.

Nous avons calculer la PFD_{avg} du SIS selon une seconde voie en utilisant le logiciel GRIF (module SIL). L'évolution des PFD de chaque sous-système et du SIS en fonction du temps est donnée à la Figure 2.6. La valeur obtenue est presque identique à celle du calcul manuel.

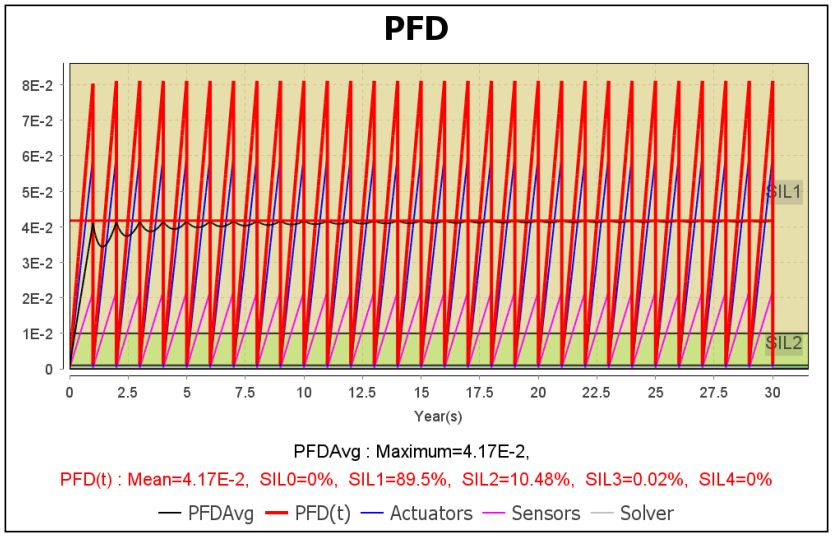


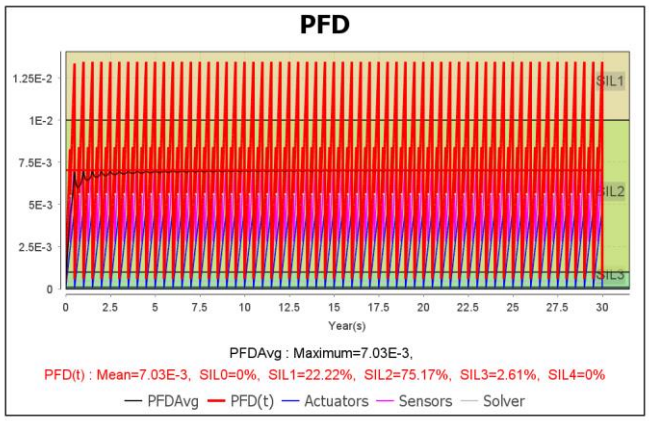
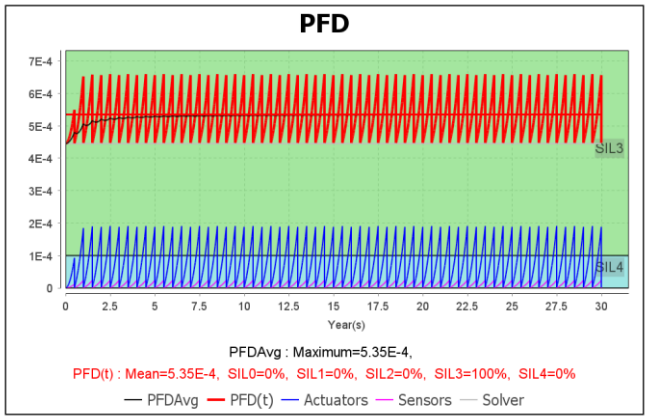
Figure 2.6 : Graphique PFD et SIL du SIS

- ***Validation du SIS***

Le SIL requis est égal au SIL atteint (SIL 1). Par conséquent, ce SIS permet d'atteindre la réduction de risque nécessaire en abaissant la fréquence du risque BLEVE à un niveau inférieur à la fréquence tolérable. Ainsi, il ramène le risque BLEVE à un niveau tolérable, correspondant au niveau (E/G5) selon la matrice des risques. Nous pouvons alors valider le SIS proposé.

Pour plus de sécurité du système face au risque BLEVE, nous pouvons améliorer les performances probabilistes du SIS proposé en y apportant des modifications. Il serait préférable que ces modifications soient portées sur les maillons faibles du SIS: MOV 3510 et PI 3501B. Le Tableau 2.13 représente les modifications proposées et les performances probabilistes résultantes.

Tableau 2.13 : Amélioration de la performance du SIS proposé

Modifications proposées	PFD et SIL du SIS
Type de la vanne: - Remplacement de la MOV 3510 par une vanne de dépressurisation marche/arrêt avec ($\lambda_{DD} = 1\times 10^{-6}$/h, $\lambda_{DU} = 0{,}8\times 10^{-6}$/h) **&** **Test de la vanne et du capteur:** - Réduction de la fréquence de test complet du capteur et du vanne en passant de 1 an à 6 mois - Test partiel (PST) du capteur (30% de seuil = 5 bars) chaque 3 mois	
Architecture de la vanne et du capteur - Ajout d'un capteur et d'une vanne d'autres marques en redondance active avec une configuration 1oo2. Le capteur a ($\lambda = 1.2\times 10^{-6}$/h, DC=80). La vanne a ($\lambda = 1\times 10^{-6}$/h, DC=30) **&** **Test de la vanne et du capteur** -Test echelonné des capteurs et des vannes : le capteur 1 et la vanne 1 sont testés pour la première fois après 6 mois, puis tous les 12 mois. Quant au capteur 2 et à la vanne 2, ils sont testés avec une fréquence de 12 mois.	

Les résultats présentés dans la Figure 2.6 et les figures du Tableau 2.13 nous ont permis d'extraire le SIL du SIS étudié de deux manières :

- Le niveau SIL correspond à la zone SIL où la boucle passe le plus de temps. En fait, une boucle avec un niveau SIL2, par exemple, ne peut pratiquement jamais rester à son niveau SIL de façon permanente au fil du temps.
- La valeur PFD_{avg} est utilisée pour dériver la valeur SIL à l'aide du Tableau 1.1.

Les deux propositions précédentes conduisent à des niveaux SIL meilleurs du SIS (SIL 2, SIL3) par rapport à celui de sa conception initiale (SIL 1).

2.4. Conclusion

Ce chapitre a présenté la mise en œuvre du processus de gestion des risques industriels proposé, associée à l'application de techniques adaptées sur un système industriel réel : sphère de stockage de butane 305TK002. L'objectif principal était de maîtriser le risque de BLEVE,

considéré comme l'un des scénarios accidentels les plus critiques pour ce type d'installation. Cette mise en œuvre a été conduite selon les étape suivantes :

- *Analyse qualitative du risque* de *BLEVE* à l'aide de la méthode HAZOP. Cette méthode a permis d'identifier les scénarios d'accidents BLEVE pouvant survenir dans la sphère de stockage du butane.
- *Analyse quantitative du risque* BLEVE à l'aide de la méthode LOPA et le logiciel ALOHA, afin d'estimer respectivement sa fréquence d'occurrence et sa gravité de ses conséquences.
- *Evaluation du risque* BLEVE à l'aide de la matrice des risques de RA2K, construite selon le principe ALARP. Cette évaluation a montré que son niveau est inacceptable et nécessite donc une réduction.
- Réduction du risque BLEVE selon la norme IEC 61508- IEC 61511. Nous avons proposé de concevoir un SIS intégrant le capteur PI 3501B, le PLC et la vanne MOV 3510 dans une boucle destinée à déclencher automatiquement la dépressurisation de la sphère. Ce système, dont la performance est évaluée à SIL1, permet de ramener le risque BLEVE à un niveau tolérable. Par ailleurs, pour plus de sécurité du système face au risque BLEVE, nous avons proposé des améliorations des performances probabilistes du SIS.

Ainsi, la mise en œuvre du processus proposé a démontré la pertinence de l'approche méthodologique retenue, alliant rigueur normative et applicabilité pratique. Cette démarche assure une traçabilité complète des décisions de sécurité, depuis l'identification des dangers jusqu'à la mise en place des mesures de maîtrise.

Chapitre 3

Approche probabiliste dans l'évaluation de la performance des systèmes de sécurité

3.1. Introduction

La performance probabiliste des systèmes est un domaine essentiel de la sûreté de fonctionnement, qui vise à garantir qu'un système remplisse ses fonctions de manière fiable, sécurisée et durable, même en présence de défaillances. Contrairement aux approches déterministes, qui supposent des comportements fixes et prévisibles, l'analyse probabiliste intègre les incertitudes et les variabilités inhérentes aux composants, aux environnements d'exploitation et aux interactions complexes entre sous-systèmes.

En adoptant une perspective probabiliste, il devient possible de modéliser des événements tels que les défaillances ou les réparations, et d'estimer les performances des systèmes dans des conditions réelles. Cette approche s'appuie sur des outils statistiques et mathématiques, tels que l'estimation empirique, les lois de probabilité et certaines méthodes d'analyse comme les arbres de défaillances (AdD) ou les chaînes de Markov, afin d'estimer des indicateurs clés tels que la fiabilité, la disponibilité et la maintenabilité. Cela permet non seulement de prédire leur comportement au fil du temps, mais aussi d'identifier les points faibles potentiels et d'optimiser les stratégies de conception, de maintenance et de redondance. L'objectif ultime est de concevoir des systèmes plus robustes et fiables, minimisant ainsi les risques de pertes humaines, environnementales ou économiques.

3.2. Attributs de la performance probabiliste des systèmes de sécurité

La performance probabiliste fait référence à la performance d'un système évaluée par des méthodes probabilistes. Cela signifie que la performance n'est pas déterministe mais plutôt soumise au hasard ou à l'incertitude. Cette performance est caractérisée par des attributs ou propriétés spécifiques. L'essentiel de ces attributs est présenté dans ce qui suit.

3.2.1. Fiabilité et disponibilité

La fiabilité et la disponibilité sont deux concepts clés en ingénierie de la fiabilité, mais ils mesurent des aspects différents de la performance d'un système. Voici une explication détaillée de leurs définitions et de leurs différences.

- ***Fiabilité R(t)***

La fiabilité est la probabilité qu'un système ou composant fonctionne *sans aucune défaillance* pendant un intervalle de temps donné [0, *t*], sous des conditions d'utilisation spécifiques. Elle mesure la capacité du système à *survivre continuellement* jusqu'à l'instant *t*, sans interruption [101].

▪ ***Définition mathématique*** : $R(t) = P$ (le système fonctionne sans défaillance de 0 à t).

▪ ***Caractéristiques*** **:**

- Ne tient pas compte des réparations une fois le système en panne (le système est supposé *non réparable*).
- Décroît avec le temps (la probabilité de survie diminue), telle que : $R(t_1) > R(t_2)$ $si\ t_1 < t_2$, et elle varie de 1 à 0 sur l'intervalle du temps [0, +∞ [, avec les limites : $\lim_{t\to 0} R(t) = 1,\ \lim_{t\to +\infty} R(t) = 0.$

La défiabilité $F(t)$ est le complément à 1 de la fiabilité : $F(t) = 1 - R(t)$.

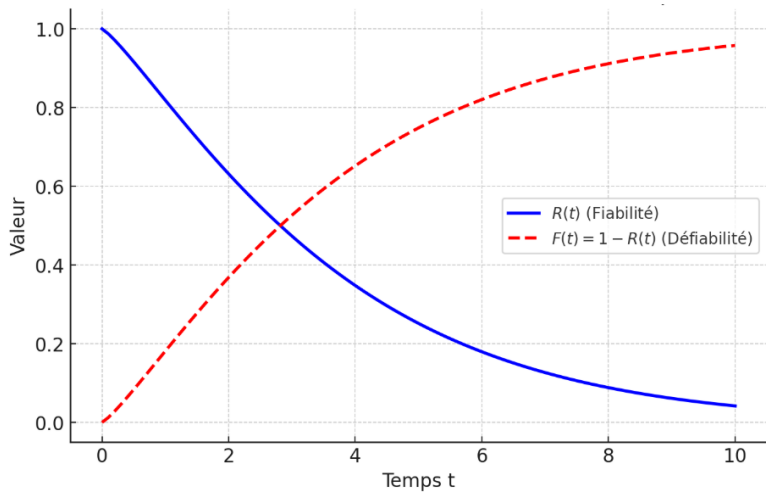


Figure 3.1 : Evolution de la fiabilité et de la défiabilité en fonction du temps

- ***Disponibilité A(t)***

La *disponibilité* est la probabilité que le système soit *opérationnel à un instant t* donné, en incluant les périodes de remise en service après chaque défaillance et réparation. Elle mesure l'*accessibilité* du système à un moment précis, même si des pannes antérieures ont eu lieu [102, 103].

▪ ***Définition mathématique*** : A(t) = P (le système fonctionne à l'instant t).

▪ ***Caractéristiques*** :

- Prend en compte à la fois la fiabilité (temps de bon fonctionnement) et la maintenabilité (temps de réparation) pour un système réparable. C'est-à-dire, elle dépend à la fois du *taux de défaillance* (la fréquence des défaillances) et du *taux de réparation* (la rapidité des réparations).
- Peut converger vers une valeur limite (disponibilité asymptotique) différente de 0.

L'indisponibilité $U(t)$ est le complément à 1 de la disponibilité : $U(t) = 1 - A(t)$

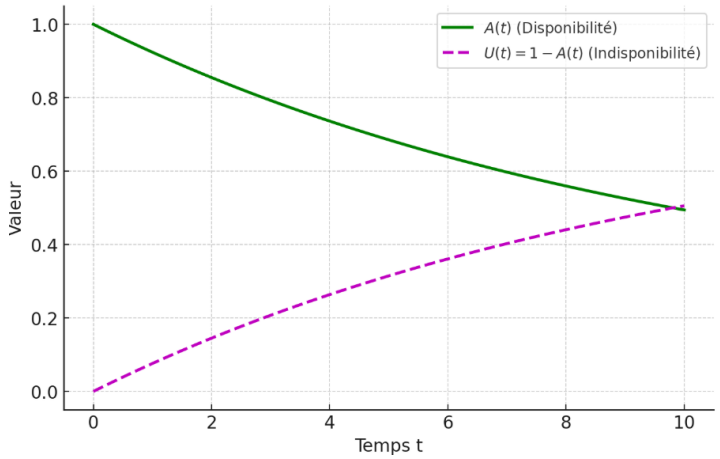


Figure 3.2 : Evolution de disponibilité et d'indisponibilité en fonction du temps

- ***Différence entre la fiabilité et la disponibilité***

La différence entre la fiabilité et la disponibilité se voit dans leur définition et leurs caractéristiques. Voici une représentation comparative.

1. *Perspective temporelle :*
   - La fiabilité considère une période continue [0, t]
   - La disponibilité considère un instant précis t
2. *Réparations :*
   - La fiabilité ne prend pas en compte les réparations (une fois en panne, le système reste en panne)
   - La disponibilité prend en compte les réparations (le système peut être réparé et redevenir disponible)
   - La disponibilité et la fiabilité sont identiques si un composant est irréparable : $A(t)$=$R(t)$. Par contre, s'il est réparable : $A(t) \geq R(t)$.
3. *Comportement à long terme :*
   - La fiabilité tend vers 0 avec le temps
   - La disponibilité peut tendre vers une valeur stable
4. *Application* ***:***
   - La fiabilité est cruciale pour les systèmes non réparables ou les missions critiques sans possibilité d'intervention (ex. une ampoule électrique)

- La disponibilité est plus importante pour les systèmes réparables où des interruptions temporaires sont acceptables (ex. une machine de production)

3.2.2. Maintenabilité M(*t*)

La maintenabilité est la probabilité qu'un système ou composant défaillant puisse être *réparé dans un intervalle de temps donné* [0, *t*], sous des conditions spécifiques (outils, compétences, procédures disponibles). Elle mesure l'*efficacité* (la facilité et la rapidité) *des actions de maintenance* pour restaurer le système à un état opérationnel [104, 105].

- ***Définition mathématique*** : M(*t*) = P (réparation achevée dans l'intervalle [0, *t*] | système en panne à *t* = 0)
- ***Caractéristiques*** :
  - *Temps de réparation* : dépend de la complexité du système, de l'accessibilité des composants, et des ressources de maintenance.
  - *Conception pour la maintenabilité* : facilité de diagnostic, modularité, standardisation des pièces, documentation technique.
  - *Liée à la disponibilité* : une maintenabilité élevée (réparations rapides) améliore la disponibilité A(*t*).
  - *Evolution dans le temps :* c'est une fonction croissante du temps avec M (0) = 0 (impossibilité de réparer instantanément) et $\lim_{t\to+\infty} M(t) = 1$ (toute panne finit par être réparée si le temps est suffisant).

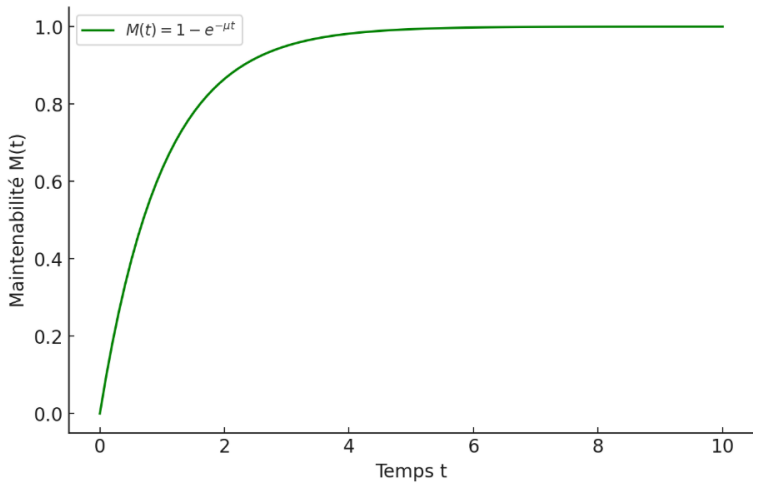


Figure 3.3 : Evolution de maintenabilité en fonction du temps

Il faut noter que la performance d'un système désigné par l'acronyme FDMS illustre l'importance de considérer conjointement la Fiabilité, la Disponibilité, la Maintenabilité et la

Sécurité pour concevoir, analyser ou améliorer un système, car ces attributs sont fortement interconnectés (voir Figure 3.4).

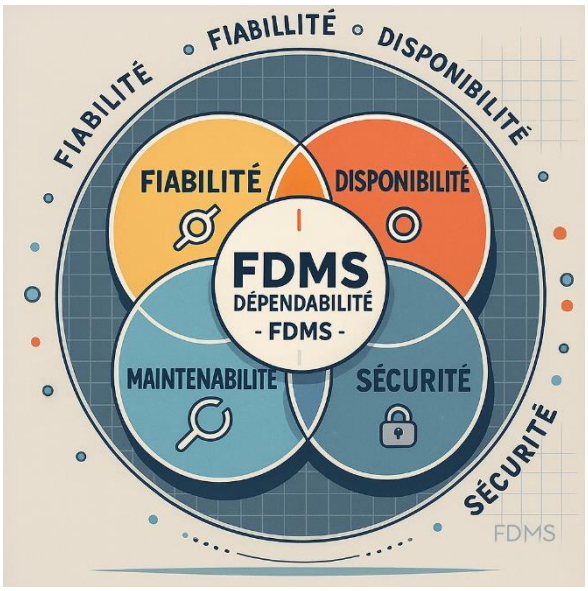


Figure 3.4 : Interconnexion des FDMS selon le diagramme de Venn

3.3. Tests périodiques (essai périodique)

Les tests périodiques sont des tests planifiés à intervalles fixes (mensuels, annuels, etc.) pour vérifier le bon fonctionnement du système. Ils ont pour objectifs de détecter les défaillances silencieuses (pannes non visibles en fonctionnement normal) et maintenir l'intégrité du système. La norme CEI 61511 en donne la définition suivante : « *essai périodique destiné à détecter les anomalies dangereuses cachées dans un SIS 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* » [106]. A titre d'exemple, cela peut concerner la vérification trimestrielle des vannes de sécurité d'un réacteur chimique, le test annuel des capteurs de fumée dans une usine, etc.

Plusieurs types de tests peuvent être établies en fonction de la manière selon laquelle ses tests sont conduits. Dans c qui suit, nous présentons les types les plus rencontrés dans les pratiques industrielles.

3.3.1. Tests parfaits et tests imparfaits

Les tests peuvent être parfaits ou imparfaits, selon leur capacité à révéler toutes les défaillances dangereuses non détectées en exploitation [107, 108]. Le Tableau 3.1 présente la différence entre ces deux types de tests.

Tableau 3.1 : Différences entre tests parfaits et tests imparfaits

Tests parfaits	Tests imparfaits
Détectent *toutes les pannes possible*s dans le système.	Détectent *seulement un sous-ensemble de pannes* (limités par les moyens techniques ou le temps)
Idéal mais souvent irréaliste en pratique	*Réalistes,* mais laissent un *risque résiduel.*
Exemple : Simulation d'une surpression réelle pour tester une vanne de décharge	*Exemple :* test électrique partiel de la vanne sans vérifier sa réponse mécanique sous pression

3.3.2. Tests complets et tests partiels

Cette classification est réalisée selon l'étendue de la vérification effectuée sur la chaîne de sécurité [109, 110]. Le Tableau 3.2 présente la différence entre ces deux types de tests.

Tableau 3.2 : Différences entre tests complets et tests partiels

Test complet	Test partiel
Vérifie *tous les composants* et fonctions du système	Vérifie *un sous-ensemble critique* (ex. 30% des modes de défaillances)
Avantage : couverture maximale	*Avantage :* gain de temps et coût réduit
Inconvénient : long et coûteux	*Risque* : pannes non détectées dans les zones non testées
Exemple : test complet de fin de course d'une vanne de sécurité	*Exemple* **:** test partiel de fin de course d'une vanne de sécurité (PST : *Partial Stroke Test*)

3.3.3. Tests simultanés et test échelonnés

Selon la stratégie de planification adoptée, les tests peuvent être réalisés simultanément ou de façon échelonnée (décalée) [111]. Le tableau 3.3 présente la différence entre ces deux types de tests.

Tableau 3.3 : Différences entre tests simultanés et tests test échelonnés

Test simultané	Test échelonné
Tous les composants testés en même temps	Composants testés *séquentiellement* (par zone, sous-système, etc.)
Avantage : rapide et efficace	*Avantage :* minimise l'indisponibilité du système
Risque : arrêt complet du système pendant le test	*Exemple :* tester une ligne de production à la fois dans une usine multi-lignes
Exemple : arrêt total d'une plateforme pétrolière pour tester toutes les vannes de sécurité	*Exemple :* test des pompes incendie d'un bâtiment étage par étage

3.4. Paramètres de la performance probabiliste des systèmes de sécurité

Dans un cadre de sûreté de fonctionnement, la *défaillance* et la *maintenance* sont des notions fondamentales permettant d'évaluer et d'améliorer la fiabilité, la disponibilité et la maintenabilité des systèmes techniques.

Une *défaillance* correspond à la cessation de l'aptitude d'une entité à accomplir une fonction requise. C'est le passage de l'état de marche à l'état d'échec [112].

Face aux défaillances, *la maintenance* joue un rôle crucial pour garantir la disponibilité des systèmes. Elle se décline en plusieurs stratégies, notamment la maintenance corrective (réparation après défaillance) et la maintenance préventive (actions menées pour éviter la défaillance).

3.4.1. Durées caractéristiques

Les durées liées à la fiabilité et à la maintenabilité des systèmes sont des mesures temporelles utilisées pour évaluer la performance et la disponibilité des équipements. Voici les principales durées utilisées [113, 114]:

- ***MTTF*** (*Mean Time To first Failure*) : ***Temps Moyen Avant la première Défaillance***
  Durée moyenne avant qu'un système ou un composant ne tombe en panne, applicable aux systèmes *non réparables* (ex. : ampoule électrique).
- ***MTTR*** (*Mean Time To Repair*) : ***Temps Moyen de Réparation***
  Durée moyenne nécessaire pour réparer un système après une défaillance, incluant le diagnostic, la réparation et les tests.
- **MUT** (*Mean Up Time*) : ***Temps Moyen de bon Fonctionnement***
  Durée moyenne pendant laquelle un système est opérationnel entre deux pannes (synonyme de temps de disponibilité).
- **MDT** (*Mean Down Time*) : ***Temps Moyen d'Indisponibilité***
  Durée moyenne d'indisponibilité d'un système après une panne, incluant la détection, le diagnostic, la logistique, la réparation active et les tests et redémarrage.
- **MTBF** (*Mean Time Between Failures*) : ***Temps Moyen Entre Défaillances***
  Durée moyenne entre deux pannes consécutives pour un système réparable. Calculé par : *MTBF = MUT + MDT*.

Remarques :

- *Le MTTF et le MTBF* sont souvent confondus : le premier s'applique aux systèmes non réparables, le second aux systèmes réparables.
- *Le MTTR fait partie du MDT*, mais ce dernier peut inclure des délais supplémentaires (ex. : attente de pièces).

Ces durées sont représentées dans la Figure 3.5.

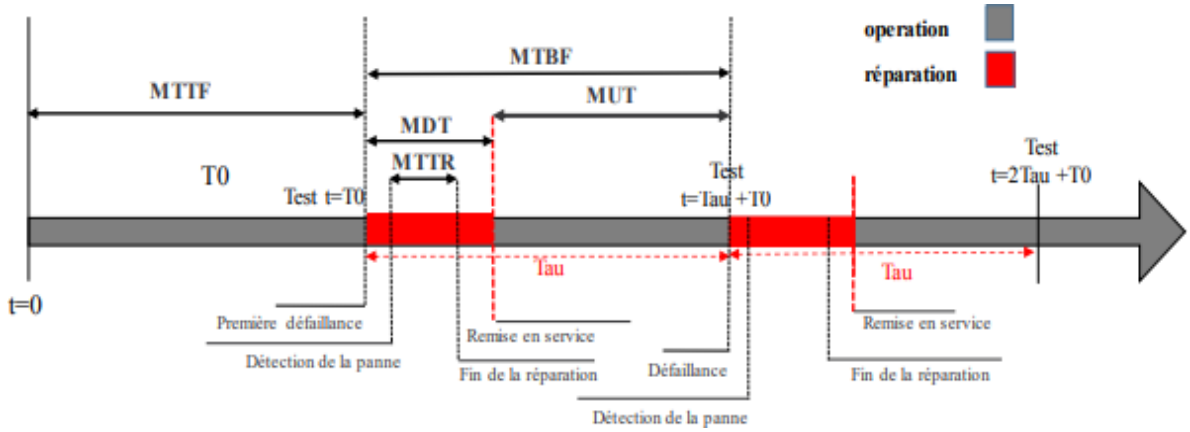


Figure 3.5 : Durées liées à la fiabilité, la disponibilité et à la maintenabilité des systèmes

3.4.2. Taux caractéristiques

Dans le domaine de la fiabilité et de la maintenabilité des systèmes, deux taux principaux sont utilisés : taux de défaillance $\lambda(t)$ et taux de réparation $\mu(t)$.

3.4.2.1. Taux de défaillance $\lambda(t)$

3.4.2.1.1. Définitions

Le taux de défaillance (ou *taux de défaillance instantané*) $\lambda(t)$ est une mesure *instantanée* de la probabilité qu'un système ou composant, ayant *survécu jusqu'à l'instant t*, tombe en panne dans l'intervalle de temps suivant $[t, t+\Delta t]$ [115, 116].

- ***Formulation mathématique :***

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P(\text{défaillance dans } [t,t+\Delta t] \mid \text{survie jusqu'à } t)}{\Delta t} \qquad (3.1)$$

- ***Interprétation et comportement :*** la variation du taux de défaillance dans le temps est présentée sous forme d'une courbe en baignoire (voir Figures 3.6 et 3.7).

