REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Faculté de Technologie

Département de Génie Electrique

N° d'ordre : D012123001D

THESE

Présentée en vue de l'obtention du diplôme de

Doctorat en sciences

Filière

Automatique

Spécialité

Automatique Avancé

Contribution à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS).

Présentée par : Mme METATLA Hassina

Devant le jury composé de :

Lachouri Abderrezak	Professeur	Président	Université de Skikda
Rouainia Mounira	Professeur	Encadreur	Université de Skikda
Hariz Saliha	MCA	Examinateur	Université d'Annaba
Khelif Rabia	Professeur	Examinateur	Université d'Annaba
Bendib Riad	MCA	Invité	Université de Skikda

Année universitaire : 2022-2023

Dédicaces

Je dédie ce travail de thèse

A la mémoire de mon cher père, que dieu l'accueille dans son vaste paradis.

A chère ma mère

A ma fille et mon fils

A mes frères

A mes sœurs

A mes amis

Remerciements

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

J'adresse toute ma gratitude à ma directrice de thèse Madame. MOUNIRA ROUAINIA, professeur à l'université de Skikda, de m'avoir proposé ce thème de thèse très intéressant, pour ces critiques pertinentes et pour son soutien.

Je tiens à exprimer mes sincères remerciements à monsieur A.LACHOURI de l'université de Skikda d'en présider le jury de thèse.

Je suis profondément reconnaissante à monsieur R.KHELIEF, professeur à l'université d'Annaba et madame S.HARIZ Maître de conférence de l'université d'Annaba d'avoir accepté de participer à mon jury de thèse.

J'exprime mes profonds remerciements à monsieur R.BENDIB, maître de conférences à l'université de Skikda, pour sa souplesse, sa patience et ses conseils judicieux

Un grand merci à monsieur E. MECHHOUD, maître de conférences à l'université de Skikda pour leur aide et leur encouragement.

Je tiens enfin à remercier celles et ceux qui m'ont encouragé et soutenu moralement tout au long de cette période : ma petite famille, et mes collègues.

Liste des acronymes

AdD	Arbre des Défaillances
AMDEC	Analyse des Modes de Défaillance de leurs Effets et de leurs Criticités
APR	Analyse Préliminaire de Risque
AFNOR	Association Française de Normalisation
ALARP	As Low As Reasonably Practicable (aussi faible que raisonnablement possible)
BdF	Bloc de Fiabilité
BPCS	Basic Process Control System
BMS	Burner Management System (Barrières de Sécurité pour gérer les Chaudières)
BP	Barlow et Proschan (Facteur d'importance de Barlow et Proschan)
CIF	Critical Importance Factor (Facteur d'importance Critique)
CCF	Common Cause Failure
DIF	Diagnostic Importance Factor (Facteur d'importance de Diagnostic)
DC	Diagnostic Coverage (Couverture du Diagnostic)
DD	Dangerous Detected failures (Défaillances dangereuses détectées)
DU	Dangerous Undetected failures (Défaillances dangereuses non détectées)
DCC	Défaillance de Cause Commune
E_i	L'état E_i
E/E/EP	Electrique / Electronique / Electronique Programmable
EN	European Norm (Norme Européenne)
ER	Evénement Redouté
EUC	Equipment Under Control (équipement à protéger)
ESD	Emergency Shut Down System (Système d'arrêt d'urgence)
F&G	Fire and Gas System (Système Feu et Gaz)
FMDS	Fiabilité, Maintenabilité, Disponibilité et Sécurité
FTA	Fault Tree Analysis
GdM	Graphes de Markov
GRIF	Graphiques Interactifs pour la Fiabilité
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitation)
HFT	Hardware Fault Tolerance (Tolérance aux défaillances matérielles)

HIPPS	High Integrity Pressure Protection System (Système de protection contre les hautes pressions à haute fiabilité)
IEC	International Electrotechnical Comission
IPL	Independent Protection Layer
ISA	Instrument Society of America
ISO	International Organisation for Standardization
KooN	K out of N (K parmi N)
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection)
LPG	Liquefied Petrol Gas (Pétrole et Gaz liquéfié)
LS	Logic Solver (Unité de Traitement Logic)
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance)
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)
MGL	Multiple Greek Letter (Méthode des Lettres Grecques Multiples)
NF	Norme Française
Pdd	Probabilité de défaillance dangereuse d'un élément de l'architecture KooN
Pdds	Probabilité de défaillance dangereuse du système en KooN
Pdnd	Probabilité de défaillance non dangereuse d'un élément de l'architecture KooN
Pdns	Probabilité de défaillance non dangereuse du système en KooN
PFD	Probability of Failure on Demand (Probabilité de défaillance à la demande)
PFH	Probability of Failure per Hour (Probabilité de défaillance par Heure)
P&ID	Piping &Instrumentation Diagram
PLC	Programmable Logic Controller
PT	Transmetteurs
PVST	Partial Valve Stroke Testing (Test de Course Partielle de la Vanne)
RA1K	Raffinerie de Skikda
RAMS	Reliability, Availability, Maintenability and Security
RAW	Reliability Achievement Word (Facteur d'Augmentation de Risque)
RBD	Reliability Block Diagram
RdP	Réseaux de Pétri
RRW	Reliability Reduction Word (Facteur Réduction de Risque)
SD	Safe detected Failures (Défaillances sûres détectées)
SIF	Safety Instrumented Function (Fonction Instrumenté de Sécurité)

SIL	Safety Integrity Level (Niveau d'intégrité de Sécurité)
SF	Sécurité Fonctionnelle
SFF	Safe Failure Fraction (proportion des défaillances en sécurité)
SIS	Safety Instrumented System (Système Instrumenté de sécurité)
SRCF	Safety Related commande Functions (Fonctions de Commande Relatives à la Sécurité)
SRS	Safety related System (Système Relatif à la sécurité)
SU	Safe Undected Failures (Défaillances sûres non détectées)
TMC	Turbo Machinery Control System (Barrières de Sécurité pour gérer les Machines Tournantes
WHCP	Well Head Control Panel (Barrières de Sécurité pour contrôler la Pression ou la Température des puits)
β	Taux de défaillances de Cause Commune

Abstract

The Safety Instrumented Systems (SISs) are vital safety barriers, widely used in industrial plants to reduce the probability of hazardous situations such as gas leakages and fires explosions. A Safety instrumented systems are being installed on both onshore and offshore and are able to assure and control many Safety Instrumented Functions (SIFs).

The objective of this work is to evaluate the dependability of a safety-instrumented system (SIS) based on an onshore, High Integrity Pressure Protection Systems (HIPPS), and located in SKIKDA Refinery (RA1k). This type of SIS are widely used in oil & gas industrial plants, to play the role of a barrier between high pressure and low-pressure section in the installation. We achieve functional and dysfunctional analysis of the HIPPS reliability parameters with and without consideration of the Common Cause Failures (CCFs). The Reliability Block Diagram (RBD) is used for functional aspect and Fault Tree Analysis (FTA) technique is employed for dysfunctional aspect.

-In the first part we effectuates a HIPPS diagnostic study (without consideration of CCFs), by calculation of the deferent dependability parameter: reliability R(t), probability of failure F(t), instantaneous unavailability U(t) et the frequency W(t). Also the following Importance Measures (IMs): **Birnbaum measure, or the MIF, Lambert measure (CIF), Fussel Vesely measure (DIF), Risk Achievement Worth (RAW), Risk Reduction Worth (RRW**) **and Barlow and Proschan measure (BP)** by the proposed methodology. Main purpose of those IMs is to identify weaknesses, or the most vulnerable parts in our considered HIPPS, and may serve as resource allocation factors for scheduled HIPPS maintenance in order to minimize its down time and cost-efficient operation of our system.

-In the second part a study with account of CCFs, we modelize the CCFs by the Beta factor model and illustrate the negative impact of this type of failure on the global HIPPS reliability, in the objective to take care against this type of failure. A comparative study on HIPPS dependability with and without considering Common Cause Failures (CCFs) is realized; as a result, we quantify the effects of CCFs on overall HIPPS performances such as HIPPS reliability reduction, HIPPS Safety Integrity Level (SIL) degradation, and the decrease of HIPPS Mean Down Time (MDT), and production capacity.

The obtained simulation results help us in implementing a HIPPS maintenance planning from a quantitative point of view, and on the other hand, this thesis shows the HIPPS capacity in keeping its safety and reliability characteristics in presence of the CCFs. In addition, our analysis proves the robustness, accuracy, and the suitability of the used methodology for CCFs assessment.

Keywords: HIPPS; CCFs; FTA; RBD; SIL; MIF; CIF; DIF; RAW; RRW ; BP.

Résumé

Diverses sécurités sont mises en œuvre lorsque les installations industrielles automatisés présentent des risques pour l'homme, l'environnement ou les biens. Ces types de sécurités utilisent des moyens contribuant soit à la prévention soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les systèmes instrumentés de sécurité (SIS) sont souvent utilisés comme moyens de protection pour réaliser des fonctions instrumentées de sécurité (SIF).

Le présent travail de thèse a pour objectif d'évaluer la sûreté de fonctionnement d'un système instrumenté de sécurité. Nous considérerons le cas particulier d'un système à haute intégrité contre les surpressions, (High Integrity Pressure Protection System (HIPPS)), utilisé en industrie pétrole et gaz pour la protection contre les évènements de surpression qui peuvent causer des dommages à l'environnement, aux infrastructures et au personnel. Le rôle primordial du HIPPS a attiré notre attention pour analyser les performances d'un HIPPS existant à la plateforme on-shore Raffinerie de SKIKDA (RA1K) en présence et en absence des défaillances de cause commune (DCC), pour quantifier l'effet de ce type de défaillance sur les paramètres fiabilistes du système. Les Blocs diagrammes de fiabilité (BdF), sont utilisés pour la modélisation de l'aspect fonctionnelle du système, tandis que les Arbres de Défaillances (AdD) sont utilisés pour la modélisation de l'aspect dysfonctionnelle. Nous procédons par deux étapes :

-La première étape est consacré à une étude de diagnostic, ou phase d'analyse sans considération des DCC pour le système considéré par l'usage des deux techniques Bloc de Fiabilité (BdF) et Arbre de Défaillance (AdD), à travers laquelle nous avons calculé les différents paramètres de la sûreté de fonctionnement la fiabilité R(t), probabilité de défaillance F(t),l'indisponibilité instantanée U(t) et la fréquence W(t). Ainsi que les facteurs d'importances suivants :**Facteur d'Importance Marginale (de Birnbaum (MIF)), Facteur d'Importance Critique (de Lambert (CIF)), Facteur d'Importance de Diagnostic (de Fussel Vesely (DIF)), facteur d'augmentation de risque (Risk Achievement Worth (RAW)), facteur de réduction de Risque (Risk Reduction Worth (RRW**)),**et le facteur d'importance de Barlow and Proschan (BP).**Ces mesures d'importances nous permis d'aboutir à un classement pour les composants du HIPPS permettent l'identification des constituants les plus vulnérables vis-à-vis le fonctionnement du système, et par conséquent de cibler et orienter les actions de maintenance à préalable.

-La deuxième étape est dédiée pour la modélisation des DCCs par le modèle du facteur Beta et la démonstration de l'effet négatif de ce type de défaillance sur les performances globales du HIPPS comme la réduction de la fiabilité du HIPPS ; la dégradation du niveau d'intégrité de sécurité (SIL) du système considéré ; l'augmentation de la durée moyenne d'indisponibilité après défaillance (Mean Down Time (MDT) du HIPPS, et la capacité de production. Le modèle du facteur Beta est utilisé pour la modélisation des DCCs au niveau des sous-systèmes transmetteurs et vannes.

Les résultats de simulation obtenus nous permettent la mise en œuvre d'une politique de maintenance préventive et corrective pour les différents composants du HIPPS d'un point de vue quantitatif, en d'autre part ces résultats expliquent la capacité du HIPPS à conserver ses caractéristiques de fiabilité et de sûreté en présence des DCC. En outre mous prouvons la robustesse, l'exactitude et la convenance des blocs diagrammes de fiabilité et des arbres de défaillances pour le traitement et l'évaluation des DCC au niveau du HIPPS.

<u>Mots-Clés</u> : HIPPS; DCCs; SIL; AdD; BdF; MIF; CIF; DIF; RAW; RRW; BP

ملخص

تتطلب الصناعات البيتروكيميائية والغازية موارد مالية ضخمة، من حيث المنشآت والمعدات، وكذلك اليد العاملة المؤهلة. من أجل رفع مردودية هذه الصناعات لابد من ضمان موثوقية عالية للأنظمة والهياكل المستعملة فيها من خلال استعمال الوسائل والطرائق اللازمة سواءا للتنبؤ بالأخطار التي قد تتعرض لها المنشآت أو للحماية مع اتخاذ التدابير اللازمة لذلك .تشكل انظمة السلامة المجهزة (SIS) حاجز أمان فعال وضروري لصد ومواجهة مختلف المخاطر في المركبات الصناعية لقدرتها على انجاز وظائف حماية متعددة (SIFs) .

العمل المقدم في هذه الأطروحة يسلط الضوء على نظام الحماية عالي الموثوقية ضد الضغط المرتفع (HIPPS) المتواجد في مركب تكرير البترول والغاز (مصفاة سكيكدة RA1K) وذلك لأهميته في حماية المنشآت بحيث يعتبر حاجز أمان ضد ارتفاع الضغط، الذي قد يؤدي إلى نتائج كارثية على غرار الإنفجار والذي يؤثر بشكل سلبي على البنى التحتية للمنشآت الصناعية كما يسبب أضرار بالغة على الإنسان والتي قد تؤدي إلى حالات الموت وكذلك تتسبب في التأثير على سلامة البيئة والمحيط. وهذا الأخير يشغل مكانة هامة في إنجاز العملية الصناعية وضمان السير الحسن للإنتاج. إذ أن الأعطاب والتوقفات التي تكون على مستوى ال HIPPS قد تؤدي إلى التوقف الكلي للعملية الصناعية. ولأهميته البالغة، قمنا بدراسة تحليلية لمختلف عوامل الجودة للنظام المقترح في وجود وغياب الاعطاب ذات السبب المشترك (DCCs)، بهدف تقييم وتكميم تأثير هذا النوع من الأعطاب على مختلف عوامل الجودة. نستعمل مخططات كتل الموثوقية (BdF) من أجل النمذجة الوظيفية لنظام HIPPS، بينما نستعمل طريقة تحليل شجرة الأعطال من أجل النمذجة اللاوظيفية أي في حال العطب. فقد قمنا بتحقيق دراسة كمية وكيفية على مرحلتين

-المرحلة الأولى: تمثلت في دراسة تشخيصية ال HIPPS باستعمال تقنيتين: مخططات كتل الموثوقية (BdF) وطريقة تحليل شجرة الأعطال (AdD) ، تميزت بدراسة كمية و كيفية لمختلف عوامل الجودة والسلامة التالية: الموثوقية R(t)، إحتمالية العطب F(t) ، إحتمالية العطب اللحظي U(t) ، والتواتر W(t) .

إضافة إلى ذلك قمنا بحساب عوامل الأهمية التالية:عامل بيرنوب (MIF)، عامل لامبيرث (CIF)، عامل فاسيل فيسلي (DIF)، عامل مكبر ا الخطر (RAW)، عامل مصغر الخطر (RRW) وعامل بارلو وبروسكان (BP) . بهدف تقييم أهمية كل عنصر من عناصر نظام ال HIPPS . سمحت لنا هذه القياسات إلى الوصول لتصنيف لمكونات ال HIPPS والذي يفيدنا في تحديد وإبراز العناصر الأكثر تسببا في تشغيل أو تعطيل النظام وبالتالي إستهداف وتوجيه إجراءات الصيانة الخاصة بكل عنصر بصفة مسبقة.

-المرحلة الثانية : في هذه المرحلة قمنا بنمذجة الأعطاب ذات الفشل المشترك (DCCs) بواسطة نموذج بيتا (Beta) بإستعمال التقنيات السابقة وبواسطتها قمنا بتبيين الأثر السلبي ل (DCCs) على الموثوقية R(t)

وعلى مستوى تكامل السلامة (SIL) وكذلك على متوسط وقت التوقف بعد العطل (MDT)، بالإضافة إلى نقصان القدرة الإنتاجية.

النتائج التي تحصلنا عليها من خلال دراستنا أثبتت دقة وملاءمة كل من تقنيتي مخططات كتل الموثوقية (BdF) وشجرة الأعطاب (AdD)في تقييم ومعالجة الأعطاب ذات الفشل المشترك (DCCs)على مستوى النظام المدروس، وكذلك أثبتنا قدرة ال HIPPS في الحفاظ على خصائص الجودة والسلامة في ظل وجود (DCCs)

الكلمات المفتاحية: نظام الحماية عالي الموثوقية، الأعطاب ذات الفشل المشترك، نموذج بيتا، مستوى تكامل السلامة، مخطط كتل الموثوقية، تحليل شجرة الأعطاب، قياس الأهمية.

Liste des tableaux

Table des matières

Liste des figures

Introduction générale

Face à la complexité croissante des problèmes rencontrés dans le domaine industriel, particulièrement dans les installations pétrolières, les contraintes économiques, les exigences contractuelles et réglementaires et la prise de conscience accrue des risques, ont généré un besoin de confiance et d'appréciation de ce niveau de confiance de la part des utilisateurs dans les installations livrées. L'enjeu est donc de donner un niveau de confiance justifié qui répond aux attentes et exigences de l'utilisateur au meilleur coût.

Dans les marchés de conception, réalisation et d'exploitation des usines de production et fabrication de plus en plus il y fait référence aux études complètes de sûreté de fonctionnement des installations. La sûreté de fonctionnement qui a acquis son nom et sa forme actuelle au cours du dernier demi-siècle, rassemble une large palette d'outils et de méthodes au service de la maîtrise des risques, pour placer dans un système étudié une sorte d'efficacité, d'innocuité et de confiance justifiée et partagée. Les fondements de cette confiance peuvent prendre des formes variées, il s'agit toujours d'analyser le système en termes de fiabilité, maintenabilité, disponibilité et sécurité (concept « FMDS ») [1].

Les démarches de maîtrise des risques dans les complexes industrielles, visent en priorité à réduire le risque existant, inhérent à une application donnée, à un niveau jugé tolérable et à maintenir dans le temps. Cette réduction est souvent obtenue par l'utilisation d'une methodologies d'analyse de risque dont les plus connues sont l'Analyse Préliminaire de Risque (APR), l'Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticité (AMDEC), l'étude de danger et d'exploitabilité (Hazop pour Hazard and Operability), l'étude des couches de protection (Layer Of Protection Analysis (LOPA)), l'analyse par Arbre de Défaillance (AdD) et l'analyse fonctionnelle par Bloc de Fiabilité (BdF). Et aussi par l'interposition successive de plusieurs barrières de protection entre la source de danger qui est généralement un procédé industriel et les cibles potentielles que sont: les personnes, les biens et l'environnement [2].

Parmi les éléments importants qui nous ramènent à contrôler et à réduire les dangers et les menaces internes ou externes, on trouve les capteurs, les unités de traitements logiques et les actionneurs qui constituent les systèmes instrumentés de sécurité (SIS), lesquels ayant pour rôle de diminuer les risques d'occurrence d'évènements dangereux tout en garantissant la protection des personnes, des biens, des équipements matériels et de l'environnement.

Les SIS, aussi appelés boucles de sécurité, sont utilisés pour exécuter des fonctions de sécurité (Safety Intrumented Functions (SIFs)). Ils comprennent le matériel et les logiciels nécessaires pour obtenir la fonction de sécurité désirée. Ces systèmes peuvent atteindre un niveau d'intégrité de sécurité important appelé (Safety Integrity Level (SIL)) en conformité avec les normes en vigueur telles que, la norme (Commission Européenne International), CEI 61508 et la norme CEI 61511, qui traitent de la sécurité fonctionnelle des systèmes industriels [3] [4].

L'objectif premier des systèmes instrumentés de sécurité (SIS), est la détection des situations dangereuses (augmentation de la pression ou de température, fuite de gaz...), pouvant mener à un accident (incendie, explosion, rejet d'un produit dangereux. . . etc.) et de mettre en œuvre un ensemble de réactions nécessaires à la mise en sécurité de l'équipement à protéger *(EUC : Equipment Under Control).*C'est-à-dire dans un état stable ne présentant pas de risque pour les opérateurs humains et équipements.

Les niveaux d'intégrité de sécurité SILs, issus de la norme IEC 61508 sont des objectifs de sécurité utiles à l'évaluation des risques. Ils donnent une mesure de la réduction du risque obtenue par les moyens de protection fournis par le SIS. La détermination du niveau d'intégrité de sécurité dépend du calcul de la probabilité de défaillance sur demande (Probability of Failure on Demand) PFDavg. Les méthodes usuelles de calcul du PFDavg, pour les SISs sont des méthodes probabilistes issues des études traditionnelles de sûreté de fonctionnement ou des données de fiabilité relatives aux composants (taux de défaillance, taux de réparation, tests périodiques… etc.) peuvent être connues avec précision et validées par le retour d'expérience.

Notre travail de thèse a été effectué sur un système de protection contre les hautes pressions de haute fiabilité (High Integrity Pressure Protection System (HIPPS)). Le HIPPS est une application spécifique d'un système instrumenté de sécurité conçu et intégré conformément aux normes CEI 61508 et CEI 61511. Le HIPPS peut être utilisé à la fois dans les plateformes on-shore et off-shore, il est considéré comme l'un des meilleurs choix pour protéger les installations pétrole et gaz.

Parmi les problèmes rencontrés au niveau du HIPPS ou bien au niveau des systèmes instrumentés de sécurité : ***les défaillances de la cause commune (DCC).*** Pour améliorer la fiabilité ou la disponibilité des installations, une technique très efficace consiste à introduire de la redondance [2] pour la réalisation des fonctions critiques. Cela consiste à installer plusieurs composants fonctionnant en parallèle là où un seul suffirait. Ainsi, lorsque l'un d'entre eux tombe en panne, les autres continuent à assurer la fonction, permettant ainsi d'effectuer la réparation de celui qui est en panne. Les défaillances de causes communes sont des défaillances susceptibles d'entraîner plusieurs défaillances simultanées (ou d'augmenter notablement le taux de défaillance de plusieurs composants), mettant ainsi la redondance en défaut. Parmi les causes communes les plus fréquemment rencontrées on peut citer, à titre non exhaustif, les défauts de conception ou de fabrication, les alimentations communes (électriques, hydrauliques, air comprimé...), l'environnement (incendie, inondation, corrosion...) et, bien entendu, le facteur humain. La présence des défauts de causes communes limite les améliorations pouvant être apportées à la fiabilité d'un système [5].

Les DCCs constituent un sous ensemble de l'ensemble des défaillances dépendantes, ou l'ensemble des évènements dépendants affectant deux composants ou plus, au même moment ou dans un petit intervalle de temps et résultant directement d'une cause partagée [5] [6]. De manière pratique les fiabilistes utilisent une classification basée sur des causes génériques pour analyser ce type de défaillance, ils considèrent que les défaillances qui affectent les composants d'un système résultent soit d'agressions externes (de l'environnement), soit d'erreurs humaines commises à la conception, à la fabrication ou bien en exploitation. L'étude des Défaillances de Causes Communes (DCC) dans les systèmes programmés est un axe actif de recherche dans les domaines du nucléaire, de la pétrochimie, de l'aérospatial…etc.

Notre thèse est organisée en quatre chapitres :

Les fondamentaux de la sûreté de fonctionnement, ainsi que le principe de la méthodologie utilisée pour la modélisation fonctionnelle et dysfonctionnelle du HIPPS, étapes et les outils utilisées en diagnostic des pannes, sont décrites au premier chapitre.

Dans le deuxième chapitre nous décrivons, la constitution, le rôle, les différentes architectures des systèmes instrumentés de sécurité (SIS), ainsi que les différents détails du HIPPS (le principe de fonctionnement, les types de HIPPS, le SIL, cycle de vie…etc.), qui présente le système considéré comme un cas d'étude dans cette thèse.

Le troisième chapitre est consacré à la définition des défaillances de la cause commune (DCC), et à la description de leurs empruntés à la littérature pour montrer le principe de chacun.

La modélisation fonctionnelle par BdF et dysfonctionnelle par AdD du HIPPS avec et sans DCC font l'objet du quatrième chapitre. Une étude comparative est également réalisée dans l'objectif de monter l'effet des DCCs sur les performances du HIPPS.

Une conclusion générale des travaux réalisés dans le cadre de cette recherche est présentée à la fin de cette thèse. Nous proposons également des perspectives et approfondissements ouverts par cette thèse.

Chapitre 1

Analyse de Sûreté de fonctionnement et Diagnostic des pannes

1.1. Introduction

L'étude de sûreté de fonctionnement comporte deux volets complémentaires : une analyse fonctionnelle et une analyse dysfonctionnelle. Plusieurs méthodes sont utilisées dans ce cadre telles que : Analyse des Modes de Défaillance de leurs Effets et de leur Criticité (AMDEC), Analyse Préliminaire des Risques (APR), HAZard and OPerability Study (HAZOP), l'Arbre de Défaillances (AdD), les Blocs Diagramme de Fiabilité (BdF), Graphes de Markov (GdM), Réseaux de Petri (RdP).

Les réglementations actuelles imposent que les installations industrielles présentent le moins de risques possibles durant leurs utilisation. C'est dans la phase de conception que l'on doit intégrer les éléments nécessaires à la **sûreté de fonctionnement** de ces installations. Deux approches permettent cette diminution du risque, la prévention en minimisant la probabilité d'apparition d'un risque, la protection en limitant les conséquences d'un dysfonctionnement. Dans ce premier chapitre nous décrivons les fondamentaux de la sûreté de fonctionnement (SdF), nous définissions ses différents paramètres (fiabilité, disponibilité, maintenabilité et la sécurité ainsi que la métrique de la SdF), par la suite nous décrivons le principe de la méthodologie utilisée ainsi le calcul probabiliste des facteurs d'importances, exposons aussi leurs intérêts pour la détection des composants critiques.

1.2. La sûreté de fonctionnement

1.2.1. Définition

Définition 1 : La sûreté de fonctionnement est la science de défaillances, elle inclut ainsi leur connaissance, leur évaluation, leur prévision, leur mesure et leur maîtrise. Au sens strict, c'est la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans la qualité du service délivré

Définitions 2 (**Laprie 89**): la sûreté de fonctionnement d'un systèmeInformatique est la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre.

Définitions 3 (**CEI 50 191**) : Aptitude d'une entité à assumer une ou Plusieurs fonctions requises dans des conditions données [6].

1.2.2. Les différents critères de la sûreté de fonctionnement

Dès lors que la sécurité ou la disponibilité d'un système est mise en défaut, on incrimine sa fiabilité. Enfin, en cas de dysfonctionnement, il convient de remettre le système en conditions de fonctionnement initial : c'est là qu'intervient la maintenabilité. Ces quatre caractéristiques constituent la sûreté de fonctionnement d'un dispositif. Les principaux critères relatifs à la sûreté :

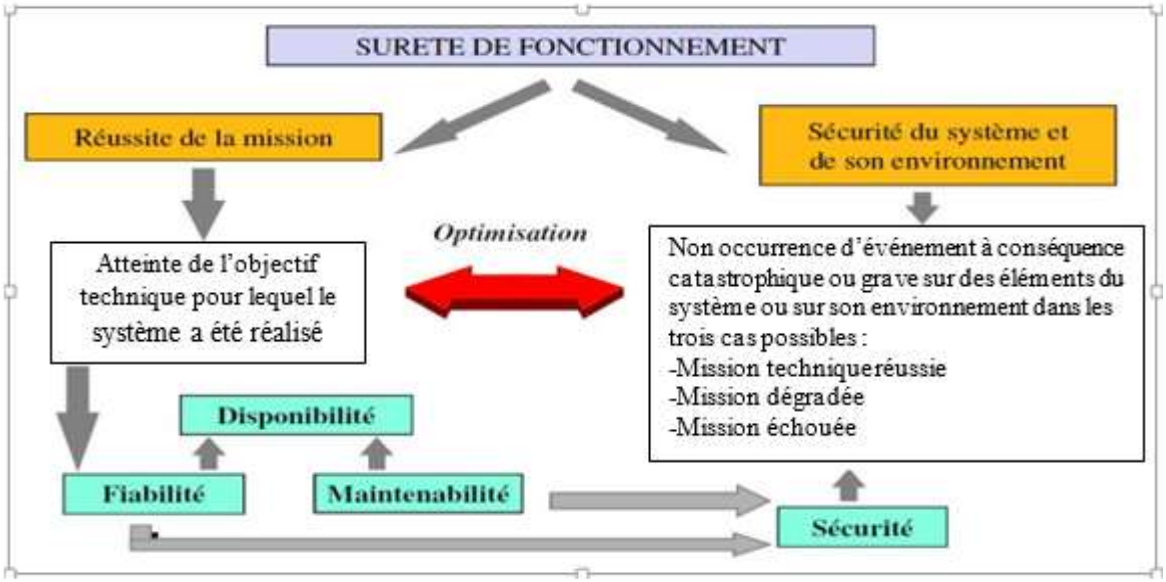


Figure 1.1 : Les composantes de la Sdf [7]

1.2.2.1. La fiabilité

La fiabilité est la probabilité de non-défaillance d'un équipement sur un intervalle de temps donné [8]. Le praticien lui substitue souvent la **MTBF** (mean time between failure) ou temps moyen entre deux pannes .Cette grandeur se situe, typiquement, entre 10000 et 20000 heures.