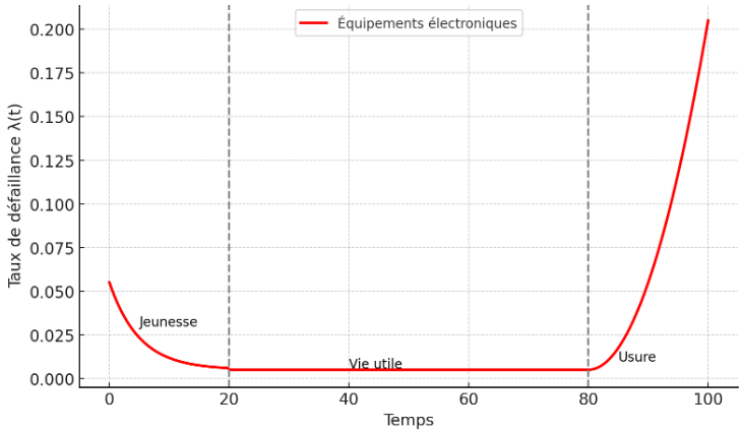


Figure 3.6 : Variation du taux de défaillance pour les équipements électroniques

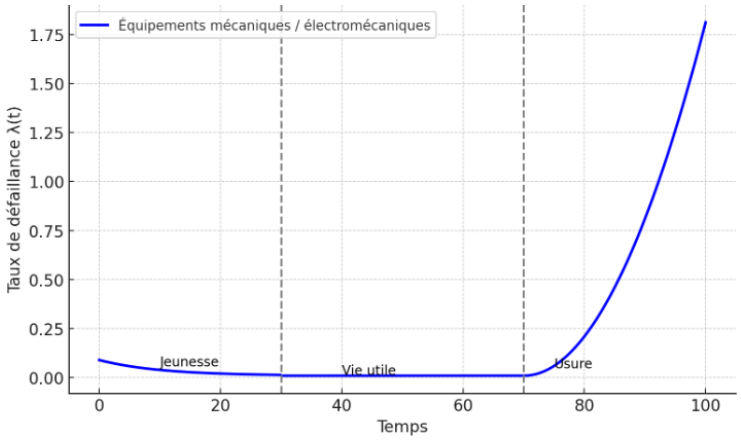


Figure 3.7 : Variation du taux de défaillance pour les équipements mécanique

La courbe en baignoire montre trois phases distinctes [117, 118, 119] :

1. ***Phase de jeunesse*** (diminution du taux de défaillance) : taux de défaillance initial plus élevé dû à des défauts de fabrication, de montage ou de mise en service. Ce taux diminue généralement assez rapidement.
2. ***Phase de vie utile*** (taux de défaillance constant) : taux de défaillance relativement bas et stable, où l'équipement fonctionne correctement sous conditions normales d'utilisation (la plupart des défaillances dues aux défauts initiaux ont été corrigées)
3. ***Phase d'usure*** (augmentation du taux de défaillance) : avec l'ancienneté et l'usure des composants (ex. fatigue mécanique, corrosion, etc.), le taux de défaillance augmente de manière plus ou moins prononcée.

Généralement, les composants électroniques ont une période de défaillances précoces due aux défauts de fabrication, suivie d'une longue phase de vie utile avec un faible taux de défaillance, puis une phase d'usure progressive (Figure 3.6). Les équipements mécaniques et électromécaniques présentent souvent une courbe en baignoire plus marquée dans la phase

d'usure, car les pièces mobiles subissent une usure physique plus importante que les circuits électroniques (Figure 3.7).

Remarques :

- Le taux de défaillance λ(t) décrit *comment le risque évolue dans le temps*.
- Il permet de prédire les défaillances et d'optimiser les stratégies de maintenance (prédictive, conditionnelle).

3.4.2.1.2. Taux de défaillances selon la norme IEC 61508

La norme IEC 61508 [120] classe les défaillances en fonction de leur *impact sur la sécurité* et de leur *détectabilité*, tout en distinguant les *causes aléatoires* des *causes systématiques* ainsi que *les causes indépendantes* des *causes communes*. Chaque catégorie s'associe un taux de défaillance spécifique.

A. Classification des défaillances par effet sur la fonction de sécurité

- ***Défaillance sûre (S) :*** ne compromet pas la fonction de sécurité. Exemple : un capteur de température indiquant une valeur trop élevée de manière erronée, entraînant un arrêt préventif (arrêt non nécessaire mais sûr).
- ***Défaillance dangereuse (D) :*** compromet la fonction de sécurité, risquant de provoquer un accident. Exemple : un capteur de température défaillant et indiquant une valeur sécuritaire alors que le système est en surchauffe.

B. Classification des défaillances par détectabilité

- ***Défaillance détectée (D) :*** identifiée par des *diagnostics automatiques* (p. ex., autotests, surveillance en temps réel). Exemple : un circuit de diagnostic détecte une panne d'un actionneur et active un système redondant.
- ***Défaillance non détectée (U) :*** Non identifiée par les diagnostics, restant latente jusqu'à une sollicitation de la fonction de sécurité (tests ou une vraie sollicitation). Exemple : une dérive progressive d'un capteur non surveillée, masquant un état dangereux.

C. Combinaison des catégories (S/D/D/U) : les défaillances sont regroupées en 4 types.

- ***Sûre détectée (SD) :*** impact minimal, car le système peut réagir (p. ex., maintenance préventive).
- ***Sûre non détectée (SU) :*** peut réduire la disponibilité mais ne menace pas la sécurité.

- ***Dangereuse détectée (DD) :*** risque atténué grâce à la détection (p. ex., basculement vers un composant de secours).
- ***Dangereuse non détectée (DU) :*** la plus critique, car le système reste aveugle vis-à-vis des déviations potentielles.

D. Classification des défaillances par causes

- ***Défaillances aléatoires (matérielles)*** : imprévisibles, dues à l'usure, aux contraintes environnementales, etc. Gérées par *la redondance* et les diagnostics.
- ***Défaillances systématiques*** : prévisibles issues d'erreurs de conception, de logiciel, de procédures ou humaines dans les processus. Prévenues par des *méthodologies rigoureuses* (ex. : revues de conception, tests logiciels).
- ***Défaillance de cause commune (CCF)*** : une défaillance aléatoire ou systémique peut être due à une défaillance de cause commune. Elle représente un mode de défaillance systémique où une seule cause (ex. : surtension, erreur de conception, environnement extrême) entraîne la défaillance simultanée de plusieurs canaux redondants. Cela réduit l'efficacité des architectures tolérantes aux pannes. Les défaillances de cause commune compromettent donc la redondance, un mécanisme de sécurité essentiel. Elle est critique dans l'évaluation de la fiabilité des systèmes redondants.

E. Décomposition du taux de défaillance aléatoire d'un canal (λ)

Avant de présenter les différentes partitions des taux de défaillances, il convient de signaler que selon la CEI 61508 les défaillances systématiques ne sont pas quantifiables car elles sont de nature déterministe liées à des défauts initiés par des erreurs humaines (spécification, conception, exploitation, etc.), et non à des processus aléatoires. Les défaillances systématiques nécessitent des contrôles qualitatifs (management) plutôt que des mesures probabilistes.

Le taux de défaillance total (λ) d'un composant ou canal se divise comme suit :

$$\lambda = \lambda_S + \lambda_D \tag{3.2}$$

Avec :

λ_S: taux de défaillances sûres.

λ_D: taux de défaillances dangereuses.

En prenant en compte la classification par détectabilité, nous obtenons les quatre taux suivants :

$$\begin{cases} \lambda_S = \lambda_{SD} + \lambda_{SU} \\ \lambda_D = \lambda_{DD} + \lambda_{DU} \end{cases} \quad (3.3)$$

Avec :

λ_{SD}: taux de défaillances sûres détectées.

λ_{SU}: taux de défaillances sûres non détectées.

λ_{DD}: taux de défaillances dangereuses détectées.

λ_{DU}: taux de défaillances dangereuses non détectées.

La capacité de détection des défaillances est matérialisée par des taux de couverture de diagnostics :

$$\begin{cases} \lambda_{SD} = DC_S\ \lambda_S \\ \lambda_{SU} = (1 - DC_S)\ \lambda_S \\ \lambda_{DD} = DC\ \lambda_D \\ \lambda_{DU} = (1 - DC)\ \lambda_D \end{cases} \quad (3.4)$$

DC_S et DC représentent respectivement l'efficacité du système à détecter ses propres défaillances sûres et dangereuses.

En plus des couvertures de diagnostics, la CEI 61508 introduit le concept de proportion de défaillances en sécurité (SFF : Safe Failure Fraction), qui reflète le comportement *fail-Safe*.

$$SFF = \frac{\lambda_{SD}+\lambda_{SU}+\lambda_{DD}}{\lambda} \quad (3.5)$$

Plus la SFF est élevée, meilleur est le niveau de sécurité (selon la CEI 61508). La SFF intervient dans la détermination des contraintes d'architectures (procédure Route 1_H), permettant de définir le niveau SIL admissible (ex. : SIL 2 requiert SFF ≥ 60% pour un composant de type A).

Par ailleurs, afin de prendre en compte la contribution des défaillances de cause commune (CCF), chacune des répartitions (*x = SD, SU, DD ou DU*) de l'Equation (3.4) peut être écrite sous la forme suivante en se fondant sur le modèle du facteur β :

$$\lambda_x = \lambda_x^{ind} + \lambda_x^{CCF} = (1 - \beta_x)\ \lambda_x + \beta_x\ \lambda_x \quad (3.6)$$

Avec :

λ^{ind} : taux de défaillances individuelles (indépendantes).

λ^{CCF} : taux de défaillances de cause commune.

Il faut noter que même avec un faible λ_{DU} individuel, une CCF peut rendre la probabilité de défaillance globale inacceptable. En pratique, la CCF ajoute un terme supplémentaire qui augmente significativement la probabilité de défaillance. Par conséquent, ignorer la CCF conduit à une sous-estimation des risques.

3.4.2.2.Taux de réparation $\mu(t)$

Le taux de réparation $\mu(t)$ est une mesure instantanée de la probabilité qu'un système ou composant défaillant soit *réparé dans l'intervalle de temps* $[t, t+\Delta t]$, sachant qu'il n'a pas encore été réparé jusqu'à l'instant t [122].

Il quantifie *l'efficacité des processus de maintenance* et est un paramètre clé pour évaluer la maintenabilité et la disponibilité d'un système.

- ***Formulation Mathématique :***

$$\mu(t) = \lim_{\Delta t \to 0} \frac{\mathrm{P}(\text{réparation dans } [t,t+\Delta t] \mid \text{non réparé jusqu'à } t)}{\Delta t} \tag{3.7}$$

- ***Interprétation et comportement :***

Le taux de réparation $\mu(t)$ est directement lié au MTTR (*Mean Time To Repair*). Le MTTR peut être défini de deux manières [122]:

- *MTTR agrégé* : Inclut *toutes les phases de MDT.* Le taux de réparation μ(t) intègre toutes les étapes du processus de maintenance.
  1. *Détection :* Délai pour identifier qu'une panne s'est produite.
  2. *Diagnostic* : Identifier la cause de la panne.
  3. *Logistique :* Temps d'attente pour les pièces, les outils ou l'équipe.
  4. *Réparation active* : Remplacement ou réparation du composant défaillant.
  5. *Tests et redémarrage* : Vérification du bon fonctionnement.
- *MTTR restreint* : ne couvre que *la réparation active*.

Le taux de réparation peut varier en fonction de l'âge du système ou du composant, ainsi que des conditions de maintenance et de fonctionnement (voir Tableau 3.4). Contrairement au taux de défaillance $\lambda(t)$, le taux de réparation $\mu(t)$ ne suit pas naturellement une courbe en baignoire. Sa variabilité est plutôt dictée par les facteurs du Tableau 3.4.

Tableau 3.4: Facteurs Influençant $\mu(t)$

Facteur	Impact sur μ(t)	Exemple
Age du système	Les systèmes vieillissants peuvent nécessiter des réparations plus longues (pièces obsolètes, usure généralisée).	Un moteur industriel de 20 ans : temps de réparation augmentant avec l'âge (μ(t) ↓).
Conditions de maintenance	Des ressources limitées (manque de pièces détachées, personnel non formé) réduisent μ(t).	Un serveur en région isolée : délais de réparation allongés (μ(t) ↓).
Contexte opérationnel	Des environnements hostiles (températures extrêmes, accès difficile) compliquent les réparations.	Une éolienne offshore : maintenance dépendante des conditions météorologiques (μ(t) ↓).
Complexité de la panne	Certaines pannes nécessitent des diagnostics approfondis ou des procédures spécialisées.	Une panne logicielle cryptique : temps de diagnostic accru (μ(t) ↓).

3.5. Bases de données génériques liés à la fiabilité, la disponibilité et à la maintenabilité des systèmes

Plusieurs bases de données ont été créées au fil du temps sur la base des résultats d'exploitation, des résultats des tests en laboratoire et du retour d'expérience. La possession de données sur la fiabilité ou la maintenabilité constitue une ressource précieuse pour l'évaluation des risques. Ces informations peuvent être spécifiques à un système ou partagées entre plusieurs systèmes.

Le processus de dégradation des équipements (modes de défaillance, mécanismes et causes), les conditions d'exploitation et l'évolution technologique sont autant de facteurs essentiels au calcul des taux de défaillance et à l'élaboration de modèles prédictifs. Toutefois, il est difficile d'en tenir compte dans leur totalité. En effet, les données disponibles sont souvent inadaptées aux systèmes et environnements réels, ce qui signifie que ces sources ne permettent pas une évaluation précise de la fiabilité. Ainsi, les informations collectées ne permettent qu'une exploitation partielle des données. Néanmoins, ces bases restent indispensables pour obtenir des estimations proches de la réalité dans les nouvelles conceptions. A cet égard, nous avons présenté plusieurs bases de données dans différents domaines et mis en évidence leurs limites d'utilisation.

3.5.1. Bases de données pour la sûreté de fonctionnement

Les bases de données constituent un élément clé du recueil, de la gestion et de l'analyse des données relatives aux équipements et aux systèmes dans le domaine de la sûreté de fonctionnement. Les experts en fiabilité et en maintenance peuvent, grâce à ces bases de données, améliorer les performances de leurs équipements et de leurs systèmes, réduire les

temps d'arrêt et les risques de pannes et de défaillances. Dans ce contexte, il est possible de classer les bases de données en trois catégories principales, selon leur objectif et leur contenu.

- Bases de données particulières à une entreprise ou un site industriel : il s'agit de données collectées à partir d'équipements similaires, exploités sous les mêmes conditions par l'entreprise.
- Les bases de données relatives à un secteur particulier, par exemple le nucléaire, la défense, etc., contiennent des données et des informations ayant trait à ce secteur. Ces bases de données, qui sont établies et maintenues par des organisations axées autour d'une industrie particulière, comprennent des données détaillées sur l'équipement, les systèmes utilisés dans ce secteur.
- Bases de données à caractère générique : les données sont issues de plusieurs secteurs d'activité et à partir de sources diverses. Elles possèdent souvent des expressions mathématiques comme les modèles de régression pour estimer, par exemple, des taux de défaillance.

Le Tableau 3.5 montre des bases de données de fiabilité les plus connues [123, 124, 125, 126] . La principale information figurant dans ces bases de données est le taux de défaillance des composants.

Tableau 3.5 : Bases de données de fiabilité

Base de données	Organisation	Version actuelle	Domaine principal	Description
PDS Data Handbook	DNV	6ème édition (2021)	Pétrole et gaz	C'est un manuel avec des données de fiabilité génériques sur les composants des systèmes instrumentés de sécurité
Exida SERH	Exida	4ème édition (2021)	Sécurité fonctionnelle	Données de fiabilité pour les équipements de sécurité et systèmes instrumentés de sécurité (SIS).
OREDA	SINTEF	6ème édition (2015)	Pétrole et gaz	Collection de données de fiabilité pour les équipements offshore et onshore de l'industrie pétrolière et gazière (se concentre sur les équipements de procédé et mécaniques (pompes, compresseurs, etc.) à des fins de disponibilité et de maintenance.)
PERD	CCPS/ AIChE	Version 2008	Industrie chimique	Base de données sur la fiabilité des équipements de traitement chimique

En outre, il existe d'autres bases de données adaptées à certains secteurs ou catégories de machines, telles que celles relatives aux automobiles et aux avions [127, 128]. Les exigences particulières de l'utilisateur et de l'industrie concernée déterminent le choix de la base de données.

3.5.2. Restrictions liées à l'utilisation des bases de données

L'utilisation de bases de données peut s'avérer précieuse pour l'analyse de fiabilité dans divers secteurs, en fournissant des informations sur la fiabilité des composants et des systèmes. Cependant, il est important de noter que ces bases de données présentent certaines limites d'utilisation, notamment :

- *Qualité des données :* les bases de données peuvent contenir des erreurs, des données incomplètes ou obsolètes, ce qui peut affecter la précision des analyses de fiabilité.
- *Spécificité des données* : les données peuvent être limitées à certains secteurs ou contextes, rendant leur application à d'autres domaines moins pertinents.
- *Mise à jour et actualisation* : la fréquence de mise à jour des bases de données peut être insuffisante, rendant certaines données obsolètes ou non représentatives des conditions actuelles. Dans des secteurs comme l'électronique, les données deviennent rapidement obsolètes en raison de l'innovation, limitant leur utilité pour des systèmes modernes.
- *Biais des données* : certaines bases de données peuvent refléter des biais liés aux méthodes de collecte, aux échantillons utilisés ou aux sources d'information.
- *Manque de contexte opérationnel* : les conditions spécifiques (température, pression, maintenance) ou les contextes critiques (p. ex., environnements extrêmes) influençant la fiabilité ne sont pas toujours documentées, limitant l'applicabilité des données à d'autres scénarios.
- *Limites statistiques* : les petits échantillons ou données non représentatives (p. ex., pannes rares non capturées) rendent les modèles statistiques peu fiables pour prédire les risques.
- *Accessibilité et droits d'utilisation* : certaines bases de données sont soumises à des restrictions d'accès, nécessitant des licences payantes ou des autorisations spécifiques.
- *Confidentialité et sécurité* : l'utilisation de certaines bases de données peut être soumise à des réglementations strictes en matière de protection des données et de confidentialité.
- *Compatibilité et intégration* : il peut être difficile d'intégrer certaines bases de données avec d'autres systèmes informatiques ou logiciels d'analyse.

- *Complexité d'interprétation* : l'analyse requiert une expertise pointue (statistique, domaine métier) pour éviter des erreurs d'interprétation, ce qui peut limiter son utilisation par des non-spécialistes.

En conclusion, bien que les bases de données puissent être un outil efficace pour les études de fiabilité, il est essentiel de prendre en compte les contraintes liées à leur utilisation ainsi que de les exploiter de manière appropriée et intelligente.

3.5.3. Certaines formules utilisées dans le cadre du retour d'expérience

- ***Fréquence d'un événement (w)*** [129, 130]: nombre d'événements observés par unité de temps (heure, an, ...). L'événement peut être une défaillance, réparation, sollicitation, …

$$w = \frac{n}{T} \tag{3.8}$$

Avec :

n : nombre d'événements observés sur la période *T*.

T : période d'observation (surveillance). Pour un groupe constitué de *m* composants surveillés chacun sur une période *d* : $T = m \times d$.

Cette formule peut être utilisée pour calculer les fréquences des demandes et des déclenchements des SIFs.

- ***Taux de défaillance (λ)*** [129, 130]***:*** nombre de défaillances observées par unité de temps (heure, an, ...). Nous faisons l'hypothèse que ce taux est constant (durée de vie utile : les périodes de rodage et de vieillissement sont exclues).

$$\lambda = \frac{n}{\tau} \tag{3.9}$$

Avec :

n : nombre de défaillances observées sur la période τ.

τ : durée cumulée de bon fonctionnement. Pour un groupe constitué de *m* composants surveillés chacun sur une période *d* : $\tau = \sum_{i=1}^{m} \tau_i$. Ou τ_i représente la durée cumulée de bon fonctionnement du composant *i*. Autrement dit, $\tau_i = d - \sum_j DT_j^i$. DT_j^i indique la *j*ème durée d'indisponibilité (*Down Time*) du composant *i*.

Pour une défaillance détectée lors d'un test périodique, la *DT* correspondante doit être prise égale à : $\frac{T_1}{2}$ + temps de réparation. Pour les défaillances détectées par les diagnostics, seuls les temps de réparation sont considérés.

$\sum_j DT_j^i$ représente la durée cumulée d'indisponibilité du composant i sur la période d'observation d. Dans le cas où cette durée est négligeable devant d, alors $\tau \approx T$ et donc $\lambda \approx w$. La formule (2) est utilisée pour calculer les différents taux de défaillances précédents :

$$\begin{cases} \lambda_{DD} = \frac{n_{DD}}{\tau} \\ \lambda_{DU} = \frac{n_{DU}}{\tau} \\ \lambda_{SD} = \frac{n_{SD}}{\tau} \\ \lambda_{SU} = \frac{n_{SU}}{\tau} \end{cases} \quad (3.10)$$

Avec :

n_{DD} : nombre de défaillances dangereuses détectées par les tests de diagnostic ou d'une manière concomitante à leur occurrence.

n_{DU} : nombre de défaillances dangereuses détectées par les tests périodiques ou par une vraie demande (sollicitation).

n_{SD} : nombre de défaillances sûres détectées par les tests de diagnostic ou d'une manière concomitante à leur occurrence.

n_{SU} : nombre de défaillances sûres détectées par les tests périodiques.

- ***Taux de défaillance (λ) dans de le cas de 0 défaillances observées*** [129, 130]**.**

$$\lambda = \frac{\chi^2(\alpha,\ 2)}{2T} \quad (3.11)$$

$\chi^2(\alpha,\ 2)$ représente la distribution du Khi-deux à 2 degrés de liberté et un risque d'erreur égale à α (niveau de confiance = 1- α).

L'avantage de l'Equation (3.11) est la possibilité de calculer le $\lambda_{70\%}$ (α = 30%) dans le cas de 0 défaillances, paramètre requis par la CEI 61511 (2016) : $\lambda_{70\%} = \frac{1.2}{T}$.

- ***Intervalles de confiance relatifs au taux de défaillance :*** $[\lambda_{inf}, \lambda_{sup}]$

L'incertitude liée au taux de défaillance est souvent mise en évidence par la détermination d'un intervalle contenant sa vraie valeur, selon une confiance donnée. Les bornes de cet intervalle sont généralement calculées à l'aide de la distribution du Khi-deux :

$$\begin{cases} \lambda_{inf} = \frac{\chi^2\left(1-\frac{\alpha}{2},\ 2n\right)}{2\tau} \\ \lambda_{sup} = \frac{\chi^2\left(\frac{\alpha}{2},\ 2n+2\right)}{2\tau} \end{cases} \quad (3.12)$$

Les bornes de l'intervalle dépendent du risque d'erreur (α) que le vrai taux de défaillance n'y soit pas inclus. Généralement, α est pris égale à 10%, ce qui conduit à l'établissement d'un l'intervalle bilatéral à 90% de confiance : [$\lambda_{5\%}$, $\lambda_{95\%}$].

- ***Borne sup du taux de défaillance (intervalle unilatéral)*** *:* λ_{sup}

L'équation (8) est utilisée pour calculer la borne supérieure de l'intervalle unilatéral du taux de défaillance avec un certain niveau de confiance, par exemple $\lambda_{70\%}$ (α = 30%). Il convient de préciser qu'une confiance minimale de 70% est requise par la CEI 61511 : 2016.

$$\lambda_{sup} = \frac{\chi^2(\alpha,\ 2n+2)}{2\tau} \tag{3.13}$$

- ***Durées moyennes de réparation : MTTR et MRT*** [129, 130]

La MTTR (Mean Time To Restoration), représente la durée moyenne de restauration (réparation) d'un canal suite à une défaillance dangereuse détectée, tandis que la MRT (Mean Repair Time) représente la durée moyenne de réparation d'un canal suite à une défaillance dangereuse no détectée. L'estimation de ces deux paramètres est triviale :

$$\begin{cases} MTTR = \frac{\sum_{i=1}^{n_{DD}} TTR_i^{DD}}{n_{DD}} \\ MRT = \frac{\sum_{i=1}^{n_{DU}} TTR_i^{DU}}{n_{DU}} \end{cases} \tag{3.14}$$

Avec :

n_{DD} : représente le nombre de réparations liées aux défaillances dangereuses détectées.

n_{DU} : représente le nombre de réparations liées aux défaillances dangereuses non détectées.

TTR_i^{DD} : est la durée de la ième réparation suivant une défaillance dangereuse détectée.

TTR_i^{DU} : est la durée de la ième réparation suivant une défaillance dangereuse non détectée.

- ***Couvertures des diagnostics et des tests : DC, PTC, …*** [129, 130]

$$\begin{cases} DC = \frac{n_{DD}}{n_D} \\ PTC = \frac{n_{DU}^{TP}}{n_{DU}} \\ C_i = \frac{n_{DU}^{i}}{n_{DU}} \end{cases} \tag{3.15}$$

Avec :

n_{DD} : nombre de défaillances dangereuses détectées par les tests de diagnostic ou d'une manière concomitante à leur occurrence.

n_{DU} : nombre de défaillances dangereuses détectées par les tests périodiques ou par une vraie demande (sollicitation).

n_D : nombre de défaillances dangereuses.

n_{DU}^{TP} : nombre de défaillances dangereuses détectées par les tests périodiques.

n_{DU}^{i} : nombre de défaillances dangereuses détectées par les tests partiels de type *i* (y compris les inspections).

Note : un moyen efficace pour déterminer la couverture des différents types de tests est d'organiser les différentes informations relatives aux modes de défaillances et les moyens de détection respectives à l'aide de la méthode AMDEC.

- ***Probabilité de défaillance à la sollicitation*** [129, 130] **:** cette probabilité concerne le non fonctionnement de certains équipements lors des sollicitations (pompe de secours, source d'énergie de secours, …). Cela concerne également la défaillance d'un opérateur ou groupe d'opérateurs à réaliser une action déterminée en réponse à une situation spécifique, par exemple action liée à une alarme. L'estimation ponctuelle de cette probabilité est donnée par la relation suivante :

$$p = \frac{k}{n} \tag{3.16}$$

Avec :

k : nombre de réalisation de l'événement étudié (défaillance à la sollicitation).

n : nombre de sollicitations.

Note : cette estimation peut également être appliquée aux SIFs et aux autres couches de protection (soupapes de sécurité, par exemple). Il reste tout de même recommander de calculer la probabilité de défaillance d'une barrière de sécurité donnée en utilisant les taux de défaillances correspondant.

Pour caractériser l'incertitude liée à cette probabilité, une estimation par intervalle de confiance est généralement effectuée. Plusieurs formules existent dans la littérature pour estimer les bornes de cet intervalle (avec une confiance = 1- α). Nous préconisons dans cette procédure celle fondée sur la loi Beta :

$$\begin{cases} p_{inf} = Beta\left(\frac{\alpha}{2};\ k,\ n-k+1\right) \\ p_{sup} = Beta\left(1-\frac{\alpha}{2};\ k+1,\ n-k\right) \end{cases} \tag{3.17}$$

La borne supérieur d'un intervalle de confiance unilatéral (avec $1-\alpha$ de confiance) peut être déterminée ainsi :

$$p_{sup} = Beta(1-\alpha;\ k+1,\ n-k) \tag{3.18}$$

Dans le cas de 0 défaillances observées, la relation précédente se réduit à :

$$p_{sup} = 1-\alpha^{1/n} \tag{3.19}$$

3.6. Formules analytiques pour l'évaluation de la performance des SIS

Comme nous l'avons mentionné précédemment, la probabilité moyenne de défaillance dangereuse à la demande (PFD_{avg}) et la fréquence moyenne de défaillance dangereuse (PFH), sont les principaux indicateurs de performance liés à la fiabilité du SIS.

Malgré la puissance de modélisation élevée et la meilleure précision de calcul des méthodes d'analyse (AdD, chaines de Markov, …), les analystes de sécurité privilégient encore l'utilisation de formules simplifiées, surtout si elles sont fournies par les normes internationales et les directives industrielles. Il est à noter que chaque sous-système SIS (S, LS et FE) est considéré comme un système KooN, où K canaux identiques sur N doivent fonctionner pour que le sous-système fonctionne. Autrement dit, la défaillance de N-K+1 canaux entraîne la défaillance du sous-système. La performance probabiliste d'une fonction de sécurité, assurée par un SIS donné, est déterminée en calculant et en combinant les performances de ces trois sous-systèmes (S, LS et FE). Ceci peut être exprimé par les formules suivantes [129, 130] :

$$PFD_{avg}^{SIS} = PFD_{avg}^{S} + PFD_{avg}^{LS} + PFD_{avg}^{FE} \tag{3.20}$$

$$PFH^{SIS} = PFH^{S} + PFH^{LS} + PFH^{FE} \tag{3.21}$$

Les probabilités de défaillances de sécurité (PFS, STR) ne sont pas prises en compte dans notre étude.