1.2.2.2. La sécurité

La sécurité est la capacité du système à réagir convenablement à des défaillances de ses constituants, sans provoquer d'accidents de personnes ni de dommage des installations[8].

1.2.2.3. La disponibilité

Définition : La disponibilité de *S* est son aptitude à être en état d'accomplir une fonction requise, dans des conditions données et à un instant donné ou pendant un intervalle de temps donné, en supposant que les ressources externes sont fournies[8].

Note : Cette définition concerne la disponibilité instantanée et moyenne**.**

Mesure : La disponibilité de *S* à l'instant *t* est mesurée par la probabilité, notée $A_S(t)$:

$$\mathrm{A(t)} = \text{prob (S non défaillant à l'instant t)}$$

1.2.2.3.1. L'indisponibilité correspondante est définie par :

$$\bar{A} = \mathrm{(t)} = \text{prob (S défaillant à l'instant } \mathbf{t})$$

$$U_s(\mathrm{t}) = Q_s(\mathrm{t}) = 1 - A_s(\mathrm{t}) = \overline{A_s} \qquad (\mathbf{1.1})$$

1.2.2.3.2. La disponibilité moyenne sur un intervalle de temps est :

$$\boldsymbol{A_{moy}(\mathrm{t1},\mathrm{t2}) = \frac{1}{t1-t2}\int_{t2}^{t1} A\,(t)dt} \qquad \mathbf{(1.2)}$$

1.2.2.3.3. La disponibilité asymptotique (stationnaire) :

$$A(\infty) = \lim_{t\to\infty} A(t) = \frac{MUT}{MUT+MDT} = \frac{MUT}{MTBF} \qquad \mathbf{(1.3)}$$

1.2.2.3.4. La disponibilité moyenne asymptotique :

$$A_{moy} = \lim_{t \to \infty} A_{moy}(0, t) \qquad \textbf{(1.4)}$$

Pour les systèmes possédant un régime stationnaire : **Amoy (∞) = A(∞)**

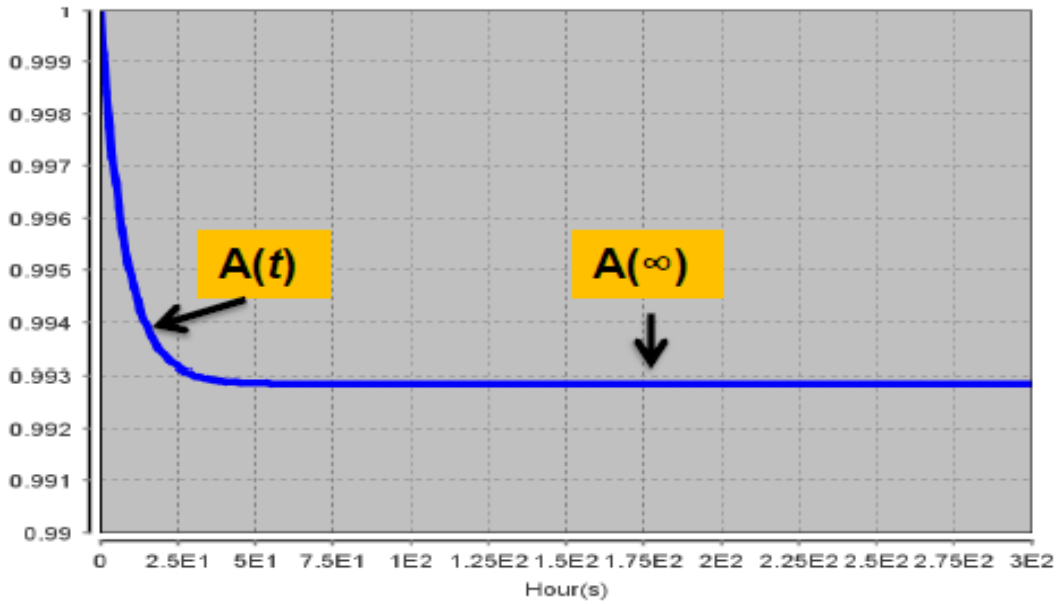


Figure 1.2 : la disponibilité [9]

La disponibilité s'exprime par le rapport **:** $\frac{\textbf{MUT}}{\textbf{MUT+MDT}}$

Comme la fiabilité, plusieurs types de disponibilités peuvent être utilisés :

1.2.2.3.5. Disponibilité opérationnelle : Do

Elle caractérise le fonctionnement effectif de l'équipement. Tout type de temps d'arrêt inclus dans le temps requis est à prendre en compte pour son calcul.

1.2.2.3.6. Disponibilité intrinsèque : D_I

Elle caractérise les qualités intrinsèques de l'équipement. La carence des moyens extérieurs et des moyens de maintenance n'est pas pris en compte pour son calcul.

1.2.2.3.7. Disponibilité point de vue maintenance : D_M

Tout type de temps d'arrêt inclus dans le temps requis est à prendre en compte pour son calcul. Sauf les temps d'arrêt relatifs à la carence des moyens extérieurs.

1.2.2.4. La maintenabilité

La maintenabilité est la capacité d'un système à être simplement et rapidement réparé et ainsi diminuer les temps d'intervention. La maintenabilité d'un système est souvent caractérisée lors de sa conception, elle se calcule suivant les temps moyens d'intervention [10].

1.3. Les entraves à la sûreté de fonctionnement

Parmi les entraves au bon fonctionnement d'un système on en distingue essentiellement quatre, cité comme suit (Figure I.3) :

1.3.1. La faute

Il s'agit d'un événement anormal susceptible de nuire au comportement global du système [10]. On en distingue plusieurs catégories classées selon leur :

- ***Nature* :** accidentelle ou intentionnelle
- ***Origine* :** physique /humaine, interne/externe, opérationnelle/conceptuelle.
- ***Persistance* :** transitoire, intermittente ou bien permanente.

1.3.2. L'Erreur

C'est un état transitoire du système dû à la manifestation d'une faute, il peut mener à une défaillance comme il peut initier un rétablissement si le système inclut des méthodes de recouvrement[10].

1.3.3. Le Défaut

Le défaut est le non satisfaction aux exigences de l'utilisation prévue[10].

1.3.4. La Défaillance/panne

Elle survient lorsque le comportement du système dévie de sa mission, autrement dit, le service rendu différé de celui attendu. Cette divergence par rapport à la spécification peut se révéler au niveau du temps de réponse comme au niveau des valeurs de sorties. Les défaillances sont nombreuses, elles sont classifiées hiérarchiquement selon leur ordre de gravite en :

- **panne franche (fail-stop) :** une défaillance permanente qui engendre l'arrêt total du fonctionnement du système.
- **panne d'omission :** absence de réponse pendant un cycle d'activité du système, à caractère souvent temporaire.
- **panne byzantine :** le système se comporte aléatoirement, c'est d'ailleurs le type de défaillance le plus compliqué à traiter.

Ces entraves s'imbriquent : une défaillance d'un composant représente une faute au niveau du système globale et ainsi de suite selon le schéma ci-dessous :

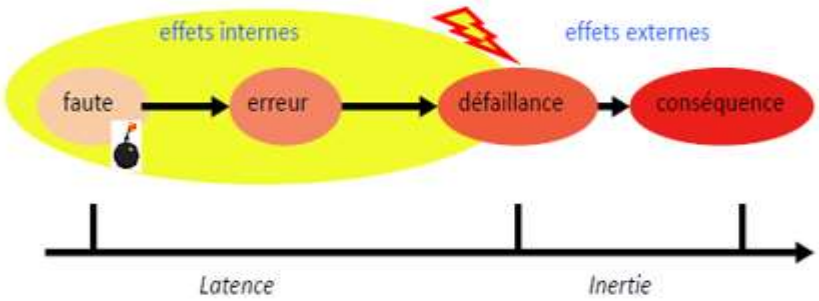


Figure 1.3 : Cycle d'apparition d'une défaillance [10]

1.4. Les moyens de la sûreté de fonctionnement

Les moyens sont des solutions éprouvées pour casser les enchaînements faute-défaillance et donc améliorer la fiabilité du système par :

- L'évitement des fautes
- Suppression des fautes
- Tolérance aux fautes
- Prévision des fautes

1.4.1. Le but de la sûreté de fonctionnement

La sûreté de fonctionnement est une notion générique qui mesure la qualité de service délivré par un système de manière à ce que l'utilisateur ait en lui une confiance justifiée. Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système, mesurée par les grandeurs probabilistes associées : fiabilité, maintenabilité, disponibilité, et sécurité [1].

1.4.2. Indicateurs de sûreté de fonctionnement :

Certains indicateurs vont caractériser le fonctionnement prévu du système, tels que le MTTF, le MDT et le MUT [1].

Le MTTF($Mean\ Time\ To\ Failure$) est l'estimation de la durée moyenne s'écoulant entre la mise en service du système et la survenance de la première panne.

Le MDT ($Mean\ down\ time$) est le temps moyen séparant la survenance d'une panne et la remise en état opérationnel du système. Il se décompose en plusieurs phases :

- Durée de détection de la panne (1) ;
- Durée de diagnostic de la panne (2) ;
- Durée d'intervention jusqu'au début de la réparation (3) ;
- Durée de la réparation (4) ;

- Durée de remise en service du système (5).

Le MUT(Mean up time) est le temps moyen qui sépare une remise en service opérationnelle du système de la survenance de la panne suivante. Ces deux derniers indicateurs ne sont pertinents que dans le cas de systèmes réparables. Leur somme **MUT+MDT** représente le temps moyen qui sépare deux pannes consécutives du système. On le note **MTBF** (Mean time between failure). L'ensemble de ces indicateurs peut être représenté sur le schéma suivant (Figure I.4)

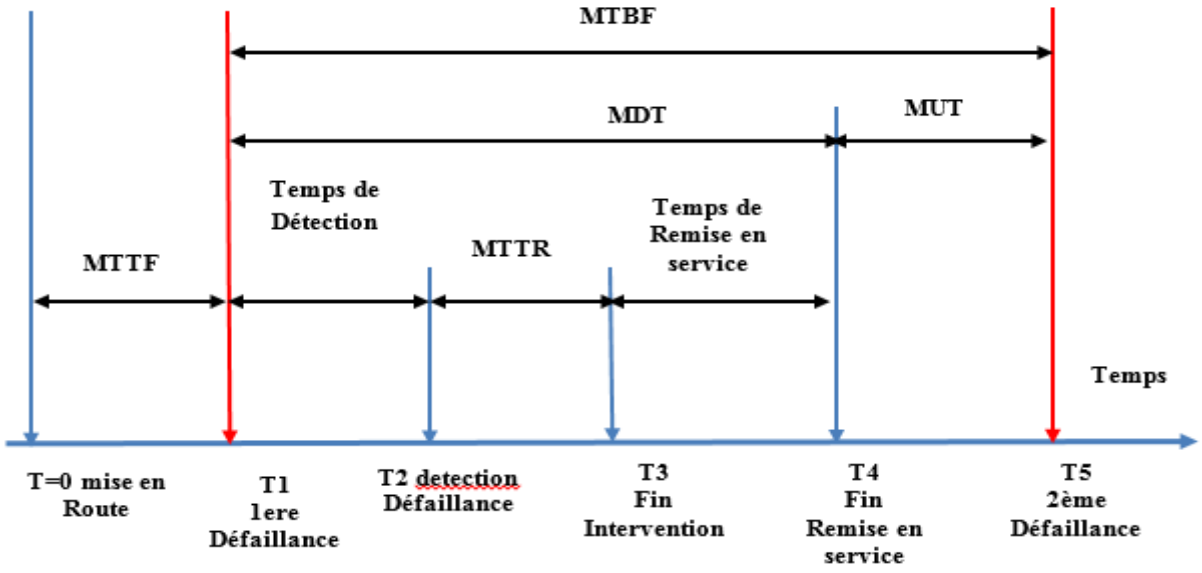


Figure 1.4 : Les indicateurs de fiabilité [1]

1.5 Surveillance et Diagnostic des pannes

Dans un grand nombre d'applications industrielles, une demande croissante est apparue en matière de sûreté fonctionnelle, basée sur la surveillance en continu de l'évolution de la structure du procédé considéré, et qui nécessite des moyens technologiques ainsi que la connaissance de techniques d'analyse appropriées.

La surveillance est un dispositif passif, informationnel, qui analyse l'état du système et fournit des indicateurs. La surveillance consiste notamment à détecter et classer les défaillances en observant l'évolution du système, puis à les diagnostiquer en localisant les éléments défaillants et en identifiant les causes premières.

Le rôle de la surveillance des procédés industriels est de détecter en temps réel les défauts et d'éviter leur propagation, cela consiste à générer des alarmes à partir des informations délivrées par des capteurs. Elle traite les données disponibles en ligne, afin d'obtenir son état de fonctionnement. Elle recueille les signaux en provenance du procédé et de la commande et reconstitue l'état réel du

système commandé. Des seuils sont définis sur des variables clés par des experts du procédé selon des critères de sécurité concernant les hommes, l'installation et son environnement. Elle a un rôle passif vis-à-vis du système de commande et du procédé. Cependant, la complexité et la taille de l'installation augmentent rapidement la quantité d'informations à analyser, rendant la surveillance plus complexe. Il est donc très utile d'adjoindre à la surveillance, une aide à la décision à travers un module de diagnostic.

1.5.1. La détection

La détection des situations anormales est une étape délicate dans la surveillance d'un système de production, elle permet de détecter tout écart du comportement normal du système et alerte les opérateurs humains de la présence d'un défaut. La localisation permet de remonter à l'origine de l'anomalie et de localiser le ou les composants défectueux. Cette localisation est importante puisque la propagation d'une panne provoque souvent l'apparition de nouveaux défauts. Enfin, l'identification détermine l'instant d'apparition de la panne, sa durée et son importance. Le diagnostic aide donc les opérateurs humains à surveiller un procédé complexe et par conséquent prendre une décision pour effectuer une reprise de la commande [11]

1.5.2. Le diagnostic

C'est l'analyse après détection de défaut qui détermine le type de panne et sa nature, donc on pourra décider de la gravite de défaillance. Le diagnostic est l'identification de la cause probable de la défaillance à l'aide d'un raisonnement logique fondé sur un ensemble d'informations provenant d'une inspection, d'un contrôle, ou d'un test. Cela résume deux tâches essentielles en diagnostic :

- Observation des symptômes de défaillances
- Identification des causes de défaillances à l'aide d'un raisonnement logique fondé sur des observations.

C'est un système d'aide à la décision, son objectif est de localiser les composants ou les organes défaillants d'un procédé et éventuellement de déterminer les causes. Le diagnostic établit donc un lien de cause à effet entre un symptôme observé et la défaillance qui est survenue, tout en considérant qu'un même symptôme peut apparaître pour différentes causes.

1.5.3. La supervision

L'objectif de la supervision est de surveiller et de contrôler l'exécution d'une opération et le fonctionnement d'une installation. Elle a donc un rôle décisionnel et opérationnel en vue de la reprise de la commande. La supervision élabore des solutions correctives en ayant la connaissance des causes, ou des organes ayant générés une défaillance. [11]

La reprise constitue la dernière étape de surveillance, elle consiste à élaborer une solution corrigeant le comportement du système, elle permet de réaliser de deux fonctions.

- La fonction de décision : à l'aide des informations fournies par le diagnostic sur l'état du procédé, décide de l'ensemble des actions à enclencher pour retrouver une situation jugée nominale.
- La fonction de recouvrement : qui applique les modifications comportementales, elle permet de récupérer la défaillance apparue au niveau du système par un modèle approprié ou par un opérateur.

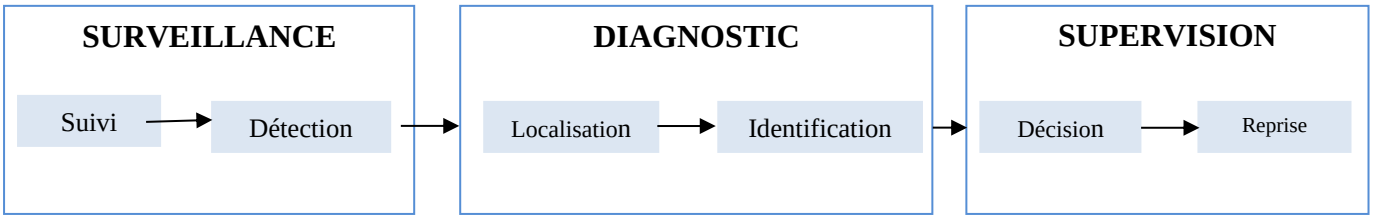


Figure 1.5 :* Surveillance, *diagnostic et supervision [11]

1.6. Méthodes d'analyse de la sûreté de fonctionnement

Il existe plusieurs méthodes, ces méthodes se déclinent en trois principaux types :

- Méthodes qualitatives : celles dans lesquelles les risques sont exprimés par des mots.
- Méthodes quantitatives : celles dans lesquelles les risques sont exprimés par des chiffres.
- Méthodes semi-quantitatives : dans lesquelles en trouve des mots et des chiffres.

L'évaluation de la sûreté de fonctionnement d'un système consiste à analyser les défaillances des composants pour estimer leurs conséquences sur le service rendu par le système. Les

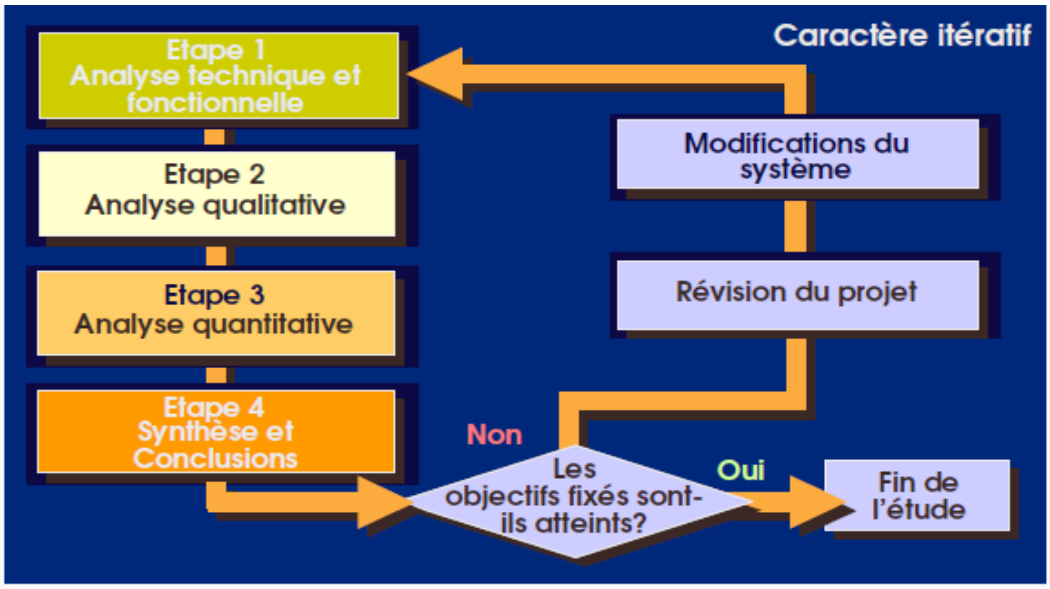


Figure 1.6 : Cycle d'analyse de la SdF traditionnel [7].

Les principes des méthodes utilisées lors d'une analyse de la sûreté de fonctionnement dans cette thèse sont décrits ci-dessous.

1.6.1. Blocs diagrammes de Fiabilité (BdF)

La méthode des blocs diagrammes de fiabilité est une des premières méthodes à avoir été utilisée pour analyser les systèmes et permettre des calculs de fiabilité. Elle est aussi appelée la Méthode du Diagramme de Succès (MDS). C'est une représentation de la logique de fonctionnement des systèmes car elle est souvent proche de leur schéma fonctionnel. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existant entre ces blocs. En outre, dans cette modélisation, les systèmes doivent vérifier les deux hypothèses suivantes :

- Hypothèse d'états binaires.
- Indépendance des états de fonctionnement ou de défaillance des composants.

Les BdF sont ainsi utilisés dans de nombreux domaines industriels pour les systèmes non réparables, mais ils peuvent également, sous certaines conditions, être utilisés pour les calculs de fiabilité de systèmes réparables.

1.6.1.1. Diagramme série

La panne de l'un des éléments $\boldsymbol{E_i}$du système entraîne la panne du système (figure I.7). Si nous désignons par$\boldsymbol{R_s}$ la fiabilité du système et $\boldsymbol{R_i}$ la fiabilité du composant $\boldsymbol{E_i}$, alors la fiabilitédu système est donnée par (1.5) :

$$R_s = \prod_{i=1}^{n} R_i \qquad (1.5)$$

Où **n :** est le nombre de composants du système.

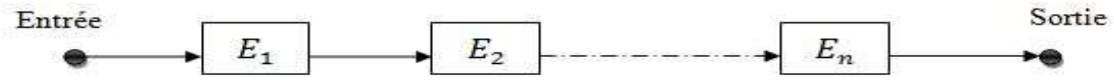


Figure 1.7* : *Bloc diagramme de fiabilité d'un système série [6]

1.6.1.2. Diagramme parallèle

La panne de tous les éléments $\boldsymbol{E_i}$ du système entraîne la panne du système (Figure I.5).Si un seul des éléments fonctionne alors il conduit au fonctionnement du système. Dans ce cas, la fiabilité du système est donnée par (1.6) :

$$R_s = \prod_{i=1}^{n}[1-(1-R_i)] \qquad (1.6)$$

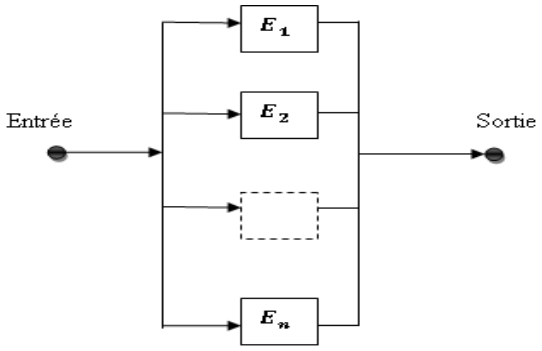


Figure 1.8 : Bloc diagramme de fiabilité d'un système parallèle [**1**]

1.6.1.3. Diagramme en redondance k/n

Les systèmes à n composants qui fonctionnent si et seulement si au moins k de leurs composants fonctionnent, sont appelés des systèmes k parmi n (k/n) (cf. figure I.6). On ne dispose pas d'une expression générale de la fiabilité d'un système k/n. Néanmoins, dans le cas où tous les composants du système ont la même fiabilité R, la fiabilité totale du système est donnée par (1.7) :

$$R_s = \sum_{i=k}^{n} c_i^n \, R^i (1-R)^{n-i} \qquad (1.7)$$

1.6.1.4. Diagramme complexe

Les diagrammes complexes sont des diagrammes qui ne peuvent pas être réduits à des combinaisons séries et/ou parallèles. Pour traiter les diagrammes complexes (Figure I.7), nous pouvons utiliser :

- Les liens minimaux et les coupes minimales.
- La fonction de structure.
- Le théorème des probabilités totales.
- La table de vérité.

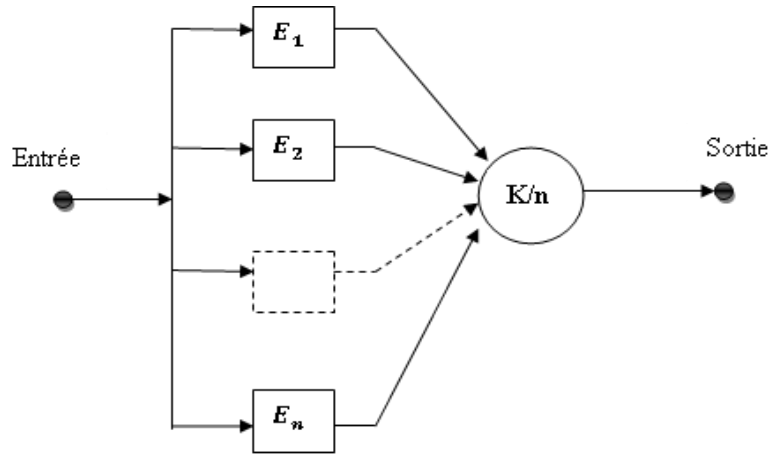


Figure 1.9 : Bloc diagramme de fiabilité d'un système k/n [**1**].

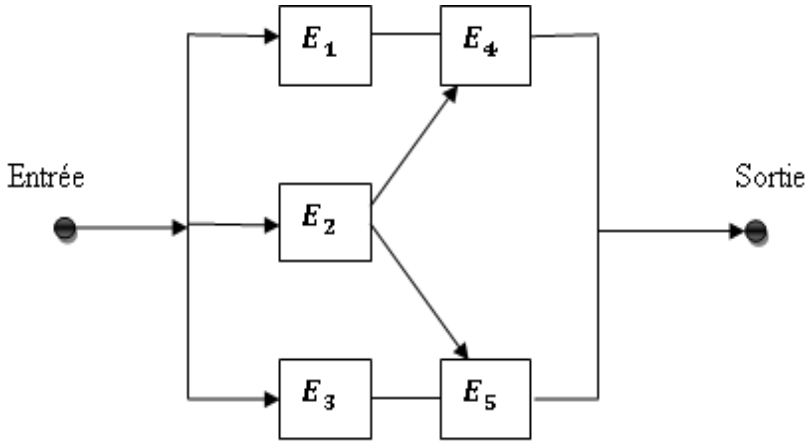


Figure 1.10 : Bloc diagramme de fiabilité d'un système complexe [1].

1.6.2 Méthode l'arbre des défaillances (AdD)

1.6.2.1 Historique

La méthode des arbres de défaillance (aussi appelé Arbre des Causes, Arbre des Fautes ou encore Arbre des Défauts) a été introduite par Watson, en 1961, au sein de la société Bell Telecom, afin d'évaluer et d'améliorer le système de lancement de missile "Minuteman" au profit de l'US Air Force. Utilisée dans un premier temps uniquement comme outil de représentation des défaillances des systèmes, cette méthode n'a cessé d'évoluer, aussi bien d'un point de vue méthodologie de construction, que d'un point de vue traitement qualitatif et quantitatif du modèle ainsi obtenu [15][16].