3.6.1. Formules de IEC 61508 (Ed. 2010)

Les différentes formules concernant la PFD_{moy} et PFH sont regroupées respectivement aux Tableaux 3.6 et 3.7 [131]. Notons que la CEI 61508 considère que la détection d'une défaillance dangereuse, pour un SIS redondant (1oo2, 1oo3, 2oo3) ou non redondant (1oo1 et 2oo2) et fonctionnant en mode fortes demandes ou demande continue, conduit à la mise à l'arrêt d'urgence (activation de la fonction de sécurité) du système surveillé. Ceci, bien entendu, reste vrai pour les défaillances de cause commune ; d'où l'absence du terme $\beta_D \lambda_{DD}$ au niveau du tableau 3.7.

Tableau 3.6 : Formules analytiques relatives aux PFD_{moy} des architectures KooN selon la CEI 61508-6

Architectures	***PFD_{moy}***
1*oo*1	$(\lambda_{DU} + \lambda_{DD})t_{CE}$
1*oo*2	$2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
1*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
2*oo*2	$2\lambda_D t_{CE}$
2*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$

Avec :

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

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

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

- *MTTR (mean time to restoration) : temps moyen de restauration d'une défaillance dangereuse détectée.*
- *MRT (mean repair time) : temps moyen de réparation d'une défaillance dangereuse non détectée.* La norme suppose que $MTTR \cong MRT$.
- $\beta_{DU} = \beta$; $\beta_{DD} = \beta_D$.
- La norme ne tient pas compte des défaillances de cause commune pour les architectures série, en l'occurrence la configuration 2*oo*2.

Tableau 3.7 : Formules analytiques relatives aux *PFH* des architectures KooN selon la CEI 61508-6

Architectures	***PFH***
1*oo*1	λ_{DU}
1*oo*2	$2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$
1*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 (1-\beta)\lambda_{DU} t_{CE} t_{GE} + \beta\lambda_{DU}$
2*oo*2	$2\lambda_{DU}$
2*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU}$

3.6.2. Approche SINTEF

Aux tableaux 3.8 et 3.10 sont présentées respectivement les différentes formules concernant les PFD_{moy} et PFH [132]. Il convient de noter que ces tableaux, donnés par l'organisme SINTEF dans son document [SINTEF, 2011], sont des approximations basées sur le fait de négliger, d'une part, les contributions des défaillances dangereuses détectées et, d'autre part, le facteur β devant l'unité.

Tableau 3.8 : Formules analytiques simplifiées relatives aux PFD_{moy} des architectures KooN selon SINTEF

Voting	PFD calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU} \cdot \tau /2$
1oo2	$\beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2/3$
2oo2	-		$2 \cdot \lambda_{DU} \cdot \tau /2$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^3 /4$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$[\lambda_{DU} \cdot \tau]^2$
3oo3	-		$3 \cdot \lambda_{DU} \cdot \tau /2$
1ooN; N = 2, 3,…	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{1}{N+1} \cdot (\lambda_{DU} \cdot \tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau /2$	+	$\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU} \cdot \tau /2$

Tableau 3.9 : Exemple de valeurs du facteur C_{MooN}

$M \setminus N$	$N = 2$	$N = 3$	$N = 4$	$N = 5$	$N = 6$
$M = 1$	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
$M = 2$	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
$M = 3$	-	-	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
$M = 4$	-	-	-	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
$M = 5$	-	-	-	-	$C_{5oo6} = 4.5$

Tableau 3.10 : Formules analytiques simplifiées relatives aux *PFH* des architectures KooN selon SINTEF

Voting	PFH calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		λ_{DU}
1oo2	$\beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau]^2/\tau$
2oo2	-		$2 \cdot \lambda_{DU}$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau]^3/\tau$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU}$	+	$3 \cdot [\lambda_{DU} \cdot \tau]^2/\tau$
3oo3	-		$3 \cdot \lambda_{DU}$
MooN, M<N; N = 2, 3, ...	$C_{MooN} \cdot \beta \cdot \lambda_{DU}$	+	$\frac{N!}{(N-M+1)!(M-1)!} \cdot \left[(\lambda_{DU} \cdot \tau)^{N-M+1}/\tau\right]$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU}$

Remarque :

Il existe plusieurs logiciels sur le marché pour le calcul des performances probabilistes des SIS. Certains sont basés sur des formules simplifiées, tandis que d'autres utilisent des modèles avancés tels que les AdD (module SIL du logiciel GRIF, par exemple) ou les chaines de Markov (module SILver du logiciel ExSILentia, par exemple).

3.7. Conclusion

Ce chapitre a posé les fondements théoriques et méthodologiques essentiels de l'évaluation probabiliste des performances des systèmes de sécurité, en mettant en lumière son

importance pour la sûreté de fonctionnement dans des contextes industriels critiques. Contrairement aux approches déterministes, l'analyse probabiliste intègre les incertitudes inhérentes aux systèmes complexes, offrant ainsi une vision réaliste de leur résilience face aux défaillances.

Les principaux concepts fiabilité $R(t)$, disponibilité $A(t)$ et maintenabilité $M(t)$ ont été rigoureusement définis et différenciés, soulignant leurs rôles complémentaires dans l'évaluation globale de la performance. Leurs indicateurs associés (MTTF, MTTR, MTBF, MDT) et taux ($\lambda(t)$, $\mu(t)$) ont été analysés, illustrant leur interdépendance et leur impact sur la disponibilité opérationnelle.

L'importance des bases de données génériques (OREDA, SINTEF, exida SERH) a été soulignée, bien que leurs limites (qualité, spécificité, obsolescence) nécessitent une utilisation vigilante. A ce titre, nous avons présenté certaines formules mathématiques pouvant être utiliser pour exploiter le propre retour d'expérience. De plus, les formules analytiques permettant le calcul des deux performances clé des SIS (PFD_{avg} et PFH) fournies par la CEI 61508 et l'organisme SINTEF ont été présentées.

L'ensemble des notions développées constitue une base indispensable pour la mise en œuvre d'une évaluation rigoureuse et quantitative des systèmes de sécurité critiques, en vue de garantir leur efficacité opérationnelle et leur conformité réglementaire.

Chapitre 4

Développement d'une formulation analytique du PFH fondée sur l'approche binomiale

4.1. Introduction

Le quatrième chapitre est consacré à l'étude approfondie des formules de la PFH utilisées dans le cadre de l'évaluation de la performance des systèmes instrumentés de sécurité. En particulier, il présente une généralisation de la PFH, fondée sur une approche binomiale, permettant une modélisation plus souple et plus précise des différentes configurations de systèmes redondants.

Ce chapitre s'inscrit donc dans une démarche critique d'évaluation des formules de calcul de la PFH fournies dans la IEC 61508 (Edition 2010) [133]. L'étude se concentre sur les architectures redondantes courantes (1oo1, 1oo2, 1oo3, 2oo2, 2oo3) et vise à quantifier l'impact des choix de modélisation sur les résultats relatifs à la PFH. Nous allons vérifier si les écarts potentiels soulèvent une question opérationnelle : *dans quelle mesure les simplifications normatives altèrent-elles l'évaluation des risques ?*

Ce chapitre articule une analyse en deux volets complémentaires :

- Identifier les écarts conceptuels entre les deux approches (traitement des défaillances détectées/non détectées, modélisation des causes communes, rôle du temps de réparation),
- Quantifier leur impact numérique sur les résultats de la PFH dans des scénarios réalistes.

4.2. Nouvelle formulation de la PFH basée sur une approche binomiale

4.2.1. Approche générique

Dans cette approche, le temps de réparation MRT pour les défaillances dangereuses non détectées n'est pas pris en compte. Cette hypothèse est valable, car le MRT peut être négligé devant l'intervalle de test périodique (T_1). La fréquence des défaillances, PFH dans notre cas, d'une configuration KooN pourrait être caractérisée comme suit :

$$PFH_{KooN}(t) = C_{N-K}^{N}\ q_{(t)}^{N-K}\ \left(1 - q(t)\right)^{K}\ K\ \lambda_D \qquad (4.1)$$

Où :

$C_{N-K}^{N} = \frac{N!}{(N-K)!K!}$

$q\ (t)$: probabilité de défaillance dangereuse dépendant du temps pour un canal donné dans l'architecture KooN. Cela inclut les contributions des défaillances détectées (DD) et non détectées (DU) : q_{DD}(t) and q_{DU}(t), respectivement.

$$q(t) = q_{DD}(t) + q_{DU}(t) \qquad (4.2)$$

Avec :

$$q_{DD}(t) = \frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}}\left(1 - e^{-(\lambda_{DD}+\mu_{DD})\cdot t}\right) \simeq q_{DD}(\infty) = \frac{\lambda_{DD}}{\lambda_{DD}+\mu_{DD}} \simeq \lambda_{DD}\,.\,MTTR$$

$$q_{DU}(t) \simeq 1 - e^{-\lambda_{DU}\cdot t} \simeq \lambda_{DU}\,.\,t \text{ (entre deux intervalles de tests)}$$

Etant donné que $q(t)$ peut être négligé par rapport à l'unité, soit $1 - q(t) \approx 1$, et en tenant compte des quantités ci-dessus, l'Equation (4.1) peut être réécrite sous la forme suivante :

$$PFH_{KOON}(t) = K\ \mathrm{C}_{N-K}^{N}\ [\lambda_{DD}\,.MTTR + \lambda_{DU}\,.t]^{N-K}.\lambda_{D} \qquad (4.3)$$

4.2.2. Formule de la PFH_{KooN}^{ind}

4.2.2.1. Formulation générique

Il convient de noter que l'équation (4.3) est une approximation conservatrice. De plus, elle ne traite que des défaillances indépendantes (sans défaillances communes : CCF). C'est pourquoi les taux de défaillance doivent être remplacés par leurs parties indépendantes selon le modèle du facteur β [134]. Notons que, pour les architectures de type 1ooN (K = 1), le dernier taux de défaillance doit être conservé tel quel, car il n'y a qu'une seule possibilité de faire échouer la configuration (un seul canal restant en marche). Ainsi, l'équation (4.3) devient :

$$PFH_{KooN}^{ind}(t) = K\,.\,\mathrm{C}_{N-K}^{N}\,[(1-\beta_D)\,\lambda_{DD}\,.MTTR + (1-\beta).\lambda_{DU}\,t\,]^{N-K}\,.\,[\,f_1(\beta_D)\lambda_{DD} + f_1(\beta)\,.\,\lambda_{DU}] \qquad (4.4)$$

Où :

$$f_1(x) = \begin{cases} 1-x & si\ \ K \neq 1\ (K>1) \\ 1 & si\ \ K = 1 \end{cases}$$

L'Equation (4.4) représente la fréquence de défaillance indépendante due à toutes les combinaisons possibles de défaillances (sans prise en compte des CCF). Pour rendre compte de la capacité d'arrêt d'urgence (shutdown) de l'architecture KooN suite à la détection d'une défaillance totale de cette dernière, il faut retirer la combinaison constituée de (N−K+1) défaillances DD, soit :

$$PFH_{KooN}^{ind}(t) = K\,.\,\mathrm{C}_{N-K}^{N}\ [(\,1-\beta_D)\,\lambda_{DD}\,MTTR\,]^{N-K}\cdot f_1\,(\beta_D)\,\lambda_{DD}$$
$$= K\,\mathrm{C}_{N-K}^{N}\,[(\,1-\ \beta_D)\,MTTR\,]^{N-K}\,\lambda_{DD}^{N-K+1}\,.\ f_1\ (\beta_D) \qquad (4.5)$$

Par conséquent, la partie indépendante de la PFH qui considère la capacité d'arrêt d'urgence est donnée par l'équation (4.6) :

$$PFH_{KooN}^{ind}\,(t) = K\,.\,\mathrm{C}_{N-K}^{N}\{[(1-\beta_D)\lambda_{DD}\,.MTTR + (1-\beta).\lambda_{DU}.t]^{N-K}\,[f_1(\beta_D)\,\lambda_{DD} + f_1(\beta).\lambda_{DU}] - [(\,1-\ \beta_D)\,MTTR\,]^{N-K}\,\lambda_{DD}^{N-K+1}\,.\ f_1\ (\beta_D)\} \qquad (4.6)$$

La PFH moyenne correspondante peut être calculée sur l'intervalle de test [0, T_1] comme suit :

$$PFH_{KooN}^{ind} = \frac{1}{T_1}\int_0^{T_1} PFH_{KooN}^{ind}(t)\,dt$$

$$= \frac{K.C_{N-K}^{N}}{T_1}\Big\{[f_1(\beta_D)\,\lambda_{DD} + f_1(\beta).\lambda_{DU}]\int_0^{T_1}[(1-\beta_D).\,\lambda_{DD}.MTTR + (1-\beta)\lambda_{DU}\,t\,]^{N-K}dt - f_1(\beta_D).\lambda_{DD}^{N-K+1}.[(1-\beta_D)\,MTTR\,]^{N-K}.\,T_1\Big\}$$

$$= K.C_{N-K}^{N}.\Big\{\frac{[f_1(\beta_D).\lambda_{DD}+f_1(\beta).\lambda_{DU}]}{T_1.(1-\beta).\lambda_{DU}(N-K+1)}\{[(1-\beta)\,\lambda_{DU}.T_1 + (1-\beta_D)\,\lambda_{DD}.MTTR]^{N-K+1} - [(1-\beta_D)\lambda_{DD}.MTTR]^{N-K+1}\} - f_1(\beta_D)\,\lambda_{DD}^{N-K+1}\,[(1-\beta_D)\,MTTR]^{N-K}\Big\} \quad (4.7)$$

4.2.2.2. Formules du PFH^{ind} pour les architectures standards

Les formules du PFH^{ind} pour les configurations usuelles (1oo1, 1oo2, 1oo3, 2oo2, 2oo3), dérivées de la formule générale (4.7), sont données ci-après (cf. Tableau 4.1). Les expressions sont obtenues en fonction des paramètres K et N spécifiques à chaque configuration.

Tableau 4.1 : Formules de la PFH_{KooN}^{ind} pour les architectures usuelles

KooN	**Formules PFH_{KooN}^{ind}**
1oo1	λ_{DU}
1oo2	$[2(1-\beta_D)\lambda_{DD}\cdot MTTR + (1-\beta)\lambda_{DU}\cdot T_1]\,(\lambda_{DD} + \lambda_{DU}) - 2(1-\beta_D)\lambda_{DD}^2 MTTR$
1oo3	$[3(1-\beta_D)^2\lambda_{DD}^2 MTTR^2 + 3(1-\beta_D)\,\lambda_{DD}\,MTTR(1-\beta)\lambda_{DU}\,T_1 + (1-\beta)^2\lambda_{DU}^2 T_1^2]\,(\lambda_{DD} + \lambda_{DU}) - 3(1-\beta_D)^2\lambda_{DD}^3 MTTR^2$
2oo2	$2(1-\beta)\lambda_{DU}$
2oo3	$[6(1-\beta_D)\lambda_{DD}MTTR + 3(1-\beta)\lambda_{DU}T_1]\cdot[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}] - 6(1-\beta_D)^2\lambda_{DD}^2 MTTR$

L'examen du Tableau 4.1 montre que la PFH_{KooN}^{ind} moyenne des configurations 1oo1 et 2oo2 sont indépendantes des tests périodiques et MTTR, à l'inverse de celle liée aux configurations 1oo2, 1oo3 et 2oo3.

4.2.2.3. Résultats numériques

Le Tableau 4.2 regroupe les valeurs de la PFH_{KooN}^{ind} pour chacune des configurations précédentes, calculées à partir des formules du Tableau 4.1 avec les paramètres suivants : $\lambda_D = 2.5 \times 10^{-5} h^{-1}$; $MTTR$ = 8h ; $T_1 = 8760h$; $\beta \in \{0.1, 0.2\}$; $\beta_D = \beta/2$; DC $\in \{0, 0.6, 0.9, 0.99\}$

Tableau 4.2 : Résultats de la *PFH* (h^{-1}) sans CCF

DC (%)	B (%)	1oo1	1oo2	1oo3	2oo2	2oo3
0	10	2.500×10^{-5}	4.928×10^{-6}	9.712×10^{-7}	4.500×10^{-5}	1.330×10^{-5}
	20	2.500×10^{-5}	4.380×10^{-6}	7.674×10^{-7}	4.000×10^{-5}	1.051×10^{-5}
60	10	1.000×10^{-5}	1.973×10^{-6}	1.561×10^{-7}	1.800×10^{-5}	5.505×10^{-6}
	20	1.000×10^{-5}	1.754×10^{-6}	1.234×10^{-7}	1.600×10^{-5}	4.525×10^{-6}
90	10	2.500×10^{-6}	4.936×10^{-7}	9.965×10^{-9}	4.500×10^{-6}	1.399×10^{-6}
	20	2.500×10^{-6}	4.388×10^{-7}	7.887×10^{-9}	4.000×10^{-6}	1.171×10^{-6}
99	10	2.500×10^{-7}	4.937×10^{-8}	1.250×10^{-10}	4.500×10^{-7}	1.406×10^{-7}
	20	2.500×10^{-7}	4.389×10^{-8}	1.002×10^{-10}	4.000×10^{-7}	1.183×10^{-7}

Nous constatons que plus le DC est élevé, plus PFH^{ind} diminue (car λ_{DU} baisse) et que plus β est élevé, plus PFH^{ind} diminue (car $(1-\beta_D)\lambda_{DD}$ et $(1-\beta)\lambda_{DU}$ diminuent). Cette tendance est confirmée par les courbes de la Figure 4.1 qui montrent l'évolution de PFH^{ind} en fonction du taux de diagnostic (*DC*) et du facteur de cause commune *(β)*.

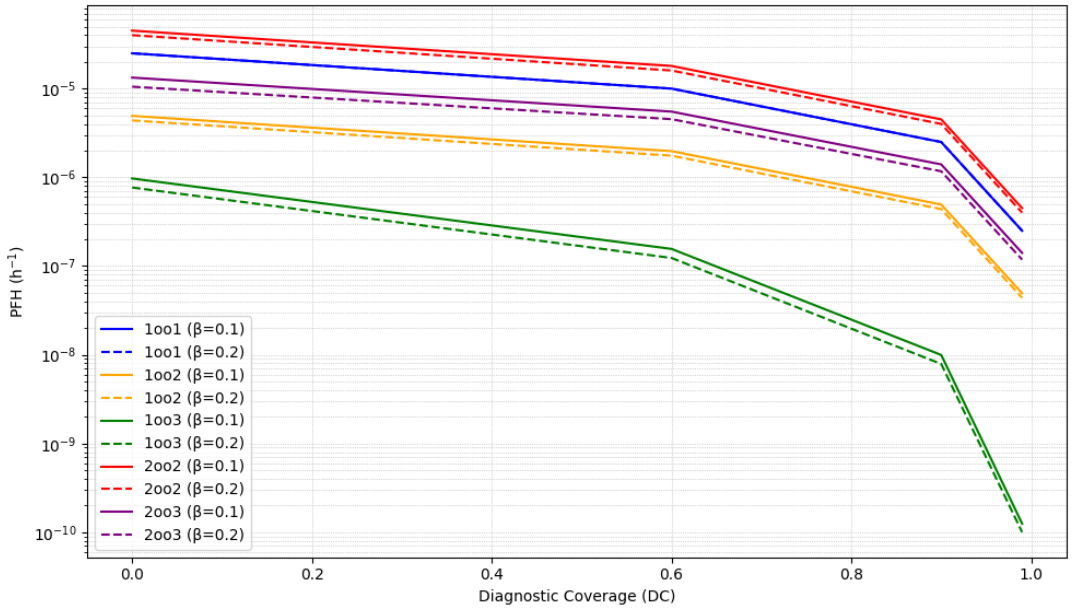


Figure 4.1 : Evolution de la PFH^{ind} selon DC et β pour différentes architectures KooN

4.2.3. Formule de la PFH^{CCF}_{KooN}

4.2.3.1. Contribution générique des CCFs

La norme CEI 61508 considère la contribution des défaillances de cause commune (CCF) par l'ajout de la quantité $\beta\ \lambda_{DU}$. Bien entendu, la contribution des défaillances détectées de cause commune ($\beta_D\lambda_{DD}$) n'est pas prise en compte du fait de l'hypothèse de mise à l'arrêt à la suite de la détection d'une défaillance totale de l'architecture. $\beta\lambda_{DU}$ représente la défaillance de

l'architecture KooN sachant qu'aucune défaillance ne s'est déja produite : c'est à dire, à partir de l'état initial (q = 0). Cependant, une CCF peut se produire en tant que deux canaux restent fonctionnels. Aussi, la contribution des CCFs relatives aux défaillances détectées doit être prise en compte si le nombre de défaillances DD dans la séquence reste toujours inférieur à N-K+1 (ceci est géré via le paramètre *r*).

La contribution des CCFs peut donc être généralisée comme suit :

$$PFH_{KooN}^{CCF} = \sum_{q=0}^{N-K} f_2(q)\, C_q^N q(t)^q \left(1 - q(t)\right)^{N-q} [\, f_3(q,r)\, \beta_D \lambda_{DD} + \beta \lambda_{DU}] \qquad (4.8)$$

Avec :

$$f_2(q) = \begin{cases} 1 & si\ N - q > 1\ \ et\ \ q < N - K + 1 \\ 0 & sinon \end{cases}$$

$$f_3(q,r) = \begin{cases} 1 & si\ N - q + r < N - K + 1 \\ 0 & sinon \end{cases}$$

q représente le nombre de défaillances (détectées ou non) produites dans un état donné de la configuration KooN. Donc la contribution des CCFs n'est seulement possible que si deux canaux restent opérationnels ($q \leq N - 2 \rightarrow N - q > 1$). Come le nombre des défaillances dans une séquence est limité à $N - K + 1$, nous rajoutons une restriction supplémentaire : $q < N - K + 1$. Ces deux conditions gèrent la quantité $f_2(q)$. La norme CEI 61508 ne considère que le cas de q = 0 : $\beta \lambda_{DU}$.

r représente le nombre de défaillances dangereuses détectées dans la séquence avant l'occurence d'une défaillance détectée de cause commune ($\beta_D \lambda_{DD}$). Pour un nombre de défaillance donné (q), la contribution $\beta_D \lambda_{DD}$ n'est comptabilisée que si le nombre r plus le nombre (N-q) ne depasserait pas N − K + 1: d'ou la candition $N - q + r < N - K + 1$ définissant $f_3(q,r)$. La contribution de $\beta_D \lambda_{DD}$, dans une séquence de défaillance contenant moins de $N - K + 1$ défaillances dangereuses détectées (DD), n'est pas considérée dans la CEI 61508.

Pour tenir compte du nombre de défaillances DD (*r*) inclus dans le nombre de défaillances q, nous devons réécrire $q(t)^q$ sous la forme binomiale :

$$q(t)^q = \left((1 - \beta_D)\lambda_{DD}\, MTTR + (1 - \beta).\lambda_{DU}\, t\right)^q = \sum_{r=0}^{q} C_r^q\ [(1 - \beta_D)\lambda_{DD}\, MTTR]^r\ [(1 - \beta)\, \lambda_{DU}\, t]^{q-r} \qquad (4.9)$$

En insérant l'Equation (4.9) dans l'Equation (4.8) et en négligeant $q(t)$ devant l'unité, on obtient :

$$PFH_{KooN}^{CCF}(t) = \sum_{q=0}^{N-K}\left(f_2(q)\, C_q^N \sum_{r=0}^{q}\left\{C_r^q\, [(1-\beta_D)\lambda_{DD}MTTR]^r\, [(1-\beta)\lambda_{DU}\, t\,]^{q-r}\, \cdot \right.\right.$$
$$\left.\left.[f_3(q,r)\, \beta_D\lambda_{DD} + \beta\lambda_{DU}]\right\}\right) \quad (4.10)$$

La quantité moyenne de l'Equation (4.10) est obtenue en intégrant sur la période [0, T_1]:

$$PFH_{KooN}^{CCF} = \frac{1}{T_1}\sum_{q=0}^{N-K}\left(f_2(q)\, C_q^N \sum_{r=0}^{q}\left\{C_r^q\, [(1-\beta_D)\lambda_{DD}MTTR]^r\, [f_3(q,r)\, \beta_D\lambda_{DD} + \right.\right.$$
$$\left.\left.\beta\lambda_{DU}]\, [(1-\beta)\lambda_{DU}\,]^{q-r}\, \int_0^{T_1} t^{q-r}dt\right\}\right) \quad (4.11)$$

$$PFH_{KooN}^{CCF} = \frac{1}{T_1}\sum_{q=0}^{N-K}\left(f_2(q)\, C_q^N \sum_{r=0}^{q}\left\{C_r^q\, [(1-\beta_D)\lambda_{DD}MTTR]^r\, [f_3(q,r)\, \beta_D\lambda_{DD} + \right.\right.$$
$$\left.\left.\beta\lambda_{DU}]\, [(1-\beta)\lambda_{DU}\,]^{q-r} \cdot \frac{{T_1}^{q-r+1}}{q-r+1}\right\}\right) \quad (4.12)$$

D'un point de vue pratique, les cas où $q > 0$ peuvent être négligés. Dans ce manuscrit, par prudence, nous ajoutons le cas $q = 1$. En utilisant l'Equation (4.12), nous obtenons :

$$PFH_{KooN}^{CCF} \approx f_2(0)\, \beta\lambda_{DU} + f_2(1)\, N\left\{(1-\beta)\lambda_{DU}\, \frac{T_1}{2}\, [f_3(1,0)\, \beta_D\lambda_{DD} + \beta\lambda_{DU}] + \right.$$
$$\left.(1-\beta_D)\lambda_{DD}MTTR\, \beta\, \lambda_{DU}\right\} \quad (4.13)$$

Notons que :

$f_2(0) = 1$ seulement si N > 1.

$f_2(1) = 1$ seulement si N-1 > 1 et 1 < N-K+1.

$f_3(1,0) = 1$ seulement si K=1 (architectures 1ooN).

4.2.3.2. Formules de la PFH_{KooN}^{CCF} pour les architectures standards

Les formules de la PFH_{KooN}^{CCF} pour les configurations 1oo1, 1oo2, 1oo3, 2oo2 et 2oo3, dérivées de la formule générale (4.12), sont données au Tableau 4.3. Les expressions sont simplifiées en tenant compte des fonctions de sélection $f_2(q)$ et $f_3(q,r)$, et des paramètres K et N spécifiques à chaque configuration.

Tableau 4.3 : Formules de la PFH_{KooN}^{CCF} pour les architectures standards

KooN	***Formules*** $\boldsymbol{PFH_{KooN}^{CCF}}$
1oo1	0
1oo2	$\beta\lambda_{DU}$
1oo3	$\beta\lambda_{DU} + 3\left[(1-\beta)\lambda_{DU}\frac{T_1}{2}(\beta_D\lambda_{DD} + \beta\lambda_{DU}) + (1-\beta_D)\lambda_{DD}\,MTTR\,\beta\lambda_{DU}\right]$
2oo2	$\beta\lambda_{DU}$
2oo3	$\beta\lambda_{DU} + 3\left[(1-\beta)\lambda_{DU}\frac{T_1}{2} + (1-\beta_D)\lambda_{DD}\,MTTR\right]\beta\lambda_{DU}$

4.2.3.3. Résultats numériques

Les valeurs de la PFH_{KooN}^{CCF} pour les différentes configurations, calculées à partir des formules du Tableau 4.3, sont regroupées au Tableau 4.4. Le jeu de paramètres suivant a été utilisé : $\lambda_D = 2.5 \times 10^{-5} h^{-1}$; $MTTR$ = 8h ; $T_1 = 8760h$; $\beta \in \{0.1, 0.2\}$; $\beta_D = \beta/2$; DC $\in \{0, 0.6, 0.9, 0.99\}$.