1.6.2.2 Définition

L'ADD ou en anglais (Fault tree Analysis FTA) est l'une des techniques connues par leurs utilisations dans l'analyse de la sécurité et de la fiabilité des processus. Cette méthode déductive permet de combiner les composants par identification des causes relatives aux événements redoutés et des fonctions d'un système. La méthode consiste en une représentation graphique des multiples causes d'un événement redouté. [16]

1.6.2.3 Déroulement de l'AdD : L'analyse par Arbre de Défaillances se déroule généralement en 4 étapes :

1. Spécification du système et de ses frontières.
2. Spécification des événements redoutés préalablement identifiés par exemple par AMDE.
3. Construction des arbres de défaillances : On cible les événements redoutés un par un et on essaye d'identifier les successions et les combinaisons d'événements de base permettant de les atteindre**.**
4. Le niveau de détail ou de résolution de l'étude est aussi à définir. Par exemple, est-il nécessaire d'étendre l'analyse jusqu'aux composants, ou suffit-il de s'arrêter au niveau des sous-systèmes pour satisfaire aux objectifs de l'étude ?

1.6.2.4 Méthodologie arbre de défaillances

Démarche : L'arbre de défaillance est une méthode déductive, qui fournit une démarche systématique pour identifier les causes d'un évènement unique intitulé évènement redouté.
Le point de départ de la construction de l'arbre est l'évènement redouté lui-même (également appelé évènement du sommet). Il est essentiel qu'il soit unique et bien identifier (en utilisant l'APR par exemple). À partir de là, le principe est de définir des niveaux successifs d'évènements tels que chacun est une conséquence d'un ou plusieurs évènements du niveau inférieur.

Les étapes de démarche de l'AdD sont les suivantes :

1. Pour chaque évènement d'un niveau donné, le but est d'identifier l'ensemble des évènements immédiats nécessaires et suffisants à sa réalisation. Des opérateurs logiques (portes) permettent de définir précisément les liens entre les évènements des différents niveaux.
2. Le processus déductif est poursuivi niveau par niveau jusqu'à ce que les spécialistes concernés ne jugent pas nécessaire de décomposer des évènements en combinaison d'évènements de niveaux inférieurs, notamment parce qu'ils disposent d'une valeur de probabilité d'occurrence

de l'évènement analysé. Ces évènements non décomposés de l'arbre sont appelés évènements élémentaires (ou évènements de bases).

Notons que :

1. Il est nécessaire que les évènements soient indépendants entre eux.
2. Leur probabilité d'occurrence doit pouvoir être quantifiée (condition nécessaire seulement dans le cas où l'arbre est destiné à une analyse quantitative).
3. L'approche déductive de l'arbre de défaillance permet de focaliser exclusivement sur les défaillances contribuant à l'évènement redouté.

1.6.2.5 Construction de l'arbre

1. La ligne la plus haute ne comporte que l'évènement dont on cherche à décrire comment il peut se produire (événement sommet ou événement redouté).
2. Chaque ligne détaille la ligne supérieure en présentant les combinaisons susceptibles de produire l'évènement de la ligne supérieure auquel elles sont rattachées.
3. Les relations sont représentées par des liens logiques, dont la plupart sont des « portes OU » et des « portes ET ».

A partir de l'évènement sommet, on construit en utilisant le symbolisme de logique booléenne, une arborescence (schéma graphique en forme d'arbre inversé) représentant l'enchaînement logique des évènements intermédiaires jusqu'à la mise en cause des évènements élémentaires (défaillance d'un composant). Il est ainsi possible d'identifier toutes les défaillances élémentaires pouvant conduire à l'évènement redouté. Les liens entre les différents évènements sont réalisés grâce à des opérateurs logiques, (et, ou, k-sur-n …). Cette méthode utilise une représentation graphique qui permet de présenter les résultats dans une structure arborescente développée généralement et surtout pour les structures compliquées par un algorithme du diagramme de décision binaire. [7]

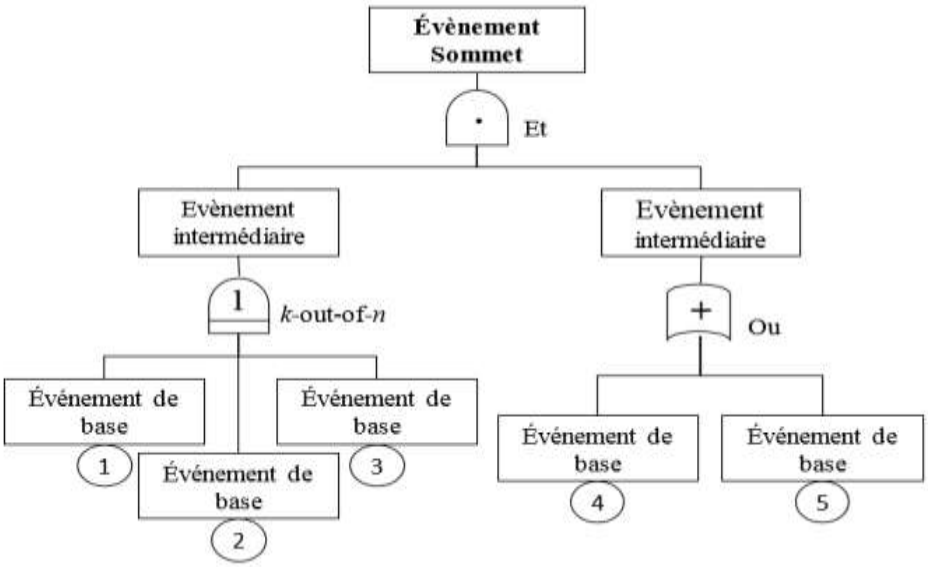


Figure 1.11 : Structure d'un AdD [7]

La construction de l'arbre de défaillance est une phase importante de la méthode car sa complétude conditionne celle de l'analyse qualitative ou quantitative qui sera réalisée par la suite.

1.6.2.6 Analyse qualitative

L'arbre de défaillance étant construit, deux types d'exploitation qualitative peuvent être réalisés :

1. L'identification des scénarios critiques susceptibles de conduire à l'évènement redouté. Par l'analyse des différentes combinaisons de défaillances menant à l'évènement sommet, l'objectif est ici d'identifier les combinaisons les plus courtes appelées coupes minimales (ensemble d'événements de base et de conditions suffisant pour produire l'événement-sommet).
2. La mise en œuvre d'une procédure d'allocation de barrières. Ce deuxième type d'exploitation qualitatif permet d'allouer un certain nombre de barrières de sécurité (technique ou d'utilisation) en fonction de la gravité de l'évènement redouté et des contraintes normatives éventuelles [15].

1.6.2.7 Analyse quantitative

Une étude probabiliste peut avoir deux objectifs :

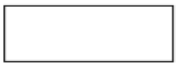
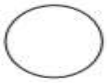
1. L'évaluation rigoureuse de la probabilité d'occurrence de l'évènement redouté.
2. Le tri de scénarios critiques (en partant des coupes minimales de plus fortes probabilités).

Ces calculs ne peuvent se concevoir que si chaque évènement élémentaire peut être probabilisé à partir d'une loi soigneusement paramétrée et de la connaissance du temps de mission associé à l'évènement redouté et / ou à l'aide de données issues du retour d'expérience. [7]

1.6.2.8 Représentation graphique

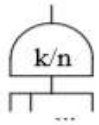
Différents symboles graphiques sont utilisés pour la représentation des événements de l'arbre

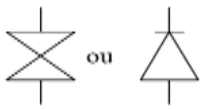
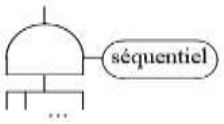
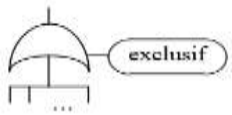
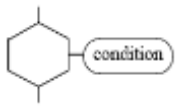
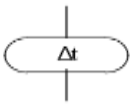
Tableau 1. 1 : Représentation des événements [7].

Symbole graphique	Signification du symbole
	Evénement intermédiaire Les causes de cet événement sont développées.
	Evénement de base élémentaire. Ne nécessite pas de futur développement. Exemple : Défaillance première d'un composant
	Evénement de base non élémentaire Ne peut être considéré comme élémentaire, mais ses causes ne sont pas et ne seront pas développées.
	Evénement à développer Ne peut être considéré comme élémentaire. Ses causes ne sont pas développées, mais le seront ultérieurement.
	Evénement "Maison". Survenant normalement pendant le fonctionnement du système.
	Evénement "Condition". Utilisé avec certaines portes afin de préciser la condition à satisfaire pour que l'opération logique réalisée par chacune de ces portes s'effectue.

Pour représenter la relation de causalité entre les événements de base jusqu'à l'événement sommet on utilise déférent types des portes logiques. Les portes les plus représentatives sont décrites au Tableau 1.2. [13]

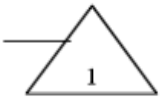
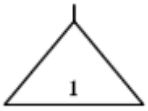
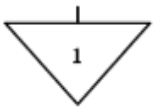
Tableau 1. 2 : Représentation des portes [7].

Symbole graphique	Signification du symbole
	Porte "Et" L'événement de sortie est réalisé si tous les événements d'entrée sont réalisés.
	Porte "Ou" L'événement de sortie est réalisé si au moins un des événements d'entrée est réalisé.
	Porte "K-sur-N" (ou porte combinaison) L'événement de sortie est réalisé si au moins K des N événements d'entrée sont réalisés.

	Porte "Non" L'événement de sortie est réalisé si l'événement d'entrée ne l'est pas.
	Porte "Et avec condition" L'événement de sortie est réalisé si tous les événements d'entrée sont réalisés et si la condition est réalisée. Ici, il faut aussi que les événements d'entrée apparaissent séquentiellement.
	Porte "Ou avec condition" L'événement de sortie est réalisé si au moins un des événements d'entrée est réalisé et si la condition est réalisée. Ici, l'événement de sortie est réalisé si un et un seul des événements d'entrée est réalisé.
	Porte "Si" L'événement de sortie est réalisé si l'événement d'entrée est réalisé et si la condition est réalisée.
	Porte "Délai" L'événement de sortie est réalisé si l'événement d'entrée est réalisé depuis et pendant Δt.

Pour finir, il existe des symboles appelés renvois de sous-arbres (aussi appelé transferts de sous-arbres) qui sont utilisés pour éviter de répéter les sous-arbres identiques ou semblables.

Tableau 1. 3 : Représentation des transferts ou renvois [7]

Symbole graphique	Signification du symbole
	Identificateur de renvoi : Le sous-arbre commençant par l'événement d'entrée de l'identificateur est transféré aux emplacements signalés par le ou les renvois associés à l'identificateur. Plusieurs renvois peuvent être en liaison avec le même identificateur.
	Renvoi identique : La partie de l'arbre qui devrait suivre est identique à celle définie après l'identificateur de renvoi associé.
	Renvoi semblable : La partie de l'arbre qui devrait suivre est semblable à celle définie après l'identificateur de renvoi associé.

1.6.3. Analyse de Markov

La méthode de graphes de Markov est utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation.

A chaque transition, de l'état $\boldsymbol{E_i}$ vers l'état $\boldsymbol{E_j}$, est associé un taux de transition $\boldsymbol{T_{ij}}$ défini de telle sorte que ($\boldsymbol{T_{ij}}.\boldsymbol{dt}$) est égal à la probabilité de passer de $\boldsymbol{E_i}$ vers $\boldsymbol{E_j}$, entre deux instants très proches t et $\boldsymbol{t+dt}$ sachant que l'on est en $\boldsymbol{E_i}$ à l'instant de temps **t**.

Les états sont classés en deux catégories :

- Des états de fonctionnement : ce sont les états où la fonction du système est réalisée, des composants du système pouvant être en panne, l'état du bon fonctionnement est l'état où aucun composant n'est en panne,
- Des états de panne : ce sont des états où la fonction du système n'est plus réalisée, un ou plusieurs composants du système étant en panne.

Le processus d'analyse comprend trois parties :

- Le recensement et le classement de tous les états du système en états de bon fonctionnement ou états de panne.
- Le recensement de toutes les transitions possibles entre ces différents états et l'identification de toutes les causes de ces transitions.
- Le calcul des probabilités de se trouver dans les différents états au cours d'une période de vie de système ou le calcul des caractéristiques de sûreté de fonctionnement.

La modélisation avec les graphes de Markov permet de prendre en compte les dépendances temporelles et stochastiques plus largement que les méthodes classiques. En dépit de leur simplicité conceptuelle et leur aptitude à pallier certains handicaps des méthodes classiques.

Les graphes de Markov souffrent de l'explosion du nombre des états, car le processus de modélisation implique l'énumération de tous les états possibles et de toutes les transitions entre ces états [1].

1.7. Classification des défaillances

La classification des défaillances et les interventions appropriées sont présentées ci- dessous.

1.7.1. Défaillance :

Altération ou cessation de l'aptitude d'un bien à accomplir la fonction requise.

1.7.2. Défaillance complète :

Cessation de l'aptitude d'un bien à accomplir la fonction requise.

1.7.3. Défaillance partielle :

Altération d'un bien à accomplir la fonction requise.

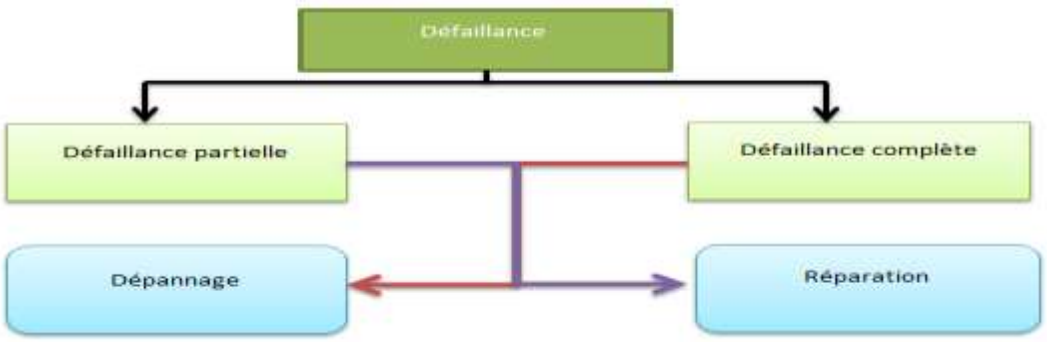


Figure 1.12 : Classification des défaillances [10]

1.8. Généralités sur la maintenance :

La maintenance industrielle est l'ensemble de toutes les actions techniques, administratives et de management durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise. La maintenance a pour but de garantir la disponibilité des équipements de production, d'obtenir le rendement maximum, de satisfaire les exigences du client, la protection de l'environnement et la sécurité des hommes et des biens et l'optimisation des coûts.

1.8.1. Définition de la maintenance

La maintenance est l'ensemble des moyens nécessaires pour maintenir et remettre les facteurs d'opérations en bon état de fonctionnement. Elle comprend l'ensemble des moyens d'entretien et leur mise en œuvre. La différence entre la maintenance et l'entretien est que ce dernier consiste à maintenir les facteurs d'opérations en état de fonctionnement.

1.8.2. Définition de l'Association Française de Normalisation (AFNOR)

La maintenance est l'ensemble des actions permettant de maintenir ou de rétablir un bien en mesure d'assurer un service bien déterminé.
La maintenance consiste à effectuer les opérations suivantes : dépannage ; entretien ; visite ; réparation ; amélioration.

1.8.3. Objectifs de la maintenance

- l'optimisation de la fiabilité de l'équipement
- l'augmentation de la productivité.
- l'amélioration de la sécurité de travail.
- ramener rapidement l'équipement à son état fonctionnel.

1.8.4. Méthodes de la maintenance

Dans le cadre de la politique de la maintenance s'effectue le choix entre les méthodes de maintenance. Le choix de la méthode est basé sur la connaissance du fonctionnement et les caractéristique du matériel, son comportement et sa manière d'exploitation ; les conditions d'application de chaque méthode ; les coûts de la maintenance et les coûts de pertes de production.

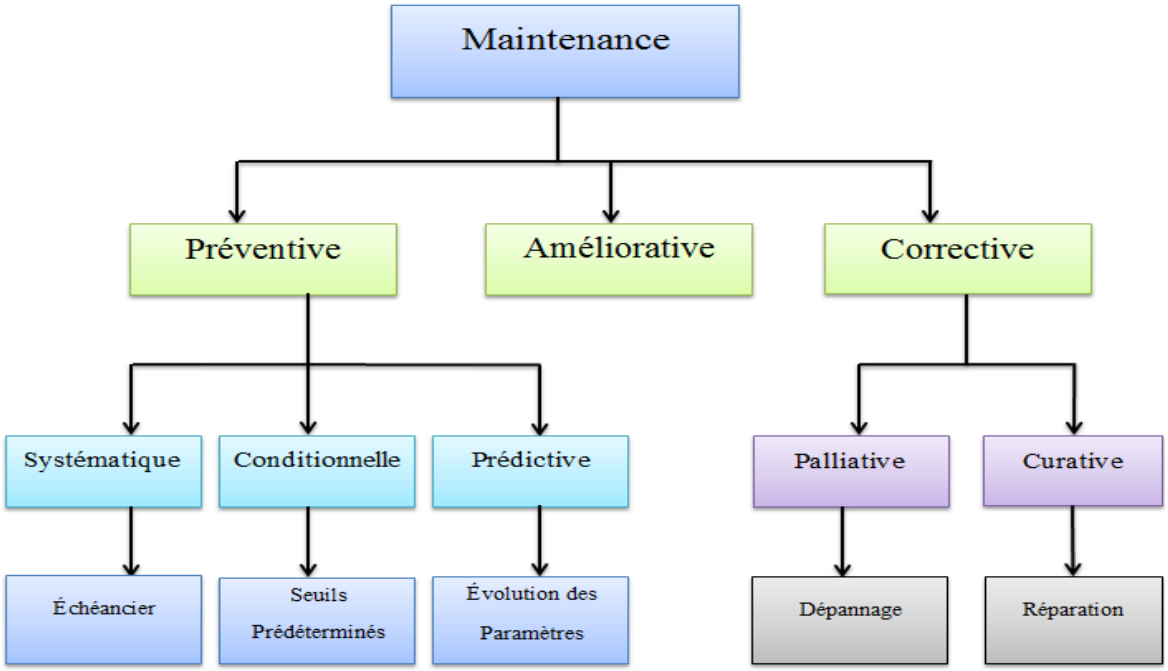


Figure 1.13 : Arbre de maintenance [18]

1.8.4.1. Maintenance préventive

Cette forme de maintenance est appliquée pour permettre d'éviter des défaillances en cours d'utilisation. Elle s'adresse aux éléments provoquant une perte de production ou coûts d'arrêts imprévisibles classés comme important pour l'entreprise.

1.8.4.1.1. Principaux objectifs de la maintenance préventive

- Augmenter la durée de vie des matériels.
- Diminuer la probabilité de défaillance en service.
- Prévenir et prévoir aussi des interventions de maintenance corrective coûteuse.
- Diminuer les temps d'arrêt forcé en cas de panne.
- Permettre l'établissement d'une maintenance corrective dans les bonnes conditions
- Eviter les consommations anormales d'énergie, de lubrifiant.
- Supprimer les causes d'accident grave

1.8.4.1.2. Maintenance préventive systématique

C'est une maintenance préventive effectuée selon un échéancier établi selon le temps ou le nombre d'unités d'usage.

Cette périodicité d'intervention est déterminée à partir de la mise en service ou après une révision partielle ou complète.

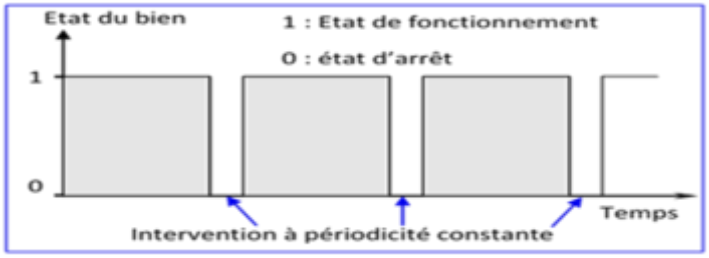


Figure 1.14 : Maintenance préventive systématique [19]

Cette méthode nécessite de connaître :

- Le comportement de matériel en exploitation.
- Les usures.
- Les modes de dégradation.
- Le temps moyen de bon fonctionnement entre deux avaries.

1.8.4.1.2.1. Pratique de la maintenance préventive systématique

Le but est de maintenir le système dans l'état de ses performances initiales. Il est procédé lors de ces interventions à différentes opérations qui peuvent être :

- Le remplacement des relais, capteurs, joints d'étanchéité, roulements, ressorts, filtres d'huile, interrupteur, sonde ….etc.
- Le réglage des pressions, des jeux, des tensions.
- Le contrôle des organes de blocage (Butée, clavettes, niveaux d'huile…etc.).

1.8.4.1.3. Maintenance préventive conditionnelle

C'est une maintenance préventive subordonnée à un type d'événement prédéterminé

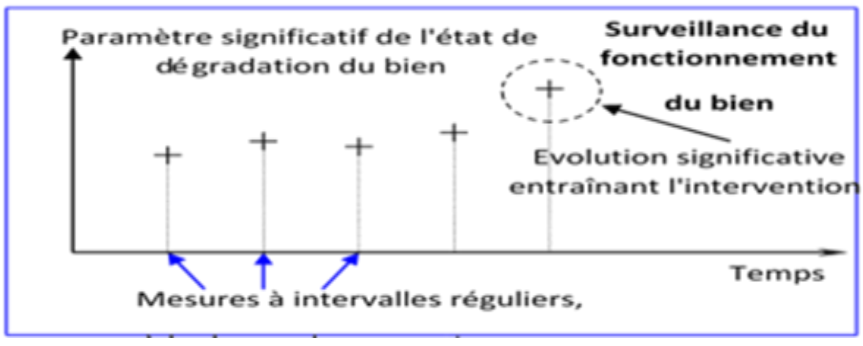


Figure 1.15 : Maintenance préventive conditionnelle [7]

Elle consiste à ne changer l'élément que lorsqu'il présente des signes de vieillissement ou d'usure mettant en danger ses performances. On s'appuie sur des mesures physiques qui sont :

a- la mesure des températures

La mesure des températures est facile. Le coût des capteurs n'est pas très élevé, les indications qu'ils peuvent donner sur le fonctionnement des machines sont précieuses. En effet, une variation de température sur une machine tournante est souvent signe de dégradation.

b- Analyse des huiles

Elle consiste à examiner les particules en suspension dans l'huile. La quantité de ces particules nous renseigne sur l'état de dégradation des machines, Le type des particules nous indique, la provenance de l'usure et par conséquence la pièce ou l'élément défaillant.

c- la mesure des vibrations et des bruits

Toutes les machines vibrent et le spectre de fréquence de leurs vibrations a un profil particulier. Le profil de ce spectre se modifie au fil du temps ce qui est signe d'une usure, alors le suivi de ce profil permet de nous renseigner sur l'état du matériel.

Les paramètres qui peuvent être mesurés sont :

- L'amplitude des vibrations
- La vitesse.
- L'accélération.

Notons que toutes les méthodes de contrôle non destructif conviennent pour faire un diagnostic.

1.8.4.2. La maintenance corrective :

- **Définition :** La maintenance corrective est une maintenance effectuée après défaillance.

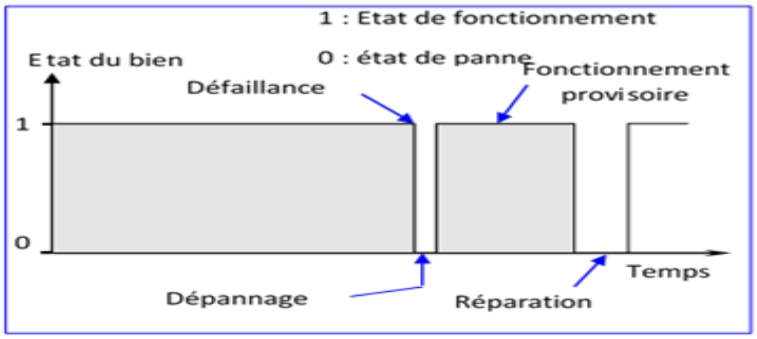


Figure 1.16 : Maintenance corrective [7]

Elle permet de redonner au matériel des qualités perdues nécessaires à son utilisation, et pour cela on fait l'analyse des modes de défaillance pour mieux appréhender les risques de défaillances, et ainsi de les éviter, en mettant en place :

- Des éléments de secours.
- Des technologies plus performantes.
- Une maintenance préventive plus efficace.

- Des diagnostics des pannes plus rapides.

Cette maintenance peut se traduire par deux types d'intervention.

- **Le premier type est provisoire**, avec des interventions palliatives (simples dépannages).
- **Le second type a un caractère définitif**, avec des interventions curatives (réparations ayant pour but de supprimer durablement les défaillances).

1.8.4.2.1. Maintenance curative

Ce type de maintenance permet de remettre définitivement en état le système aprèsl'apparition d'une défaillance (Figure I.14). Cette remise en état du système est une réparationdurable. Les équipements réparés doivent assurer les fonctions pour lesquelles ils ont étéconçus. Une réparation est une opération définitive de la maintenance curative qui peut êtredécidée soit immédiatement à la suite d'une défaillance, soit après un dépannage, ce type demaintenance, provoque donc une indisponibilité du système

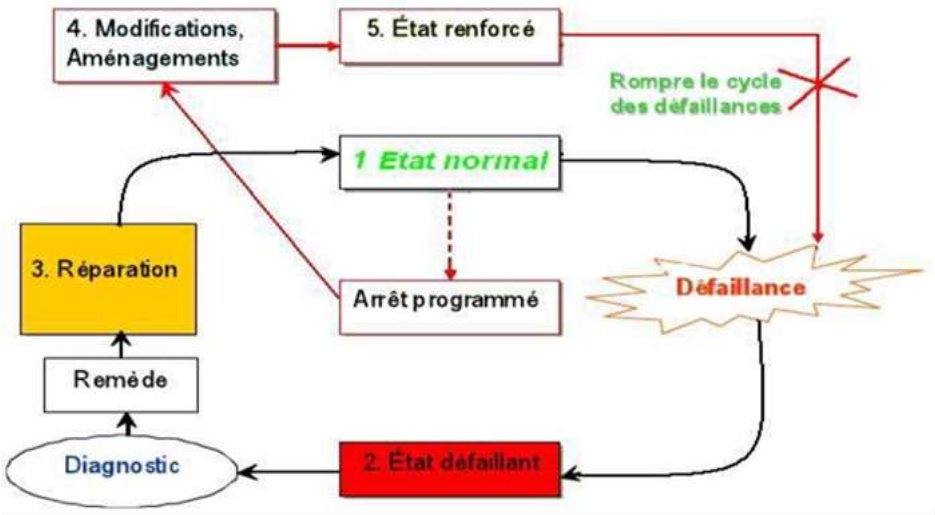


Figure 1.17 :Maintenance curative ou réparation [18].

1.8.4.2.2. Maintenance palliative

La maintenance palliative revêt un caractère temporaire, provisoire (Figure I.15). Elle estprincipalement constituée d'opérations qui devront toutefois être suivies d'opérationscuratives (réparations). Ledépannage est une opération de maintenance palliative qui estdestinée à remettre le système en état provisoire de fonctionnement de manière à ce qu'il puisse assurer une partie des fonctions requises. Les opérations de dépannage sont souvent decourte durée et peuvent être nombreuses . Son coût est très élevé, pour plusieurs raisons:

Le plus souvent, ces solutions sont un peu coûteuses. D'où l'intérêt de faire une étude derentabilité pour savoir s'il est préférable de subir les inconvénients des pannes plutôt que desubir les coûts qu'entraîneraient ces solutions.

Non respect des dates de livraisons, d'où le risque de perdre des clients qui vont chercherdes concurrents,

- Recours aux heures supplémentaires qui coûtent chers,
- Baisse de la qualité des produits,
- Absence de la sécurité dans les lieux de travail,

Pour remédier à ces pannes, on a recours :

- Aux équipements de secours ou en attente qui peuvent entrer directement en fonction à laplace de l'équipement défectueux,
- Besoin d'une équipe d'entretien hautement qualifiée et compétente.

Le plus souvent, ces solutions sont un peu coûteuses. [2]. D'où l'intérêt de faire une étude derentabilité pour savoir s'il est préférable de subir les inconvénients des pannes plutôt que desubir les coûts qu'entraîneraient ces solutions.