Tableau 4.4 : Résultats de la PFH_{KooN}^{CCF} (h^{-1})

DC (%)	**B (%)**	**1oo1**	**1oo2**	**1oo3**	**2oo2**	**2oo3**
0	10	0.000E+00	2.500E-06	3.239E-06	2.500E-06	3.239E-06
	20	0.000E+00	5.000E-06	6.314E-06	5.000E-06	6.314E-06
60	10	0.000E+00	1.000E-06	1.207E-06	1.000E-06	1.119E-06
	20	0.000E+00	2.000E-06	2.369E-06	2.000E-06	2.211E-06
90	10	0.000E+00	2.500E-07	2.908E-07	2.500E-07	2.575E-07
	20	0.000E+00	5.000E-07	5.725E-07	5.000E-07	5.134E-07
99	10	0.000E+00	2.500E-08	2.875E-08	2.500E-08	2.509E-08
	20	0.000E+00	5.000E-08	5.666E-08	5.000E-08	5.016E-08

L'examen de ce Tableau permet les constats suivants :

- Architectures 1oo2 et 2oo2 : les valeurs de la PFH (CCF) sont identiques dans tous les cas. Ceci est logique d'un point de vue physique : les deux architectures comportent deux canaux et la contribution CCF provient uniquement de l'état opérationnel initial (q = 0) (le type de l'architecture n'affecte pas la contribution des CCF à partir de l'état initial).
- Architectures 1oo3 et 2oo3 : pour les deux valeurs de β (0.1 et 0.2), les architectures 1oo3 et 2oo3 présentent la même tendance générale :
  - Lorsque DC = 0, les valeurs de PFH sont identiques.
  - A mesure que le taux de couverture diagnostique (DC) augmente, la PFH du 1oo3 devient progressivement plus élevée que celle du 2oo3.

- Cette différence relative croît avec DC :
  - Pour β = 0.1, elle passe d'environ 7.9% à 14.6% lorsque DC augmente de 0.6 à 0.99.
  - Pour β = 0.2, la tendance est similaire, avec des écarts allant d'environ 7.2% à 13%.

Ainsi, quelle que soit la valeur de β, l'architecture 1oo3 reste légèrement plus pénalisée que la 2oo3 lorsque la couverture diagnostique augmente, mais la différence demeure modérée et cohérente entre les deux cas.

- La différence entre les architectures 1oo3 et 2oo3 est expliqué par le terme : $3(1-\beta)\lambda_{DU}\frac{T1}{2}\beta_D\,\lambda_{DD}$, qui ne figure pas dans la formule de la PFH(2oo3). Cette contribution conduit à un arrêt d'urgence dans le cas de la configuration 2oo3. Ce terme explique également l'augmentation de la différence entre les deux architectures quant DC augmente.
- La PFH diminue avec l'augmentation du DC.
- Doubler le facteur β conduit à une contribution CCF double pour les architectures 1oo2 et 2oo2. Pour les architectures 1oo3 et 2oo3, l'augmentation est légèrement inférieure à 2 fois en raison des termes (1-β) et (1-β_D).
- Le constat le plus important que l'on puisse tirer : l'architecture 1oo3 présente une vulnérabilité aux CCF plus élevée que 2oo3, en termes de PFH, contrairement à la perception courante selon laquelle « plus de redondance est toujours plus sûr ».

La Figure 4.2 montre davantage les constats précédents.

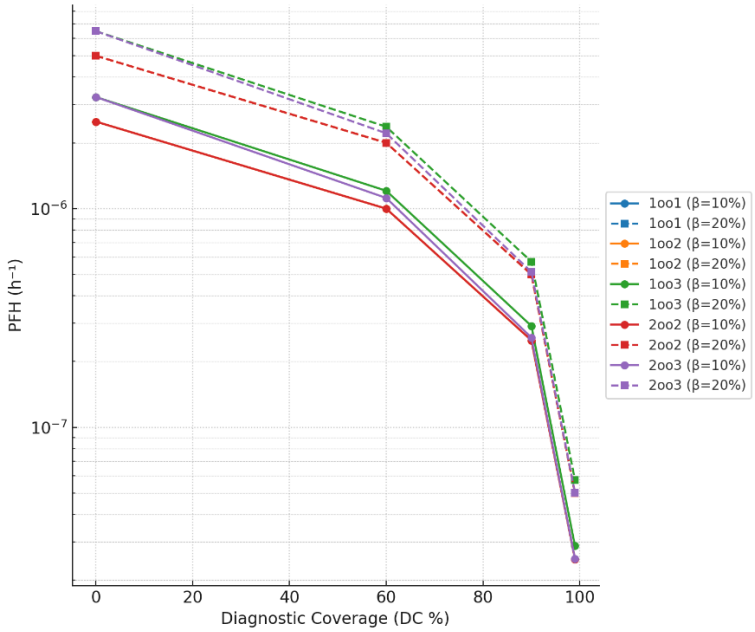


Figure 4.2 : Evolution de la PFH_{KooN}^{CCF} en fonction de DC et β

4.2.4. Formules PFH globales

4.2.4.1. Formules PFH pour les architectures standards

La PFH globale d'une architecture KooN est obtenue par l'addition des termes individuels et de cause commune respectifs : $PFH_{KooN} = PFH_{KooN}^{ind} + PFH_{KooN}^{CCF}$. Ces deux termes sont respectivement donnés par les Equations (4.7) et (4.12). Le Tableau 4.5 regroupe les formules complètes des architectures KooN usuelles. Pour des fins de comparaisons, nous fournissons les formules de la CEI 61508 (Tableau 4.6) et celles présentées dans la référence [135] (Tableau 4.7). Les termes en gras représentent la contribution des CCFs.

Tableau 4.5 : Formules de *PFH* proposées

KooN	***PFH***
1oo1	λ_{DU}
1oo2	$[2(1-\beta_D)\lambda_{DD} \cdot MTTR + (1-\beta)\lambda_{DU} \cdot T_1](\lambda_{DD} + \lambda_{DU}) - 2(1-\beta_D)\lambda_{DD}^2 MTTR + \boldsymbol{\beta\lambda_{DU}}$
1oo3	$[3(1-\beta_D)^2\lambda_{DD}^2 MTTR^2 + 3(1-\beta_D)\lambda_{DD} MTTR(1-\beta)\lambda_{DU} T_1 + (1-\beta)^2\lambda_{DU}^2 T_1^2](\lambda_{DD} + \lambda_{DU}) - 3(1-\beta_D)^2\lambda_{DD}^3 MTTR^2 + \boldsymbol{\beta\lambda_{DU}} + \mathbf{3}\left[\mathbf{(1-\beta)\lambda_{DU}}\frac{\boldsymbol{T_1}}{\mathbf{2}}\mathbf{(\beta_D\lambda_{DD} + \beta\lambda_{DU})} + \mathbf{(1-\beta_D)\lambda_{DD}\, MTTR\, \beta\lambda_{DU}}\right]$
2oo2	$2(1-\beta)\lambda_{DU} + \boldsymbol{\beta\lambda_{DU}}$
2oo3	$[6(1-\beta_D)\lambda_{DD} MTTR + 3(1-\beta)\lambda_{DU} T_1] \cdot [(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}] - 6(1-\beta_D)^2\lambda_{DD}^2 MTTR + \boldsymbol{\beta\lambda_{DU}} + \mathbf{3}\left[\mathbf{(1-\beta)\lambda_{DU}}\frac{\boldsymbol{T_1}}{\mathbf{2}} + \mathbf{(1-\beta_D)\lambda_{DD}\, MTTR}\right]\boldsymbol{\beta\lambda_{DU}}$

Tableau 4.6 : Formules de *PFH* fournies par la CEI 61508 (Ed. 2010)

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

Avec :

- $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
- $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

- MRT (*Mean Repair Time*) : temps moyen de réparation pour les défaillances dangereuses non détectées (DU).

La CEI 61508 ne considère pas les CCFs pour les configurations NooN. Pour les autres architectures, la contribution des CCFs est identique : $\beta\lambda_{DU}$.

Tableau 4.7 : Formules de PFH présentées dans la référence [135]

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

Avec :

- $t_{CE1}=\frac{(1-\beta)\lambda_{DU}}{\lambda_D^{ind}}\left(\frac{T_1}{2}+MRT\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D^{ind}}\,MTTR$
- $t_{GE1}=\frac{(1-\beta)\lambda_{DU}}{\lambda_D^{ind}}\left(\frac{T_1}{3}+MRT\right)+\frac{(1-\beta_D)\lambda_{DD}}{\lambda_D^{ind}}\,MTTR$
- $\lambda_D^{ind}=(1-\beta)\lambda_{DU}+(1-\beta_D)\lambda_{DD}$

Précisons que les formules du Tableau 4.5 ont été développées en s'appuyant sur des modèles markoviens. Les CCFs pour les configurations NooN sont prises en compte. Nous remarquons que les contributions de ces dernières sont très proches de celles développées dans

le cadre de cette thèse. La seule différence étant la non-considération des MRT (dans notre cas), supposés négligeable devant T_1.

L'inspection des Tableaux 4.3, 4.4 et 4.5 permet les remarques suivantes :

- Les formules proposées, ainsi que celles fournies dans [135], rendent compte de la contribution des CCF d'une manière plus large que celles de la norme IEC 61508.
- La CEI 61508 considère une contribution identique des CCFs dans les architectures redondantes.
- Les formules proposées et celles fournies dans [135] présentent des séquences de défaillances ne figurant pas dans les formules de la CEI 61508. Cela dit, cette norme ne comptabilise pas des séquences conduisant à un état dangereux et non pas à un arrêt d'urgence.

4.2.4.2. Comparaison numérique

Dans ce qui suit, nous allons procéder à une comparaison entre les différents résultats numériques fournis par les trois ensembles de formules précédentes. Nous étudions d'abord le cas des PFH individuelles. Cela permet de bien distinguer les écarts potentiels, car non masqués par l'aspect prépondérant des CCFs. Ensuite nous nous attelons au cas des contributions des CCFs, afin de vérifier l'approche proposée (voir Tableau 4.9). Finalement, nous considérons le cas global par la prise en compte simultanée des contributions individuelles et celles des CCFs. Les résultats de ce dernier cas de figure sont regroupés au Tableau 4.10.

- **Contributions individuelles ($\boldsymbol{PFH_{KooN}^{ind}}$) :** le jeu de paramètres précédents est encore considéré (MRT = MTTR). Les résultats obtenus sont donnés au Tableau 4.8. L'examen de ce Tableau permet les constats suivants :

- Pour l'architecture 1oo1, toutes les formules coïncident exactement, car elles présentent la même formule analytique (λ_{DU}).
- Pour l'ensemble des architectures, les valeurs de PFH diminuent avec l'augmentation de DC. De plus, les formules proposées et celles présentées dans [135] produisent des résultats presque identiques. Ceci peut être considéré comme une validation mutuelle. Notons que l'aspect non-conservatif des formules proposées est imputable à la non-considération des durées MRT.
- Les formules de la CEI 61508 donnent des valeurs numériques inférieures par rapport aux autres formules (sauf dans le cas de l'architecture 2oo2). L'écart constaté augmente avec l'augmentation du DC donc celle de λ_{DD} (voir Figure 4.3). Nous

pouvons expliquer cette tendance par la non prise en compte de la CEI 61508 de certaines séquences de défaillances contenant des défaillances DD.

- Pour l'architecture 2oo2, les résultats de l'IEC 61508 sont conservatifs. Ceci est explique par le fait que l'expression analytique utilisée (2 λ_{DU}) incorpore les deux partitions de défaillances individuelles et de causes commune.

Tableau 4.8 : Comparaisons des *PFH* individuelles

KooN	***DC* (%)**	***β* (%)**	**Formules proposées**	**Formules IEC 61508**	**Formules Réf [135]**
1oo1	0	10	2.500E-05	2.500E-05	2.500E-05
		20	2.500E-05	2.500E-05	2.500E-05
	60	10	1.000E-05	1.000E-05	1.000E-05
		20	1.000E-05	1.000E-05	1.000E-05
	90	10	2.500E-06	2.500E-06	2.500E-06
		20	2.500E-06	2.500E-06	2.500E-06
	99	10	2.500E-07	2.500E-07	2.500E-07
		20	2.500E-07	2.500E-07	2.500E-07
1oo2	0	10	4.928E-06	4.443E-06	4.937E-06
		20	4.380E-06	3.510E-06	4.388E-06
	60	10	1.973E-06	7.366E-07	1.977E-06
		20	1.754E-06	6.054E-07	1.757E-06
	90	10	4.936E-07	4.742E-08	4.945E-07
		20	4.388E-07	3.969E-08	4.396E-07
	99	10	4.937E-08	5.533E-10	4.946E-08
		20	4.389E-08	4.657E-10	4.397E-08
1oo3	0	10	9.712E-07	8.781E-07	9.757E-07
		20	7.674E-07	6.167E-07	7.709E-07
	60	10	1.561E-07	6.042E-08	1.570E-07
		20	1.233E-07	4.592E-08	1.241E-07
	90	10	9.965E-09	1.008E-09	1.003E-08
		20	7.887E-09	7.949E-10	7.937E-09
	99	10	1.250E-10	1.466E-12	1.257E-10
		20	1.002E-10	1.168E-12	1.008E-10
2oo2	0	10	4.500E-05	5.000E-05	4.500E-05
		20	4.000E-05	5.000E-05	4.000E-05
	60	10	1.800E-05	2.000E-05	1.800E-05
		20	1.600E-05	2.000E-05	1.600E-05
	90	10	4.500E-06	5.000E-06	4.500E-06
		20	4.000E-06	5.000E-06	4.000E-06
	99	10	4.500E-07	5.000E-07	4.500E-07
		20	4.000E-07	5.000E-07	4.000E-07
2oo3	0	10	1.330E-05	1.333E-05	1.333E-05
		20	1.051E-05	1.053E-05	1.053E-05
	60	10	5.505E-06	2.210E-06	5.515E-06
		20	4.525E-06	1.816E-06	4.534E-06
	90	10	1.399E-06	1.422E-07	1.402E-06
		20	1.171E-06	1.191E-07	1.174E-06
	99	10	1.406E-07	1.660E-09	1.409E-07
		20	1.183E-07	1.397E-09	1.186E-07

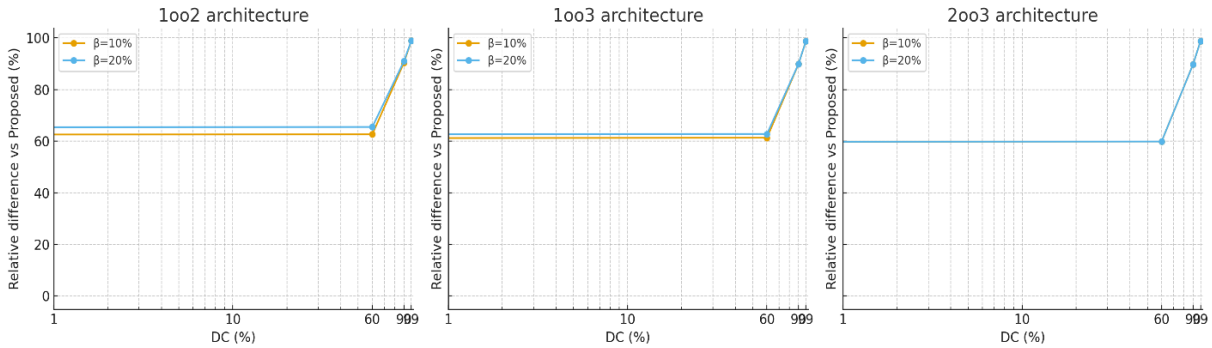


Figure 4.3 : Différence relative entre les formules proposées et de celles de la CEI 61508

- **Contribution des CCFs (PFH_{KooN}^{CCF}) :** les résultats obtenus sont donnés au Tableau 4.9.

Tableau 4.9 : Comparaisons des *PFH* CCFs

KooN	*DC* (%)	*β* (%)	Formules proposées	Formules IEC 61508	Formules [Omeiri]
1oo1	0	10	0.000E+00	0.000E+00	0.000E+00
		20	0.000E+00	0.000E+00	0.000E+00
	60	10	0.000E+00	0.000E+00	0.000E+00
		20	0.000E+00	0.000E+00	0.000E+00
	90	10	0.000E+00	0.000E+00	0.000E+00
		20	0.000E+00	0.000E+00	0.000E+00
	99	10	0.000E+00	0.000E+00	0.000E+00
		20	0.000E+00	0.000E+00	0.000E+00
1oo2	0	10	2.500E-06	2.500E-06	2.500E-06
		20	5.000E-06	5.000E-06	5.000E-06
	60	10	1.000E-06	1.000E-06	1.000E-06
		20	2.000E-06	2.000E-06	2.000E-06
	90	10	2.500E-07	2.500E-07	2.500E-07
		20	5.000E-07	5.000E-07	5.000E-07
	99	10	2.500E-08	2.500E-08	2.500E-08
		20	5.000E-08	5.000E-08	5.000E-08
1oo3	0	10	3.239E-06	2.500E-06	3.240E-06
		20	6.314E-06	5.000E-06	6.316E-06
	60	10	1.207E-06	1.000E-06	1.208E-06
		20	2.369E-06	2.000E-06	2.369E-06
	90	10	2.908E-07	2.500E-07	2.909E-07
		20	5.725E-07	5.000E-07	5.726E-07
	99	10	2.875E-08	2.500E-08	2.875E-08
		20	5.666E-08	5.000E-08	5.667E-08
2oo2	0	10	2.500E-06	0.000E+00	2.500E-06
		20	5.000E-06	0.000E+00	5.000E-06
	60	10	1.000E-06	0.000E+00	1.000E-06
		20	2.000E-06	0.000E+00	2.000E-06
	90	10	2.500E-07	0.000E+00	2.500E-07
		20	5.000E-07	0.000E+00	5.000E-07
	99	10	2.500E-08	0.000E+00	2.500E-08
		20	5.000E-08	0.000E+00	5.000E-08
2oo3	0	10	3.239E-06	2.500E-06	3.240E-06
		20	6.314E-06	5.000E-06	6.316E-06
	60	10	1.119E-06	1.000E-06	1.119E-06
		20	2.211E-06	2.000E-06	2.211E-06

	90	10	2.575E-07	2.500E-07	2.575E-07
		20	5.134E-07	5.000E-07	5.134E-07
	99	10	2.509E-08	2.500E-08	2.509E-08
		20	5.016E-08	5.000E-08	5.016E-08

L'inspection du Tableau 4.9 soulève les observations suivantes :

- L'architecture 1oo1 n'est pas vulnérable aux CCFs : contribution nulle.
- Pour l'architecture 1oo2, les trois ensembles de formules fournissent les mêmes contributions, puisque la même formule est utilisée ($\beta\lambda_{DU}$).
- La CEI 61508 fournie les mêmes contributions CCF pour les architectures redondantes.
- Pour l'architecture 2oo2 les formules proposées et celles figurant dans [135] engendre des résultats identiques, d'une part, et similaires au cas de la configuration 1oo2 ($\beta\lambda_{DU}$). Quant à la CEI 61508, des valeurs nulles sont dérivées. En effet, cette norme ne considère pas les CCFs. Cependant, la contribution individuelle ($2\ \lambda_{DU}$) comptabilise deux fois les CCFs : $2\ \lambda_{DU} = 2(1-\beta)\lambda_{DU} + \boldsymbol{2\beta\lambda_{DU}}$. C'est pour cette raison que la CEI 61508 fournie une contribution individuelle supérieure à celle donnée par les autres approches pour l'architecture 2oo2.
- Pour les architectures 1oo3 et 2oo3, les formules proposées et de la référence [135] induisent des valeurs numériques presque identiques, tandis que la CEI 61508 engendre des valeurs très légèrement optimistes. L'écart des valeurs diminue avec l'augmentation de DC (voir Figure 4.4).

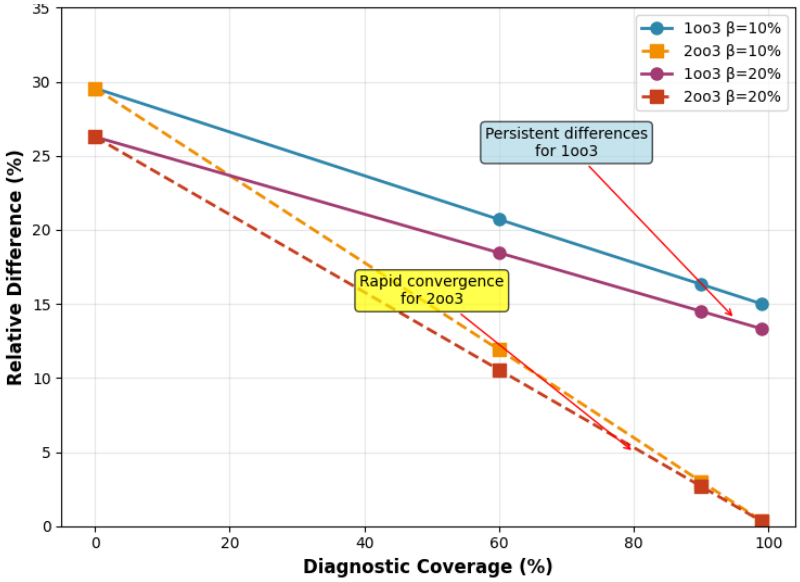


Figure 4.4 : Différence relative entre les résultats des formules proposées et de celles de la CEI 61508 (CCFs)

- **PFH globales (PFH_{KooN}) :** les résultats obtenus sont donnés au Tableau 4.10. Ces résultats tiennent compte des deux contributions précédentes (la somme). Cela dit, les remarques faites précédemment (pour les deux cas) restent valables.

Tableau 4.10 : Comparaisons des *PFH* globales

KooN	*DC* (%)	β (%)	Formules proposées	Formules IEC 61508	Formules [135]
1oo1	0	10	2.500E-05	2.500E-05	2.500E-05
		20	2.500E-05	2.500E-05	2.500E-05
	60	10	1.000E-05	1.000E-05	1.000E-05
		20	1.000E-05	1.000E-05	1.000E-05
	90	10	2.500E-06	2.500E-06	2.500E-06
		20	2.500E-06	2.500E-06	2.500E-06
	99	10	2.500E-07	2.500E-07	2.500E-07
		20	2.500E-07	2.500E-07	2.500E-07
1oo2	0	10	7.428E-06	6.943E-06	7.437E-06
		20	9.380E-06	8.510E-06	9.388E-06
	60	10	2.973E-06	1.737E-06	2.977E-06
		20	3.754E-06	2.605E-06	3.757E-06
	90	10	7.436E-07	2.974E-07	7.445E-07
		20	9.388E-07	5.397E-07	9.396E-07
	99	10	7.437E-08	2.555E-08	7.446E-08
		20	9.389E-08	5.047E-08	9.397E-08
1oo3	0	10	4.210E-06	3.378E-06	4.216E-06
		20	7.081E-06	5.617E-06	7.087E-06
	60	10	1.363E-06	1.060E-06	1.365E-06
		20	2.492E-06	2.046E-06	2.493E-06
	90	10	3.008E-07	2.510E-07	3.009E-07
		20	5.804E-07	5.008E-07	5.805E-07
	99	10	2.888E-08	2.500E-08	2.888E-08
		20	5.676E-08	5.000E-08	5.677E-08
2oo2	0	10	4.750E-05	5.000E-05	4.750E-05
		20	4.500E-05	5.000E-05	4.500E-05
	60	10	1.900E-05	2.000E-05	1.900E-05
		20	1.800E-05	2.000E-05	1.800E-05
	90	10	4.750E-06	5.000E-06	4.750E-06
		20	4.500E-06	5.000E-06	4.500E-06
	99	10	4.750E-07	5.000E-07	4.750E-07
		20	4.500E-07	5.000E-07	4.500E-07
2oo3	0	10	1.654E-05	1.583E-05	1.657E-05
		20	1.682E-05	1.553E-05	1.685E-05
	60	10	6.624E-06	3.210E-06	6.634E-06
		20	6.736E-06	3.816E-06	6.745E-06
	90	10	1.657E-06	3.922E-07	1.660E-06
		20	1.684E-06	6.191E-07	1.687E-06
	99	10	1.657E-07	2.666E-08	1.660E-07
		20	1.685E-07	5.140E-08	1.688E-07

- ***Architecture 1oo1 :*** résultats identiques pour trois ensembles des formules.
- ***Architecture 1oo2 :*** la formule nouvellement proposée et celle fournie dans [135] exhibent des résultats très proches. La formule de la CEI 61508 présente des valeurs

numériques moindres. Toutefois, l'ensembles des formules résultent dans le même SIL en fonction des paramètres utilisés.

- ***Architecture 1oo3 :*** mêmes remarques précédentes, mais l'écart relatif à la formule de la CEI 61508 s'est réduit à cause de la dominance de la contribution des CCFs au détriment des contributions individuelles.
- ***Architecture 2oo2 :*** la formule de la CEI 61508 fournie des valeurs légèrement supérieures à celles des deux autres ensembles de formules à cause de la double prise en compte du terme $\beta\lambda_{DU}$, comme nous l'avions déjà indiqué.
- ***Architectures 2oo3 :*** les écarts avec la formule normative s'accentuent avec l'augmentation du DC. Pour les DC 90% et 99%, la CEI 61508 présente des SILs moindres, ce qui est dangereux (voir Figure 4.5). Ceci est imputable à la forte contribution des défaillances individuelles devant celles des CCFs (tendance inversée avec l'architecture 1oo3).
- ***En conclusion :*** pour les architectures NooN, la CEI 61508 présente des résultats conservatifs est donc acceptables. Dans le cadre de l'architecture 1oo2, la CEI 61508 engendre des résultats non conservatifs qui pourraient conduire à des SILs moindres. Pour les architectures redondantes d'ordre supérieur (à partir de 1oo3), les écarts avec les formules normatives se réduisent et le risque d'avoir des SIL inférieurs est très faible. En revanche, pour les architectures de vote majoritaire (comme 2oo3), il est fort probable que les formules normatives induisent des SILs bas, surtout pour des valeurs de DC élevées.

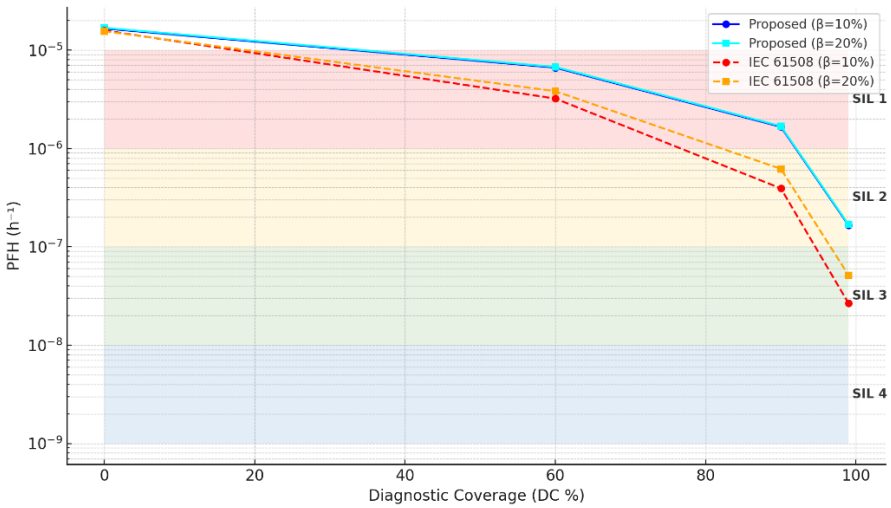


Figure 4.5 : PFH relative à l'architecture 2oo3

4.3. Conclusion

L'objet premier du quatrième chapitre était le développement d'une formulation analytique générale et inédite relative à la PFH des configurations KooN, en se basant sur une approche binomiale. Cette généralisation rend compte de l'hypothèse selon laquelle l'EUC est mis à l'arrêt en cas de détection de N-K+1 défaillances dangereuses. Elle comptabilise donc toutes les séquences de défaillances possibles conduisant à un état dangereux, sans tenir compte des séquences engendrant des arrêts de sécurité. Une deuxième spécificité de cette proposition est la prise en compte des toutes les séquences de défaillances de causes communes tout en respectant l'hypothèse énoncé précédemment. En effet, le modèle proposé pour la contribution des CCFs est unique.

Nous avons également effectué des comparaisons numériques avec les formules de la CEI 61508, d'une part, et celles proposées dans [135] en utilisant une approche markovienne, d'autre part. Les formules développées dans le cadre de ce travail doctoral et celles de [135] fournissent des résultats presque identiques. En revanche, ils révèlent des écarts conceptuels et numériques parfois significatifs (cas de l'architecture 2oo3), avec des implications directes sur les niveaux SIL. Les écarts conceptuels concernent la non prise en compte de la CEI 61508 de certaines séquences de défaillances contenant des défaillances DD, ce qui peut conduire à une sous-estimation de la PFH. Les nouvelles formules offrent une modélisation plus granulaire des défaillances, intégrant à la fois des combinaisons exhaustives des défaillances individuelles et des contributions explicites des CCFs. Notons que *la rigueur de modélisation n'est pas un luxe académique, mais une exigence opérationnelle pour les systèmes critiques.*

Ces conclusions appellent à une révision ciblée des standards, intégrant les avancées récentes en modélisation des défaillances.