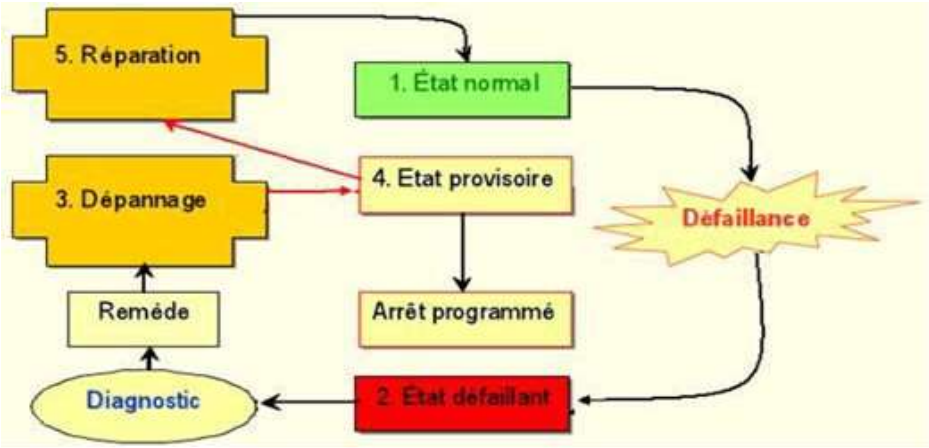


Figure 1.18 : Maintenance palliative [18].

1.8.4.3. La maintenance améliorative :

vise à augmenter la fiabilité, la maintenabilité, la disponibilité et la sécurité d'un équipement ou d'un sous-ensemble. Ce type de maintenance fait partie des interventions de grande maintenance, avec les travaux de rénovation et de remise à neuf.

Les évolutions provoquées par les TIC (Technologies d'Information et de Communication).Sont rencontrées aussi bien en maintenance préventive qu'en maintenance corrective. En préventif, les

TIC permettent, par exemple, de faire des relevés d'information à distance, notamment pour le prédictif. Les TIC aident aussi au démontage en rendant accessible la documentation de l'équipement à distance. En correctif, les TIC peuvent également aider à l'établissement de diagnostic.

1.9. Facteurs d'importance

Lors de l'analyse de fiabilité des systèmes, il est essentiel de pouvoir identifier les composants qui jouent un rôle plus important que d'autres en termes de fiabilité. En pratique, cette identification se fait au moyen des facteurs d'importance, qui cherchent à mesurer l'effet du fonctionnement ou de la défaillance d'un composant sur la défaillance ou le fonctionnement du système complet. Les facteurs d'importance d'un composant cherchent donc à mesurer l'amplitude de modification de la probabilité de fonctionnement ou de défaillance du système, conditionnellement à l'état du composant étudie.

1.9.1. Définitions et objectif

Les facteurs d'importance sont des indicateurs visent à évaluer les contributions relatives des différents composants du système au risque global. Il existe de nombreux facteurs d'importance dans la littérature.

Au niveau de la conception de système, il est important de pouvoir répondre à des questions telles que :

- Quel composant faut-il améliorer pour augmenter la fiabilité du système ?
- Quels sont les paramètres des composants qui ont le plus d'influence sur la fiabilité du système ?

Au niveau de l'exploitation, il s'avère intéressant de répondre à des questions telles que :

- Quelles sont les coupes minimales les plus importantes sachant que le système est en panne ?
- quel composant faut-il réparer en priorité ?

L'objectif du calcul des facteurs d'importance est de répondre à ces questions. Dans ce chapitre, nous étudions les Cinq principaux facteurs d'importance probabilistes utilisés et leurs différentes interprétations :

- Le facteur d'importance Marginale (Marginal Importance Factor (MIF)).
- Le facteur de diminution du risque (Risk Reduction Worth (RRW)).
- Le facteur d'augmentation du risque (Risk Acheivement Worth (RAW)).
- Facteur d'Importance Critique (Critical Importance Factor (CIF)).
- Facteur d'Importance de Diagnostic (Diagnostic Importance Factor (DIF)).

1.9.2. Différents facteurs d'importance :

1.9.2.1 Facteur d'importance de Birnbaum (MIF)

Le facteur d'importance marginal, noté MIF(S, e), est défini comme suit :

$$\boldsymbol{MIF(S,e) = \frac{dp_r(S)}{dp_r(e)}} \qquad (\mathbf{1.8})$$

Ce facteur d'importance peut être interprété comme la probabilité pour que le système se trouve dans un état de fonctionnement ayant e comme composant critique, sachant que e est en fonctionnement, soit :

$$\boldsymbol{MIF(S,e) = p_r(S/e) - \ p_r(\ S/\bar{e}\ )} \qquad (\mathbf{1.9})$$

À titre d'exemple, considérons la disponibilité d'un système. Le facteur d'importance marginal du composant e est le taux avec lequel la disponibilité du système augmente quand la disponibilité du composant e augmente [20][21]

1.9.2.2. Facteur d'importance de Lambert (CIF)

Ce facteur est la probabilité pour qu'un événement de base e soit défaillant et critique sachant que le système global est défaillant. Autrement dit, il s'agit de la probabilité que le composant e ait provoqué la défaillance du système sachant que le système est défaillant.

$$\boldsymbol{CIF(S,e) = \frac{p_r(e)}{p_r(S)}.MIF(S,e)} \qquad (\mathbf{1.10})$$

Ce facteur peut aussi être calculé pour une coupe minimale, il s'agit alors de la probabilité que la coupe minimale ait provoqué la défaillance du système sachant que le système est défaillant. Ce facteur indique ainsi le poids respectif de chaque coupe minimale dans leur contribution à la défaillance du système.

Ce facteur nous renseigne sur les augmentations / diminutions de risque associées à l'augmentation / diminution de la défiabilité d'un événement de base associé à un système. Dans la pratique, il trouvera son intérêt dans la maintenance optimisée par la fiabilité (RCM en anglais), où l'on intervient sur de l'existant et en faible proportion. Il indiquera sur quels composants il est intéressant de faire de la maintenance préventive, et ceux sur lesquels la maintenance corrective suffit. [22][23][24].

1.9.2.3 Facteur d'importance de Fussell Vesely (DIF)

Le facteur d'importance de diagnostic, notée DIF(S, e), est définie comme suit.

$$\boldsymbol{DIF(S,e) = p_r(e\ /\ S) = \frac{p_r(e)}{p_r(S)}.p_r(S\ /\ e)} \qquad (\mathbf{1.11})$$

Le DIF(S, e) est la probabilité pour que le composant e soit en panne sachant que le système est en panne. Ce facteur tient son nom de son utilité dans le diagnostic des causes de défaillance d'un système.

Enfin signalons que ce facteur représente la part des coupes dans lesquelles apparaît au moins une fois l'événement de base e, il indique alors le gain en disponibilité que l'on peut atteindre sur le système global, résultant d'une fiabilisation totale de e.

Cet indicateur est notamment précieux dans la phase de conception d'un système, là où des modifications fonctionnelles et/ou de design importantes peuvent intervenir, et faire varier le risque associé à un système dans d'importantes proportions [25].

1.9.2.4. Facteur d'augmentation du risque (RAW)

Le facteur d'augmentation du risque, désigné par RAW(S, e), est défini comme suit :

$$\boldsymbol{RAW(S,e) = \frac{p_r(s\ /\ e)}{p_r(S)}} \qquad (\mathbf{1.12})$$

Il montre dans quelles proportions augmente le risque associé à un système quand la défiabilité de l'événement de base e est portée à 1.

Ce facteur apporte son intérêt en permettant d'identifier les points communs, qui, en cas de défaillance rendent indisponible l'ensemble des barrières. Il permet ainsi d'extraire des événements de base à probabilité très faible mais dont la perte se traduit par une forte augmentation du risque. Il est un indicateur de l'importance de maintenir le niveau actuel de la fiabilité du composant [25] [26].

1.9.2.5 Facteur de diminution du risque (RRW)

Le facteur de diminution du risque, noté RRW(S, e), est défini comme suit :

$$\boldsymbol{RRW(S,e) = \frac{p_r(S)}{p_r(S\ /\ \bar{e})}} \qquad (\mathbf{1.13})$$

Il représente la diminution maximale du risque, il peut être approché en augmentant la fiabilité du composant. Par conséquent, ce facteur peut être utilisé pour sélectionner des composants qui sont les meilleurs candidats pour les efforts visant à améliorer la fiabilité du système [28]

- Ces facteurs d'importances peuvent donner des résultats différents pour les composants d'un même système. Cela est duaux égalisé qui les définissent.

- Pour identifier les composants qui peuvent améliorer significativement la fiabilité d'un système, le facteur d'importance de Birnbaum est le plus approprié.
- Pour identifier les composants qui ont causé la défaillance du système, nous pouvons utiliser soit le facteur d'importance critique, soit le facteur Vesely-Fussell. Nous pouvons ainsi établir une liste des composants qui doivent être réparés en priorité.
- Ces facteurs d'importance dépondent du temps : à différents instants nous pouvons avoir pour un même composant des facteurs d'importance différents.

1.11. Conclusion

La sûreté de fonctionnement est un terme générique rassemblant la fiabilité, la maintenabilité, la disponibilité et la sécurité des systèmes, est aujourd'hui un facteur décisif dans les choix de stratégie technologique, économique et sociétale d'un projet. La sûreté de fonctionnement (SdF) fait partie des enjeux majeurs, cette notion désigne à la fois un ensemble de moyens et de résultats produits par ces moyens : des méthodes et des outils pour caractériser et maîtriser les effets des aléas, des pannes et des erreurs. Au court de ce chapitre nous avons abordé les concepts de base de la surveillance et le diagnostic des pannes, qui ont pour objectif d'assurer la sécurité du système physique.

Au cours de ce premier chapitre nous avons détaillé deux méthodes d'analyse des risques, arbres de défaillances et blocs diagrammes de fiabilité. Celles-ci permettent une identification systématique des composantes du risque, les différentes situations dangereuses, évènements redoutés, les coupes minimales, causes, conséquences, ou accidents potentiels.

L'étude des facteurs d'importance constitue une partie essentielle des études de la sûreté de fonctionnement du système. Selon les problèmes rencontrés, nous pouvons utiliser différents facteurs d'importances. En présence de connaissance suffisent pour établir des valeurs de taux de défaillance précises, il est préférable d'utiliser les facteurs d'importance probabilistes. Ainsi, pour identifier les composants qui permettent d'augmenter la fiabilité des systèmes, le facteur de Birnbaum semble le plus adapté. Pour dresser la liste des composants qui ont causé la défaillance de système et qui doivent donc être réparés, nous nous devons utiliser le facteur d'importance de Lambert ou de Vesely-Fussel. L'emploi d'autres facteurs définis dans la littérature (Facteur RAW et RRW….etc.) peut s'avérer nécessaire selon l'objectif de l'étude réalisée.

Chapitre 2

Les Systèmes Instrumentés de sécurité (SIS)

2.1 Introduction

Les systèmes industriels sont susceptibles de générer des phénomènes dangereux (incendie, explosion, rejets de matière dangereuse…etc.), dont les conséquences sont de plus en plus dévastatrices les personnes, les biens et l'environnement. Diverses sécurités doivent être mises en œuvre. Le rôle de ces moyens est la contribution soit à la prévention, soit à la protection pour réduire les risques de dysfonctionnement.

Les Systèmes Instrumentés de Sécurité (Safety Instrumented System : SIS), constituent une barrière d'une importance capitale dans le processus de réduction de risque. Ces barrières garantissent un fonctionnement sûr des installations en surveillant d'une manière continue leurs paramètres opératoires (température, pression, débit, niveau, concentration…), et pour cela les SIS réalisent des Fonctions Instrumentées de Sécurité (Safety Instrumented Fonction : SIF) afin de mettre le processus dans un état de repli de sécurité s'il se trouve dans des conditions dangereuses de fonctionnement.

La norme CEI 61508 (Commission International d'Electrotechnique), [IEC61508, 2010] qui porte particulièrement sur les systèmes électriques/électronique/électronique programmable de sécurité (E/E/PE). Elle a été élaborée entant que cadre technique dans le but d'encadrer leur conception et exploitation. Cette norme a été adoptée par de nombreuses règlementations nationales, comme moyen recommandé pour obtenir un SIS de haute fiabilité. Un des intérêts de cette norme est d'être générique et donc d'être applicable dans tous les secteurs où la sécurité peut être traitée avec des systèmes E/E/PE : industries manufacturières, industries des process continus, nucléaires, ferroviaires…etc. Cette norme est très générale, c'est pour cela que ses concepteurs ont développé des normes sectorielles s'appliquant à des secteurs bien précis. Parmi ces principales normes la norme CEI61511, qui concerne les SIS, elle permet de définir des exigences relatives aux spécifications, à la conception, à l'installation à l'exploitation et l'entretien d'un SIS, de telle manière qu'il puisse être mis en œuvre en toute confiance et de maintenir les processus dans un état de sécurité convenable.

2.2 Systèmes instrumentés de sécurité

2.2.1 Définition d'un SIS

La norme CEI 61511 [IEC61511 03] définit les systèmes instrumentés de sécurité de la façon suivante : système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).

La norme CEI 61508[IEC61508 02] définit quant à elle les systèmes relatifs aux applications de sécurité par un système (E/E/PE) (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.

Les systèmes instrumentés de sécurité sont donc utilisés comme moyens de prévention et comportent une proportion grandissante de systèmes électriques, électroniques ou encore électroniques programmables (E/E/EP). Ces systèmes sont complexes ce qui rend difficile dans la pratique la connaissance de chaque mode de défaillance par l'examen des comportements

Un système instrumenté de sécurité est un système visant à mettre le procédé en état stable ne présentant pas de risque pour l'environnement et les personnes lorsque le procédé

s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu…). [2]

2.2.2 Constitution d'un SIS

Les SIS sont constitués de différents éléments unitaires reliés entre eux par des moyens de transmissions. Au minimum, on retrouve en série un capteur, une unité de traitement et un actionneur.

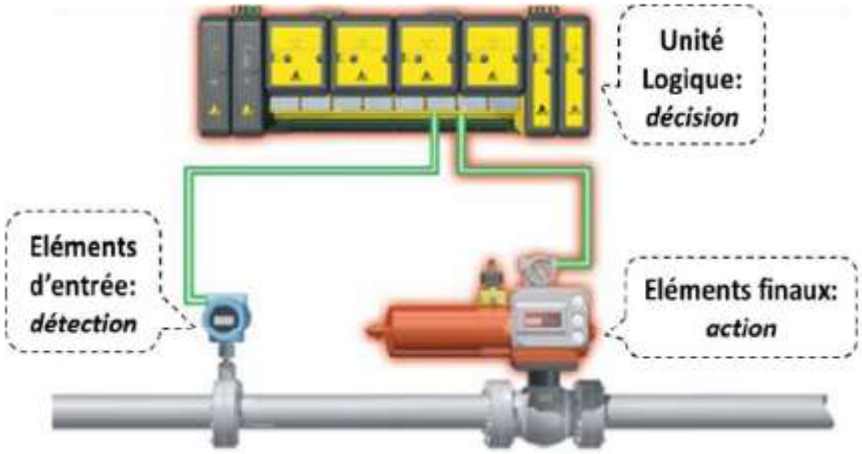


Figure 2.1 : Composition type d'un SIS [31].

1. Sous-système « *Eléments d'entrée (S)* » : constitué d'un ensemble d'éléments d'entrée (capteurs, transmetteurs, détecteurs) qui surveillent l'évolution des paramètres représentatifs du comportement de l'EUC (température, pression, débit, niveau…).

2. Sous-système « *Unité Logique (LS)* » : comprend un ensemble d'éléments logiques (APIds, eg: S7-400FH, Triconex, ABB800/A) qui récoltent l'information en provenance du sous-système S et réalisent le processus de prise de décision qui s'achève éventuellement, si l'un des paramètres dévié au-delà d'une valeur-seuil, par l'activation du sous-système FE.

3. Sous-système « *Eléments Finaux (FE)* » : agit directement (vanne d'arrêt d'urgence) ou indirectement (alarme) sur le procédé pour neutraliser sa dérivée en le mettant, en général, dans un état sûr. [4]

2.2.3 Propriétés d'un SIS

Un certain nombre de propriétés caractérisent les systèmes instrumentés de sécurité :

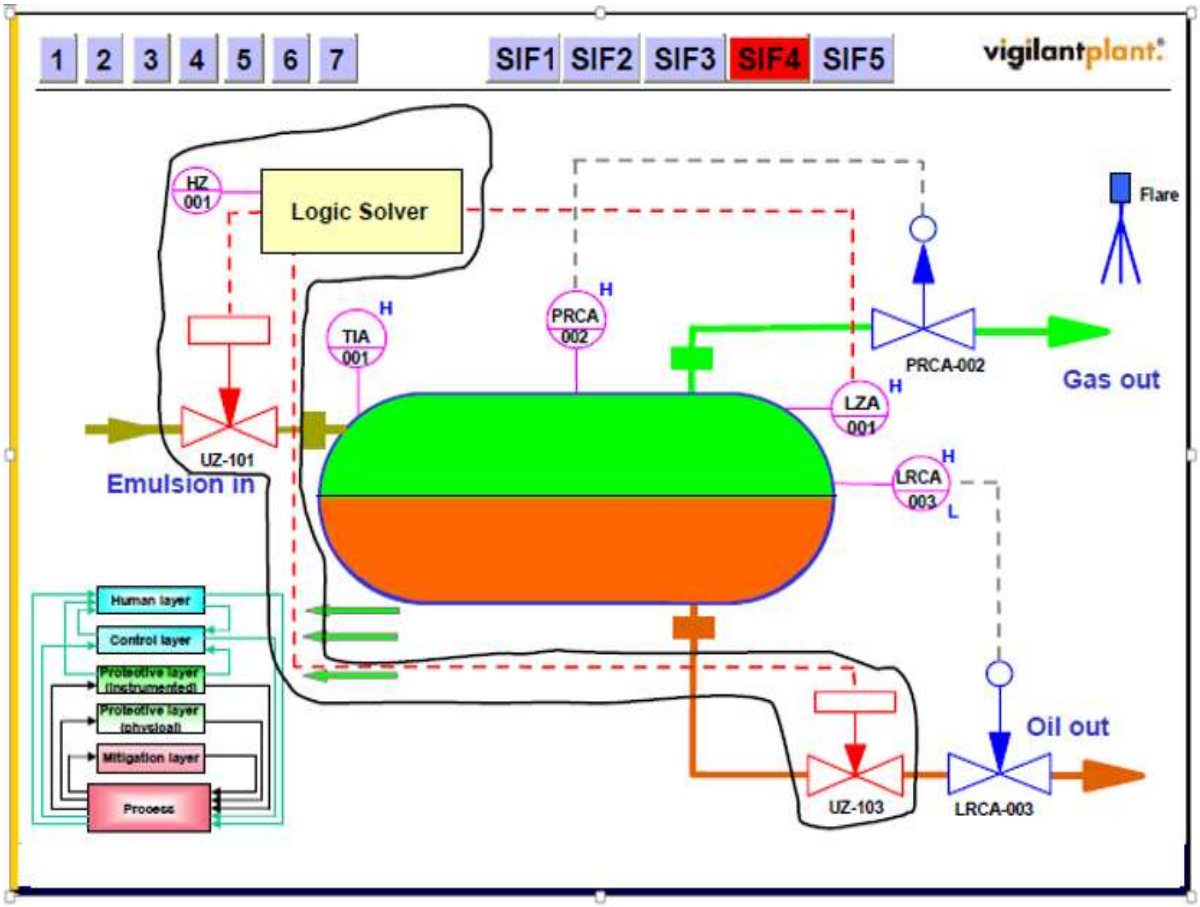
- Les systèmes instrumentés de sécurité nécessitent une source d'énergie extérieure pour remplir leur fonction de sécurité.
- On retrouve tout ou partie de ces différents éléments pour constituer des chaînes de sécurité.
- Plusieurs capteurs ou actionneurs peuvent être reliés à une même unité de traitement.
- Toutes les combinaisons de capteurs, d'unité de traitement et d'actionneurs qui sont exigées pour accomplir des fonctions de sécurité sont considérées comme une partie de systèmes instrumentés de sécurité.

- Les capteurs, l'unité de traitement, les éléments finaux sont des équipements de sécurité et réalisent des sous-fonctions de sécurité. L'ensemble des sous fonctions réalise la fonction de sécurité. [3] [4]

2.3 Fonction instrumentée de sécurité (SIF)

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité, pour le but de maintenir le process en état sécurité [2].

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique



.Figure 2.2 : Fonction instrumentée de sécurité 1 [2].

Dans la figure 2.2 le HZ001 représente un bouton d'arrêt d'urgence local, dans le cas où l'opérateur sur site observe une fuite du gaz ou bien du feu, il doit immédiatement appuyer sur ce bouton d'arrêt d'urgence pour isoler le processus et minimiser le niveau du risque, et par la suite on peut décrire le rôle du SIS comme suit :

Dans le cas où il aura une activation du HZ001, pour une raison ou autre, le System SIS doit rapidement fermer les vannes de sécurité UZ-101 et UZ-103 pour garder le processus dans un état sécurisé, et donner l'équipe de feu et gaz au niveau de l'unité d'intervenir pour éliminer la source du danger.

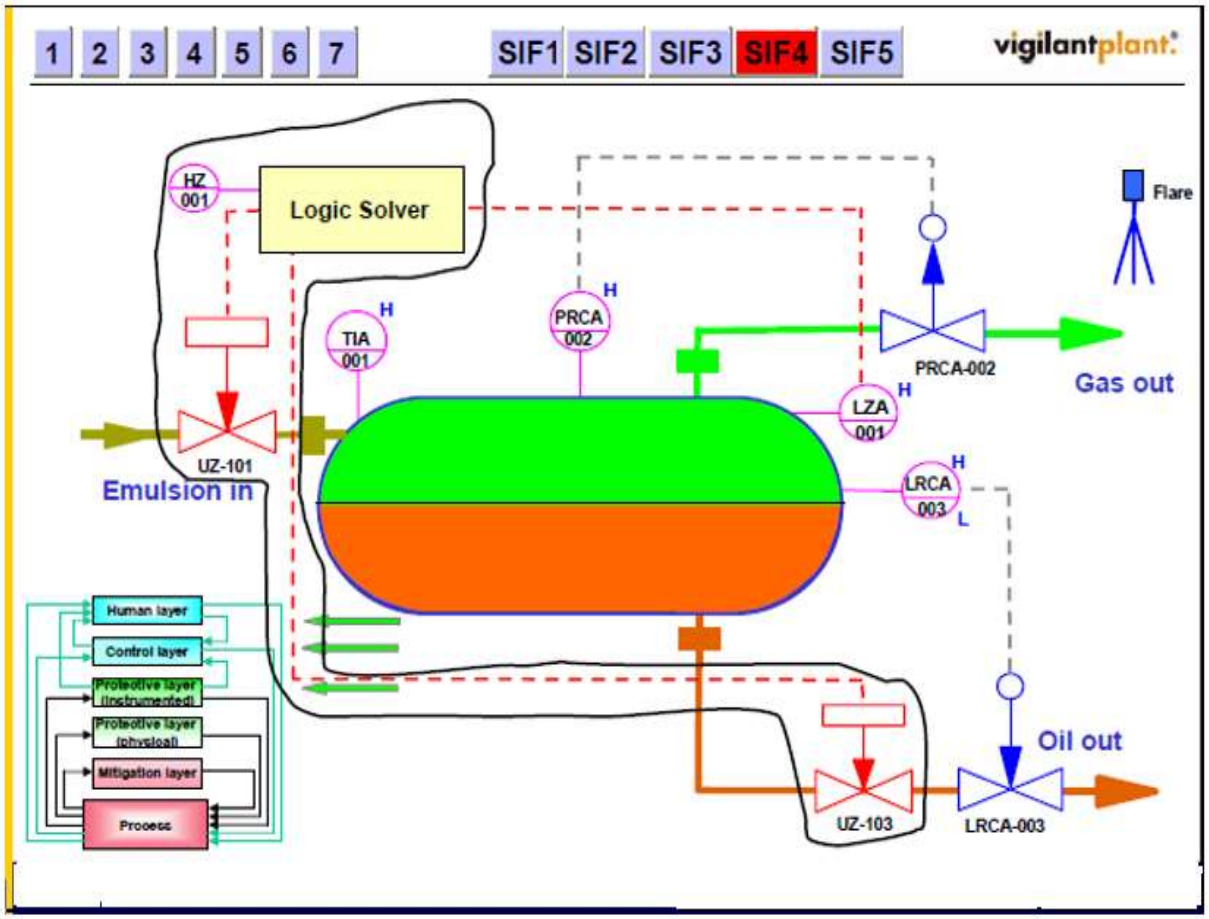


Figure 2.3 Fonction instrumentée de sécurité 2 [2].

Dans la figure 2.3, le PIZA001, montre un arrêt dépressuriser de l'unité, c.-à-d., un arrêt avec l'envoi du gaz vers la torche pour le brûler, dans ce cas, on peut décrire le rôle du SIS comme suit :

Dans le cas d'arrêt de l'unité, dans le cadre d'une maintenance préventive, l'unité de séparation doit être arrêtée et le bac sera vidé, et par la suite le SIS doit fermer immédiatement les vannes de sécurité UZ-101 et UZ-103 et ouvrir la vanne de torche UZ-102 afin de brûler le gaz vers l'atmosphère.

2.3.1. Temps de réponse de la SIF

Le temps entre l'apparition du facteur déclenchant et l'exécution des actionneurs sur site : vannes, pompes, relais…etc. doit être très minime de l'ordre de milliseconde.

Tous les systèmes d'arrêt d'urgences disponibles sur le marché mondial doivent accomplir les exigences du SIL 3, ce qui rend leur temps d'intervention très rapide [2] [3].

$$\text{Temps}_{SIF} = T_{Transmetteurs} + T_{Interfaces} + T_{Unité\ de\ traitement} + T_{Interfaces} + T_{Eléments\ finaux}$$

2.4 La sécurité fonctionnelle

La norme CEI 61511-1, fournit la définition suivante : « La sécurité fonctionnelle est le sous-ensemble de la sécurité globale se rapportant au processus et au BPCS (Basic Process Control System), qui dépend du fonctionnement correct du SIS et d'autres couches de protection. » la sécurité fonctionnelle est la réduction des risques fournie par les fonctions mises en œuvre afin de garantir l'exploitation sécurisée du procédé [9].

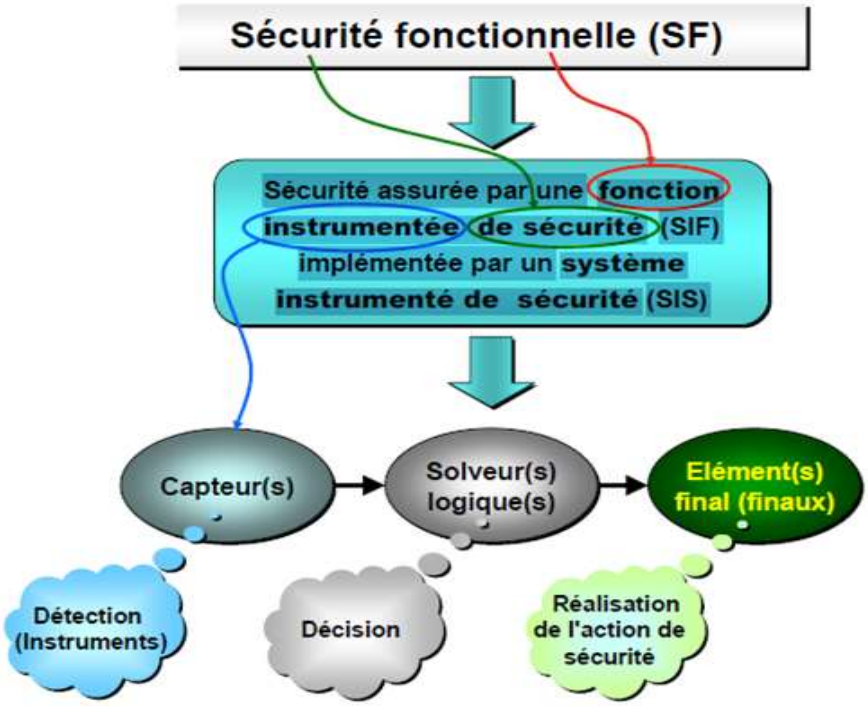


Figure 2.4 : Sécurité fonctionnelle [2].

2.5 Evaluation du niveau d'intégrité de sécurité (SIL)

La norme CEI 61508 fixe le niveau d'intégrité de sécurité (Safety Integrity Level : SIL), qui doit être atteint par un SIS, qui réalise la Fonction Instruménté de Securité (SIF). Elle donne le SIL en fonction de sa probabilité de défaillance moyenne (PFD_{avg}) sur demande pour les SIS faiblement sollicités (moins d'une sollicitation par an) (Tableau 2.2), ou en fonction de probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités ou agissant en mode continu (Tableau 2.3). L'allocation du SIL se fait par des méthodes qualitatives et semi qualitatives, alors que l'évaluation du PFD_{avg} des SIS qui doit satisfaire au SIL exigé se fait par des méthodes quantitatives. [3][4]

Tableau 2.1 : Niveaux d'intégrité de sécurité en fonction de la Probabilité moyenne de défaillances PFD_{avg} [3].			
FONCTIONNEMENT A FAIBLE SOLLICITATION			
Niveau d'intégrité de sécurité (SIL)	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})	Réduction de risqué cible (RR)	Maximum défaillances acceptables
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	10 ≤RR<100	Une défaillance dangereuse chaque 10 ans
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	100 ≤RR<1000	Une défaillance dangereuse chaque 100 ans
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	1000 ≤RR <10000	Une défaillance dangereuse chaque 1000 ans
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	10000≤RR <100000	Une défaillance dangereuse chaque 10,000 ans

La probabilité de défaillance moyenne à la sollicitation notée PFD_{avg} correspond à la valeur de la probabilité de défaillance à la sollicitation $PFD(t)$ moyenne sur la période de temps tests notée TI. Cette probabilité s'exprime comme suit :

$$\boldsymbol{PFD_{\text{avg}} = \frac{1}{TI}\int_0^{TI} PFD(t)dt} \qquad \textbf{(2.1)}$$

Tableau 2.2 : Niveaux d'intégrité de sécurité en fonction de la Probabilité de défaillance Dangereuse par heure PFH [3].			
FONCTIONNEMENT A FORTE SOLLICITATION			
Niveau d'intégrité de sécurité (SIL)	Probabilité de défaillance Dangereuse par heure (PFH)	Réduction de risqué cible (RR)	Maximum défaillances acceptables
1	$10^{-6} \leq PFH < 10^{-5}$	$10^5 \leq RR < 10^6$	Une défaillance dangereuse chaque 100000 ans.
2	$10^{-7} \leq PFH < 10^{-6}$	$10^6 \leq RR < 10^7$	Une défaillance dangereuse chaque 1000000 ans
3	$10^{-8} \leq PFH < 10^{-7}$	$10^7 \leq RR < 10^8$	Une défaillance dangereuse chaque 10000000 ans
4	$10^{-9} \leq PFH < 10^{-8}$	$10^8 \leq RR < 10^9$	Une défaillance dangereuse chaque 100000000 ans

Un SIS peut être représenté sous la forme d'une combinaison de plusieurs éléments, la PFD_{avg} des différents éléments qui le compose. D'une maniérée générale, un SIS est composé des trois sous-systèmes présentés sur la figure 2.5.

Pour chaque sous- système, en fonction de son architecture et de la connaissance des donnée de fiabilité ($\lambda, MTTR, TI, etc$ ...), il est possible d'évaluer leursPFD_{avg} .
La PFD du système présenté en figure II.16 s'exprime comme suit :

$$\boldsymbol{PFD_{\text{avg}} = PFD_{\text{avg}}\,(SSC) + PFD_{\text{avg}}\,(SSL) + PFD_{\text{avg}}\,(SSEF)} \qquad \textbf{(2.2)}$$

- PFD_{avg} (SSC) : probabilité de défaillance moyenne à la sollicitation du sous-système capteur.
- PFD_{avg} (SSL) : probabilité de défaillance moyenne à la sollicitation du sous-système logique.
- PFD_{avg} (SSEF) : probabilité de défaillance moyenne à la sollicitation du sous-système élément final.
- Les formules de calculs (relatives au schéma-bloc) permettent d'évaluer le PFD « globale » du système sont les suivant :
- Bloc en parallèle :

$$\boldsymbol{PFD_{globale} = \prod_{i=1}^{n} PFD_i} \qquad \textbf{(2.3)}$$

- Bloc en série :

$$\boldsymbol{PFD_{globale} = \sum_{i=1}^{n} PFD_i} \qquad \textbf{(2.4)}$$

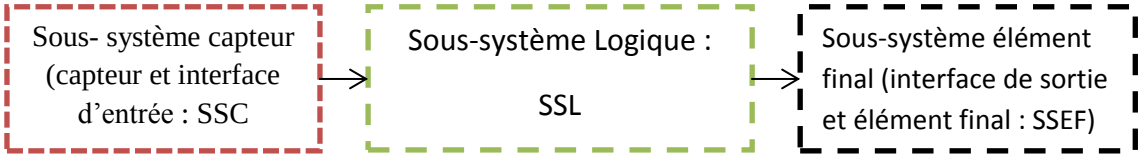


Figure 2.5 Schéma respectif d'un SIS [2]

2.5.1. Exemples pratiques des process industriels

2.5.1.1. Process 1

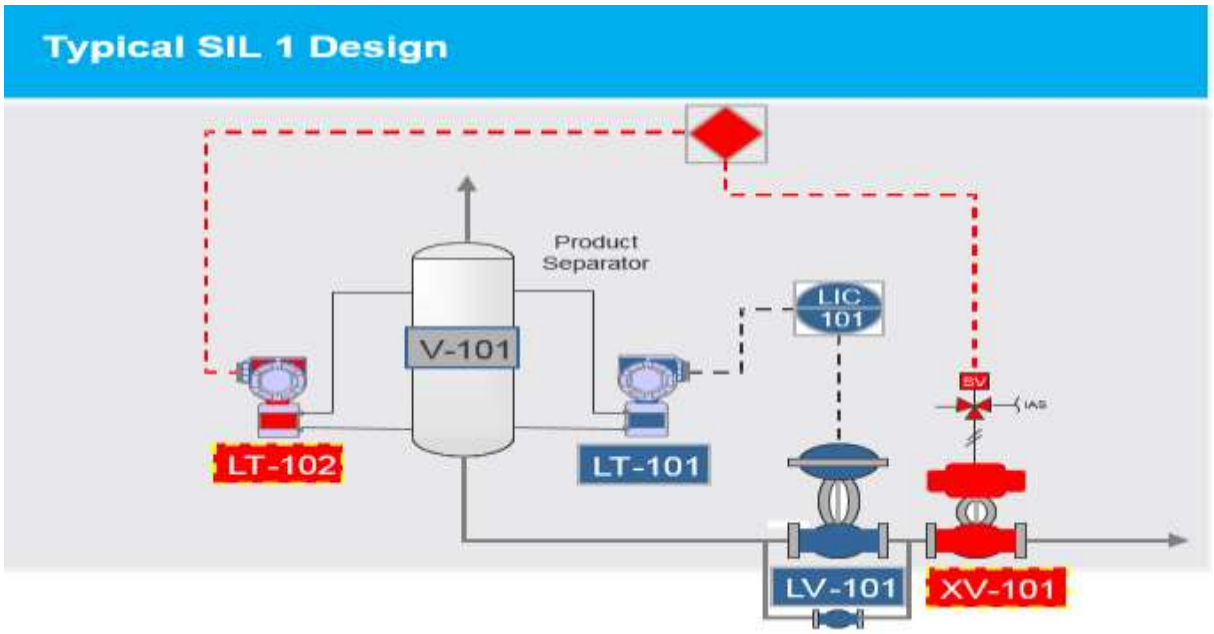


Figure 2.6 : Configuration1 d'un SIS conçu pour réaliser le SIL#1 [2].

La figure 2.6 montre l'architecture d'un système qui doit accomplir le SIL #1, on constate l'absence de la redondance que ce soit au niveau des capteurs ou bien ou niveau des actionneurs, ce type d'architecture est utilisé dans les processus industriel avec risque futile et importance minimum.

2.5.1.2. Process 2

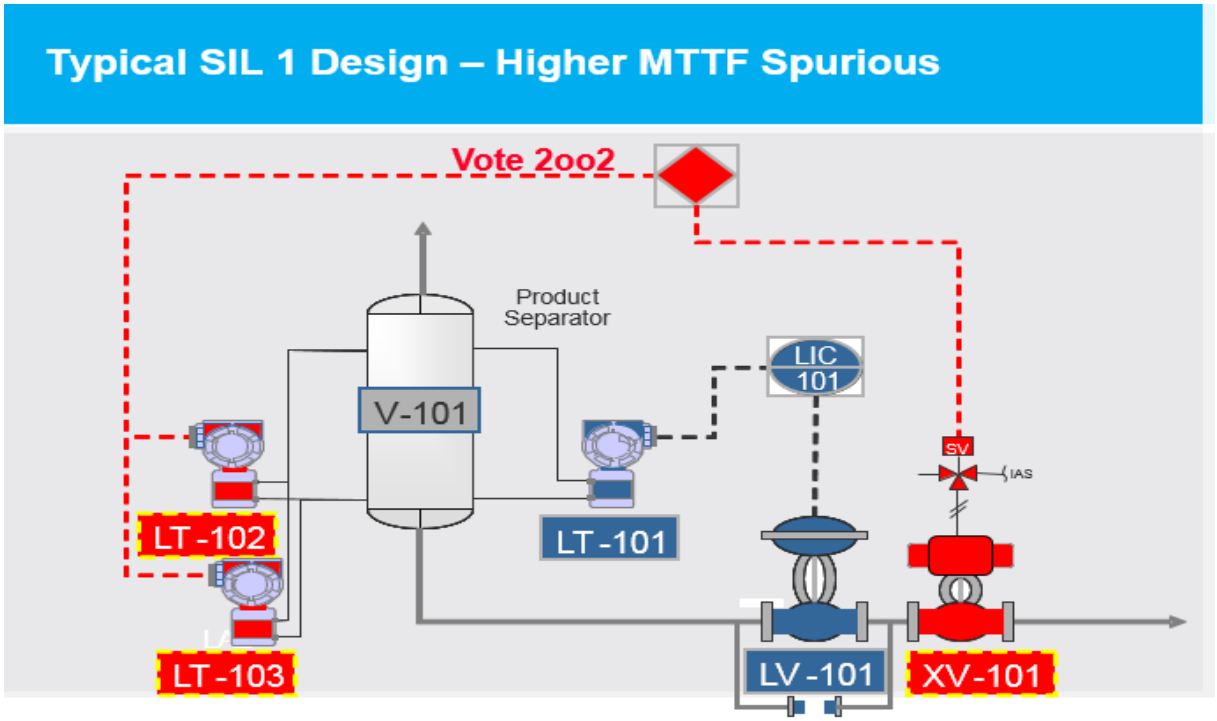


Figure 2.7 : Configuration2 d'un SIS conçu pour réaliser le SIL#1 [2].

La figure 2.7 montre l'architecture d'un système SIL #1, on constate la présence de la redondance au niveau des capteurs avec un system de vote (2oo2) mais pas au niveau des actionneurs, ce type d'architecture est utilisé dans les processus industriel avec risque modérée et importance considérée.

2.5.1.3. Process 3

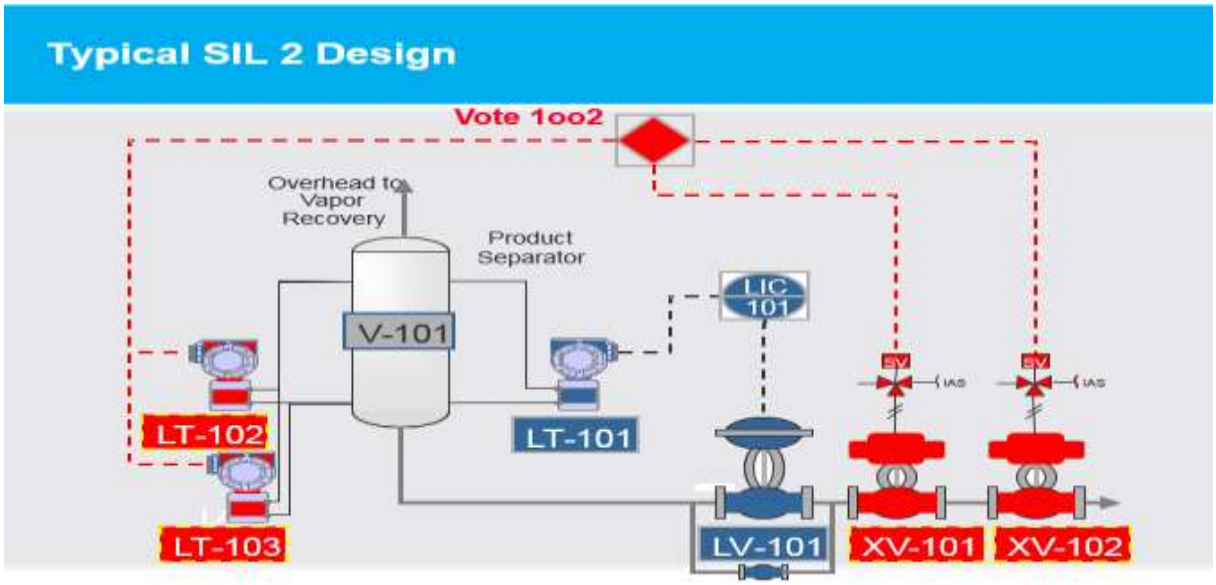


Figure 2.8 : Configuration1 d'un SIS conçue pour réaliser le SIL #2 [2].

Cette figure montre l'architecture d'un système SIL #2, on constate la présence de la redondance au niveau des capteurs avec un system de vote (1oo2) ce qui rend le risque relativement important, ainsi qu'au niveau des actionneurs, ce type d'architecture est utilisé dans les processus industriel avec risque important.

2.5.1.4. Process 4

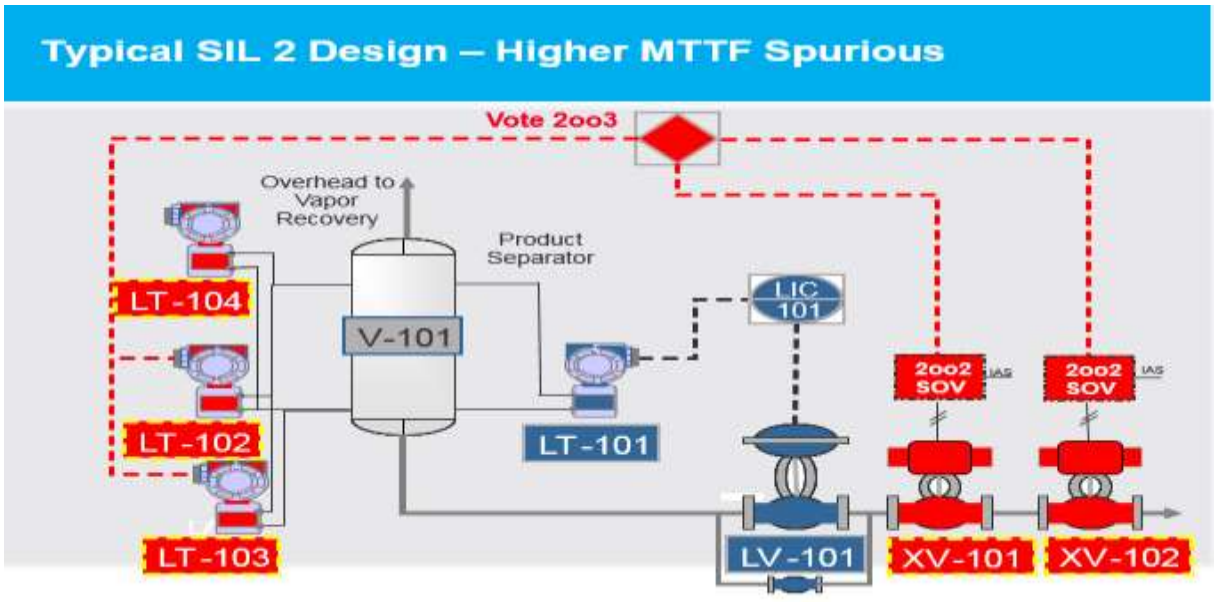


Figure 2. 9 : Configuration2 d'un SIS conçue pour réaliser le SIL #2 [2].

Cette figure montre l'architecture d'un système SIL #2, on constate la présence de la redondance au niveau des capteurs avec un system de vote (2oo3) ce qui rend le risque très important ainsi qu'au niveau des actionneurs avec système de vote (2oo2) pour assurer l'isolement du processus à travers la fermeture des vannes XV, ce type d'architecture est utilisé dans les processus industriel avec risque très d' importance très élevée.

2.6 Redondance au sein d'un SIS

Pour améliorer le niveau de confiance d'un système instrumenté de sécurité, il est possible, entre autres, de la doubler totalement (redondance totale), ou de doubler une partie de ses composants (redondance partielle de la barrière de sécurité). A noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance. Tous les éléments constituant un système instrumenté de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs et même les moyens de transmission [4].

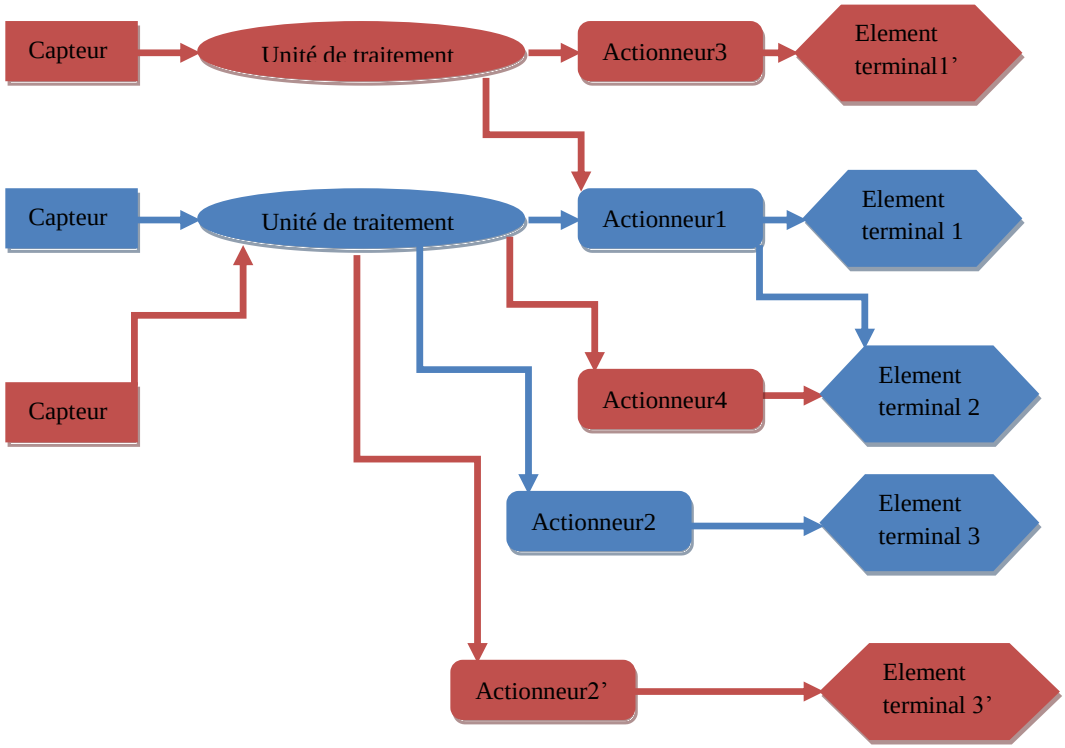


Figure 2.10 : Schéma d'un SIS complexe avec redondance [31].

On peut distinguer plusieurs types de redondance :

- **la redondance active (chaude)** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.
- **la redondance passive (froide)** qui est une redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est en fonctionnement, le reste n'étant utilisé sur sollicitation qu'en cas de défaillance de la partie en fonctionnement.

- **la redondance majoritaire m/n** qui est une redondance telle qu'une fonction n'est assurée que si au moins m des n moyens existants sont en état de fonctionner ou en fonctionnement. [2]

2.7 Architectures d'un SIS

Les architectures les plus souvent rencontrées relatives à ce dernier type de redondance sont les suivantes :

2.7.1 Architecture 1*oo*1

Cette architecture de base est composée d'un seul canal et qu'en conséquence toute défaillance dangereuse induit la perte de la fonction de sécurité en cas de demande. De plus, toute défaillance sûre conduit à l'exécution de cette fonction en absence de demande. Cette architecture minimale, qui ne tolère pas de défaillance, ne peut être utilisée dans des applications de sécurité. [2]

Figure 2.11: Architecture 1oo1

2.7.2 Architecture 1*oo*2

Cette architecture se compose de deux canaux identiques fonctionnant en redondance chaude : chaque canal peut réaliser la fonction de sécurité. Il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande. A ce titre, la défaillance sûre de l'un ou l'autre des deux canaux conduit le système surveillé vers un état de repli sûr (activation de la fonction de sécurité).[13]

Figure 2.12: Architecture 1oo2

2.7.3 Architecture 2*oo*2

Cette architecture consiste en deux canaux en parallèle de sorte que les deux canaux doivent demander la fonction de sécurité pour que celle-ci soit activée : fonctionnement série au sens fiabiliste. Le système a donc un comportement dangereux dès qu'une défaillance dangereuse survient dans un des deux canaux. En revanche, le déclenchement intempestif (activation de la fonction de sécurité en absence de demande) ne se réalise que si les deux canaux observent des défaillances sûres.[13]

Figure 2.13 : Architecture 2oo2

Il est important de signaler que pour les architectures séries (*NooN*) une seule défaillance dangereuses engendre la non-exécution de la fonction de sécurité en présence de demande, alors que *N* défaillances sûres sont nécessaires pour conduire à un déclenchement intempestif du SIS.

2.7.4 Architecture 2*oo*3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul canal donne un résultat différent des deux autres canaux.

Ceci dit, le nombre de défaillances nécessaires aussi bien à l'empêchement de l'exécution de la fonction de sécurité qu'au déclenchement intempestif du SIS s'élève à deux.[2]

Figure 2.14 : Architecture 2oo3/2oo4 [2].

D'une manière générale, pour une architecture *KooN* ces deux nombres sont établis ainsi :

- ***N – K*+1** représente le nombre de défaillances dangereuses dont l'occurrence induit la perte de la fonction de sécurité.
- ***K*** représente le nombre de défaillances sûres dont l'occurrence conduit à l'activation intempestive de cette même fonction. [2][8]

Tableau 2.3 : Comparaison des architectures 1oo2, 2oo2 et 2oo3 [2]

Architecture	Disponibilité	Sécurité
1oo2	La défaillance non dangereuse de l'un des deux éléments entraine un déclenchement intempestif : $Pdnds = 2 * Pdnd$	Deux défaillances dangereuses sont nécessaires pour que le système ne puisse pas remplir sa fonction : $Pdds = (Pdd)^2$
2oo2	La défaillance dangereuse des deux éléments est nécessaire pour observer un déclenchement intempestif : $Pdnds = (Pdnd)^2$	La défaillance dangereuse de l'un des deux éléments suffit pour que le système ne puisse pas remplir sa fonction : $Pdds = 2 * Pdd$
2oo3	La défaillance dangereuse de deux éléments sur trois est nécessaire pour observer un déclenchement intempestif : $Pdnds = 3 * (Pdnd)^2$	Deux défaillances dangereuses sont nécessaires pour que le système par remplir sa fonction : $Pdds = 3 * (Pdd)^2$

Note :
Pdd : probabilité de défaillance dangereuse d'un élément de l'architecture ***KooN***
Pdds **:** probabilité de défaillance dangereuse du système en ***KooN***
Pdnd **:** probabilité de défaillance non dangereuse d'un élément de l'architecture ***KooN***
Pdns **:** probabilité de défaillance non dangereuse du système en ***KooN***

2.8. Tests au niveau des systèmes instrumentés de sécurité

Les normes et directives en matière de sécurité imposent de vérifier régulièrement l'état de fonctionnement des éléments constituant la chaîne de sécurité. Le niveau de SIL attribué à un SIS est calculé en prévoyant des tests périodiques sur les différents éléments qui composent le système. Les normes mentionnent clairement les tests en ligne et hors ligne comme une condition pour maintenir le niveau de SIL pour les systèmes de sécurité. Si toutes les défaillances étaient détectées, il ne serait pas nécessaire de vérifier périodiquement les éléments entrant dans la composition d'un SIS.

Le problème posé parfois est celui de la périodicité de ces tests et la planification des arrêts des procédés pour maintenance qui deviennent de moins en moins fréquents. En effet, il paraît déraisonnable d'interrompre délibérément la production dans un procédé pour tester une vanne qui ne sera peut-être jamais sollicitée. Du coup, dans certains cas, il faut parfois attendre six ans pour avoir l'occasion de tester une vanne d'arrêt hors ligne. Généralement ces tests sont établis pour vérifier et contrôler le bon fonctionnement des SISs, deux types de tests qui sont faits au niveau de SIS [2][18].

2.8.1 Test de diagnostic

Le test en ligne (en fonctionnement) pour détecter des défauts, les tests de diagnostic sont effectués périodiquement et automatiquement pour détecter les défauts latents cachés qui empêchent le SIS (Safety Integrated System) de répondre à une demande**.** Le diagnostic (test en ligne) et les inspections visuelles sont des moyens très importants pour vérifier si un SIS est capable d'atteindre ses fonctions de sécurité et de révéler les défaillances qui entravent la mise en sécurité du procédé au moment où il y a une demande.

Le diagnostic est un moyen de détection en ligne des déviations, des dégradations et des divergences et il est souvent réalisé par du matériel et du logiciel dédiés et implémentés dans les dispositifs.[18].

II.8.2 Test périodique

La norme CEI61508, définit le test périodique comme un essai effectué pour révéler des défauts non détectés dans un système instrumenté de sécurité, de telle sorte que, au besoin, le système puisse être restauré dans sa fonctionnalité de conception.

Test périodique hors ligne réalisé pour détecter des pannes dans un système de telle sorte que le système puisse être réparé afin de revenir dans un état équivalent à son état initial. Dans le cas où le diagnostic converge serait minimum ou insuffisant (si on ne peut pas réaliser un test de diagnostic satisfaisant), on pourra augmenter la fréquence du proof test. En augmentant

la fréquence du proof test, on vérifiera plus souvent que la fonction de sécurité est bien disponible. Le proof test est exécuté au niveau du système. C'est un test fonctionnel de la fonction de sécurité hors fonctionnement automatique sans perturbation de process (activité périodique devant être conduite selon une procédure afin de détecter les défauts latents qui empêchent le système de sécurité de remplir sa fonction de sécurité ; le système de sécurité entier doit être testé). [31]

2.8.3 Test de Course Partielle de la Vanne (Partiel Valve Stroke Testing (PVST))

Les actionneurs constituent le maillon le plus faible de la boucle de sécurité. C'est pourquoi bon nombre de fabricants et chercheurs se sont penché sur la question afin de proposer des solutions. Un cas particulier des actionneurs est celui des vannes utilisées dans les systèmes instrumentés de sécurité. Ces vannes sont considérées comme les composants les plus fragiles du fait qu'elles restent sans bouger pendant de longues périodes, et les obturateurs auront tendance à se coller. Une solution proposée tant par les fabricants que les chercheurs consiste à réaliser des tests périodiques sur une partie de course de l'obturateur de la vanne appelé PVST (Partial Valve Stroke Testing : Test Partiel de la Course de Vanne).