Chapitre 5

Développement d'une formulation analytique du PFD_{avg} avec tests échelonnés

5.1. Introduction

Ce chapitre traite de la modélisation probabiliste des systèmes instrumentés de sécurité (SIS), en se focalisant sur le calcul de la probabilité de défaillance dangereuse sur demande (PFD_{avg}) pour des architectures KooN soumises à des tests échelonnés ou décalés (*staggered tests)*. Cette stratégie de tests à l'avantage de réduire la PFD_{avg}, par rapport aux tests simultanés. Notons qu'une formulation analytique générale tenant compte de ce type de test est inexistante. Ce chapitre tente donc de combler une lacune majeure des modèles existants, par la prise en compte de la politique des tests échelonnés dans le calcul de la PFD_{avg}. Plus précisément, nous donnons des clarifications concernant cette politique de tests, nous étudions son impact sur la PFD_{avg} et nous fournissons une généralisation de cette quantité valable pour toute architecture KooN.

5.2. Stratégie de tests échelonnés

Cette stratégie consiste à tester plusieurs éléments selon un ordre chronologique et non pas d'une manière simultanée, tout en conservant la même périodicité de tests (même T_1) pour ces différents éléments [136]. Pour ce faire, il convient tout simplement de distinguer les instants des premiers tests de ces éléments (θ_i), où *i* représente l'élément *i* (voir Figure 5.1).

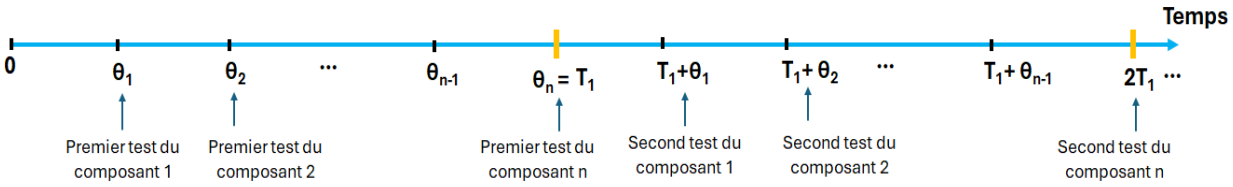


Figure 5.1 : Chronologie des tests échelonnés dans une architecture constituée de *n* éléments

Il importe de signaler que cette manière de tests pour les architectures redondantes ne nécessite pas l'arrêt de production (shutdown), car un seul élément (canal) est testé à la fois.

Si l'on ne considère que les défaillances dangereuses non détectées (DU) et négligeons les temps de réparations, la probabilité de défaillance dangereuse d'un canal *i* peut être écrite sous la forme suivante :

$$PFD_i(t) = \begin{cases} 1 - e^{-\lambda_{DUi}\, t}, \ si\ 0 \le t \le \theta_i \\ \\ 1 - e^{-\lambda_{DUi}\left((t-\theta_i) - Int\left(\frac{t-\theta_i}{T_1}\right)\cdot T_1\right)}, \ si \ \ t > \theta_i \end{cases} \tag{5.1}$$

Avec :

λ_{DUi} : taux de défaillance dangereuse non détectée du composant i.

θ_i : instant du premier test du composant i.

T_1 : intervalle de test périodique.

Int : partie entière de la division.

La figure 5.2 représente l'évolution de la PFD d'un seul canal en fonction du temps. Notons que pour un seul canal, la PFD_{avg} (quand t augmente) n'est pas différente de celle obtenue sans décalage du test : $\theta_1 = T_1$ (voir Figure 5.3).

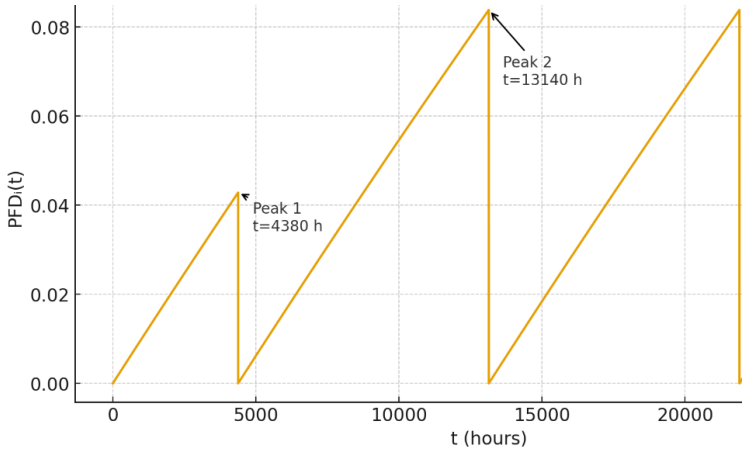


Figure 5.2 : Evolution de la PFD d'un seul canal en fonction du temps (λ_{DU}=1E-5/h ; T_1= 8760 et θ_1=4380)

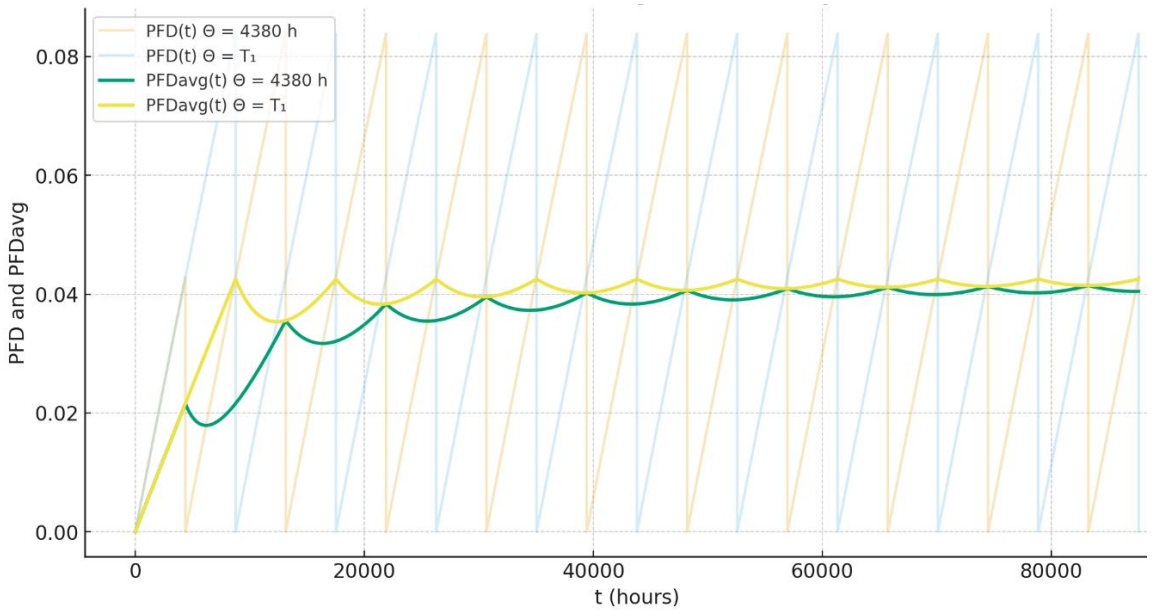


Figure 5.3 : Evolution de la PFD_{avg} d'un seul canal en fonction du temps (λ_{DU}=1E-5/h ; T_1= 8760)

La Figue 5.3 montre qu'avec l'augmentation du temps la différence initiale entre les deux cas se réduit nettement. Sur plusieurs cycles, les deux courbes PFD_{avg} convergent vers la même valeur asymptotique (dans notre cas, environ $0.0425 \approx \lambda_{DU} \frac{T_1}{2}$). Ceci s'explique par le fait que l'effet de θ_1 n'affecte que les premiers cycles. Après plusieurs cycles, le système atteint un régime périodique permanent où la PFD_{avg} à long terme ne dépend plus du moment où le premier test a eu lieu (θ_1).

5.3. Etablissement de la PFD_{avg} des architectures usuelles

Nous allons dans cette section établir les formules analytiques relatives aux architectures KooN classiques. Précisons que le cas de l'architecture 1oo1 a été traité dans la section précédente.

5.3.1. Architecture 1oo2

Considérons le cas de l'architecture 1oo2, où chaque canal est testé à intervalles réguliers T_1, avec un décalage temporel θ_1 entre les tests des deux canaux. Selon la Figure 5.1, l'instant du premier test pour le premier canal est θ_1, tandis que ce du deuxième canal est $\theta_2 = T_1$. Les courbes de la PFD de chaque canal sont fournies à la figure 5.4.

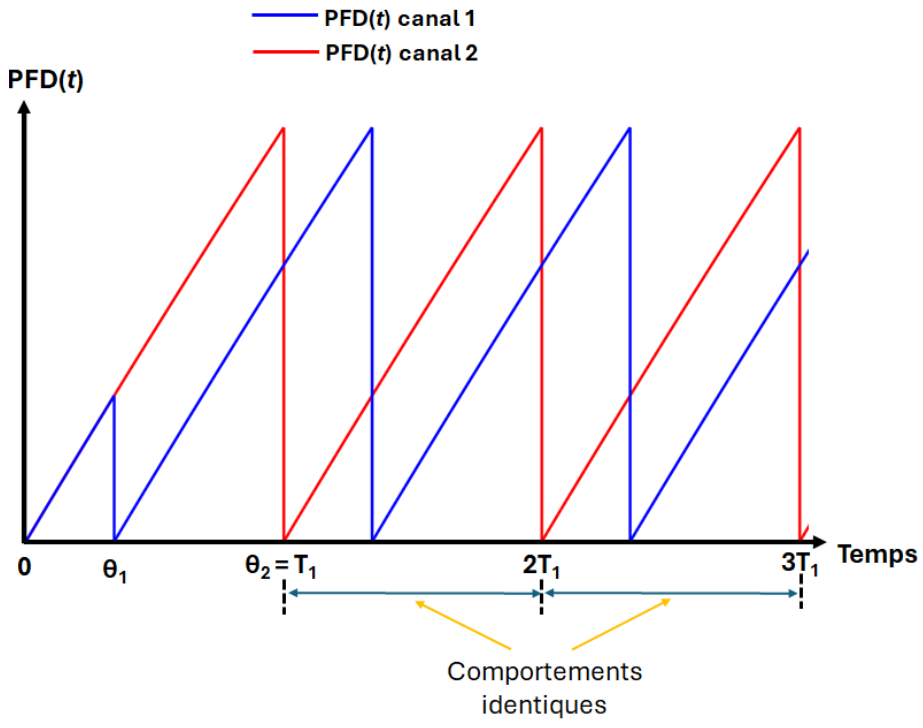


Figure 5.4 : Evolution de la PFD de chacun des deux canaux

L'indisponibilité du système 1oo2 en fonction de celles des deux canaux est donnée par l'expression suivante :

$$PFD_{1oo2}(t) = PFD_1(t) \cdot PFD_2(t) \tag{5.2}$$

Où $PFD_1(t) \cdot PFD_2(t)$ sont données par la relation (5.1). Elle peut être simplifiée sous une forme linéaire (Equation 5.3) si les taux de défaillances sont trop faibles ($\lambda_{DU}\, t << 1$).

$$PFD_i(t) = \begin{cases} \lambda_{DUi}\, t\,, \; si\; 0 \le t \le \theta_i \\ \lambda_{DUi}\left((t-\theta_i) - Int\left(\frac{t-\theta_i}{T_1}\right)\cdot T_1\right), \; si \;\; t > \theta_i \end{cases} \tag{5.3}$$

La PFD_{avg} de l'architecture 1oo2 peut facilement être obtenue sur une période d'observation *T*.

$$PFD_{1oo2}^{avg}(0,T) = \frac{1}{T}\int_0^T PFD_1(t)\, PFD_2(t)\, dt \tag{5.4}$$

Comme le comportement de l'architecture 1oo2 est identique après le premier cycle de tests périodiques (voir Figure 5.4), nous pouvons limiter cet intégral sur une seule période d'amplitude T_1 (par exemple, l'intervalle [T_1, $2T_1$]).

$$PFD_{1oo2}^{avg}(0,T) \approx\; PFD_{1oo2}^{avg}(T_1, 2T_1) = \frac{1}{T_1}\int_{T_1}^{2T_1}\; PFD_1(t)\cdot PFD_2(t)\, dt \tag{5.5}$$

Pour simplifier cette intégration, nous changeons ses bornes de 0 à T_1 et réécrivons les probabilités de défaillances des deux canaux comme suit :

$$PFD_1(t) \approx \begin{cases} \lambda_{DU}\,(t + T_1 - \theta_1)\,, \; si\; 0 \le t \le \theta_1 \\ \lambda_{DU}(t-\theta_1)\,, \;\; si\; \theta_1 < t \le T_1 \end{cases} \tag{5.6}$$

$$PFD_2(t) \approx\; \lambda_{DU}\, t\;,\;\; 0 \le t \le T_1 \tag{5.7}$$

L'intégrale de l'Equation (5.5) peut donc être réécrit comme suit :

$$PFD_{1oo2}^{avg}(T_1, 2T_1) = \frac{1}{T_1}\int_0^{T_1}\; PFD_1(t)\cdot PFD_2(t)\, dt \tag{5.8}$$

En considérant les relations (5.6) et (5.7) :

$$PFD_{1oo2}^{avg} = \frac{1}{T_1}\left(\int_0^{\theta_1} PFD_1(t)\cdot PFD_2(t)\,dt + \int_{\theta_1}^{T_1} PFD_1(t)\cdot PFD_2(t)\,dt\right)$$

$$= \frac{1}{T_1}\left(\int_0^{\theta_1} \lambda_{DU}^2\,(t + T_1 - \theta_1)\,t\;\;dt + \int_{\theta_1}^{T_1} \lambda_{DU}^2\,(t-\theta_1)\,t\,dt\right)$$

$$PFD_{1oo2}^{avg} = \lambda_{DU}^2\left(\frac{T_1^2}{3} + \frac{\theta_1^2}{2} - \frac{T_1\theta_1}{2}\right) \quad (5.9)$$

Pour le cas des tests simultanés ($T_1 = \theta_1$), on retrouve la fameuse expression $\lambda_{DU}^2\frac{T_1^2}{3}$ [137]. Bien entendu, la quantité donnée par la relation (5.9) est inférieure à celle relative aux tests simultanés, car $\theta_1 < T_1$.

Il serait intéressant de définir la valeur de θ_1 pour laquelle la PFD_{1oo2}^{avg} est minimale. Pour ce faire, il suffit de rechercher la valeur de $\theta_1$qui annule la dérivée de PFD_{1oo2}^{avg} par rapport à θ_1. Autrement dit, la variation de PFD_{1oo2}^{avg} en fonction de la variation de θ_1(voir Figure 5.5).

$$\frac{d}{d\theta_1}\left(PFD_{1oo2}^{avg}\right) = 0 \Longrightarrow \lambda_{DU}^2\left(\theta_1 - \frac{T_1}{2}\right) = 0 \;\Longrightarrow\; \theta_1 = \frac{T_1}{2} \quad (5.10)$$

Pour cette valeur de θ_1, l'expression (5.9) devient :

$$PFD_{1oo2}^{avg} = \lambda_{DU}^2 T_1^2\cdot\frac{5}{24} \approx \lambda_{DU}^2\frac{T_1^2}{3}\cdot\frac{5}{8} = 0.625\,\lambda_{DU}^2\frac{T_1^2}{3} = 0.625\,PFD_{1oo2}^{avg\,(\text{tests simultanés})} \quad (5.11)$$

Le nombre 0.2083 peut être vu comme un facteur de réduction optimal dû au décalage des tests liés à l'architecture 1oo2. La Figure 5.6 montre la différence entre le comportement d'une architecture 1oo2 sans et avec stratégie de tests échelonnés ($\theta_1 = T_1/2$).

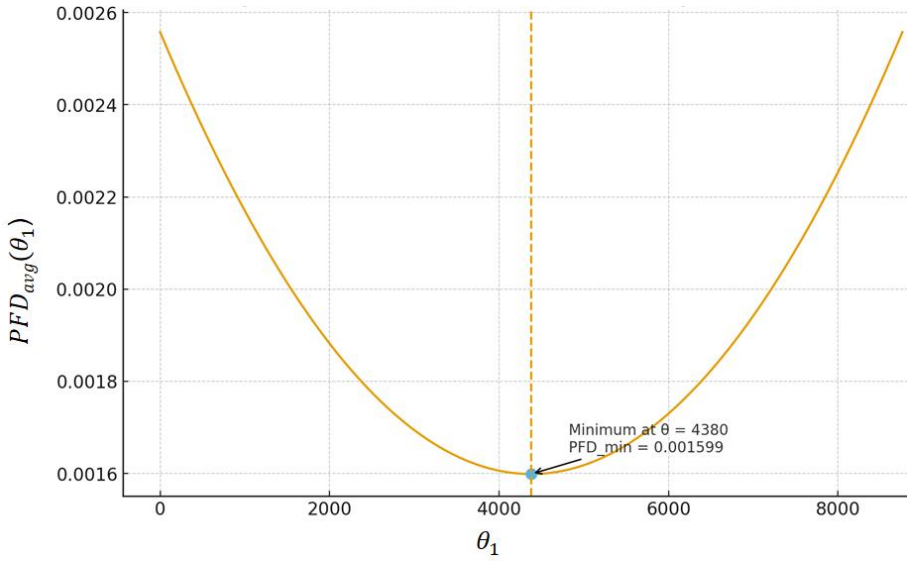


Figure 5.5 : Variation de la PFD_{1oo2}^{avg} en fonction de θ_1

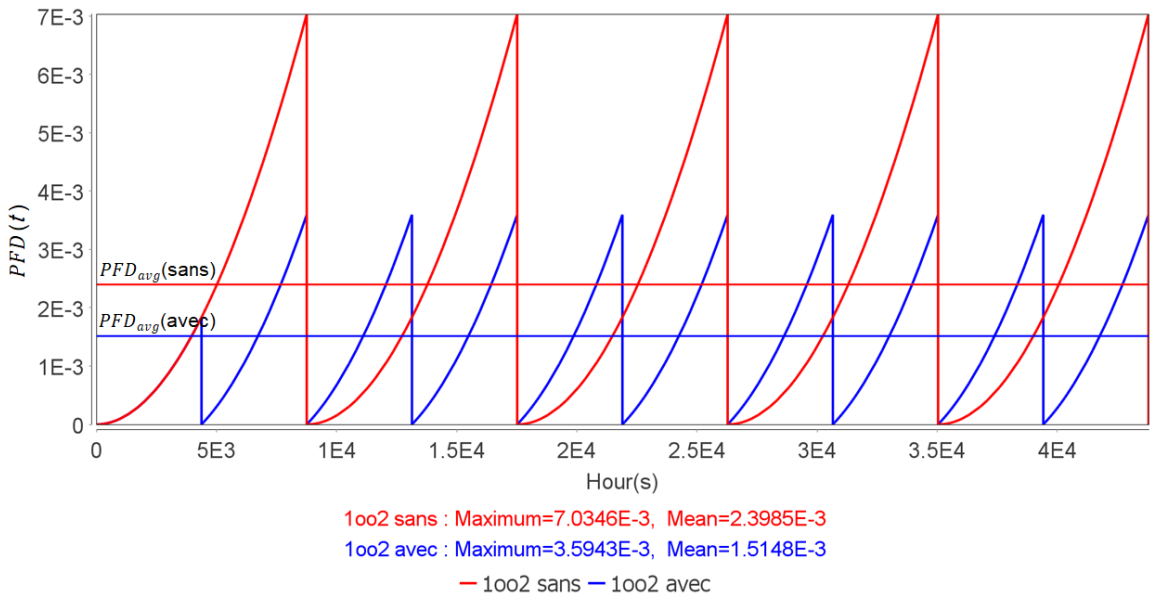


Figure 5.6 : PFD_{1oo2}^{avg} sans et avec stratégie de tests échelonnés

5.3.2. Architecture 2oo2

Nous allons traiter cette architecture afin de confirmer les conclusions relatives au cas d'un seul canal (1oo1) : la PFD_{avg} ne dépendrait plus du décalage quand t augmente. Cela signifierait que la formule classique de la PFD_{avg} (sans décalage) [137] reste valable. Comme dans le cas de l'architecture 1oo2, chaque canal est testé à intervalles réguliers T_1, avec un décalage temporel θ_1 entre les tests des deux canaux. L'instant du premier test pour le premier canal est θ_1, tandis que ce du deuxième canal est $\theta_2 = T_1$. Les courbes de la PFD de chaque canal sont les mêmes fournies à la Figure 5.4. La PFD_{2oo2}^{avg} est obtenu comme suit :

$$PFD_{2oo2}^{avg}(T_1, 2T_1) = \frac{1}{T_1}\int_0^{T_1} \left(PFD_1(t) + PFD_2(t) - PFD_1(t)\cdot PFD_2(t)\right) dt$$

$$\approx \frac{1}{T_1}\int_0^{T_1} \left(PFD_1(t) + PFD_2(t)\right) dt$$

$$PFD_{2oo2}^{avg} = \frac{1}{T_1}\left(\int_0^{\theta_1}\left(PFD_1(t) + PFD_2(t)\right) dt + \int_{\theta_1}^{T_1}\left(PFD_1(t) + PFD_2(t)\right) dt\right)$$

$$= \frac{1}{T_1}\left(\int_0^{\theta_1} \left(\lambda_{DU}\,(t + T_1 - \theta_1) + \lambda_{DU}\,t\right) dt + \int_{\theta_1}^{T_1}\left(\lambda_{DU}\,(t-\theta_1) + \lambda_{DU}\,t\right) dt\right)$$

$$PFD_{2oo2}^{avg} = \frac{\left(\lambda_{DU}T_1\theta_1 + \lambda_{DU}\left(T_1^2 - T_1\theta_1\right)\right)}{T_1} = \lambda_{DU}T_1 \qquad (5.12)$$

Remarquons l'indépendance de cette expression vis-à-vis de θ_1. De plus, elle peut être obtenue sans considérer les tests échelonnés (cas classique) :

$$PFD_{2oo2}^{avg}(sans\ décalage) = \frac{\lambda_{DU}T_1}{2} + \frac{\lambda_{DU}T_1}{2} = \lambda_{DU}T_1 \quad (5.13)$$

Donc, le constat avancé ci-avant est confirmé et peut être généralisé pour les systèmes série (1oo1, 2oo2, 3oo3, …).

La Figure 5.7 montre la différence entre le comportement d'une architecture 2oo2 sans et avec stratégie de tests échelonnés. L'examen de cette figure montre que malgré la dissimilitude des PFD(t), les PFD_{avg} sont quasiment identiques. Notons également que la valeur de la PFD_{avg} (avec) est très légèrement supérieure à celle de PFD_{avg} (avec). Ceci est dû à la valeur utilisée de λ_{DU}.

Toutes ces conclusions nous mènent à avancer que les tests échelonnés n'ont pas d'effets tangibles quant à l'amélioration des performances des architectures série (NooN).

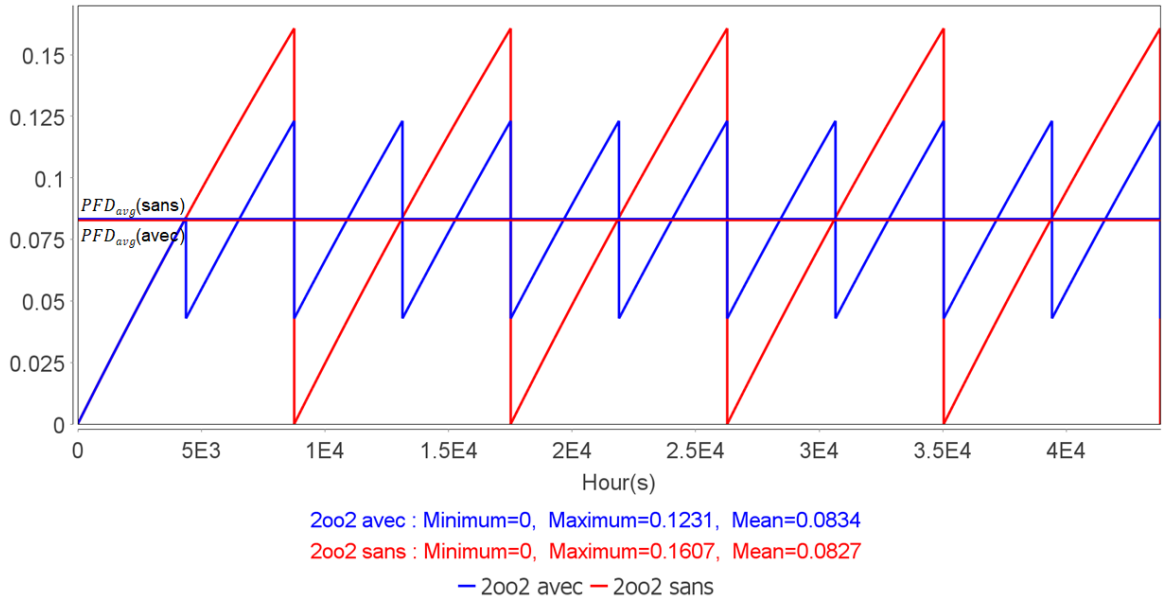


Figure 5.7 : PFD_{2oo2}^{avg} sans et avec stratégie de tests échelonnés

5.3.3. Architecture 1oo3

Chaque canal est testé à intervalles réguliers T_1. Selon la Figure 5.1, les instants des premiers tests pour les trois canaux, sont θ_1, θ_2 et $\theta_3 = T_1$, respectivement. Les courbes de la PFD de chaque canal sont fournies à la Figure 5.8.

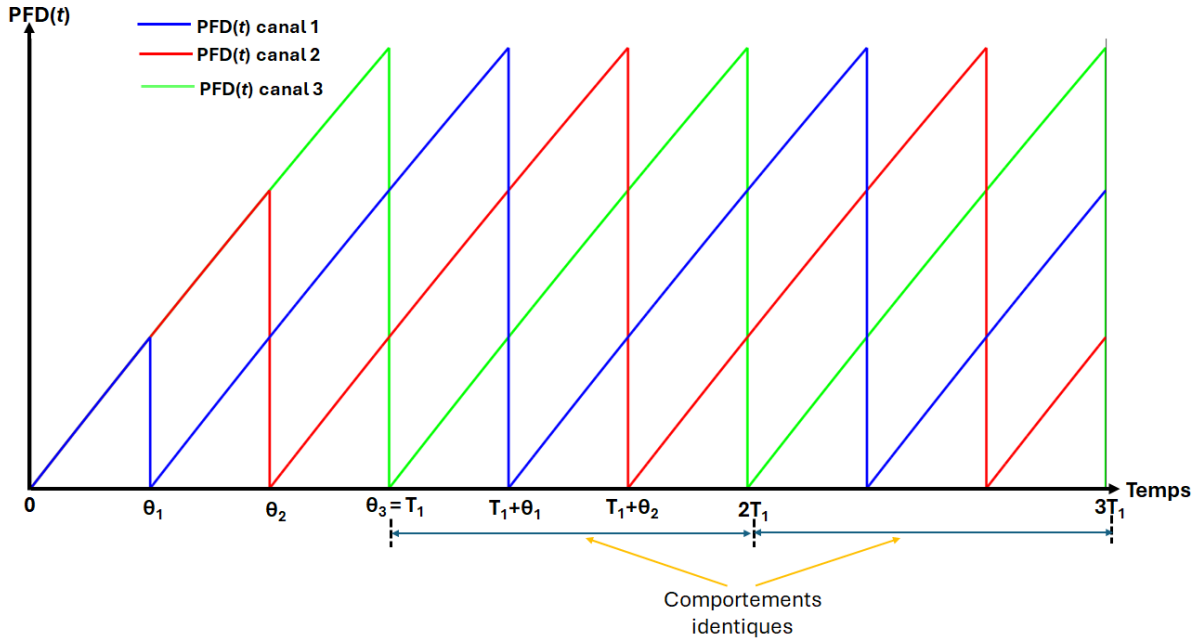


Figure 5.8 : Evolution de la PFD de chacun des trois canaux

La PFD_{avg} de l'architecture 1oo3 peut être obtenue sur une période d'observation T comme suit.

$$PFD_{1oo3}^{avg}(0,T) = \frac{1}{T}\int_0^T PFD_1(t)\,PFD_2(t)\,PFD_3(3)\,dt \qquad (5.14)$$

Cette intégration peut être simplifiée en poursuivant la même démarche utilisée dans le cadre de l'architecture 1oo2. A ce titre, les probabilités des différents canaux sur une période d'amplitude T1 sont données aux Tableau 5.1.

Tableau 5.1. Probabilités de défaillance des différents canaux

Périodes	**$0 \longrightarrow \theta_1$**	**$\theta_1 \longrightarrow \theta_2$**	**$\theta_2 \longrightarrow \theta_3 = T_1$**
Canal 1	$\lambda_{DU}\,(t + T_1 - \theta_1)$	$\lambda_{DU}\,(t - \theta_1)$	$\lambda_{DU}\,(t - \theta_1)$
Canal 2	$\lambda_{DU}\,(t + T_1 - \theta_2)$	$\lambda_{DU}\,(t + T_1 - \theta_2)$	$\lambda_{DU}\,(t - \theta_2)$
Canal 3	$\lambda_{DU}\,(t + T_1 - \theta_3)$	$\lambda_{DU}\,(t + T_1 - \theta_3)$	$\lambda_{DU}\,(t + T_1 - \theta_3)$

$$PFD_{1oo3}^{avg} = \frac{1}{T_1}\left(\int_0^{\theta_1} \lambda_{DU}^3\,(t + T_1 - \theta_1)(t + T_1 - \theta_2)t\;\; dt + \int_{\theta_1}^{\theta_2} \lambda_{DU}^3\,(t - \theta_1)(t + T_1 - \theta_2)t\;dt + \int_{\theta_2}^{T_1} \lambda_{DU}^3\,(t - \theta_1)(t - \theta_2)t\;dt\right)$$

$$PFD_{1003}^{avg} = \frac{\lambda_{DU}^3}{12}\left[3T_1^3 + 6\theta_1(\theta_1 + \theta_2)(T_1 - \theta_2) + 4\left(\theta_1^3 + \theta_2^3 - T_1^2(\theta_1 + \theta_2)\right)\right] \qquad (5.15)$$

Nous pouvons facilement remarquer que pour les tests simultanés, $\theta_1 = \theta_2 = 0$, on retrouve le cas classique : $PFD_{1oo3}^{avg} = \lambda_{DU}^3 \frac{T_1^3}{4}$ [137].

Par ailleurs, si les instants des premiers tests sont uniformément distribués sur T_1 ($\theta_i = \frac{i}{N} T_1$), les trois termes de l'intégral précédent deviennent identiques. Cette distribution assure une PFD_{avg} minimale. Cela dit, l'expression (5.15) peut être mise sous la forme suivante :

$$PFD_{1oo3}^{avg} = \frac{3\,\lambda_{DU}^3}{T_1} \int_0^{\frac{T_1}{3}} \prod_{i=0}^{2} \left(t + i\frac{T_1}{3}\right) dt$$

$$= \lambda_{DU}^3 \frac{T_1^3}{12} = \frac{1}{3}\lambda_{DU}^3 \frac{T_1^3}{4} = \frac{1}{3} PFD_{1oo3}^{avg\ (\text{tests simultanés})} \qquad (5.16)$$

La réduction apportée par les tests échelonnés à la performance de l'architecture 1oo3 est presque le double de celle apportée à l'architecture 1oo2 (1/3 < 5/8). La Figure 5.9 montre la différence entre le comportement d'une architecture 1oo3 sans et avec stratégie de tests échelonnés. L'examen de cette figure montre bien l'avantage des tests échelonnées dans la réduction de la PFD_{avg}.

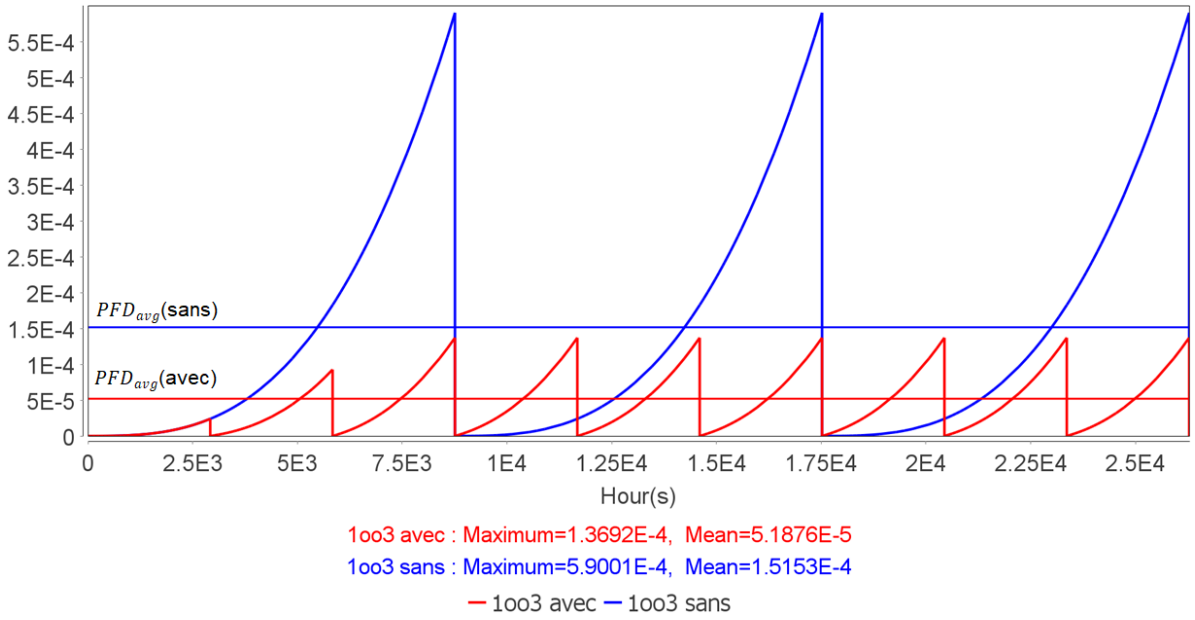


Figure 5.9 : PFD_{1oo3}^{avg} sans et avec stratégie de tests échelonnés

5.3.4. Architecture 2oo3

Les différentes données de test de l'architecture 1oo3 restent valables pour cette architecture à vote majoritaire. Il en est de même pour les courbes relatives aux PFD de chaque canal fournies à la Figure 5.8. Les probabilités des différents canaux sur une période d'amplitude T1 sont donc celles données aux Tableau 5.1. Pour cette architecture, la

défaillance de deux canaux conduit à sa défaillance. La PFD correspondante peut être écrite ainsi :

$$PFD_{2oo3}^{avg} = \frac{\lambda_{DU}^2}{T_1}\left(\int_0^{\theta_1}\left((t+T_1-\theta_1)(t+T_1-\theta_2)+(t+T_1-\theta_1)t+(t+T_1-\theta_2)t\right)\,dt+\int_{\theta_1}^{\theta_2}\left((t-\theta_1)(t+T_1-\theta_2)+(t-\theta_1)t+(t+T_1-\theta_2)t\right)\,dt+\int_{\theta_2}^{T_1}\left((t-\theta_1)(t-\theta_2)+(t-\theta_1)t+(t-\theta_2)t\right)\,dt\right) \quad (5.17)$$

La solution de cet intégral conduit à la forme suivante :

$$PFD_{2003}^{avg} = \lambda DU^2\left(T_1^2 - T_1\theta_2 + \theta_1^2 - \theta_1\theta_2 + \theta_2^2\right) \quad (5.18)$$

Pour le cas des tests simultanés, $\theta_1 = \theta_2 = 0$, on retrouve la formule classique : $PFD_{2oo3}^{avg} = \lambda_{DU}^2 T_1^2$. Si la stratégie des tets uniformes est adoptée, la relation (5.18) se réduit à :

$$PFD_{2oo3}^{avg} = \frac{2\,\lambda_{DU}^2 T_1^2}{3} = \frac{2}{3} PFD_{2oo3}^{avg\ (\text{tests simultanés})} \quad (5.19)$$

Donc, les tests échelonnés uniformément produisent un facteur de réduction égale à 2/3. Rappelons que ce facteur est égal à 5/8 pour l'architecture 1oo2 et 1/3 pour l'architecture 1oo3. La différence entre le comportement d'une architecture 2oo3 sans et avec stratégie de tests échelonnés est exhibée à la Figure 5.10.

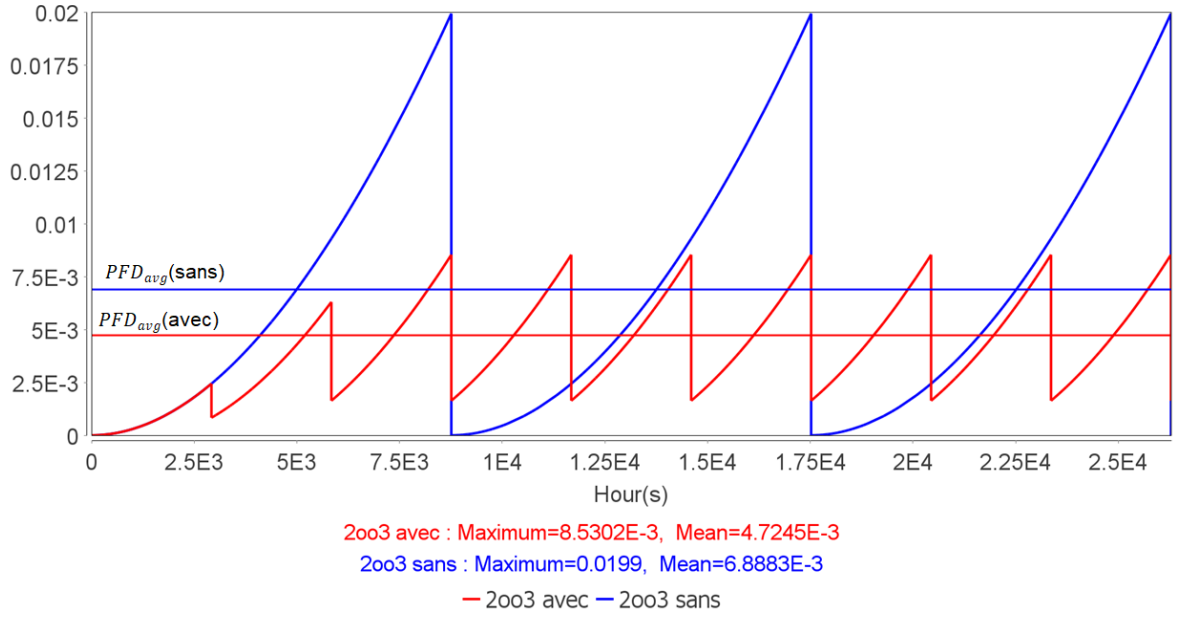


Figure 5.10 : PFD_{2oo3}^{avg} sans et avec stratégie de tests échelonnés

5.4. Généralisation des formules PFD_{avg}

5.4.1. Cas général des architectures KooN

Dans cette section, nous allons proposer des expressions génériques pour une architecture KooN avec prise en compte des tests échelonnés. Nous nous intéressons en particulier au cas des tests uniformes, $\theta_i = \frac{iT_1}{N}$, car cette stratégie est la plus pratique et la plus efficace en termes de réduction de la PFD_{avg} [136].

Avant d'entamer les cas particuliers de généralisation, nous donnons l'expression générale de la PFD(t) d'une architecture KooN constituée de N canaux hétérogènes. Dans notre cas, les canaux sont homogènes (identiques), mais leurs probabilités sont différentes à cause des décalages induits par les tests échelonnés. Elles sont donc hétérogènes en termes de probabilité et non pas en termes de type.

$$PFD_{KooN}(t) = \sum_{j=N-K+1}^{N} \sum_{i_1=1}^{N-j+1} \sum_{i_2=i_1+1}^{N-j+2} \cdots \sum_{i_j=i_{j-1}+1}^{N} \left(\frac{\prod_{s=1}^{j} PFD_{i_s}(t) \cdot \prod_{m=1}^{N} (1-PFD_m(t))}{\prod_{s=1}^{j} (1-PFD_{i_s}(t))} \right) \quad (5.20)$$

Les termes $PFD_{i_s}(t)$ et $PFD_m(t)$ correspondent aux probabilités des différents canaux et sont données par l'Equation (5.1). Bien entendu, la relation (5.20) fournies une valeur exacte de la probabilité de défaillance instantanée de l'architecture considérées. Une forme simplifiée peut être obtenue en ne considérant que les combinaisons minimales de défaillance ($j = N - K + 1$) et en négligeant les $PFD_{i_s}(t)$ et $PFD_m(t)$ devant l'unité :

$$PFD_{KooN}(t) \approx \sum_{i_1=1}^{K} \sum_{i_2=i_1+1}^{K+1} \cdots \sum_{i_{N-K+1}=i_{N-K}+1}^{N} \left(\prod_{s=1}^{N-K+1} PFD_{i_s}(t) \right) \quad (5.21)$$

Si nous nous plaçons dans le cadre de la distribution uniforme des instants des premiers tests sur l'intervalle [0, T_1], nous pouvons dériver une formulation plus simple. Cette dite simplification est due au fait que le comportement des architectures est identique sur les intervalles $[\theta_i,\ \theta_{i+1}]$, comme nous pouvons le constater sur les Figures 5.6, 5.7, 5.9 et 5.10. Cela dit, il suffit d'intégrer sur le premier intervalle [0, θ_1]. Bien entendu, la borne inferieure de cette intervalle ne correspond pas à l'origine de l'axe t, mais au début d'un intervalle où l'architecture a atteint un régime périodique stationnaire.

En utilisant l'Equation (5.3) au lieu de (5.1), la probabilité de défaillance $PFD_i(t)$ d'un canal donné sur l'intervalle [0, θ_1] peut être écrite comme suit :

$$PFD_i(t) \approx \lambda_{DU}(t + T_1 - \theta_i) = \lambda_{DU}\left(t + T_1 - i\frac{T_1}{N}\right) = \lambda_{DU}\left(t + (N-i)\frac{T_1}{N}\right) \quad (5.22)$$

La PFD_{avg} d'une architecture KooN peut être obtenue à partir de l'intégration de la formule (5.21). Si l'on considère les simplifications précédentes (intégration sur la période [0, $\theta_1 = \frac{T_1}{N}$]) et la formule (5.22), nous obtenons l'expression ci-dessous :

$$PFD_{KooN}^{avg} \approx \frac{N\,\lambda_{DU}^{N-K+1}}{T_1} \int_0^{\frac{T_1}{N}} \left(\sum_{i_1=1}^{K} \sum_{i_2=i_1+1}^{K+1} \cdots \sum_{i_{N-K+1}=i_{N-K}+1}^{N} \left(\prod_{s=1}^{N-K+1} \left(t + (N - i_s)\frac{T_1}{N} \right) \right) \right) dt \tag{5.23}$$

Si l'on considère la configuration 2oo3, la relation (5.23) devient :

$$\mathrm{PFD}_{2oo3}^{avg} \approx \frac{3\lambda_{DU}^2}{T_1} \int_0^{\frac{T_1}{3}} \left(\sum_{i_1=1}^{2} \sum_{i_2=i_1+1}^{3} \prod_{s=1}^{2} \left(t + (3 - i_s)\frac{T_1}{3} \right) \right) dt \;= \frac{2\,\lambda_{DU}^2 T_1^2}{3} \tag{5.24}$$

Le Tableau 5.2 regroupe les formules analytiques de certaines architectures KooN (K ≠ 1, N).

Tableau 5.2 : Formules PFD_{avg} pour certaines architectures KooN (K ≠ 1, N)

2oo3	$\frac{2}{3}\lambda_{DU}^2 T_1^2$	5oo6	$\frac{5}{3}\lambda_{DU}^2 T_1^2$	5oo8	$\frac{4}{9}\lambda_{DU}^4 T_1^4$	8oo9	$\frac{3}{2}\lambda_{DU}^2 T_1^2$
2oo4	$\frac{3}{8}\lambda_{DU}^3 T_1^3$	2oo7	$\frac{6}{35}\lambda_{DU}^6 T_1^6$	6oo8	$\frac{7}{12}\lambda_{DU}^3 T_1^3$	2oo10	$\frac{3}{40}\lambda_{DU}^9 T_1^9$
3oo4	$\frac{3}{4}\lambda_{DU}^2 T_1^2$	3oo7	$\frac{5}{14}\lambda_{DU}^5 T_1^5$	7oo8	$\frac{4}{3}\lambda_{DU}^2 T_1^2$	3oo10	$\frac{7}{90}\lambda_{DU}^8 T_1^8$
2oo5	$\frac{2}{5}\lambda_{DU}^4 T_1^4$	4oo7	$\frac{2}{3}\lambda_{DU}^4 T_1^4$	2oo9	$\frac{4}{45}\lambda_{DU}^8 T_1^8$	4oo10	$\frac{7}{120}\lambda_{DU}^7 T_1^7$
3oo5	$\frac{3}{5}\lambda_{DU}^3 T_1^3$	5oo7	$\frac{7}{9}\lambda_{DU}^3 T_1^3$	3oo9	$\frac{7}{72}\lambda_{DU}^7 T_1^7$	5oo10	$\frac{1}{20}\lambda_{DU}^6 T_1^6$
4oo5	$\frac{4}{5}\lambda_{DU}^2 T_1^2$	6oo7	$\frac{7}{6}\lambda_{DU}^2 T_1^2$	4oo9	$\frac{1}{9}\lambda_{DU}^6 T_1^6$	6oo10	$\frac{1}{9}\lambda_{DU}^5 T_1^5$
2oo6	$\frac{5}{12}\lambda_{DU}^5 T_1^5$	2oo8	$\frac{7}{48}\lambda_{DU}^7 T_1^7$	5oo9	$\frac{5}{36}\lambda_{DU}^5 T_1^5$	7oo10	$\frac{7}{60}\lambda_{DU}^4 T_1^4$
3oo6	$\frac{2}{3}\lambda_{DU}^4 T_1^4$	3oo8	$\frac{1}{6}\lambda_{DU}^6 T_1^6$	6oo9	$\frac{2}{9}\lambda_{DU}^4 T_1^4$	8oo10	$\frac{7}{36}\lambda_{DU}^3 T_1^3$
4oo6	$\frac{5}{6}\lambda_{DU}^3 T_1^3$	4oo8	$\frac{5}{18}\lambda_{DU}^5 T_1^5$	7oo9	$\frac{7}{27}\lambda_{DU}^3 T_1^3$	9oo10	$\frac{5}{6}\lambda_{DU}^2 T_1^2$

5.4.2. Cas spécifiques des architectures NooN et 1ooN

Voyons maintenant les deux cas extrêmes : NooN et 1ooN.

- ***Cas des architectures NooN***

Les termes de sommations de la relation (5.23) correspondent à la somme des $PFD_i(t)$ des différents canaux, car N-K+1 =1 (une seule défaillance suffit).

$$PFD_{NooN}^{avg} = \frac{N\,\lambda_{DU}}{T_1}\int_0^{\frac{T_1}{N}} \sum_{i=1}^{N}\left(t + (N-i)\frac{T_1}{N}\right)dt = \frac{N\,\lambda_{DU}}{T_1}\int_0^{\frac{T_1}{N}} \sum_{i=0}^{N-1}\left(t + i\frac{T_1}{N}\right)dt = N\,\lambda_{DU}\frac{T_1}{2} \tag{5.25}$$

Donc, comme nous l'avons déjà signalé concernant les architectures 1oo1 et 2oo2, la politique des tests échelonnées n'a pas d'impact sur la performance sécuritaire.

- ***Cas des architectures 1ooN***

Cette fois-ci, les termes de sommations de la relation (5.23) correspondent au produit des $PFD_i(t)$ des différents canaux (la défaillance de l'ensemble des canaux est nécessaire).

$$PFD_{1ooN}^{avg} = \frac{N\,\lambda_{DU}^{N}}{T_1}\int_0^{\frac{T_1}{N}} \prod_{i=1}^{N}\left(t + (N-i)\frac{T_1}{N}\right)dt = \frac{N\,\lambda_{DU}^{N}}{T_1}\int_0^{\frac{T_1}{N}} \prod_{i=0}^{N-1}\left(t + i\frac{T_1}{N}\right)dt \tag{5.26}$$

Une solution pratique de cette intégration est fournie dans (5.27).

$$PFD_{1ooN}^{avg} = \left(\lambda_{DU}\frac{T_1}{N}\right)^{N} \sum_{j=0}^{N}\frac{c(N,j)}{j+1} \tag{5.27}$$

Où $c(N,j)$ sont les nombres de Stirling de première espèce (non signés). Pour rendre ce résultat facilement utilisable, nous fournissons dans le Tableau 5.3 les valeurs de la quantité $\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$ pour N allant de 1 jusqu'à 20.

Tableau 5.3 : Valeurs de $\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$

N	$\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$	N	$\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$	N	$\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$	N	$\sum_{j=0}^{N}\frac{c(N,j)}{j+1}$
1	5.00e-1	**6**	2.41e+2	**11**	2.91e+7	**16**	4.31e+13
2	8.33e-1	**7**	1.85e+3	**12**	4.27e+8	**17**	9.09e+14
3	2.25e+0	**8**	1.70e+4	**13**	6.82e+9	**18**	2.04e+16
4	8.37e+0	**9**	1.81e+5	**14**	1.18e+11	**19**	4.83e+17
5	3.96e+1	**10**	2.18e+6	**15**	2.18e+12	**20**	1.21e+19

De plus, des expressions simplifiées pour certaines architecture 1ooN sont regroupées au Tableau 5.4. On y retrouve bien les formules développées précédemment pour les architectures 1oo1, 1oo2 et 1oo3.

Tableau 5.4 : Formules PFD_{avg} pour certaines architectures 1ooN

N	PFD_{1ooN}^{avg} formula	N	PFD_{1ooN}^{avg} formula
1	$\frac{1}{2}\lambda_{DU}T_1$	6	$\frac{19087}{11757312}(\lambda_{DU}T_1)^6$
2	$\frac{5}{24}(\lambda_{DU}T_1)^2$	7	$\frac{5257}{7906016}(\lambda_{DU}T_1)^7$
3	$\frac{1}{12}(\lambda_{DU}T_1)^3$	8	$\frac{1070017}{2642411520}(\lambda_{DU}T_1)^8$
4	$\frac{251}{7680}(\lambda_{DU}T_1)^4$	9	$\frac{25713}{1024000000}(\lambda_{DU}T_1)^9$
5	$\frac{19}{37500}(\lambda_{DU}T_1)^5$	10	$\frac{26842253}{1575296100000}(\lambda_{DU}T_1)^{10}$

5.4.3. Prise en compte des CCF

Les formules précédentes ne considèrent pas la contribution des défaillances de cause commune (CCF). Une manière simple et approximative pour la prise en compte des CCF est d'ajouter le terme $\beta\,\lambda_{DU}\frac{T_1}{2N}$ aux différentes formules obtenues et de remplacer le taux λ_{DU} par $(1-\beta)\,\lambda_{DU}$. En effet, si la politique de tests échelonnés uniformes est adoptée, cela signifie qu'une défaillance CCF serait détectée à l'occasion de chacun des tests des différents canaux : intervalle entre les différents tests est constant et égal à $\theta_1 = \frac{T_1}{N}$. De plus, les défaillances CCF existeraient sur la seconde moitié de cette intervalle. Le Tableau 5.5 regroupe les formules PFD_{avg} de certaines architectures classiques (la contribution des CCFs est en gras).

Tableau 5.5 : Formules PFD_{avg} de certaines architectures classiques incluant les CCFs

KooN	$\boldsymbol{PFD_{avg}^{KooN}}$
1oo1	$\lambda_{DU}\frac{T_1}{2}$
1oo2	$\frac{5\,((1-\beta)\lambda_{DU}\,T_1)^2}{24} + \boldsymbol{\beta\,\lambda_{DU}\frac{T_1}{4}}$
1oo3	$\frac{((1-\beta)\lambda_{DU}\,T_1)^3}{12} + \boldsymbol{\beta\,\lambda_{DU}\frac{T_1}{6}}$
2oo2	$2\,(1-\beta)\lambda_{DU}\frac{T_1}{2} + \boldsymbol{\beta\,\lambda_{DU}\frac{T_1}{4}}$
2oo3	$\frac{2\,((1-\beta)\lambda_{DU}\,T_1)^2}{3} + \boldsymbol{\beta\,\lambda_{DU}\frac{T_1}{6}}$

La prise en compte exacte des CCFs s'effectue en l'intégrant à l'Equation (5.20) de la manière suivante :

$$PFD_{KooN}(t) = \underbrace{\sum_{j=N-K+1}^{N} \sum_{i_1=1}^{N-j+1} \sum_{i_2=i_1+1}^{N-j+2} \cdots \sum_{i_j=i_{j-1}+1}^{N} \left(\frac{\prod_{s=1}^{j} PFD_{i_s}(t) \cdot \prod_{m=1}^{N} (1-PFD_m(t))}{\prod_{s=1}^{j} (1-PFD_{i_s}(t))} \right)}_{PFD_{KooN}^{ind}(t)} + PFD_{KooN}^{CCF}(t) - PFD_{KooN}^{ind}(t) \cdot PFD_{KooN}^{CCF}(t) \quad (5.28)$$

Avec :

- $PFD_{KooN}^{ind}(t)$ représente la PFD(t) des défaillances individuelles (voir la relation (5.20)). Les taux de défaillances des canaux = $(1-\beta)\,\lambda_{DU}$.
- $PFD_{KooN}^{CCF}(t)$ représente la PFD(t) due aux CCFs. Cette quantité est donné par la relation suivante :

$$PFD_{KooN}^{CCF}(t) = 1 - e^{-\beta\lambda_{DU}\left(t - Int\left(\frac{t}{\frac{T_1}{N}}\right)\cdot\frac{T_1}{N}\right)} \quad (5.29)$$

5.5. Comparaison des résultats relatifs à la PFD_{avg}

Nous allons dans ce qui suit comparer les résultats numériques relatifs à la PFD_{avg} des architectures KooN sans (non considération des termes en gras du Tableau 5.5) et avec CCF en utilisant les formules simplifiées dérivées au cours de ce chapitre, d'une part, et une évaluation exacte fondée sur l'intégration de l'Equation (5.28), d'autre part. Les architectures concernées sont : 1oo1, 2oo2, 1oo2, 1oo3 et 2oo3. Le jeu de paramètres suivant a été utilisé : $\lambda_D = 1 \times 10^{-6}\ h^{-1}$; $T_1 = 8760h$; $\beta \in \{0.1, 0.2\}$; DC $\in\{0, 0.6, 0.9, 0.99\}$. Les valeurs numériques obtenues sont fournies dans le Tableau 5.6. Pour plus de visibilité concernant l'évolution de la PFD_{avg} en fonction des paramètres DC et β, la Figure 5.10 est fournie.

Nous constatons que les formules simplifiées dérivées au cours de ce travail de recherche fournissent des valeurs numériques très proches et parfois identiques à celles obtenues à partir d'une modélisation exacte. Ceci atteste donc la validité des développements mathématiques conduits au cours de ce chapitre. Par ailleurs, la considération des CCFs limite les avantages de la redondance, en particulier pour les valeurs élevées de β qui dégradent significativement les performances des architectures redondantes. De plus, la couverture de diagnostic offre des avantages substantiels pour toutes les architectures, mais les CCF impose une limite inférieure aux PFD_{avg} atteignables.