Le problème rencontré souvent dans les vannes est le blocage en fermeture ou en ouverture, C'est pourquoi le PVST consiste à tester régulièrement les vannes sur un pourcentage de leur course (10 à 20%) afin de s'assurer que celles-ci ne resteront pas bloquées lorsqu'on en aura besoin. [31]

2.9 Classification des défaillances des systèmes instrumentés de sécurité

Pour une meilleure compréhension des formules analytiques liées aux différentes grandeurs probabilistes, une clarification des différentes paramètres fiabilistes, caractérisant les éléments constitutifs des SIS, s'impose. Cette clarification concerne La classification des défaillances des SIS :

1. La classification des défaillances des SIS selon leurs causes :

   - Défaillances aléatoires du matériel (physiques) : défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradations au sein du matériel et dont l'instant exact d'occurrence n'est pas prévisible**.**
   - Défaillances systématiques (fonctionnelles) : défaillances reliées de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés. [2]

2. La classification des défaillances selon leurs effets : toutes les défaillances (aléatoires du matériel et systématiques), selon leurs effets sur la fonction de sécurité, peuvent être classées dans l'une des deux catégories suivantes :

- Défaillances dangereuses (dangerous failure: D) : défaillance qui a la potentialité de mettre le système relatif à la sécurité (SIS) dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

- Une autre partition résulte du fait que ces défaillances peuvent être :
  - Défaillances dangereuses détectées (dangerous detected failures : DD): défaillances détectées immédiatement après leur occurrence par des tests en ligne.[5]
  - Défaillances dangereuses non détectés (dangerous undetected failures : DU): défaillances qui ne peuvent être révélées que lors de tests périodiques hors ligne (de période égale à T1).

- Défaillances en sécurité (safe failure: S) : défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité (SIS) dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

  - Défaillances en sécurité détectées (safe detected failures : SD) : défaillances détectées immédiatement après leur occurrence par des tests en ligne.
  - Défaillances en sécurité non détectées (safe undetected failures : SU) : défaillances qui ne peuvent être révélées que lors de tests périodiques hors ligne. [2]

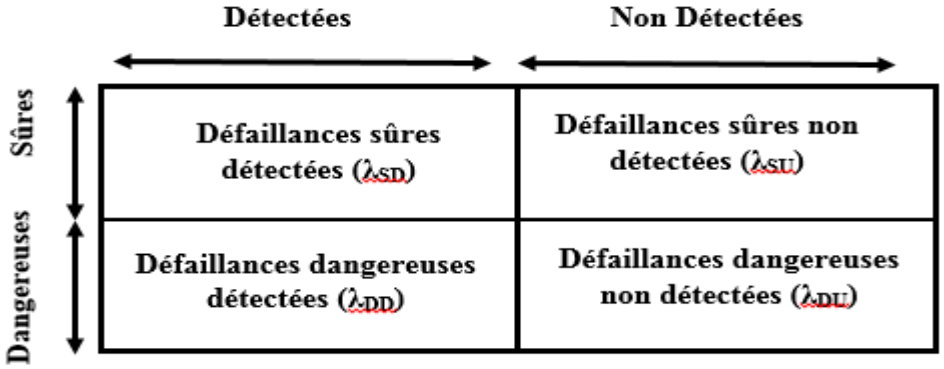


Figure 2.15 : Classification des défaillances pour les SISs [31].

3. Défaillance de cause commune (Common Cause Failure) : Une contrainte aléatoire qui provoque la défaillance de deux composants ou plus en même temps, pour la même raison. Elle diffère d'une défaillance systématique, en ce sens où elle est aléatoire et probabiliste, mais n'est pas du type cause et effet fixe et prévisible

$$\lambda = \boldsymbol{taux\ de\ défaillance} = \frac{Nbre\ pannes}{Durée\ de\ test * Nbre\ élements\ testés} \qquad \textbf{(2.5)}$$

Chaque catégorie de défaillances *aléatoires du matériel* est appréciée à travers son taux de défaillance :

Taux de défaillance aléatoires du matériel : $\boldsymbol{\lambda = \lambda D + \lambda S}$ **(2.6)**

1. Taux de défaillance aléatoire dangereuse : $\boldsymbol{\lambda D = \lambda DD + \lambda DU}$ **(2.7)**

Taux de défaillance aléatoire dangereuse détectée : $\boldsymbol{\lambda DD = DC.\lambda D}$ **(2.8)**

Taux de défaillance aléatoire dangereuse non détectée : $\boldsymbol{\lambda DU = (1 - DC).\lambda D}$ **(2.9)**

DC (Couverture de Diagnostic) **:** la capacité d'un canal à la détection « en ligne » des défaillances dangereuses, exprimée par un nombre allant de 0 à 1.

2. Taux de défaillance aléatoire en sécurité :

$$\boldsymbol{\lambda S = \lambda SD + \lambda SU} \quad \textbf{(2.10)}$$

- Taux de défaillance aléatoire en sécurité détectée :

$$\boldsymbol{\lambda SD = DCS.\lambda S} \quad \textbf{(2.11)}$$

- Taux de défaillance aléatoire en sécurité non détectée :

$$\boldsymbol{\lambda SU = (1 - DCS).\lambda S} \quad \textbf{(2.12)}$$

DCS : la capacité d'un canal à la détection « *en ligne* » des défaillances en sécurité.

4. La contribution des CCF sur des canaux redondants parallèles est prise en compte en incluant un facteur β.

- Taux de défaillances de cause commune :

$$\boldsymbol{\lambda DCC = \beta.\lambda} \quad \textbf{(2.13)}$$

- Taux de défaillances indépendantes :

$$\boldsymbol{\lambda ind = (1 - \beta).\lambda} \quad \textbf{(2.14)}$$

$$\boldsymbol{\lambda = \lambda ind + \lambda DCC = (1 - \beta).\lambda + \beta.\lambda} \quad \textbf{(2.15)}$$

2.10 Principaux paramètres de sécurité

La norme introduit également les notions suivantes :

- Le Taux de défaillances non dangereuses (Safe failure fraction = **SFF**) : décrit le taux de défaillances n'ayant pas le potentiel de mettre le système relatif à la sécurité dans un état dangereux ou inacceptable.

$$SFF = \frac{\lambda S + \lambda DD}{\lambda} \qquad (2.16)$$

- La Tolérance aux pannes hardware (Hardware Fault Tolerance (**HFT**)) est la capacité d'une unité fonctionnelle d'accomplir une fonction requise malgré certaines pannes ou erreurs. Une HFT de N signifie que N+1 erreurs peuvent entraîner la perte de la fonction de sécurité. [2]

2.11 Contraintes architecturales

2.11.1 SIS de type A

Un SIS peut être considéré de type A si son comportement en présence d'anomalies sont bien déterminé, si les modes de défaillances des de ses constituants sont bien définis, et si les données concernant leurs défaillances issues du retour d'expérience sont connues avec une bonne fiabilité. Ces systèmes sont à la base de composants simples tels que : les résistances métalliques, les transistors, relais etc. [2][3].

2.11.2 SIS de type B

Un SIS peut être considéré de type B, si une des trois conditions régissant le type A n'est pas satisfaite. Ces systèmes sont à la base de composants complexes comme les microprocesseurs…. etc. [2][3]

2.12 Application des systèmes Instrumentés de sécurité (SIS)

1. **ESD : Emergency ShutDown System :** systèmes d'arrêt d'urgence.
2. **F&G : Fire and Gas System :** systèmes feu et gaz
3. **BMS : Burner Management System :** barrières de sécurité pour gérer les chaudières.
4. **TMC : Turbo Machinery Control System** : barrières de sécurité pour gérer les machines tournantes.

5. **HIPPS : High Integrity Pressure Protection System : Système de Protection de Pression à Haute Intégrité :** barrière de sécurité pour contrôler la pression au niveau des procès et les champs de production.
6. **WHCP : Well Head Control Panel** : barrières de sécurité pour contrôler la pression ou la température des puits.

2.13. Système de Protection contre la Pression à Haute Intégrité (High Integrity Pressure Protection System : HIPPS)

Lors du fonctionnement dans des environnements à haute pression et dans les champs de production, un événement de surpression peut causer des dommages à l'environnement, aux infrastructures et au personnel. Atténuer ce risque sur les puits de production et les lignes de flux est un défi qui peut être relevé avec un HIPPS. Les HIPPS sont installés à la place des soupapes de décharge mécaniques conventionnelles pour gérer des débits élevés et des pressions élevées, réduisant le risque que les unités de production dépassent leur pression de conception. C'est un système de décharge de haute pression et de débit, qui conduisent des processus dangereux à une sécurité prévisible, état dans un certain temps sûr.

2.13.1. Historique

En 1974, la société allemande DVGW a certifié l'élément final Mokveld, y compris les initiateurs mécanique selon EN 14382 (ancienne DIN 3381). Depuis cette date, Mokveld a une expérience sur le terrain de la fermeture des vannes d'arrêt de sécurité (avec actionneur et initiateur) dans les 2 secondes. Les principales caractéristiques du HIPPS mécanique intégral de Mokveld sont :

1. Boucle de sécurité intégrée selon CEI 61508 / EN 12186.
2. Sûr et simple.
3. Option ne nécessitant pas d'énergie externe (HIPPS autonome).
4. Aucun câblage requis.
5. Précision du point de consigne <1%.
6. Système à SIL 3 ou 4.
7. Données de défaillance validées par des tiers. [32][33]

2.13.2. Définition

Le HIPPS est une application spécifique d'un système instrumenté de sécurité conçu et intégré conformément aux normes CEI 61508 et CEI 61511. Il sépare la partie aval de l'usine

de la partie amont en cas de haute pression qui protège le système contre l'explosion et le déversement de matières dangereuses et toxiques, HIPPS peut être utilisé à la fois dans les opérations de surface et sous-marines, il est considéré comme l'un des meilleurs choix pour protéger les installations et augmenter la sécurité dans les endroits où les systèmes de décompression ordinaires ne suffisent pas à garantir la sécurité. Les aspects les plus importants de HIPPS sont la sécurité, les considérations économiques et environnementales. [2][33]

2.13.3. Composant d'un HIPPS

Le système HIPPS est essentiellement composé d'un solveur logique, de deux vannes d'arrêt fonctionnant sur la logique 1oo2 et trois transmetteurs de pression fonctionnant sur la logique 2oo3. Chaque appareil a été sélectionné et conçu pour garantir que le système complet soit classé SIL 3(Probabilité de défaillance sur demande PFD entre 10^{-4} et 10^{-3}) Il est important de reconnaître que le HIPPS comprend tous les dispositifs nécessaires pour atteindre la condition de sécurité intégrée souhaitée pour le processus. Le HIPPS comprend toute la boucle de l'instrument, du capteur de terrain au solveur logique jusqu'au les éléments finaux, ainsi que d'autres dispositifs nécessaires au bon fonctionnement du SIS, comme l'utilisateur SIS interfaces, communications et alimentations. HIPPS est composé des principaux suivants sous-systèmes :

1. Initiateur / détecteur : qui détectent l'augmentation de la pression et envoient un signal à la partie suivante de la boucle, l'initiateur peut être électronique ou mécanique.
2. Solveur logique : qui prend le signal de l'initiateur et le traite pour trouver le plus approprié signal à envoyer à la troisième partie de HIPPS.
3. Élément final : qui est la dernière partie de HIPPS, il reçoit le signal du solveur logique puis entreprendre la mesure corrective, le dernier élément est une vanne de régulation qui pour exemple d'arrêt en cas de surpression. [33].

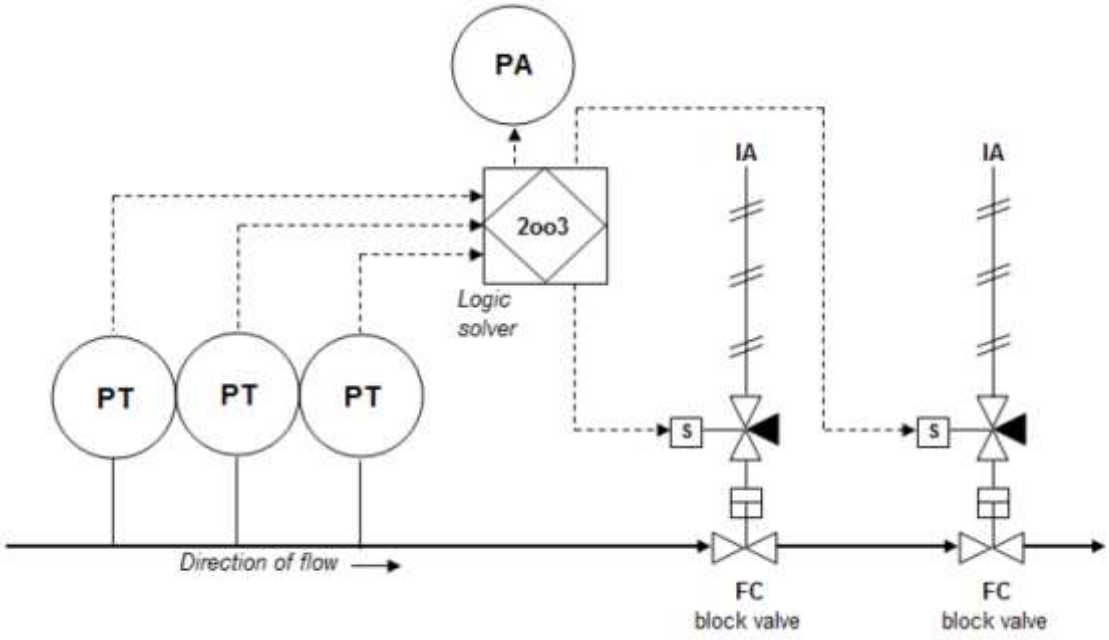


Figure 2.16 : Illustration simplifiée du HIPPS [33].

2.13.4. Types de HIPPS : Il existe deux types de HIPPS :

2.13.4.1. HIPPS hydraulique (en 1974)

Le HIPPS hydraulique (mécanique) fournit un système de protection autonome et indépendant opéré à la demande avec une pression d'entrées de capteur de un sur deux (1oo2) ou deux sur trois (2oo3) (vote), un solveur logique hydraulique et deux soupapes de sécurité à rappel par ressort à commande hydraulique. L'unité est généralement auto-alimentée et peut être équipée de commandes supplémentaires en temps réel via un groupe hydraulique (HPU). Cela met le système sous pression et ouvre les vannes d'arrêt de sécurité. Le système reste ouvert (armé) jusqu'à ce qu'une condition anormale soit détectée. Si une condition anormale est détectée, le système ferme les deux vannes des éléments finaux actionnés, protégeant la production en aval de l'installation. [34]

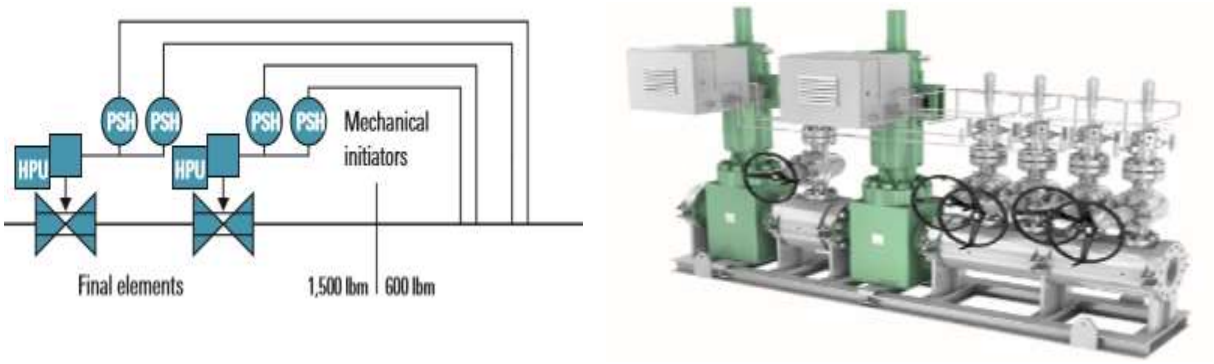


Figure 2. 17 : HIPPS hydraulique [34].

2.13.4.2. HIPPS électronique (en 2000)

Le HIPPS électronique est un système autonome et indépendant fonctionnant à la demande avec des entrées de transmetteur de pression de 1oo2 ou 2oo3 (vote), un solveur logique électronique et deux soupapes de sécurité à rappel par ressort à commande hydraulique. L'unité peut être auto-alimentée avec une pompe manuelle ou (HPU) et peut également être configuré pour fonctionner à l'aide des sources d'alimentation de l'installation. Cela met le système sous pression et ouvre les vannes d'arrêt de sécurité. Le système reste ouvert jusqu'à ce qu'une condition anormale soit détectée. Si un tel événement est détecté, le système ferme les deux vannes des éléments finaux actionnés, protégeant la production ou l'installation en aval. [35]

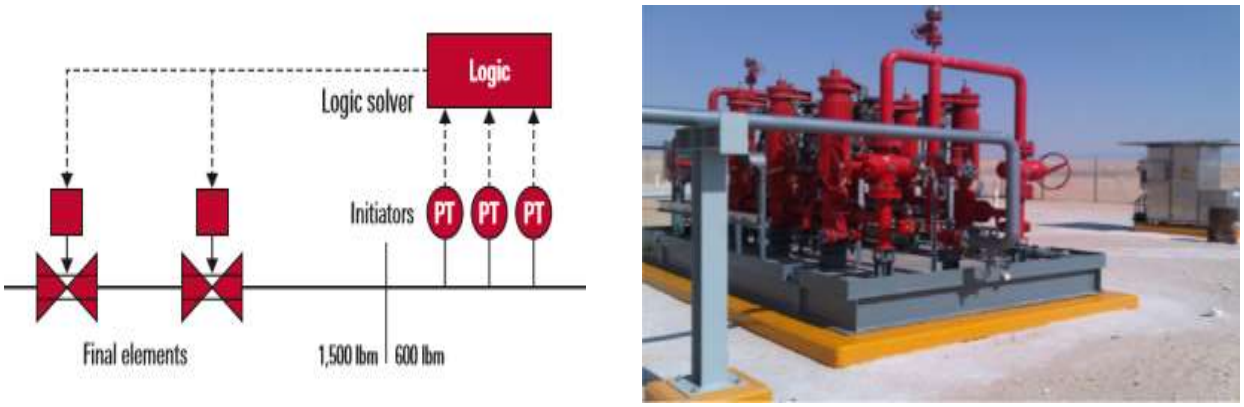


Figure 2.18 : HIPPS Électronique [35].

2.13.5. Principe de fonctionnement

La fonction principale de HIPPS est de détecter les conditions de haute pression et de fermer les vannes d'isolement pour protéger les infrastructures en aval les moins bien notées. Le système fonctionne de manière autonome et est indépendamment du processus de l'arrêt de l'installation (PSD), de l'arrêt d'urgence (ESD) ou du contrôle de système. Les HIPPS sont conçus pour être fermés en fonction du signal d'un événement de surpression et peuvent être configuré pour fonctionner sur d'autres événements, comme une perte de puissance motrice du signal de l'instrument. Elle se ferme généralement en cas de perte d'air d'instrument, d'énergie hydraulique, d'énergie électrique ou de signal d'instrument. Chaque boucle HIPPS est indépendante. Un HIPPS est conçu avec des fonctions de sécurité redondantes pour réduire le risque de défaillance à la demande et maximiser la disponibilité. Le fonctionnement d'un HIPPS est illustré dans ces étapes :

1. Les transmetteurs de pression surveillent la pression de la canalisation par rapport à une limite prédéfinie. Le nombre et les types d'émetteurs et leurs systèmes de vote est une fonction de la classification SIL. Dans un transmetteur de pression HIPPS sont configurés pour un vote 2oo3 pour atteindre SIL 3.
2. Le solveur logique HIPPS capture les signaux des transmetteurs de pression et effectue une logique de vote 2oo3, avant d'activer les solénoïdes et de fermer la canalisation. Deux types de solveurs logiques sont disponibles : PLC et câblé, tous deux offrent une redondance évolutive.
3. Le dernier élément ferme la canalisation. Les vannes sont pacifiques et conçues pour entretien [2][35].

2.13.6. Utilisation de HIPPS

Ils sont utilisés dans l'industrie pétrolière et gazière ainsi que dans les installations de gaz naturel liquéfié (GNL) et des systèmes de transport et de stockage pour assurer la sécurité des canalisations, des navires et des colis de traitement. Quelques exemples d'application de HIPPS dans l'industrie du pétrole et gaz sont mentionnés ci-dessous :

1. Connexion à longue distance de haute pression d'un réservoir marginal avec installations la surface existante.
2. Puits à haute pression connecté à une conduite d'écoulement à basse pression.
3. Protection des colonnes montantes flexibles contre les hautes pressions (structures flottantes).
4. Canalisations et stations de compression.

5. Systèmes de torchage.
6. Installations de séparation et de traitement.
7. Installations à gaz, stockage de gaz.
8. Perte de fluide de refroidissement / puissance dans les processus en aval comme le circuit de propane, circuits de réfrigération, colonnes de distillation, réchauffeurs d'amines. [5][35].

2.13.7. Avantages et inconvénients

Le HIPPS présente de nombreux avantages qui couvrent trois domaines différents :

Économique : l'utilisation de HIPPS protège de nombreux actifs tels que les vannes et les canalisations et contribuent beaucoup à la conception de ces équipements, comme avec l'existence de HIPPS la conception des canalisations n'auraient pas besoin de supporter d'énormes niveaux de pression, ce qui réduirait considérablement le coût, HIPPS conduira à des tuyaux et des navires plus légers et moins chers avec une capacité plus élevée qui conduire à une réduction des coûts de transport et de stockage.

Environnemental : l'utilisation de HIPPS rendra les autres systèmes de détente assez obsolètes, les systèmes de décompression conventionnels utilisés pour libérer les flammes dans l'air et HIPPS empêcheront cette opération.

Sécurité : HIPPS est un système très fiable qui empêchera la sur-pressurisation qui entraînera un ensemble d'équipements bien protégés comprenant des tuyaux, des vannes et des contrôleurs. [36]

HIPPS a également des inconvénients comme mentionné ci-après :

-Il est une mauvaise pratique de sécurité d'installer et de compter sur des dispositifs de décompression dans les services où le dimensionnement du dispositif est mal compris ou connu pour être inadéquat en raison de réactions chimiques, fluides de phase, ou bouchage. Dans ces applications, des alternatives, telles que HIPPS, doivent être examinées pour assurer l'atténuation des événements de surpression.

-Le principal inconvénient de HIPPS est la documentation soignée, la conception, le fonctionnement, la maintenance, et des tests pour garantir la conformité à la norme. Des Compétences réglementaires et des exigences d'application spécifique doivent être déterminées. Dans certains cas, l'approbation des autorités locales est requise. Les exigences réglementaires

et normatives doivent être comprises par toutes les parties, y compris la gestion de l'établissement et instrumentation et électrique, exploitation, et de maintenance personnelle.

- Les systèmes HIPPS sont plus complexes et nécessitent le bon fonctionnement de plusieurs appareils pour atteindre les performances d'un seul dispositif de décompression.

Enfin, il n'y a pas de tampon en caoutchouc « approuvé » dans aucune réglementation ou norme pour l'utilisation de HIPPS pour la réduction de la taille des dispositifs de décharge et du système d'évasement associé pour récipients sous pression ou canalisations. Des mises en garde importantes sont faites dans les normes et pratiques recommandées, concernant l'utilisation de HIPPS. Quelle que soit la documentation créée, l'utilisateur a la responsabilité de fournir un fonctionnement sûr et respectueux de l'environnement. [35]

2.13.8. Cycle de vie HIPPS

Le cycle de vie de la sécurité est un système de gestion qui s'efforce d'assurer un système fonctionnellement sûr si toutes les étapes sont correctement mises en œuvre. Le concept de niveau d'intégrité de sécurité (SIL) est introduit pour assurer cette fonctionnalité de système. SIL est une mesure du niveau de réduction des risques qu'une fonction instrumentée de sécurité (SIF) est capable de fournir, comme défini par sa probabilité moyenne de Panne (défaillance) à la demande (PFDavg). Le montant requis de réduction du risque est une fonction du risque non atténué du processus.

La différence entre le risque de processus et le risque tolérable est la capacité de réduction du risque requise du système de sécurité, qui est le HIPPS dans ce cas.

Le HIPPS est alors conçu pour atteindre ou dépasser ce niveau de performance. La quantité de La « sécurité » fournie par un HIPPS avec un SIL donné est catégorisée en fonction de la probabilité moyenne de Panne à la demande (PFDavg) comme indiqué dans le tableau 2.4 [35]

Tableau 2. 4 : Niveau d'intégrité de sécurité (SIL) [3].

Niveau d'intégrité de sécurité (SIL)	Probabilité de panne à la demande (PFD)	Facteur de Reduction de Risques
SIL 4	0.001% à 0.01%	100,000 à 10,000
SIL 3	0.01% à 0.1%	10,000 à 1,000
SIL 2	0.1% à 1%	1,000 à 100
SIL 1	1% à 10%	100 à 10

2.13.8.1. Probabilité de défaillance à la demande (PFD)

Une valeur qui indique la probabilité d'un échec du système à répondre à une demande. La probabilité moyenne qu'un système ne réponde pas à une demande dans un intervalle de temps spécifié est appelée PFDavg. PFD équivaut à 1 moins la disponibilité de sécurité.

2.13.8.2. Niveau d'intégrité de sécurité (SIL)

Le SIL est une Mesure quantifiable du risque utilisée comme un moyen d'établir des objectifs de performance de sécurité pour le HIPPS.

2.13.8.3. Fonction instrumentée de sécurité (SIF)

Une fonction de sécurité avec un niveau d'intégrité de sécurité spécifié, qui est nécessaire pour atteindre la sécurité fonctionnelle. Une fonction instrumentée de sécurité peut être soit une fonction de protection instrumentée de sécurité (définir SIPF) ou une fonction de commande instrumentée de sécurité (définir SICF). [2][3]

2.13.9. Sélection du niveau d'intégrité de sécurité (SIL) pour un HIPPS

Chaque scénario de surpression où le soulagement conventionnel est insuffisant doit être évalué par une équipe d'experts en génie des procédés, opérations, maintenance, système de contrôle ingénierie et sécurité. Cette équipe évaluera le risque, déterminera si un HIPPS convient à l'application et spécifiez un niveau d'intégrité de sécurité (SIL) approprié pour que la fonction de sécurité atténuer le danger. Il existe des objectifs multiformes lors de la spécification d'une exigence SIL pour HIPPS, en particulier lorsque l'on considère le nombre de codes et de normes à respecter. À minimum, le risque doit être réduit pour atteindre tous les objectifs suivants :

1. S'assurer que les directives de gestion des risques de l'entreprise sont respectées (comme tout autre SIF utilisé dans un SIS).
2. Assurez-vous que la pression de service maximale autorisée (MAWP) d'un récipient sous pression est plus élevée que la pression la plus élevée que le système peut raisonnablement atteindre.

Le HIPPS est spécifié pour être conforme aux exigences de performance SIL 3, comme prévu dans CEI 61508. [3]

2.13.10. HIPPS contre l'arrêt d'urgence (Emergency Shutdown):

Le HIPPS est un système de sécurité spécifique à l'application pour empêcher la surpression d'une canalisation, et dommages qui en résultent à l'installation et à l'équipement. C'est la dernière ligne de défense en cas de sur incident de pressurisation et ne doit pas être confondu avec un système d'arrêt d'urgence (ESD).Un système (ESD) permet un arrêt sûr et ordonné d'un processus. HIPPS est une réponse d'urgence à une montée en pression fermant rapidement la canalisation, le moment de la fermeture dépendra sur le volume protégé.

Une fois activé, le HIPPS s'éteindra automatiquement et isolera la source de la pression, avant que la pression de conception du système ne soit dépassée, évitant ainsi un Perte de confinement. En effet, HIPPS crée une barrière entre une haute pression et une basse pression de la section de tuyau. [33]

2.14. Conclusion

Les systèmes instrumentés de sécurité sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. La norme générique CEI 61508 et sa norme fille CEI 61511 pour le secteur des procédés continus sont des normes de référence pour la spécification et la conception de ce type de systèmes (SIS). Les niveaux d'intégrité de sécurité issus de la norme sont des objectifs de sécurité utiles à l'évaluation des risques. Ils donnent une mesure de la réduction du risque obtenue par les moyens de protection fournis par le SIS. La détermination du niveau d'intégrité de sécurité dépend du calcul de la probabilité de défaillance sur demande (PFD_{avg}).