Tableau 5.6 : Comparaisons des résultats PFD_{avg}

KooN	*DC* (%)	*β* (%)	Formules simplifiées		Intégration de la formule (5.28)	
			PFD_{avg} (sans CCF)	**PFD_{avg} (avec CCF)**	**PFD_{avg} (sans CCF)**	**PFD_{avg} (avec CCF)**
1oo1	0	10	4.3800E-03	4.3800E-03	4.3672E-03	4.3672E-03
		20	4.3800E-03	4.3800E-03	4.3672E-03	4.3672E-03
	60	10	1.7520E-03	1.7520E-03	1.7500E-03	1.7500E-03
		20	1.7520E-03	1.7520E-03	1.7500E-03	1.7500E-03
	90	10	4.3800E-04	4.3800E-04	4.3787E-04	4.3787E-04
		20	4.3800E-04	4.3800E-04	4.3787E-04	4.3787E-04
	99	10	4.3800E-05	4.3800E-05	4.3799E-05	4.3799E-05
		20	4.3800E-05	4.3800E-05	4.3799E-05	4.3799E-05
1oo2	0	10	1.2949E-05	2.3195E-04	1.2888E-05	2.3185E-04
		20	1.0232E-05	4.4823E-04	1.0189E-05	4.4805E-04
	60	10	2.0719E-06	8.9672E-05	2.0680E-06	8.9663E-05
		20	1.6371E-06	1.7684E-04	1.6343E-06	1.7681E-04
	90	10	1.2949E-07	2.2029E-05	1.2943E-07	2.2029E-05
		20	1.0232E-07	4.3902E-05	1.0227E-07	4.3901E-05
	99	10	1.2949E-09	2.1913E-06	1.2949E-09	2.1913E-06
		20	1.0232E-09	4.3810E-06	1.0231E-09	4.3810E-06
1oo3	0	10	4.0837E-08	1.4604E-04	4.0562E-08	1.4603E-04
		20	2.8681E-08	2.9203E-04	2.8509E-08	2.9197E-04
	60	10	2.6136E-09	5.8403E-05	2.6065E-09	5.8400E-05
		20	1.8356E-09	1.1680E-04	1.8312E-09	1.1679E-04
	90	10	4.0837E-11	1.4600E-05	4.0810E-11	1.4600E-05
		20	2.8681E-11	2.9200E-05	2.8664E-11	2.9199E-05
	99	10	4.0837E-14	1.4600E-06	4.0835E-14	1.4600E-06
		20	2.8681E-14	2.9200E-06	2.8680E-14	2.9200E-06
2oo2	0	10	7.8840E-03	8.1030E-03	7.8504E-03	8.0674E-03
		20	7.0080E-03	7.4460E-03	6.9815E-03	7.4158E-03
	60	10	3.1536E-03	3.2412E-03	3.1482E-03	3.2355E-03
		20	2.8032E-03	2.9784E-03	2.7989E-03	2.9736E-03
	90	10	7.8840E-04	8.1030E-04	7.8806E-04	8.0994E-04
		20	7.0080E-04	7.4460E-04	7.0053E-04	7.4430E-04
	99	10	7.8840E-05	8.1030E-05	7.8837E-05	8.1026E-05
		20	7.0080E-05	7.4460E-05	7.0077E-05	7.4457E-05
2oo3	0	10	4.1438E-05	1.8744E-04	4.1154E-05	1.8713E-04
		20	3.2741E-05	3.2474E-04	3.2541E-05	3.2447E-04
	60	10	6.6301E-06	6.5030E-05	6.6119E-06	6.5009E-05
		20	5.2386E-06	1.2204E-04	5.2258E-06	1.2202E-04
	90	10	4.1438E-07	1.5014E-05	4.1410E-07	1.5014E-05
		20	3.2741E-07	2.9527E-05	3.2721E-07	2.9527E-05
	99	10	4.1438E-09	1.4641E-06	4.1435E-09	1.4641E-06
		20	3.2741E-09	2.9233E-06	3.2739E-09	2.9233E-06

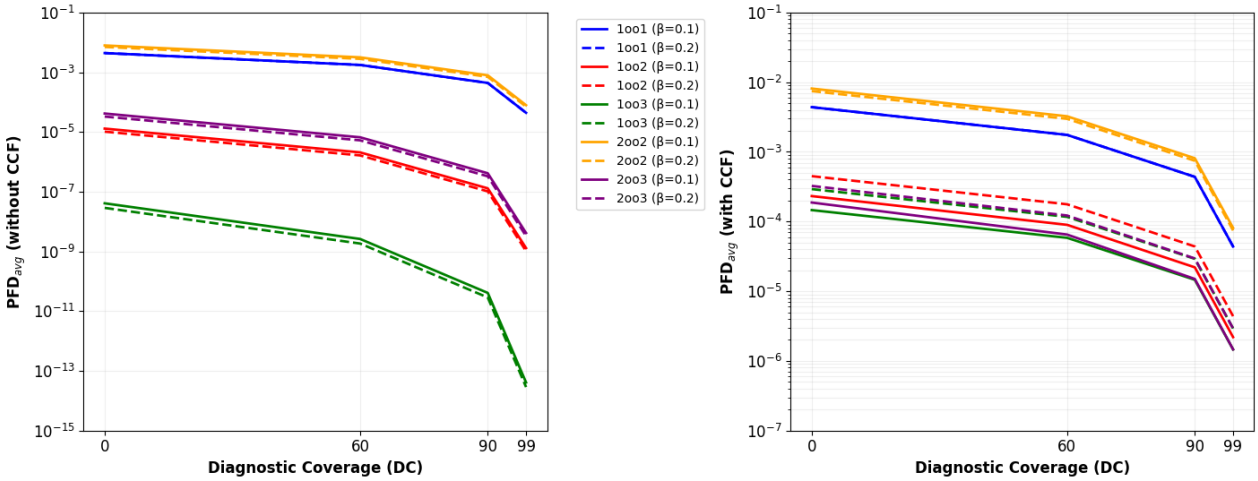


Figure 5.11 : Evolution de PFD_{avg} selon DC et β pour différentes architectures KooN

5.6. Conclusion

Nous avons traité dans ce chapitre la stratégie des tests échelonnés et surtout son impact sur la PFD_{avg} des architectures KooN. A ce titre, nous avons d'abord énoncé cette stratégie. Ensuite, nous avons développé des formules analytiques de la PFD_{avg} pour certaines architectures classiques. Puis, une généralisation de cette formulation a été établie, avec une attention particulière aux architectures NooN et 1ooN. Finalement, une comparaison numérique entre les valeurs de la PFD_{avg} fournies par les formules simplifiées proposées et celles obtenues via une modélisation exacte a été conduite. Les conclusions de cette comparaison confirment l'exactitudes des formules développées.

Annexes

Annexe A : Modélisation des effets des phénomènes dangereux avec le logiciel PHAST

A.1. Phénomènes dangereux

Les phénomènes dangereux classiquement rencontrés dans le secteur Oil & Gas sont les phénomènes dangereux suivants [138]:

- **Flash Fire (feu de nuage)** : Un flash fire correspond à la combustion d'un nuage de gaz dans une zone non encombrée. Il est considéré comme un évènement retardé sans possibilité d'évacuation. Il génère des effets thermiques mais pas d'effets de surpression. Des effets létaux sont considérés à l'intérieur du nuage enflammé. Le scénario de ce phénomène est illustré dans la Figure A.1.

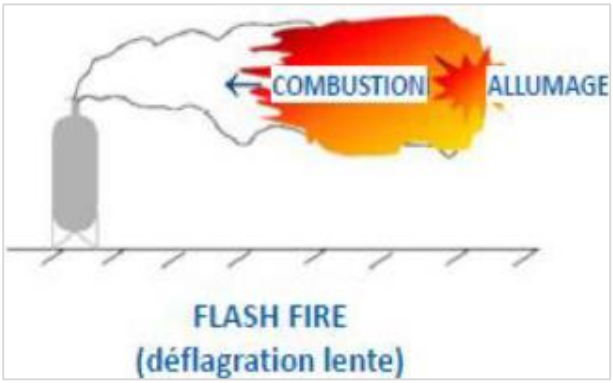


Figure A.1 : Développement du scénario de flash fire

- **Explosion d'un nuage à l'air libre (UVCE)** : L'explosion d'un nuage à l'air libre correspond à l'ignition retardée d'un nuage de gaz dans une zone encombrée et entraînant des effets de surpression. Le scénario d'UVCE est illustré dans la Figure A.2.

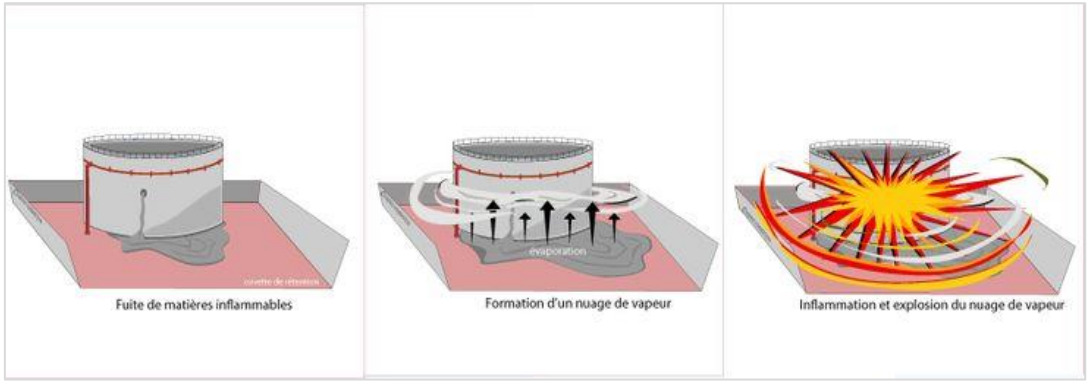


Figure A.2 : Développement du scénario de UVCE

- **Jet enflammé (Feux de chalumeau)** : Un jet enflammé correspond à une ignition instantanée d'une fuite d'hydrocarbures (liquide ou gaz) entrainant des radiations thermiques. Le jet enflammé est considéré comme un évènement sans possibilité d'évacuation. Le scénario de feux de chalumeau est illustré dans la Figure A.3.



Figure A.3 : Développement du scénario de feux de chalumeau

- **Feu de nappe** : Un feu de nappe est la combustion d'un déversement d'hydrocarbures liquides. Il est considéré comme un événement retardé avec possibilité d'évacuation. Le scénario de feu de nappe est illustré dans la Figure A.4.

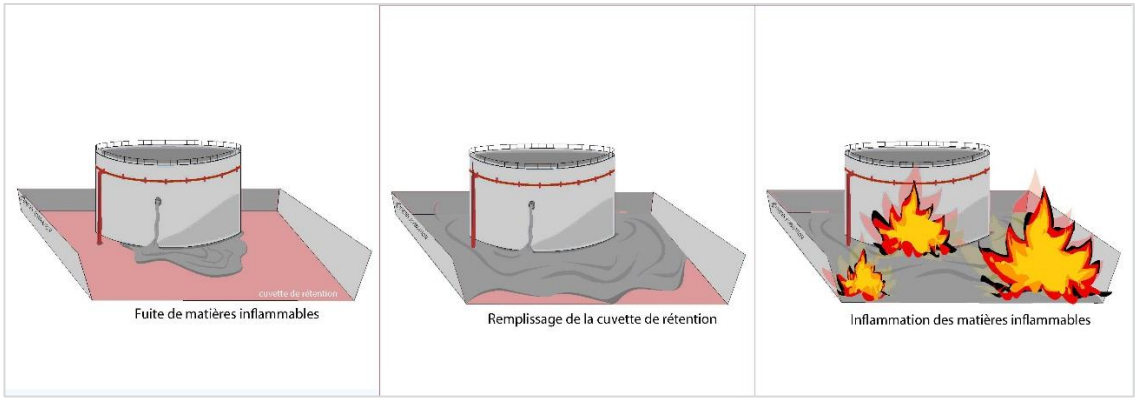


Figure A.4 : Développement du scénario de feu de nappe

- **Feu de bac et Boil-Over** : Par définition, un Boil-Over est un phénomène de moussage brutal impliquant des réservoirs atmosphériques et résultant de la transformation en vapeur, d'eau liquide contenue dans un réservoir en feu (feu de bac). Ce phénomène est à l'origine de violentes projections de combustible, du bouillonnement du contenu du bac, de l'extension des flammes et de la formation d'une boule de feu. Le Boil Over est considéré comme un phénomène à cinétique lente. En cas d'absence d'onde de chaleur dans le liquide avant le déclenchement du boil over, on l'appelle « boil-over en couche

mince », dont les effets associés sont d'ampleur limitée. Le scénario de ce phénomène est illustré dans la Figure A.5.

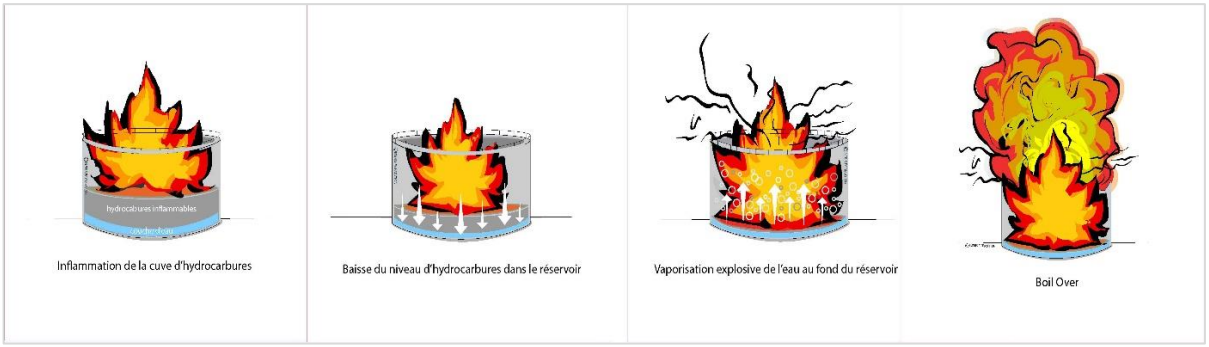


Figure A.5 : Développement du scénario de Boil-Over

- **BLEVE** : Le BLEVE (Boiling Liquid Expanding Vapour Explosion) correspond à la vaporisation violente à caractère explosif consécutive à la rupture d'un réservoir contenant un liquide à une température significativement supérieure à sa température d'ébullition à la pression atmosphérique. Le scénario de BLEVE est illustré dans la Figure 2.3.
- **Explosion d'un réservoir atmosphérique à toit fixe** : Ce phénomène correspond à l'ignition d'un mélange gazeux carburant / comburant (vapeurs d'hydrocarbures dans l'air). L'expansion des produits de combustion qui en résulte sont à l'origine d'une montée en pression dans le réservoir. L'énergie interne accumulée est libérée sous forme d'ondes de surpression et projections de missiles. Il n'a pas lieu d'être considéré si les évents des réservoirs sont suffisamment bien dimensionnés et ne permettent pas l'accumulation de vapeur. Le scénario de ce phénomène est illustré dans la Figure A.6.

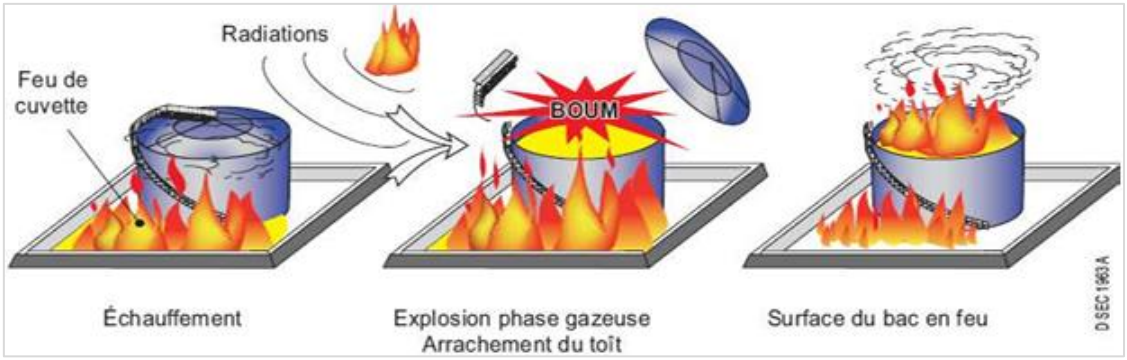


Figure A.6 : Développement du scénario d'explosion d'un réservoir atmosphérique à toit fixe

A.2. Modélisation des effets des phénomènes dangereux

Le logiciel PHAST de DNV GL (Process Hazard Analysis Software Tool) est utilisé pour l'évaluation des situations accidentelles qui présentent des risques potentiels pour la vie, les biens et l'environnement, et ainsi quantifier leur gravité. PHAST examine l'évolution d'un incident éventuel depuis sa situation initiale jusqu'à sa dispersion en champ lointain en passant par la modélisation des nappes, leurs propagations et évaporations, ainsi que les effets toxiques et inflammables. Les résultats de l'analyse peuvent être affichés sous forme de tableaux et de graphiques, pour visualisation de l'impact et évaluation des effets sur la population et l'environnement. PHAST est conçu pour se conformer aux exigences réglementaires de nombreux pays. PHAST contient des modèles adaptés à l'analyse des risques des installations industrielles offshore et onshore qui intègrent tous des retours d'expérience d'essais à plus ou moins grande échelle.

- Les modèles de rejet et de dispersion, y compris le Modèle de Dispersion Unifiée de DNV GL (UDM modifié) ;
- Les modèles d'explosion, pour calculer la surpression et les impulsions. Les modèles disponibles incluent : Baker Strehlow, le modèle d'explosion TNO multi-énergies et TNT ;

En cas d'évènements spécifiques (BLEVE, Boil Over…), des références à de la littérature spécialisée peuvent être utilisées.

A.2.1. Dispersion atmosphérique d'un nuage

La maîtrise de la géométrie du nuage et de sa dérive dans le temps, est nécessaire pour déterminer les distances « aux concentrations à risques », par rapport au point de rejet du produit. Pour le cas des gaz inflammables, la zone dangereuse du nuage (nuage formé par un mélange d'air et de produit) correspond à la zone dans laquelle la concentration du gaz est comprise entre la Limite Supérieure d'Explosibilité (L.S.E.) et la Limite Inférieure d'Explosibilité (L.I.E.). C'est dans toute cette zone que le nuage risque de s'enflammer et que l'inflammation risque de générer des surpressions.

Pour le cas des gaz toxiques, la zone dangereuse du nuage est déterminée par les seuils de concentrations des effets létaux et irréversibles.

Le modèle UDM (Unified Dispersion Model) est le cœur du logiciel PHAST. Il prend en compte les conditions météorologiques et les conditions orographiques (« rugosité » du terrain). Il s'applique aussi bien aux gaz légers qu'aux gaz lourds et réalise le calcul de

dispersion de gouttelettes de liquide prenant en compte la formation et l'évaporation d'une nappe de liquide volatile.

Le modèle UDM a fait l'objet de nombreuses validations de la part de différents organismes. Il fait partie des logiciels de dispersion qui prend en compte le plus grand nombre de données expérimentales.

A.2.2. Phénomène de Flash Fire / Explosion d'un nuage à l'air libre (UVCE)

Les phénomènes de Flash Fire et d'explosion à l'air libre (UVCE) sont en réalité le même phénomène physique, dépendant des conditions du mélange gazeux et de l'environnement. Il s'agit de la combustion retardée d'un mélange air / gaz inflammable.

En pratique les effets thermiques de l'UVCE sont dus au passage du front de flamme. Ainsi toute personne se trouvant sur le parcours de la flamme est susceptible de subir l'effet létal, mais celui-ci n'excède pas la limite extrême atteinte par le front de flamme. Ainsi, l'effet thermique de l'UVCE, ou Flash Fire sur l'homme est dimensionné par la distance à la LIE.

Les effets de surpression de l'UVCE sont produits par l'effet piston du front de flamme sur les gaz frais. Plus la propagation du front de flamme est rapide et plus son accélération est grande, plus l'amplitude de l'onde de pression est importante. Celle-ci se propage dans l'environnement à la façon d'une onde de choc dont l'amplitude s'atténue lorsque l'on s'éloigne du centre de l'explosion, de manière inversement proportionnelle à la distance.

En l'absence d'obstacles, on observe expérimentalement que la propagation de la flamme dans un mélange homogène et au repos est très faiblement accélérée, et que les niveaux de pression associés n'excèdent pas quelques millibars. Les effets thermiques du Flash Fire sont alors prépondérants.

En revanche, la présence d'un écoulement turbulent ou de gradients de concentration suffit à accélérer la flamme et à engendrer des niveaux de pression plus élevés, même en l'absence d'obstacle.

La méthode TNO multi énergy est utilisée pour calculer les distances des effets de surpression. La méthode TNO Multi Energy suppose un nuage réactionnel hémisphérique de concentration stoechiométrique. Les paramètres d'effet de surpression sont calculés en utilisant un modèle unidimensionnel à vitesse de flamme constante, défini par l'indice de sévérité de chaque zone ou « ilot » encombré. L'indice de sévérité est gradué de 1 à 10. Le choix du degré de sévérité se détermine en tenant compte de :

- La densité d'obstacles (encombrement)
- Le degré de confinement

- La réactivité du produit et la position et l'énergie des sources d'inflammation

Le tableau de Kinsella [139] ci-dessous aide à la détermination des indices de sévérité de chacune des zones de congestion.

Tableau A.1 : Tableau de Kinsella (aide à la décision du choix de degré de sévérité)

Inflammation		**Encombrement**			**Confinement**		**Classe / Sévérité**
Basse	Haute	Haut	Bas	Aucun	Oui	Non	
	X	X			X		7–10
	X	X				X	7–10
X		X			X		5–7
	X		X		X		5–7
	X		X			X	4–6
	X			X	X		4–6
X		X				X	4–5
	X			X		X	4–5
X			X		X		3–5
X			X			X	2–3
X				X	X		1–2
X				X		X	1

La masse réactionnelle est donc la masse comprise dans une ou plusieurs zones de congestion, dans son domaine d'explosibilité (c'est-à-dire entre le LIE et la LSE). L'explosion est centrée au centre du nuage.

A.2.3. Phénomène de jet enflammé et de boule de feu

Le jet enflammé ou jet chalumeau est un phénomène résultant de la combustion immédiate en champs proche de la fuite continue de gaz inflammable sous pression.

De nombreux essais expérimentaux ont été menés afin de mieux comprendre le phénomène de jet enflammé. Le jet enflammé est considéré comme ayant la forme d'un cône rayonnant. Le logiciel PHAST recommande l'utilisation des modèles suivante :

- Pour un liquide léger ou fluide diphasique, utilisation du modèle de Cook (1990) ;
- Pour un rejet de gaz inflammable horizontal, utilisation du modèle de Johnson (1994) ;
- Pour un rejet de gaz vertical, utilisation du modèle de Chamberlain (1987).

Dans le cas où le rejet continu est de courte durée, le jet enflammé n'a pas le temps nécessaire pour se stabiliser. Alors, les effets de l'ignition immédiate d'un mélange air / gaz inflammable peuvent ressembler plutôt à ceux associés à une boule de feu (de type BLEVE) qu'à ceux d'un jet enflammé (qui n'a pas eu le temps de se stabiliser).

A.2.4. Phénomène de feu de nappe

Les effets des feux de nappe sont également réalisés par le logiciel PHAST. Il emploie le modèle de la flamme solide suivant une géométrie de flamme de cylindre vertical.

L'hypothèse de la nappe à l'équilibre est réalisée afin de déterminer la surface en feu. Les surfaces de rétention sont prises en compte si l'inventaire et l'épaisseur de nappe minimal permettent d'envisager la retenue de l'inventaire.

La hauteur de flamme est quant à elle déterminée au moyen de la corrélation de Thomas prenant en compte les effets du vent.

Les données du produit (taux massique surfacique de combustion, pouvoir émissif de la flamme) et les données de l'environnement (conditions météorologiques, diamètre maximal de la flamme) sont prises en compte.

A.2.5. Phénomène de feu de bac et Boil Over

Le feu de bac est un évènement pouvant précéder un boil over. Il apparait en cas d'effacement du toit d'un bac atmosphérique. Le calcul de l'intensité d'un feu de bac est similaire à celui d'une nappe au sol.

Le boil-over est une explosion propre aux bacs de produit lourd (pétrole brut, fioul lourd…) dans lequel la vaporisation d'eau se trouvant en fond de bac propulse l'hydrocarbure enflammé sous la forme d'une colonne ou d'une boule de feu.

Deux phénomènes peuvent être identifiés en fonction de la nature du liquide inflammable :

- Le boil over classique ;
- Le boil over en couche mince.

Tableau A.2 : Comportement des produits vis-à-vis des phénomènes de boil over classique et boil over couche mince

Famille de produits	Boil Over couche mince	Boil Over classique
Essences	Non	Non
Carburéacteurs	Oui	Non
Gazole et FODs	Oui	Non
Fuels lourds	Non	Oui
Bruts	Non	Oui
Alcools	Non	Non
MTBE/ETBE	Non	Non

Dans le cas du phénomène de boil-over « classique », l'onde de chaleur descend plus rapidement que le front de flamme situé sur la partie supérieure du liquide. Aussi, lorsque l'onde

de chaleur rencontre le fond d'eau, le produit est projeté entraînant un moussage (le bac déborde) et une boule de feu.

Dans le phénomène de boil-over « en couche mince », le produit se consomme en gardant une composition homogène et aucune onde de chaleur ne se forme. La source de chaleur qui peut vaporiser le fond d'eau est le front de flamme lui-même lorsqu'il arrive à proximité immédiate du fond d'eau. Dans ce cas, on retrouve la projection du produit (boule de feu) mais les quantités en jeu sont beaucoup plus faibles et le phénomène de moussage n'est pas observé. La boule de feu est donc plus « petite » et sa durée de vie plus courte, engendrant des effets de moindre intensité.

Les effets du boil over classique, pouvant propager une onde de chaleur, est modélisé en utilisant le guide Omega13 de l'Ineris [140]. Le boil over en couche mince est modélisé au moyen de fiches de calculs fournies par le Ministère de l'Environnement français [141].

A.2.6. BLEVE

La modélisation des effets thermiques du BLEVE fait intervenir le modèle TRC Shield, qui est construit à partir d'essais réalisés par British Gas dans les années 1990 sur des capacités de GPL (propane et butane). Il permet de simuler l'évolution du phénomène dangereux dans le temps, en considérant trois phases de développement de la boule de feu :

- Phase d'inflammation du nuage et de développement de la boule de feu jusqu' à son diamètre maximal, ou phase d'expansion
- Phase de combustion de la boule de feu
- Phase d'extinction

Le modèle repose sur un certain nombre d'hypothèses et de relation empiriques spécifiques aux GPL. Les pressions de rupture retenues correspondent aux pressions de tarage des soupapes les plus couramment utilisées sur les réservoirs fixes de propane et de butane. La Table 2.6 fournit les distances d'effets associés aux effets du BLEVE, à partir de la masse maximale de gaz liquéfié contenu dans le réservoir, exprimées en kilogramme.

Tableau A.3 : Calculs des distances d'effets liées au phénomène de BLEVE

Seuil $(kW/m^2)^{4/3}\cdot s$	Butane, butène, butadiènes…	Propane, propylène
1800	$0.81 \times M^{0.471}$	$1.28 \times M^{0.448}$
1000	$1.72 \times M^{0.437}$	$1.92 \times M^{0.442}$
600	$2.44 \times M^{0.427}$	$2.97 \times M^{0.425}$

Cette approche est celle notamment utilisée en France et présentée dans la circulaire du 10 mai 2010 [142].

Annexe B : Calcul automatique de la performance des SIS avec le logiciel GRIF

B.1. GRIF-module SIL

Technologie de TotalEnergies depuis les années 1980, GRIF (Graphiques Interactifs pour la Fiabilité) comprend 3 packages et 12 modules permettant à l'utilisateur de choisir la technique de modélisation la plus appropriée pour la résolution du système étudié. SIL est l'un des sept modules appartenant au package Booléen.

Certifié par l'INERIS (l'Institut National de l'Environnement industriel et des RISques), SIL permet d'évaluer le niveau d'intégrité de sécurité SIL (Safety Integrity Level) des boucles instrumentées de sécurité. Études réalisées selon les normes IEC 61508 et IEC 61511, ce module est généralement destiné aux instrumentistes en charge de la conception ou de la maintenance des architectures SIS (Safety Instrumented System). Il est doté d'ALBIZIA, le moteur de calcul par BDD (Binary Decision Diagram) développé par TotalEnergies, capable d'effectuer des calculs analytiques exacts [143].