Au cours de ce chapitre, nous avons défini les HIPPS, qui sont un cas particulier de système instrumenté de sécurité, qui fera l'objet de notre application détaillée dans le chapitre4. Le HIPPS est spécialisé dans la protection des systèmes contre la haute pression afin d'éviter les catastrophes. HIPPS a prouvé son efficacité pour la protection et c'est donc le meilleur choix pour protéger les installations contre les catastrophes potentielles de divers aspects (protection de l'économie de l'environnement) comme en termes de vitesse d'isolation de l'installation le HIIPPS est mieux que l'arrêt d'urgence (ESD) car il dispose d'un système indépendant de celui-ci du siège de l'unité dans un délai ne dépassant pas 2 secondes également. Il est équipé d'une duplication des composants pour assurer un fonctionnement continu en cas d'endommagement de l'un de ses composants.

Chapitre 3

Défaillances de Cause Commune (DCCs)

3.1. Introduction

L'objectif de ce troisième chapitre de présenter certaines définitions relatives aux défaillances de la cause commune (DCCs), en expliquant leurs naissances leurs causes, et les moyens de défense contre ces pannes. Par la suite nous abordons les méthodes de quantification de ce type de défaillance. Les DCCs sont des défaillances en fonctionnement ou à la sollicitation pouvant affecter simultanément plusieurs composants d'un système et dûes à une même cause.

Les DCCs affectent des groupes de composants identiques ou similaires, redondants, réalisant la même fonction et œuvrant dans des conditions comparables. Les DCCs sont réduites par la diversité, mais jamais complètement. L'étude des Défaillances de Causes Communes dans les systèmes programmés constitue une problématique de recherche très importante dans les domaines du nucléaire, de la pétrochimie, de l'aérospatial….

Les DCCs constituent un sous ensemble de l'ensemble des défaillances dépendantes, ou sont l'ensemble d'évènements dépendants affectant deux composants ou plus, au même moment ou dans un petit intervalle de temps et résultant directement d'une cause partagée.

3.2. Définitions des DCCs suivant le type d'industrie

3.2.1. Industrie pétrolière et gazière

La CEI 61508 est largement utilisée dans les sociétés pétrolières et gazières, qui est la norme de base pour que les industries développent leurs propres normes. Les normes développées sur la base de la CEI 61508 sont présentées dans la figure 3.1 [3].

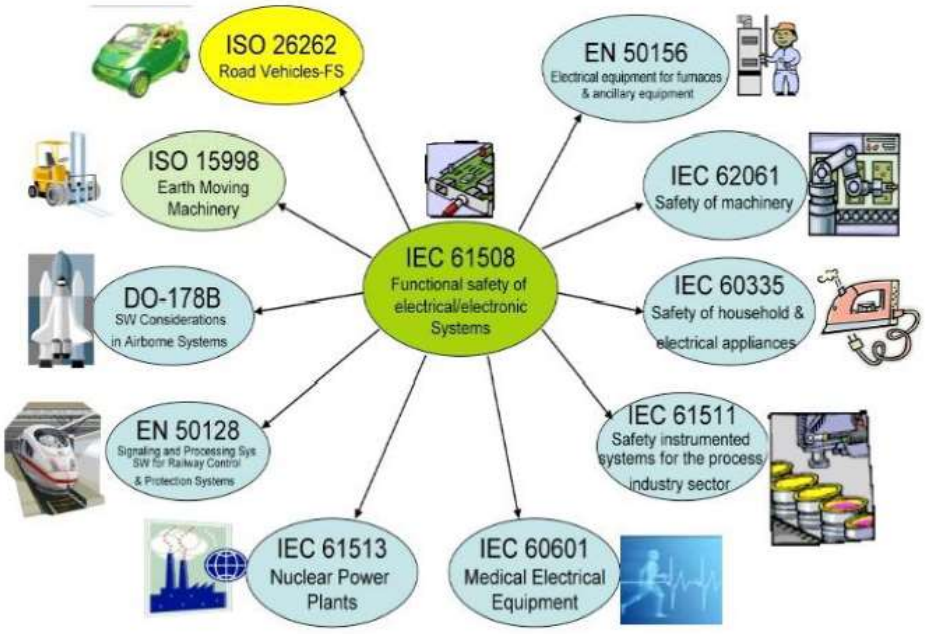


Figure 3.1 : Déclinaison de la norme CEI 61508 en normes filles [3]

Définition CEI 61508-04 : la DCC est Une défaillance qui résultant d'un ou de plusieurs événements, provoquant des défaillances simultanées de deux canaux distincts dans un système à canaux multiples, conduit à la défaillance du système.

Dans cette définition, la description des «défaillances simultanées de deux canaux séparés dans un système à canaux multiples» et «conduisant à une défaillance du système» ne peut pas être utilisée ensemble dans certaines conditions. Par exemple, dans la configuration 2oo3 ou 2oo4, deux canaux distincts défaillants en même temps n'appartiennent pas aux DCC car le système fonctionne toujours. La redondance est largement utilisée dans les systèmes instrumentés de sécurité pour améliorer la fiabilité du système. Cependant, les composants redondants exposent le système aux DCC. Par conséquent, la description de la DCC dans la CEI 61508 ne peut pas être utilisée pour la structure KooN.

La norme est principalement utilisée pour l'industrie pétrolière et gazière et l'industrie des procédés, par conséquent, cette définition est la même que celle citée dans la norme CEI 61511 qui est utilisée pour l'industrie des procédés [37].

3.2.2. Industrie mécanique

Selon la norme BS EN ISO 12100(2010), les DCC dans l'industrie des machines sont définit comme :

Défaillances de différents éléments, résultant d'un seul événement, où ces défaillances ne sont pas des conséquences les unes des autres.

BS EN ISO 12100(2010) est Sécurité des machines - Principes généraux de conception - Évaluation et réduction des risques (ISO 12100: 2010). Elle est différente de la norme BS EN 62061 : 2005. BS EN 62061: 2005 est Sécurité des machines - Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables liés à la sécurité. La définition du DCC dans la norme BS EN 62061(2005) est la suivante :

Une DCC est le résultat d'un ou plusieurs événements, provoquant des défaillances coïncidentes de deux ou plusieurs canaux séparés dans un sous-système à canaux multiples (architecture redondante), conduisant à la défaillance d'une Fonction de Commande Relative à la Sécurité (SRCF). (IEC 61508-4, 3.6.10 modifié). Dans la norme ISO 12100, «les défaillances ne sont pas des conséquences les unes des autres» sont des défaillances indépendantes, ce qui signifie que la défaillance d'un composant n'affectera pas les fonctions des autres composants. La définition du DCC dans l'ISO 62061 est modifiée sur la base de la CEI 61508-4. Comme décrit ci-dessus, la définition ne convient pas à l'architecture redondante. Cependant, la norme CEI 62061 modifie cette déclaration inexacte et présente qu'elle convient au sous-système d'architecture redondante. Cela signifie qu'une défaillance de deux ou plusieurs canaux entraînera également les défaillances du sous-système [37].

3.2.3. Industrie nucléaire

L'Agence de l'Energie Nucléaire (AEN) définit la DCC comme suit :

Défaillance dépendante dans laquelle deux ou plusieurs états de défaillance de composant existent simultanément, ou dans un court intervalle de temps, et sont le résultat direct d'une cause partagée.

Dans cette définition, la défaillance dépendante signifie, défaillance dont la probabilité ne peut être exprimée comme le simple produit des probabilités inconditionnelles des événements individuels qui l'ont provoquée. (CEI 61508, 2010).

Il s'agit d'environ deux ou plusieurs états de défaillance de composants qui existent simultanément en raison d'une cause partagée, qui n'incluent pas les défaillances en cascade. Les défaillances en cascade sont des défaillances de composants provoquées par une autre défaillance, et ce n'est pas le résultat direct d'une cause partagée. Tous les échecs cachés peuvent être révélés pendant le test fonctionnel ; par conséquent, un intervalle de temps court signifie qu'au moins un composant a échoué au prochain test fonctionnel [6][37].

3.2.4. Industrie spatiale

Selon le chercheur scientifique, Stamatelatos (2002a), la DCC est défini comme :
Échec (ou état indisponible) de plusieurs composants en raison d'une cause partagée lors de la mission du système.

Dans cette définition, les DCCs sont produits pendant la période d'exécution d'une tâche, et non pendant une période ou un intervalle de temps spécifique. Pour l'industrie aéronautique, la mission du système est la période de temps pendant laquelle un avion est en l'air pour un vol [34].

3.2.5. Définition de Watson

Sur la base des différentes définitions des DCC, Smith et Watson (1980) ont examiné neuf définitions et suggèrent que les six attributs suivants doivent être inclus dans la définition des DCC [6] :

1. Les composants concernés ne peuvent pas fonctionner comme requis.
2. Plusieurs pannes existent dans (mais sans s'y limiter) les configurations redondantes.
3. Les échecs sont de type «premier en ligne» et non le résultat de défaillance en cascade.
4. Les pannes se produisent dans un intervalle de temps critique défini (par exemple, le temps pendant lequel un avion est dans l'air pendant un vol).
5. Les pannes sont dues à un seul défaut sous-jacent ou à un phénomène physique (la cause commune des pannes).
6. L'effet des défaillances doit entraîner une désactivation majeure de la capacité du système à fonctionner comme requis.

Le premier attribut signifie que la DCC conduit à la défaillance des composants et est incapable d'exécuter la fonction requise. Le deuxième attribut présent que plusieurs défaillances peuvent exister au sein d'une architecture KooN, ce qui a modifié la déclaration peu claire de la norme CEI 61508. Pour le troisième attribut, «premier en ligne» signifie que la défaillance est causée par la cause racine comme l'erreur humaine, l'environnement, non affecté par la défaillance de l'autre composant. En d'autres termes, les défaillances en première ligne signifient des défaillances indépendantes et les défaillances en cascade ne sont pas incluses dans cette définition. Le quatrième attribut montre l'intervalle de temps pour l'apparition des DCC, qui est un intervalle de temps critique défini. L'intervalle de temps critique est différent selon les systèmes. Pour SIS, intervalle de temps signifie la période de temps entre deux tests

fonctionnels pour un même système. Cependant, pour l'industrie aéronautique, l'intervalle de temps critique est l'avion en vol pour une mission.

En se basant sur ces six attributs, Smith et Watson (1980), ont formulé la définition suivante pour la DCC :Incapacité de plusieurs éléments de première ligne à fonctionner comme requis dans une période critique définie en raison d'un défaut sous-jacent unique ou de phénomènes physiques tels que l'effet final est jugé comme une perte d'un ou plusieurs systèmes [34].

3.3. Défaillances dépendantes et indépendantes

3.3.1. Défaillances indépendantes :

Lorsque les éléments d'un système sont indépendants, cela implique que [37] :

- La défaillance d'un élément n'a aucune influence fonctionnelle sur les autres éléments du système.
- La défaillance d'un élément a un effet physique négligeable sur les autres éléments du système.
- En ajoutant des éléments redondants au système, la probabilité de défaillance peut être réduite autant que nous le souhaitons.

3.3.2. Défaillances dépendantes

3.3.2.1. Dépendance intrinsèque

Situation dans laquelle l'état fonctionnel d'un composant est affecté par l'état fonctionnel d'autres composants.

Sous-classes :

- Dépendance aux exigences fonctionnelles.
- Dépendance d'entrée fonctionnelle.
- Défaillances en cascade.

3.3.2.2. Dépendance extrinsèque

Situation dans laquelle la dépendance ou le couplage n'est pas inhérent ou prévu dans les caractéristiques fonctionnelles du système.

Les dépendances extrinsèques peuvent être liées à :

- Stress physiques ou environnementaux.
- Intervention humaine.

3.3.3. Défaillances en cascade

Défaillances en cascade : une séquence d'échecs d'élément où le premier échec déplace sa charge vers un ou plusieurs éléments à proximité de sorte que ceux-ci échouent et déplacent à nouveau leur charge vers un autre élément, etc.

Les Défaillances en cascade sont parfois appelés effet Domino [36].

3.4. Causes des DCCs

D'après Rausand (2011), les causes des DCC sont classées en deux catégories [34]:

3.4.1. Cause profonde

La cause principale de la défaillance d'un composant, si elle est corrigée, peut empêcher la récurrence de cette défaillance et des défaillances similaires.

3.4.1.1. Causes profondes typiques

On peut distinguer entre les causes pré-opérationnelles et opérationnelles :

3.4.1.1.1. Causes profondes pré-opérationnelles

Des erreurs de conception, de fabrication, de construction, d'installation et de mise en service [34].

3.4.1.1.2. Causes profondes opérationnelles : on peut les classés comme suit :

- Opération et maintenance : procédures de maintenance et d'exploitation, d'exécution, de compétence et de planification inadéquates.
- Contraintes environnementales : exposition interne et externe en dehors de l'enveloppe de conception ou événements énergétiques tels que tremblement de terre, incendie, inondation [5].

3.4.2. Facteur de couplage

Facteur qui rend plusieurs composants susceptibles de tomber en panne à partir d'une seule cause partagée.

3.4.2.1. Facteurs de couplage typiques

Rechercher des facteurs de couplage revient à rechercher des similitudes [5][6] :

- Même conception (principes).
- Même matériel.
- Même fonction.
- Même logiciel.
- Même personnel d'installation.
- Même personnel de maintenance et d'exploitation.
- Mêmes procédures.
- Même interface système / article.
- Même environnement.
- Même emplacement (physique).

Les causes profondes expliquent pourquoi les composants ont échoué. Les facteurs de couplage expliquent pourquoi plusieurs composants sont affectés, c'est-à-dire la relation entre les composants affectés. Les causes profondes sont normalement identifiées par l'analyse des causes profondes (RCA), appuyée par des listes de contrôle des causes profondes génériques (US DOE, 1992). Les causes profondes et les facteurs de couplage pourraient conduire à des DCC, comme l'illustre la figure 3.2 [34].

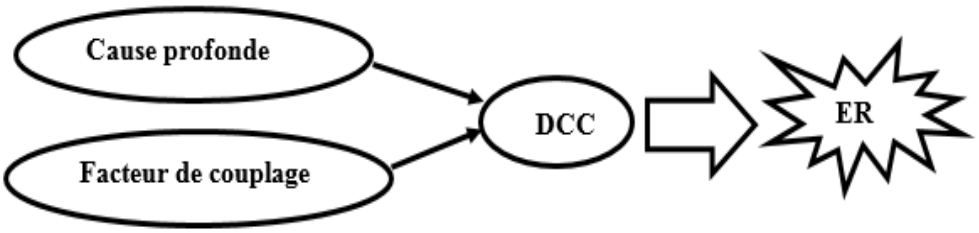


Figure 3.2 : Causes des défaillances de cause commune (DCCs) [38].

Des exemples de facteurs de couplage ont les mêmes conceptions, les mêmes procédures ou le même personnel de maintenance ou d'exploitation. La majorité des facteurs de couplage contribuant aux DCC sont liés aux aspects opérationnels (Miller, 2000). Cependant, pour économiser de l'argent et faciliter l'exploitation et la maintenance, les procédures des industries sont devenues de plus en plus standardisées. Par conséquent, des facteurs de couplage apparaissent.

3.5. Classification des DCCs

En pratique, les fiabilistes utilisent une classification basée sur des causes génériques pour analyser ce type de défaillance très important pour la sûreté des centrales nucléaires. Ils considèrent que les DCC qui affectent les composants d'un système résultent soit d'agressions externes, soit d'erreurs humaines commises à la conception, à la fabrication, ou bien en exploitation. Les défaillances peuvent être divisées, selon la nature de leurs causes en quatre grandes classes :

1. Les agressions de l'environnement : événements liés à l'environnement externe ou interne à l'installation mais extérieurs du système élémentaire considéré.
2. Les erreurs de conception : erreurs commises au cours des études des composants et du système élémentaire qui compromettent ses missions.
3. Les erreurs de fabrication : erreurs commises au cours de la fabrication des composants et du système élémentaire.
4. Les erreurs d'exploitation : erreurs commises au cours de l'exploitation des composants et du système élémentaire reconnus apte à fonctionner auparavant.

Une classification des causes des DCC, qui est présentée dans le tableau II. [38]:

Tableau 3.1 : Classification ICDE des causes courantes (NEA, 2004) [3].

Classification des causes profondes	Classification du facteur de couplage
• État des autres composants • Conception, fabrication ou insuffisance de construction	• Matériel identique / similaire : - Conception du système

• Actions humaines • Maintenance • Interne au composant • Insuffisance de procédure • Stress environnemental anormal	- Conception de matériel - Défaut de qualité matérielle • Conditions opérationnelles identiques / similaires : - Calendrier de maintenance / test - Procédure de maintenance / test - Personnel de maintenance / test - Procédure d'opération - Personnel d'exploitation • Exposition environnementale identique / similaire : interne ou externe.

De nombreux auteurs et études ont étudié les causes profondes des événements DCC. Sur la base de la modélisation des défaillances de cause commune : état et tendances (2008), les tableaux 3.2, 3.3 et 3.4 suivants sont les schémas de classification proposés pour ces événements [17].

Tableau 3.2 : Causes profondes des événements DCC (conception, fabrication, construction, installation et mise en service)[6]

Type de cause	Exemples de cause spécifique
Exigences de conception et inadéquation des spécifications	Le concepteur ne parvient pas à prévoir un accident Le concepteur ne reconnaît pas ce une action protectrice est nécessaire
Erreur de conception ou insuffisance en réalisation de conception	Installations de fonctionnement inadéquates, maintenance, test ou étalonnage Composants inadéquats Assurance qualité inadéquate
Limitations de conception	Financier/Spatial
Construction / installation / mise en service	Non-respect des instructions Contrôle de construction inadéquat

	Inspection inadéquate Tests inadéquats
Erreur de fabrication ou insuffisance	Non-respect des instructions Contrôle de fabrication inadéquat Inspection inadéquate Tests inadéquats

Tableau 3.3 : Causes profondes des événements DCC (fonctionnement) [6]

Type de cause	Exemples de cause spécifique
Absence de procédures	Absence de procédures de réparation Absence de procédures de test ou d'étalonnage
Procédures défectueuses	Procédures de réparation défectueuses Procédures de test ou d'étalonnage défectueuses
Non-respect des procédures	Non-respect des procédures de réparation Omission de suivre les procédures de test ou d'étalonnage
Insuffisance de supervision	Procédures de surveillance inadéquates Action ou surveillance inadéquate la communication
Des problèmes de communication	Communication entre le personnel de maintenance
Insuffisance de formation	Formation des opérateurs à la gestion des urgences situations

Tableau 3.4 : Causes profondes des événements DCC (environnementaux) [6].

Type de cause	Exemples de cause spécifique
Stress	Réactions chimiques (corrosion) Panne électrique Interférence électromagnétique Interaction des matériaux (érosion) Humidité Pression Radiation Température Vibration
Énergique	Tremblement de terre Feu Inonder Charges d'impact

3.6. Événement DCC

Événement DCC : événement impliquant la défaillance d'un ensemble spécifique de composants en raison d'une cause commune [6].

- Un événement DCC implique deux ou plusieurs défaillances d'éléments.
- Les défaillances d'éléments d'un événement DCC peuvent se produire simultanément ou dans un intervalle de temps (court) spécifié.
- Le fait que les défaillances d'éléments se produisent ou non en même temps dépend de la cause partagée.
- L'événement DCC est parfois appelé événement de base de cause commune (CCBE).

Si on considère par exemple le cas d'un système de m détecteurs de gaz installés dans une salle de production, une cause commune d'un événement DCC potentiel est l'augmentation de l'humidité dans la pièce. Cette cause commune entraînera une probabilité accrue de

défaillance du détecteur, mais les défaillances ne se produiront normalement pas en même temps. Le temps entre les défaillances du détecteur peut être assez long [6].

3.7. Groupe de composants de cause commune (GCCC)

Il s'agit d'un groupe de composants généralement similaires (dans la mission, le fabricant, la maintenance, l'environnement, etc.) qui sont considérés comme ayant un potentiel élevé de défaillance en raison de la même cause ou des mêmes causes.

Les composants identiques assurant la redondance dans le système doivent toujours être affectés au même GCCC.

Différents composants redondants dont les pièces sont identiques doivent toujours être affectés à un GCCC malgré leur diversité.

La sensibilité d'un groupe de composants aux DCC dépend non seulement de leur degré de similitude, mais aussi de l'existence / de l'absence de mesures défensives (barrières) contre les DCC [38].

3.8. Approche de modélisation

1. Développer un modèle logique du système (par exemple, un arbre de défaillance ou un schéma fonctionnel de fiabilité).
2. Identifier les groupes de composants de cause commune pertinents (CCCG).
3. Identifier les causes profondes pertinentes et les facteurs / mécanismes de couplage.
4. Évaluer l'efficacité des défenses DCC.
5. Établir des modèles explicites.
6. Inclure des modèles implicites.
7. quantifier la fiabilité et interpréter les résultats [38].

3.9. Types de modélisation des défaillances de cause commune

Il existe deux types de modélisation pour les DCC, il s'agit de :

- La modélisation explicite.
- La modélisation implicite.

3.9.1. Modélisation explicite

Lorsque les causes spécifiques des DCC peuvent être identifiées et que les causes sont des échecs dépendants, il est préférable de modéliser explicitement les DCC. Les événements de base dans un modèle d'arbre de défaillance sont considérés comme des causes spécifiques. Par conséquent, il est modélisé explicitement. Des exemples de causes explicites sont les erreurs humaines, les pannes de services publics ou les événements environnementaux. L'un des avantages de la modélisation explicite est que toutes les causes profondes des DCC peuvent être identifiées.

La cause partagée est identifiée comme un événement / élément de base distinct dans le modèle de fiabilité [1].

3.9.2. Modélisation implicite

Lorsque les causes des DCC sont difficiles à identifier ou ne peuvent pas être identifiées, les DCC seront modélisés implicitement. La limitation de la modélisation implicite est que les causes des défaillances ne peuvent pas être clairement identifiées.

On peut citer les modèles implicites suivants [1]:

- Le modèle des paramètres de base (BP).
  - Modèle à facteur C.
  - Le modèle de lettres grecques multiples (Multiple Greek Letter : MGL).
  - Le modèle à facteur bêta multiple (Multiple Beta Factor : MBF).
  - Le modèle du taux de défaillance binomiale (Binomial Failures Rate : BFR)
  - Le modèle Alpha Factor (Alpha Factor : AF).

La modélisation explicite et implicite sont respectivement illustrées par les figures 3.3 et 3.4.

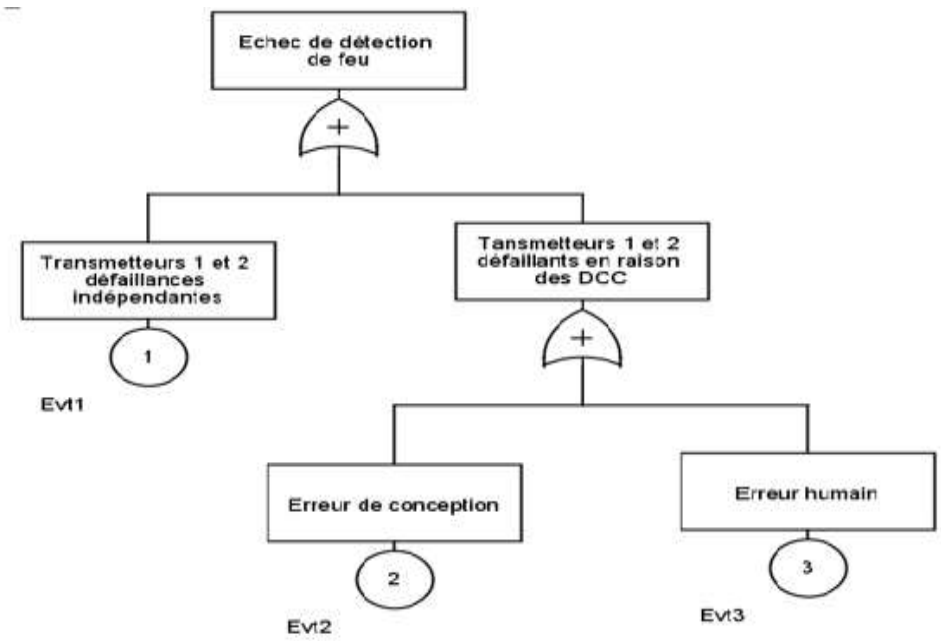


Figure 3.3. Modélisation explicite des DCCs [38].

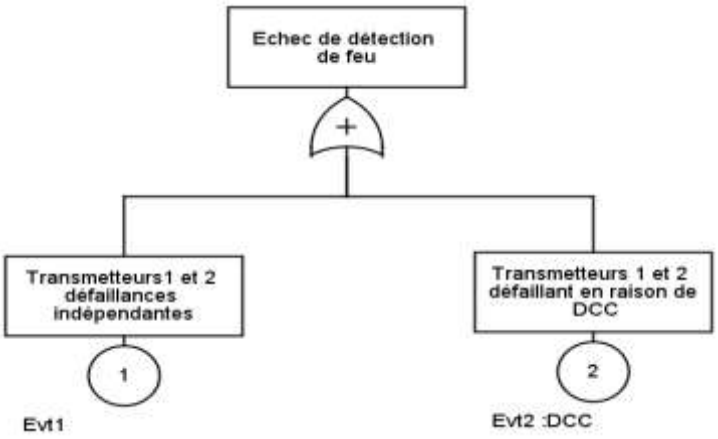


Figure 3.4 : Modélisation implicite des DCCs. [38]

3.10. Multiplicité de Défaillance

La Multiplicité de défaillance est Le nombre d'éléments dans un groupe qui échoue réellement dans l'événement DCC.

On peut distinguer entre :

- Défaillance complet (mortel) : tous les éléments du groupe échouent - cela est généralement associé à des interactions environnementales, humaines extrêmes, des exigences très dépendantes ou des interactions d'entrée.
- Défaillance partielle (non létal) plus d'un, mais pas tous les éléments échouent [38].

3.11. Modèles des Défaillances de cause commune

Les défaillances de mode commun peuvent être introduites dans l'évaluation des performances des systèmes de sécurité [19]. Les paramètres de calcul peuvent être détermines à partir de données issues du retour d'expérience. Etant donné la difficulté a obtenir de telles données, des méthodes paramétriques de modélisation et de quantification des DCC ont été développées, tels que ; le modèle du facteur β, La méthodes des lettres grecques multiples (MGL), ou bien le modèle du facteur α.

3.11.1. Méthode du facteur Alpha : α

La méthode du facteur α constitue une amélioration par rapport a la méthode MGL, car les paramètres peuvent être estimes à partir de statistiques d'événements observes et plus particulièrement à partir des données sur les défaillances du système et non des composants [20].

L'estimation des paramètres de la méthode du facteur α, est assez difficile à obtenir malgré l'existence et l'utilisation de méthodes d'approximations. L'estimation de ces paramètres peut être obtenue en introduisant un paramètre intermédiaire base sur les événements des défaillances de cause commune qui est plus facile à estimer à partir des données observées plutôt qu'à partir des défaillances du système. Cette estimation est à la base du modèle du facteur α [21].

3.11.2. Méthode du facteur Beta : β

Cette méthode a été introduite par Fleming [39]. C'est probablement le modèle le plus répandu pour traiter les DCC. La principale raison de son succès est son extrême simplicité d'utilisation [22]. Bien qu'elle puisse servir à modéliser des dépendances entre des équipements différents et non nécessairement redondants, dans la pratique, elle est le plus souvent appliquée aux systèmes redondants formes de composants identiques.

Cette méthode considère les possibilités suivantes :

- un seul composant tombe en panne du fait d'une défaillance indépendante.
- tous les composants du groupe de DCC tombent en panne simultanément, avec une seule et même cause de défaillance.

Le facteur β caractérisant une défaillance en fonctionnement peut ne pas être le même que celui relatif à une défaillance à la sollicitation pour le même groupe de composants. Le paramètre β est défini comme étant égal au pourcentage de défaillances résultant d'une cause commune [5].

Le modèle du facteur β utilisé est le modèle le plus répandu pour introduire les défaillances de mode commun dans les analyses de fiabilité [24], et pour calculer la part de ces défaillances sur la probabilité de défaillance d'un système [39].