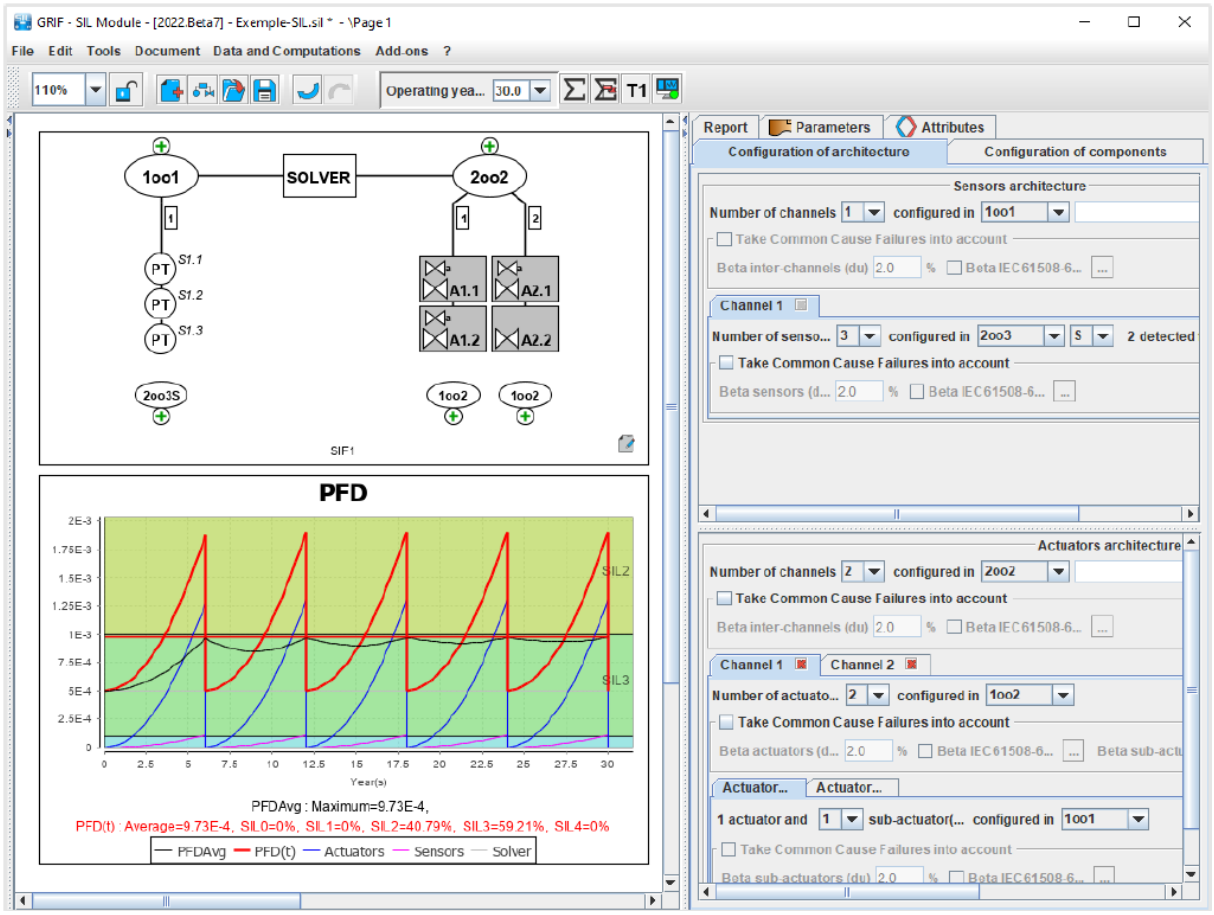


Figure B.1 : Interface du logiciel GRIF-module SIL [144]

B.2. Modélisation et calculs :

Vous pouvez définir l'architecture SIS à évaluer en sélectionnant de manière interactive les éléments composant la fonction instrumentée de sécurité (Capteurs, Solver, Actionneurs, Logique de vote KooN). Ils caractérisent ensuite chaque composant de la chaîne de sécurité en spécifiant : les paramètres de fiabilité (taux de défaillance, taux de couverture des tests de diagnostic, modes communs … ; les paramètres liés à la maintenance (périodicité et durée des tests, temps de réparation …). Le module SIL s'appuie sur la transcription de l'architecture SIS en arbres de défaillances pour lancer les calculs SIL et obtenir la PFD Average (Probability of Failure on Demand) et la PFH (Probability of Failure per Hour).

B.3. Spécificités et points forts :

- ***Calculs analytiques*** : SIL permet l'évaluation des indicateurs temporels sur chaque partie (capteurs, solveur et actionneurs) de la Fonction Instrumentée de Sécurité (SIF). Les calculs sont réalisés à l'aide du moteur de calcul ALBIZIA et portent sur la PFD / PFH. La technique de calcul utilisée (Binary Decision Diagram) produit des résultats exacts. Les résultats obtenus sont les valeurs instantanées, valeurs moyennes, valeurs maximales sur la période de calcul et les pourcentages de temps passé dans chaque SIL. Les SIF créées peuvent être réutilisées comme barrières de sécurité avec des arbres d'événements.
- ***Principales caractéristiques*** :
    - Calcul des PFD et PFH avec un algorithme précis (pas une simple approximation de la moyenne).
    - HFT et contrainte architecturale selon les normes IEC 61508 et IEC 61511.
    - Interface utilisateur graphique conviviale.
    - Configuration avancée pour les composants (Proof Test Coverage, Partial stroking, Human error, ...).
    - Calcul des déclenchements intempestifs.
    - Systèmes multi-boucles, les composants peuvent être partagés.
    - Gestion de 16 canaux de capteurs contenant jusqu'à 24 capteurs.
    - Traitement de 24 canaux d'actionneurs contenant jusqu'à 8 actionneurs.
    - Mise en œuvre de la norme IEC 61508-6 partie D pour la définition du facteur bêta

(séparation / ségrégation, diversité / redondance, ...).

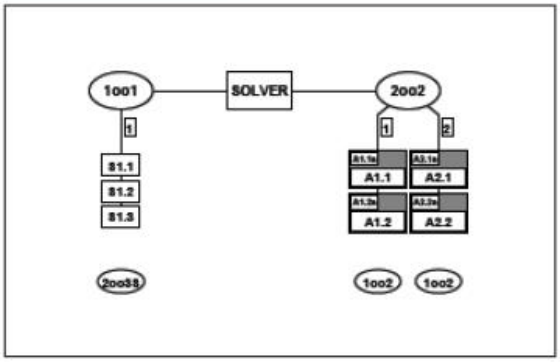
- Rapport PDF avec synthèse SIF, calendrier de maintenance (période de test de chaque composant).
- Les SIFs créés peuvent être réutilisés comme barrières de sécurité avec un arbre d'événements ou dans le module Risk.

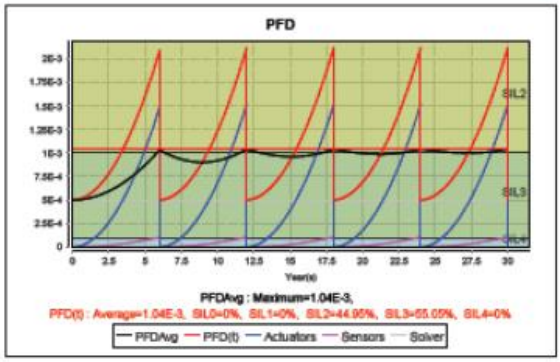
B.4. Exploitations de données et résultats :

- Base de données pour les composants : création et gestion de modèles de composants génériques (capteurs, actionneurs, solveurs).
- Synthèse des données d'entrée dans des tableaux permettant de contrôler plus facilement la qualité d'une entrée.
- Stockage des résultats dans le document et exportation dans différents formats (csv, XML, Excel, etc.).
- Visualisation des résultats sous forme de courbes, de camemberts ou d'histogrammes.
- L'impression au format vectoriel PDF génère des images de haute qualité mais de petits fichiers qui peuvent être envoyés par e-mail même avec des centaines de pages.
- Des fichiers externes (certificats PDF, images du système, ...) peuvent être inclus dans le document et faire partie du rapport complet.
- Interaction avec le système d'exploitation : possibilité de copier/coller des courbes, des systèmes ou des résultats vers des logiciels de traitement de texte, des feuilles de calcul ou des outils de présentation.

SIF Identifier : SIF1	Revision	Date	Produced by	Checked by	Validated by
	01	04/12/2014	X. XXXX	X. XXXX	TOTAL

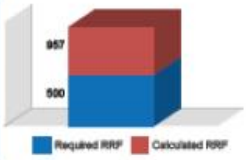
Location/Project	Plant located in Block 32
Process-Units	Separation
SIF function	Protection against overpression on separation
SIF description	Stop separation
Sensors	SIF1_S1.1, SIF1_S1.2, SIF1_S1.3
Solver	SIF1_SOLVER
Actuators	SIF1_A1.1, SIF1_A1.1a, SIF1_A1.2, SIF1_A1.2a, SIF1_A2.1, SIF1_A2.1a, SIF1_A2.2, SIF1_A2.2a
PID	10-PID-123456
Data source	OREDA
Comment	In case of high pression in LSHH 1234, the separator is shutdown.





PFDavg over 30 years = 1.0445E-3

Required SIL	Calculated SIL	Required RRF	Calculated RRF	Max SIL for sensors (architectural constraints)	Max SIL for actuators (architectural constraints)	Achieved SIL for the SIF	Conclusion of SIL for the SIF
2	2	500	957	4	4	2	Compliant



	PFD Avg	RRF	Calculated SIL	Contribution (%)
Sensor(s) Part	3.56E-5	28128.89	4	3.4%
Solver Part	5.00E-4	2000.00	3	47.86%
Actuator(s) Part	5.09E-4	1963.69	3	48.74%
SIF	1.04E-3	957.40	2	100%

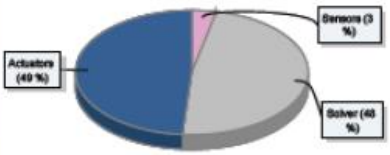


Figure B.2 : Résultats du logiciel GRIF-module SIL [144]

Bibliographie

[1] ISO. (2018). *ISO 31000:2018 – Management du risque : lignes directrices*. Genève, Suisse : Organisation internationale de normalisation (ISO).

[2] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[3] CEI. (2019). *CEI 31010:2019 – Management du risque — Techniques d'appréciation du risque*. Genève, Suisse : Commission électrotechnique internationale (CEI).

[4] ISO/IEC. (2014). *ISO/IEC Guide 51:2014 — Safety aspects: Guidelines for their inclusion in standards.* Geneva, Switzerland.

[5] INERIS. (2024). *Risques industriels liés aux ICPE : prévenir et maîtriser les accidents majeurs.* Institut national de l'environnement industriel et des risques (INERIS). Consulté le 29 octobre 2025, sur https://www.ineris.fr

[6] ISO/IEC. (2009). *ISO/IEC Guide 73:2009 — Risk management: Vocabulary.* Geneva, Switzerland: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

[7] INERIS. (2016). *Méthodologie d'analyse des risques – Guide pratique d'application de la réglementation sur les études de dangers.* Verneuil-en-Halatte, France: Institut National de l'Environnement Industriel et des Risques (INERIS).

[8] ISO/IEC. (2014). *ISO/IEC Guide 51:2014 — Safety aspects: Guidelines for their inclusion in standards.* Geneva, Switzerland.

[9] ISO. (2010). *ISO 12100:2010 — Safety of machinery: General principles for design — Risk assessment and risk reduction.* Geneva, Switzerland: International Organization for Standardization (ISO).

[10] INERIS (2016). *Guide pratique pour la mise en œuvre d'une étude de dangers.* Institut National de l'Environnement Industriel et des Risques, Verneuil-en-Halatte, France.

[11] Actu-Environnement. (s. d.). *Actu-Environnement – Média d'informations spécialisé environnement et développement durable*. Paris : Cogiterra. Repéré à : https://www.actu-environnement.com/ (consulté le 29 octobre 2025).

[12] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[13] ISO. (2018). *ISO 31000:2018 — Risk management: Guidelines.* Geneva, Switzerland: International Organization for Standardization (ISO).

[14] INERIS (2016). *Guide pratique pour la mise en œuvre d'une étude de dangers.* Institut National de l'Environnement Industriel et des Risques, Verneuil-en-Halatte, France.

[15] ISO 31010:2019, *Risk management — Risk assessment techniques.* International Organization for Standardization, Geneva.

[16] ISO 31010:2019, *Risk management — Risk assessment techniques.* International Organization for Standardization, Geneva.

[17] Kaplan, S., & Garrick, B. J. (1981). *On the Quantitative Definition of Risk.* Risk Analysis, 1(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.

[18] Modarres, M. (1993). *What Every Engineer Should Know About Reliability and Risk Analysis.* Marcel Dekker Inc., New York.

[19] Boissier, D. (2000). *Prise en compte de l'incertitude dans l'évaluation du risque industriel.* INERIS, Verneuil-en-Halatte, France.

[20] Ministère de la Transition Écologique (DGPR). (Base ARIA – Analyse, Recherche et Information sur les Accidents). URL : https://www.aria.developpement-durable.gouv.fr

[21] U.S. Chemical Safety and Hazard Investigation Board (CSB). *Incident Investigation Reports.* URL : https://www.csb.gov

[22] CCPS (Center for Chemical Process Safety). (2000). *Guidelines for Chemical Process Quantitative Risk Analysis* (2nd ed.). American Institute of Chemical Engineers (AIChE), New York.

[23] CCPS (Center for Chemical Process Safety). (2000). *Guidelines for Chemical Process Quantitative Risk Analysis* (2nd ed.). American Institute of Chemical Engineers (AIChE), New York.

[24] INERIS. (2016). *Guide pratique pour la mise en œuvre d'une étude de dangers.* Verneuil-en-Halatte, France

[25] CCPS (Center for Chemical Process Safety). (2000). *Guidelines for Chemical Process Quantitative Risk Analysis* (2nd ed.). American Institute of Chemical Engineers (AIChE), New York.

[26] INERIS. (2016). *Guide pratique pour la mise en œuvre d'une étude de dangers.* Verneuil-en-Halatte, France.

[27] ISO/IEC Guide 51:2014. *Safety aspects — Guidelines for their inclusion in standards.* Genève : ISO.

[28] ISO 31010:2019. *Management du risque — Techniques d'appréciation du risque.* Genève : Organisation internationale de normalisation (ISO).

[29] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[30] Villemeur, A. (1988). *Sûreté de fonctionnement des systèmes industriels : Fiabilité, facteurs humains, informatique.* Éditions Eyrolles, Paris

[31] ISO 31000:2018. *Management du risque — Lignes directrices.* International Organization for Standardization, Genève.

[32] Sklet, S. (2006). *Safety barriers: Classification, functions and performance. Journal of Loss Prevention in the Process Industries*, 19(5), 494–506. https://doi.org/10.1016/j.jlp.2006.05.001

[33] Bento, R. F. (2003). *Safety barriers: Concepts and applications in process safety management. Journal of Hazardous Materials*, 100(1–3), 27–36. https://doi.org/10.1016/S0304-3894(03)00071-2

[34] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[35] IEC 61511:2016. *Functional safety – Safety instrumented systems for the process industry sector.* International Electrotechnical Commission, Genève, Suisse.

[36] ISO 13702:2015. *Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines.* International Organization for Standardization, Genève, Suisse.

[37] Hollnagel, E. (2004). *Barriers and Accident Prevention.* Aldershot, UK: Ashgate Publishing

[38] 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 Bordeaux 1, France.

[39] ISO 17776:2000. *Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment.* International Organization for Standardization, Genève, Suisse.

[40] PSA (Petroleum Safety Authority Norway). (2002). *Guidelines for Barrier Management.* Stavanger, Norway

[41] Hale, A. (2003). *Safety Management in High Hazard Industries.* Oxford: Butterworth-Heinemann.

[42] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[43] Hale, A. (2003). *Safety Management in High Hazard Industries.* Oxford: Butterworth-Heinemann.

[44] Kjellén, U. (2000). *Risk Barriers and Risk Analysis in Process Industry. Journal of Loss Prevention in the Process Industries*, 13(4), 283–293. https://doi.org/10.1016/S0950-4230(00)00017-5

[45] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[46] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[47] ARAMIS Project. (2004). *Advanced Risk Assessment Methodologies for Industrial Safety.* European Commission, DG Research.

[48] Hokstad, P., & Corneliussen, L. (2003). *The PDS-method: A method for quantifying safety performance of safety barriers. Reliability Engineering & System Safety*, 80(3), 217–231. https://doi.org/10.1016/S0951-8320(03)00023-7

[49] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[50] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[51] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[52] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[53] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[54] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[55] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[56] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[57] IEC 60300-3-11:2003. *Dependability management – Part 3-11: Maintenance strategy.* International Electrotechnical Commission, Genève, Suisse.

[58] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[59] Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications* (2nd ed.). Hoboken, NJ: Wiley-Interscience.

[60] Hokstad, P., Vatn, J., Aven, T., & Sørum, L. (2003). *Specification of safety functions and safety integrity requirements.* Reliability Engineering & System Safety, 80(3), 233–242. https://doi.org/10.1016/S0951-8320(03)00024-9

[60] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[61] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[62] Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot, UK: Ashgate Publishing.

[63] CCPS (Center for Chemical Process Safety, AIChE). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: AIChE.

[64] Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot, UK: Ashgate Publishing.

[65] Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems.* Farnham, UK: Ashgate Publishing.

[66] Willey, K. (2014). *Layer of Protection Analysis (LOPA) in Process Safety Management.* Hoboken, NJ: Wiley

[67] Radu Mareş, C., & Popescu Stelea, M. (2017). *Event Tree Analysis in Industrial Risk Assessment. Environmental Engineering and Management Journal*, 16(6), 1385–1394.

[68] Modarres, M., Kaminskiy, M., & Krivtsov, V. (2016). *Reliability Engineering and Risk Analysis: A Practical Guide.* CRC Press, Boca Raton, FL.

[69] Zhao, X., Li, J., & Wang, Y. (2019). *Monte Carlo Simulation for Risk Assessment in Industrial Systems. Safety Science*, 120, 547–556. https://doi.org/10.1016/j.ssci.2019.07.015

[70] IEC 61511:2016. *Functional safety – Safety instrumented systems for the process industry sector.* International Electrotechnical Commission, Genève, Suisse.

[71] ISO/TR 12489:2016. *Safety of machinery — Functional safety and risk assessment of control systems.* International Organization for Standardization, Genève, Suisse.

[72] IEC 61511:2016. *Functional safety – Safety instrumented systems for the process industry sector.* International Electrotechnical Commission, Genève, Suisse.

[73] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[74] IEC 61511:2016. *Functional safety – Safety instrumented systems for the process industry sector.* International Electrotechnical Commission, Genève, Suisse.

[75] Chebila, M., & Innal, F. (2015). *Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. Journal of Loss Prevention in the Process Industries*, 34, 167–176. https://doi.org/10.1016/j.jlp.2015.02.002

[76] Innal, F., Dutuit, Y., & Chebila, M. (2015). *Safety and operational integrity evaluation and design optimization of safety instrumented systems. Reliability Engineering & System Safety*, 134, 32–50. https://doi.org/10.1016/j.ress.2014.10.001

[77] Omeiri, H., Innal, F., & Liu, Y. (2021). *Consistency checking of the IEC 61508 PFH formulas and new reliability measures for safety instrumented systems. Reliability Engineering & System Safety*, 209, 107437. https://doi.org/10.1016/j.ress.2021.107437

[78] Dutuit, Y., Rauzy, A., & Signoret, J.-P. (2008). A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 222*(3), 371–379. https://doi.org/10.1243/1748006XJRR147

[79] SATODEV. (2022). *GRIF: Graphical Interface for Reliability Forecasting — User Manual* (Version 2022). Villeneuve d'Ascq, France: SATODEV. Retrieved from https://www.satodev.com/en/software/grif

[80] International Electrotechnical Commission (IEC). (2001). *IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide.* Geneva: IEC.

[81] Center for Chemical Process Safety (CCPS). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York: American Institute of Chemical Engineers (AIChE).

[82] SRCM. (2020). *SIS Safety Instrumented Systems*. Retrieved October 30, 2025, from https://srcm.nl/sis-safety-instrumented-systems/

[83] CCPS (Center for Chemical Process Safety). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York, NY: American Institute of Chemical Engineers (AIChE).

[84] U.S. Environmental Protection Agency (EPA) & National Oceanic and Atmospheric Administration (NOAA). (2023). *ALOHA® (Areal Locations of Hazardous Atmospheres): User's Manual* (Version 5.4.7). Washington, DC: EPA Office of Emergency Management. Retrieved from https://www.epa.gov/cameo/aloha-software

[85] Health and Safety Executive (HSE). (2001). *Reducing Risks, Protecting People: HSE's Decision-Making Process.* Norwich, UK: HSE Books.

[86] Health and Safety Executive (HSE). (2001). *Reducing Risks, Protecting People: HSE's Decision-Making Process.* Norwich, UK: HSE Books.

[87] ISO 31010. (2019). *Risk management — Risk assessment techniques* (2e éd.). Geneva, Switzerland: International Organization for Standardization.

[88] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[89] International Electrotechnical Commission. (2016). *IEC 61511:2016 – Functional safety – Safety instrumented systems for the process industry sector.* Geneva, Switzerland: International Electrotechnical Commission (IEC).

[90] Lanternier, B., & Adjadj, A. (2008). Allocation de niveau d'intégrité de sécurité (SIL) requis conformément à la norme CEI 61511. *Revue Internationale sur l'Ingénierie des Risques Industriels, 1*(1), 34–45.

[91] SONATRACH. (2019). *Étude de dangers – SONATRACH EDD + EIA RA2K* (Rapport n° PP153689-1, Rev. 03, Document n° 1ZUAQSH-4). Activité Aval.

[92] Algeria Condensate Project – Skikda. (s.d.). *Manuel d'opération* (Procédure d'ingénierie, Document n° SC1-900-MU-PR-0003-3, Rev. 1, 113 p.).

[93] Boudjoghra, N., & Innal, F. (2023). Evaluation of Safety Instrumented System in a Natural Gas Facility According to IEC 61508 Standard. International Journal of Safety and Security Engineering, 13(5), 801–811.

[94] Boudjoghra, N., & Innal, F. (2025). Safety Lifecycle of Safety Instrumented System: Case study of a diesel storage tank. Algerian Journal of Signals and Systems (AJSS), 10(3).

[95] TNO. (2005). *Methods for the Calculation of Physical Effects (Yellow Book), 3rd edition — CPR 14E: Guidelines for Quantitative Risk Assessment.* The Hague, Netherlands: Committee for the Prevention of Disasters (CPR).

[96] Center for Chemical Process Safety (CCPS). (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment.* New York, NY: American Institute of Chemical Engineers (AIChE).

[97] Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

[98] Duijm, N. J., Montmayeul, R., Planas, E., & Kirchsteiger, C. (Eds.). (2004). *ARAMIS Project: Accidental Risk Assessment Methodology for Industries.* European Commission, Joint Research Centre (JRC), Institute for Systems, Informatics and Safety, Major Accident Hazards Bureau, Ispra, Italy.

[99] RIVM (2009). *Guidelines for Quantitative Risk Assessment (Purple Book).* RIVM Report 620066006, Bilthoven, The Netherlands.

[100] SONATRACH. (2019). *Étude de dangers – SONATRACH EDD + EIA RA2K* (Rapport n° PP153689-1, Rev. 03, Document n° 1ZUAQSH-4). Activité Aval.

[101] Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/0471475581

[102] Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/0471475581

[103] International Electrotechnical Commission. (2015). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*. Geneva, Switzerland: IEC.

[104] Blanchard, B. S., Verma, D., & Peterson, E. L. (1995). *Maintainability: A key to effective serviceability and maintenance management*. New York, NY: John Wiley & Sons.

[105] International Electrotechnical Commission. (2015). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*. Geneva, Switzerland: IEC.

[106] International Electrotechnical Commission (IEC). (2016). *IEC 61511: Functional safety – Safety instrumented systems for the process industry sector* (Parts 1–3). Geneva, Switzerland: IEC.

[107] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[108] Hokstad, P., & Corneliussen, K. (2003). *PDS method handbook: Reliability prediction method for safety instrumented systems*. Trondheim, Norway: SINTEF.

[109] International Electrotechnical Commission (IEC). (2016). *IEC 61511: Functional safety – Safety instrumented systems for the process industry sector* (Parts 1–3). Geneva, Switzerland: IEC.

[110] Hokstad, P., & Corneliussen, K. (2003). *PDS method handbook: Reliability prediction method for safety instrumented systems*. Trondheim, Norway: SINTEF

[111] International Electrotechnical Commission. (2016). *IEC 61511-1: Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements*. Geneva: IEC.

[112] International Electrotechnical Commission. (2017). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) – Part 192: Dependability*. Geneva: IEC.

[113] International Electrotechnical Commission. (2015). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*. Geneva, Switzerland: IEC.

[114] International Electrotechnical Commission. (2019). *IEC 60300-3-11: Dependability management — Part 3-11: Application guide — Reliability centred maintenance*. Geneva, Switzerland: IEC.

[115] International Electrotechnical Commission. (2015). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*. Geneva, Switzerland: IEC.

[116] Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications* (2nd ed.). Hoboken, NJ: Wiley-Interscience.

[117] International Electrotechnical Commission. (2015). *IEC 60050-192: International Electrotechnical Vocabulary (IEV) — Part 192: Dependability*. Geneva, Switzerland: IEC.

[118] Rausand, M., & Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications* (2nd ed.). Hoboken, NJ: Wiley-Interscience.

[119] Dhillon, B. S. (2006). *Maintainability, Maintenance, and Reliability for Engineers*. Boca Raton, FL: CRC Press.

[120] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[121] Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

[122] IEC 60300-3-11. (2019). *Dependability management — Part 3-11: Application guide — Reliability centred maintenance*. International Electrotechnical Commission.

[123] SINTEF. (2010). *PDS Data Handbook: Reliability data for safety instrumented systems*. Trondheim, Norway: SINTEF.

[124] Exida. (2023). *Safety Equipment Reliability Handbook (SERH)* (7th ed.). Exida LLC.

[125] OREDA (Offshore and Onshore Reliability Data). (2015). *OREDA Handbook: Offshore reliability data handbook* (6th ed.). DNV GL.

[126] CCPS (Center for Chemical Process Safety). (2018). *Process Equipment Reliability Database (PERD)*. American Institute of Chemical Engineers.

[127] U.S. Department of Defense. (1991). *MIL-HDBK-217F: Reliability Prediction of Electronic Equipment.* Washington, DC: Department of Defense.

[128] SAE International. (2009). *SAE J1739: Potential Failure Mode and Effects Analysis in Design (Design FMEA), Manufacturing and Assembly Processes (Process FMEA), and for Machinery (Machinery FMEA).* Warrendale, PA: SAE International.

[129] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[130] IEC. (2016). *IEC 61511-1: Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements.* Geneva: IEC.

[131] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[132] Hokstad, P., & Lindqvist, B. H. (2011). *PDS Data Handbook 2011 Edition – Reliability Data for Safety Instrumented Systems.* Trondheim, Norway: SINTEF.

[133] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[134] IEC 61508:2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission, Genève, Suisse.

[135] Omeiri, H. (2021). *Modélisation des performances fiabilistes des systèmes instrumentés de sécurité*, Thèse de doctorat, Université Badji Mokhtar – Annaba.

[136] Brissaud, F., Barros, A., & Bérenguer, C. (2010). Modeling imperfect maintenance and testing policies for safety instrumented systems. *Reliability Engineering & System Safety, 95*(6), 647–656.

[137] IEC. (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3* (IEC 61508-6). International Electrotechnical Commission.

[138] Previnfo. (2024). Risque industriel. Consulté le 25 octobre 2024 sur

https://www.previnfo.net/sections.php?op=printpage&artid=65.

[139] Kinsella, K. G. (1993). *A rapid assessment methodology for the prediction of vapour cloud explosions* (Research Report n° 357). Technical Research Centre of Finland.

[140] INERIS. (2010). *Boil over classique et boil over couche mince – Ω13* (Rev. 02). Institut National de l'Environnement Industriel et des Risques.

[141] GTDLI. (2007). *Le Boil-Over et autres phénomènes générant des boules de feu concernant les bacs des dépôts de liquides inflammables* (Rev. 01). Groupe de Travail Dépôts de Liquides Inflammables.

[142] MEDDTL – Ministère de l'Écologie, du Développement durable, des Transports et du Logement. (2010). *Circulaire du 10 mai 2010 récapitulant les règles méthodologiques applicables aux études de dangers, à l'appréciation de la démarche de réduction du risque à la source et aux plans de prévention des risques technologiques (PPRT) dans les installations classées en application de la loi du 30 juillet 2003*.

[143] TotalEnergies. (s. d.). Module SIL (package booléen). GRIF. https://grif.totalenergies.com/fr/produits/package-booleen/module-sil

[144] GRIF-Workshop. (2022) *Graphical interface for reliability forecasting software*. Disponible chez: http://grifworkshop.com.