3.11.3. Méthode des lettres grecques multiples (MGL)

Cette méthode est une extension du modèle du facteur β lorsque l'on considère plusieurs composants en redondance. Des paramètres supplémentaires sont ajoutés au facteur β pour traiter des niveaux élèves de redondance [39]. La probabilité totale de défaillance tient compte de l'effet de toutes les contributions indépendantes et de causes communes des différents composants. Les probabilités conditionnelles des défaillances de mode commun qu'un composant peut partager avec les composants d'un groupe de cause commune sont aussi considérées.

Les paramètres de cette méthode, sont constitués par :

- des taux de défaillance des composants qui tiennent compte des contributions des causes indépendantes et communes.
- des probabilités conditionnelles.

3.12. Description des différents modèles

3.12.1. Description du modèle facteur alpha

Facteur alpha ($\alpha_{k:m}$): fraction des événements de défaillance qui se produisent dans un groupe de m éléments et impliquent une défaillance d'exactement k éléments en raison d'une cause commune [18].

- Remarque :

Si, par exemple, $\alpha_{2:m} = 0{:}05$, cela signifie que 5% de tous les événements d'échec dans un groupe de m éléments est un DCC avec une multiplicité égale à 2.

Le modèle de facteur alpha définit les probabilités de défaillance de cause commune à partir d'un ensemble de rapports de fréquence de défaillance et de la probabilité de défaillance totale des composants Q_t. En termes de probabilités d'événement de base, les paramètres du facteur alpha sont définis comme [34].

$$\alpha_{k:m} = \frac{\binom{m}{k}.Q_{k:m}}{\sum_{k=1}^{m}\binom{m}{k}.Q_{k:m}} \qquad (3.1)$$

$\binom{m}{k}.Q_{k:m}$ est la probabilité d'un événement de défaillance impliquant exactement k éléments, et le dénominateur est la somme de ces probabilités.

$\alpha_{k:m}$ est donc la probabilité conditionnelle d'un DCC de multiplicité k, étant donné qu'un événement de défaillance s'est produit dans un groupe de m éléments.

- Exemple

$$\alpha_{1:3} = \frac{3.Q_{1:3}}{3.Q_{1:3} + 3.Q_{2:3} + Q_{3:3}}$$

$$\alpha_{2:3} = \frac{3.Q_{2:3}}{3.Q_{1:3} + 3.Q_{2:3} + Q_{3:3}}$$

$$\alpha_{3:3} = \frac{Q_{3:3}}{3.Q_{1:3} + 3.Q_{2:3} + Q_{3:3}}$$

Et $\alpha_{1:3} + \alpha_{2:3} + \alpha_{3:3} = 1$, comme prévu.

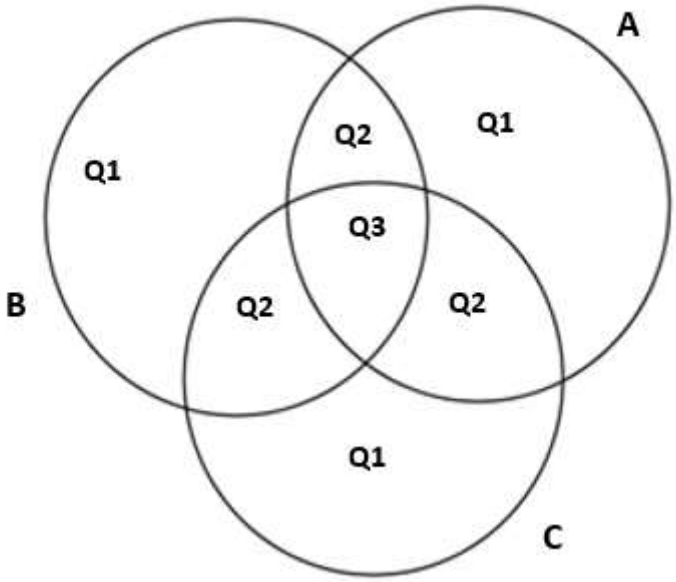


Figure 3.5 : Intersection entre Les $Q_{k:m}$ de l'exemple traité [34].

Q_t = la probabilité de défaillance totale d'un élément spécifique en raison de tous les événements indépendants et DCC.

La probabilité d'un DCC impliquant k éléments dépendra de la manière dont les éléments sont testés. Pour les tests simultanés, la probabilité est [34] :

$$Q_{k:m} = \frac{k}{\binom{m-1}{k-1}} \cdot \frac{\alpha_{k:m}}{\alpha_t} \cdot Q_t = \frac{m}{\binom{m}{k}} \cdot \frac{\alpha_{k:m}}{\alpha_t} \cdot Q_t \qquad (3.2)$$

$$\alpha_t = \sum_{k=1}^{m} k.\alpha_{k:m} \qquad (3.3)$$

Puisque le facteur alpha $\alpha_{k:m}$ est la fraction de tous les événements de défaillance qui impliquent exactement k éléments, le facteur peut être estimé comme :

$$\alpha_{k:m} = \frac{n_k}{\sum_{k=1}^{m} n_k} \qquad (3.4)$$

Pour déterminer la contribution DCC, il suffit donc d'estimer Q_t et de déterminer nk pour k = 1; 2;…;m

3.14.2. Description du modèle facteur Beta

Le modèle β représente le modèle mono-paramètre le plus répandu pour introduire les défaillances de mode commun dans les analyses de fiabilité et calculer la part de ces défaillances sur la probabilité de défaillance d'un système [39]. Il associe une fraction β du taux de défaillance d'un composant à un événement de cause commune (caractérisé par DCC) partagé par les autres composants du groupe. Ce modèle fait l'hypothèse que, lorsqu'un événement de cause commune apparaît, tous les composants du même groupe de composants de cause commune sont défaillants [3].

Si λ est le taux de défaillance d'un des composants d'un groupe de cause commune, les taux de défaillances à considérer seront [3] :

Pour les défaillances de mode commun : $\lambda_{dcc} = \beta.\lambda$ **(3.5)**

Pour les défaillances indépendantes : $\lambda_i = (1-\beta).\lambda$ **(3.6)**

Avec : $\lambda = \lambda_i + \lambda_{dcc}$ **(3.7)**

Le facteur p est défini par : $\beta = \lambda_{dcc} / \lambda = \lambda_{dcc} / \lambda_i+\lambda_{dcc}$ **(3.8)**

Pour une loi exponentielle et puisque les défaillances de mode commun et les défaillances indépendantes sont des événements indépendants, la probabilité de défaillance totale $Q_t(t)$ d'un composant s'écrit [3] [4]:

$$Q_t(t) = 1 - e^{-\lambda.t} = 1 - e^{-(\lambda i+\lambda dcc).t} \qquad (3.9)$$

Cette égalité se simplifie si on considère que $\lambda.t \ll 1$:

$$Q_t(t) = (\lambda_i+\lambda_{dcc}).t = Q_i(t)+Q_{dcc}(t) \qquad (3.10)$$

Avec : $Q_{dcc}(t)$: probabilité de défaillance d'un composant due à des causes communes.

$$Q_{dcc}(t) = 1- e^{-\beta.\lambda.t} = \beta.\lambda.t = \beta.Q_t(t) \qquad (3.11)$$

$Q_i(t)$: probabilité de défaillance indépendante d'un composant (non-due à des causes communes).

$$Q_i(t) = 1- e^{-(1-\beta).\lambda.t} = (1-\beta).\lambda.t = (1-\beta).Q_t(t) \qquad (3.12)$$

Dans le cas d'un système base sur un système 2/3 à 3 composants identiques et étant donne l'hypothèse de départ (tous les 3 composants sont affectés).on a [3] :

$$Q_1(t) = Q_i(t) = (1-\beta).Q_t(t) \quad (3.13)$$

$$Q_2(t) = 0 \quad (3.14)$$

$$Q_3(t) = Q_{dcc}(t) = \beta.Q_t(t) \quad (3.15)$$

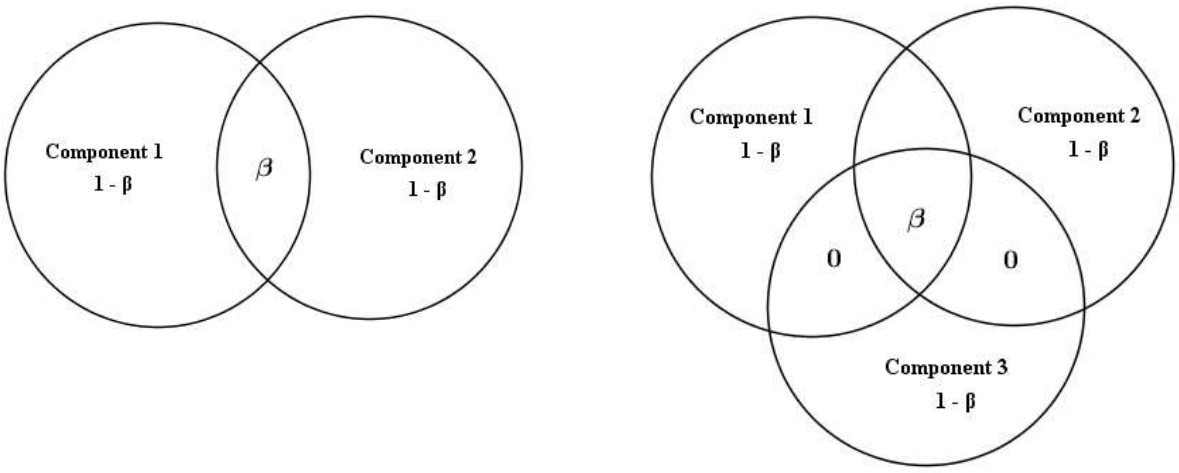


Figure 3.6. Répartition des défaillances selon le modèle Beta pour un système de 2 et 3 composants [3].

Ce modèle est donc base sur une estimation du taux de défaillance total du composant (par les bases de données classiques) et du facteur β. Il fournit des résultats corrects et plutôt plus mauvais que la réalité pour des niveaux de redondance inférieurs ou égaux à 4 [Fleming 1989] [25].

3.14.3. Description du Modèle lettre grecque multiple (MGL)

Le modèle MGL est le plus général d'un certain nombre d'extensions récentes du modèle à facteur bêta. Le modèle MGL était celui qui a été le plus fréquemment utilisé dans le cadre de l'exercice international de référence de fiabilité des défaillances de causes communes. Dans ce modèle, d'autres paramètres en plus du facteur bêta sont introduits pour rendre compte plus explicitement des redondances d'ordre supérieur et pour tenir compte de sous-groupes du groupe de composants de cause commune [38].

Les paramètres MGL se composent de la probabilité de défaillance totale du composant, qui comprend les effets de toutes les contributions de cause indépendante et commune à la défaillance de ce composant, et d'un ensemble de fractions de défaillance, qui sont utilisées pour quantifier les probabilités conditionnelles de toutes les manières possibles d'une cause commune la défaillance d'un composant peut être partagée avec d'autres composants du même groupe, en cas de défaillance d'un composant.

Pour un groupe de m composants redondants et pour chaque mode de défaillance donné, m paramètres différents sont définis. Par exemple, les quatre premiers paramètres du modèle MGL sont, comme précédemment [5].

Q_t probabilité de défaillance totale de chaque composant en raison de tous les événements de cause indépendante et commune.

β = probabilité conditionnelle que la cause d'une défaillance d'un composant soit partagée par un ou plusieurs composants supplémentaires, étant donné qu'un composant spécifique est en panne.
γ = probabilité conditionnelle que la cause d'une défaillance de composant partagée par un ou plusieurs composants soit partagée par deux ou plusieurs composants supplémentaires, étant donné que deux composants spécifiques ont échoué.

δ= probabilité conditionnelle que la cause d'une défaillance de composant partagée par deux composants ou plus soit partagée par trois composants supplémentaires ou plus étant donné que trois composants spécifiques ont échoué.

L'équation générale qui exprime la probabilité de k défaillances de composants spécifiques dues à une cause commune Q_k , en termes de paramètres MGL, est cohérente avec les définitions ci-dessus. Les paramètres MGL sont définis en termes de paramètres de modèle de paramètres de base pour un groupe de trois composants similaires comme [37] :

$$\mathbf{Q_t = Q_1^{(3)} + 2.Q_2^{(3)} + Q_3^{(3)}} \qquad \textbf{(3.16)}$$

$$\boldsymbol{\beta^{(3)}} = \frac{2.Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2.Q_2^{(3)} + Q_3^{(3)}} \qquad \textbf{(3.17)}$$

$$\boldsymbol{\gamma^{(3)}} = \frac{Q_3^{(3)}}{2.Q_2^{(3)} + Q_3^{(3)}} \qquad \textbf{(3.18)}$$

δ et les termes d'ordre supérieur sont identiques à zéro.

Pour un groupe de quatre composants similaires, les paramètres MGL sont :

$$\mathbf{Q_t = Q_1^{(4)} + 3.Q_2^{(4)} + 3.Q_3^{(4)} + Q_4^{(4)}} \qquad \textbf{(3.19)}$$

$$\boldsymbol{\delta^{(4)}} = \frac{Q_4^{(4)}}{3.Q_3^{(4)} + Q_4^{(4)}} \qquad \textbf{(3.20)}$$

Il est important de noter que les coefficients entiers dans les définitions ci-dessus sont une fonction de m, le nombre de composants dans le groupe de causes communes. Par conséquent, il est généralement inapproprié d'utiliser des paramètres MGL qui ont été quantifiés pour un

groupe de base m dans un groupe de base L, m ≠ L. Le même commentaire s'applique aux autres méthodes multi-paramètres similaires.

Les équations suivantes expriment la probabilité de pannes de plusieurs composants dues à une cause commune, Q_k en termes de paramètres MGL pour un groupe de causes communes à trois composants [37] :

$$Q_1^{(3)} = (1-\beta).Q_t(t) \quad (3.21)$$

$$Q_2^{(3)} = (1/2).\beta.(1-\gamma).Q_t(t) \quad (3.22)$$

$$Q_3^{(3)} = \beta.\gamma.Q_t(t) \quad (3.23)$$

Pour un groupe à quatre composants, les équations sont [26] :

$$\beta^{(4)} = \frac{3.Q_2^{(4)}+3.Q_3^{(4)}+Q_4^{(4)}}{Q_1^{(4)}+3.Q_2^{(4)}+3.Q_3^{(4)}+Q_4^{(4)}} \quad (3.24)$$

$$\gamma^{(4)} = \frac{3.Q_3^{(4)}+Q_4^{(4)}}{3.Q_2^{(4)}+3.Q_3^{(4)}+Q_4^{(4)}} \quad (3.25)$$

$$Q_1^{(4)} = (1-\beta).Q_t(t) \quad (3.26)$$

$$Q_2^{(4)} = (1/3).\beta.(1-\gamma).Q_t(t) \quad (3.27)$$

$$Q_3^{(4)} = (1/3).\beta.\gamma.(1-\delta).Q_t(t) \quad (3.28)$$

$$Q_4^{(4)} = \beta.\gamma.\delta.Q_t(t) \quad (3.29)$$

La généralisation de ceci est donnée par [26] :

$$Q_k = \frac{1}{\binom{m-1}{k-1}} . \prod_{i=1}^{k} \rho_i . (1 - \rho_{k+1}) . Q_t \quad (2.30)$$

K = 1;…; m

$\rho_1 = 1 , \rho_2 = \beta , \rho_3 = \gamma , \ldots$

3.15. Conclusion

Dans ce chapitre, nous avons étudié trois méthodes d'inclusion des défaillances de cause communes, méthode du facteur Alpha, du facteur Beta et la méthode des lettres grecques multiples (MGL). L'application de ces méthodes nécessite certaines adaptations. La méthode du facteur Beta est le plus communément utilisé, son inconvénient est que les causes communes de défaillances partielles ne sont pas prises en compte, ainsi une défaillance de cause commune implique forcément la défaillance de tous les composants d'un système, et non d'un quelconque sous-ensemble de composants. Ceci implique notamment que la défaillance indépendante ne soit pas exprimée en fonction de l'architecture du système. Les différences parfois importantes dans les résultats obtenus par l'application des différentes méthodes, montrent que les hypothèses utilisées sont déterminantes. Il convient donc de choisir la méthode la plus adéquate en fonction des hypothèses requises du système (architecture, hétérogénéité des composants), du degré de modélisation voulu et des informations disponibles (coefficients Beta, paramètres des défaillances de cause commune partielles).

Pour l'instant, il est impossible d'éviter les défaillances de cause commune. La seule chose que nous pouvons faire est de réduire autant que possible la production de ce type de défaillance qui peut empêcher la réalisation d'une meilleure fiabilité avec l'utilisation de la redondance. La présence de défauts de conception ou de chocs externes peut provoquer la panne de toutes les unités redondantes, en raison d'une cause commune. Pour réduire l'effet des DCC, il faut une vaste analyse des modes de défaillance, de restructuration afin d'avoir une bonne fiabilité intrinsèque et cela recommande l'utilisation de la diversité technique, la séparation physique.

Chapitre 4

Analyse fonctionnelle et dysfonctionnelle d'un HIPPS

4.1. Introduction

L'une des principales priorités des responsables de la maintenance est d'assurer une disponibilité opérationnelle maximale à leurs équipements, ainsi que de garantir la sécurité et l'efficacité des opérations de leurs installations. Comprendre les calculs et l'utilisation des indicateurs de défaillance nous permettra de déterminer avec une grande précision le moment où un système critique est plus susceptible de tomber en panne. En fonction des indicateurs de défaillance les professionnels de la maintenance peuvent développer et améliorer les meilleurs stratégies de gestion de la maintenance, ce qui leurs permet également de réduire la dépendance de leur entreprise à la maintenance réactive au profit d'une maintenance préventive, qui peut être exactement ce dont ils besoin pour stimuler la croissance de la production. Dans ce chapitre nous abordons l'analyse fonctionnelle dysfonctionnelle d'un système critique HIPPS, exploité dans la raffinerie de Skikda (RA1K), par la méthode blocs diagramme de fiabilité de fiabilité (BdF) et la méthode arbre de défaillance (AdD). L'étude est abordée en présence et en absence des défaillances de cause commune (DCCs). L'objectif étant d'effectuer une comparaison entre les résultats fournis par les deux analyses, de mettre en évidence l'impact des DCCs sur les performances globales du HIPPS, et de prouver la conformité, l'exactitude, ainsi que la robustesse des deux formalismes.

4.2. Description et principe de fonctionnement du HIPPS

Notre analyse est appliquée à un HIPPS existant dans la plateforme Onshore de la Raffinerie de Skikda (RA1K). Le rôle du HIPPS est de protéger le Pétrole et le Gaz Liquéfier (LPG) du ballon (600-S-156), des phénomènes de hautes pressions. La figure 4.1 montre l'implémentation du HIPPS dans le diagramme tuyauterie &instrumentation (Piping & Instrumentation Diagram P&ID).

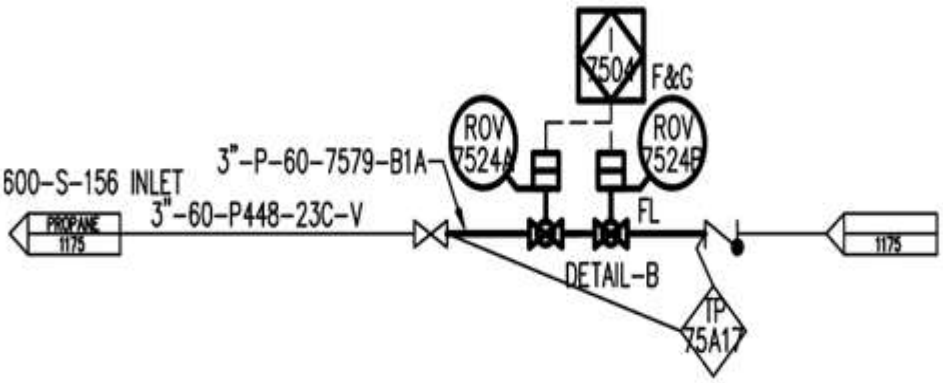


Figure4.1. P&ID du HIPPS 1-7504 –RA1K- de Skikda [41].

Le HIPPS est composé des sous-systèmes suivants :

Transmetteurs : trois transmetteurs, en étiquette PT-**7504 A/ B/ C**, en architecture de vote majoritaire (2oo3).

Unité de traitement : (Programmable Logic Controller PLC), en Redondance Modulaire Triple (Triple Modular Redundant TMR) de Triconex [43].

Eléments finaux : ce sont des vannes solénoïdes (ROV-2524 A, et ROV-2524 B). Chaque élément final compris les solénoïdes vannes (SV1, SV2 présenté dans la figure 4.2), et les Vannes d'arrêts d'urgence (Vannes d'arrêt d'urgence SDV1, SDV2), avec le système de vote 1oo2. La figure 4.2 résume le principe du fonctionnement de du système considéré.

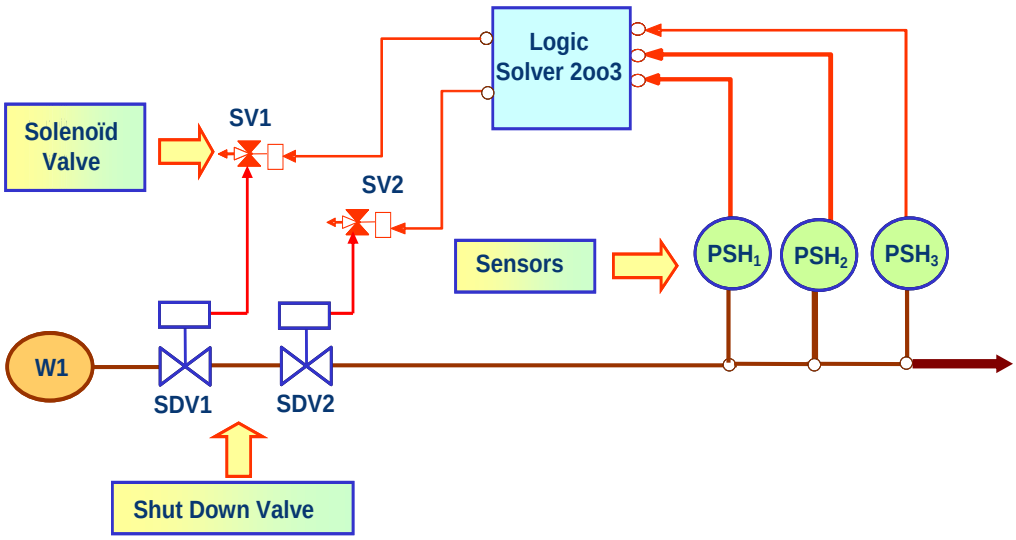


Figure 4.2 : Architecture simple de HIPPS [31].

Ce HIPPS est destiné à protéger une partie-aval d'un système de production des surpressions engendrées dans sa partie-amont.

Lorsque la pression dans la partie-aval dépasse un niveau-seuil donné, ce dépassement est détecté par les trois capteurs PSH_1, PSH_2, PSH_3, qui envoient un signal d'information au sous-système logique LS (Logic Solver) à redondance majoritaire 2 sur 3 (2oo3). Ce dernier envoie, à son tour, un signal aux vannes solénoïdes SV_1 et SV_2 qui relâchent la pression hydraulique qui maintenait les vannes d'arrêt SDV_1 et SDV_2 ouvertes. Celles-ci se ferment donc, ce qui a pour effet de faire baisser la pression dans la partie-aval de l'installation.

Ce HIPPS est classiquement constitué de trois sous-systèmes disposés en série. Le premier d'entre eux est le module composé des trois capteurs-transmetteurs PSH_1, PSH_2, PSH_3. Leurs défaillances dangereuses sont détectées après leurs survenances.

Le deuxième sous-système est l'unité logique en 2 sur 3. Son taux de défaillance et son taux de réparation sont mentionnés dans le tableau 4.1.

Le troisième sous-système est doté d'une architecture en 1 sur 2 (1oo2). Chacun de ses deux canaux se compose d'une vanne solénoïde SV_1 ou SV_2 et d'une vanne d'arrêt de sécurité SDV_1 ou SDV_2. Le taux de défaillance dangereuse non détectée des premières vaut 9E-7 $h^{-1.}$ Elles sont testées après leur mise en opération, tous les deux mois (1460 heures). Les vannes SDV_1, SDV_2 présentent deux modes de défaillance. Leurs défaillances causant le blocage en position (failure to move) sont détectées par «test périodiques étendus ». Le taux de défaillance correspondant est égal à 1.1E-6 h^{-1}, les deux vannes sont contrôlées tous 8760 heures. Notons que la production est stoppée après la détection d'une telle défaillance.

Le tableau 4.1 regroupe les différents caractéristiques fiabilistes des trois sous-systèmes constitutifs du HIPPS.

Tableau 4.1 : Caractéristiques fiabilistes des éléments constitutifs du HIPPS [41].

Taux de défaillances (λ) ***-Défaillance détectée : détectée immédiatement après sa survenue. La réparation peut commencer immédiatement après la détection.*** ***- Défaillance non détectée : elle n'est détectée qu'après avoir effectué le test périodique. Ainsi, sa réparation peut commencer.***		**Intervalle entre tests périodiques (heures)**	**Taux de réparations (μ)**
PHS1, PHS2, PHS3	3×10^{-7} (détectée)	-------	0.125
Unité de traitement : LS	9×10^{-6} (détectée)	-------	
SV1, SV2	9×10^{-7} (non détectée)	1460(2 mois)	
SDV1, SDV2 (bloquée ouverte ou fermée)	1.10×10^{-6} (non détectée)	8760 (1 an)	

La norme internationale CEI 61508 classe les performances du HIPPS selon le niveau d'intégrité de sécurité SIL. Le **SIL** dépend de la probabilité moyenne de défaillance du HIPPS $\mathbf{PFD_{avg}}$**.** Le tableau 4.2 donne le SIL du HIPPS en fonction de la valeur de sa PFD_{avg}.

Tableau 4.2 : Niveau D'intégrité (SIL) en fonction du PFD_{avg} [3].

SIL	$\mathbf{PFD_{avg}}$
4	$\mathbf{\geq 10^{-5} < 10^{-4}}$
3	$\mathbf{\geq 10^{-4} < 10^{-3}}$
2	$\mathbf{\geq 10^{-3} < 10^{-2}}$
1	$\mathbf{\geq 10^{-2} < 10^{-1}}$

4.3. Analyse des performances du HIPPS sans la prise en compte des Défaillances de Cause Commune DCCs (phase de Diagnostic)

4.3.1. Modélisation dysfonctionnelle par Arbre de défaillances (AdD)

Le principe du fonctionnement du HIPPS est présenté à la figure 4.2, on commence par l'analyse dysfonctionnelle du HIPPS via la méthode AdD. La figure 4.3 présente graphiquement la logique de dysfonctionnement du HIPPS, ce graphe est orienté et formé de plusieurs niveaux successifs tels que chaque évènement est généré par des évènements d'ordre inférieur agissant à travers des portes logiques. On procède à deux types d'analyse :

1. L'analyse qualitative qui entraîne, l'élaboration de l'arbre de défaillance du HIPPS et la détermination des Coupes Minimales (CM), ou la recherche d'une combinaison de composants qui amène à la défaillance du HIPPS. Le traitement qualitatif est indispensable pour réaliser ensuite le traitement quantitatif de l'arbre de défaillance du HIPPS.

2. L' analyse quantitative, qui engendre le calcul des différents paramètres de la sûreté de fonctionnement du HIPPS : Fiabilité R(t), Probabilité de Défaillance : F(t), l'indisponibilité instantanée : U(t), qui représente réellement le niveau du SIL, et Fréquence de l'évènement sommet W(t), la métrique MTTF, MTBF, MUT et MDT ainsi que l'analyse de sensibilité, ou l'évaluation de l'influence des divers composants constitutifs sur le fonctionnement du HIPPS (mesures d'importances).

Rappelons que les données de simulation sont tirées du Référence [41]. Les résultats de simulations sont obtenus en utilisant le logiciel GRIF-Workshop (2019) [42]. Ce type de logiciel est très utilisé en industrie. Nous avons réalisé cette implémentation en utilisant le logiciel GRIF 2019, pour une séquence temporelle de 5 ans.

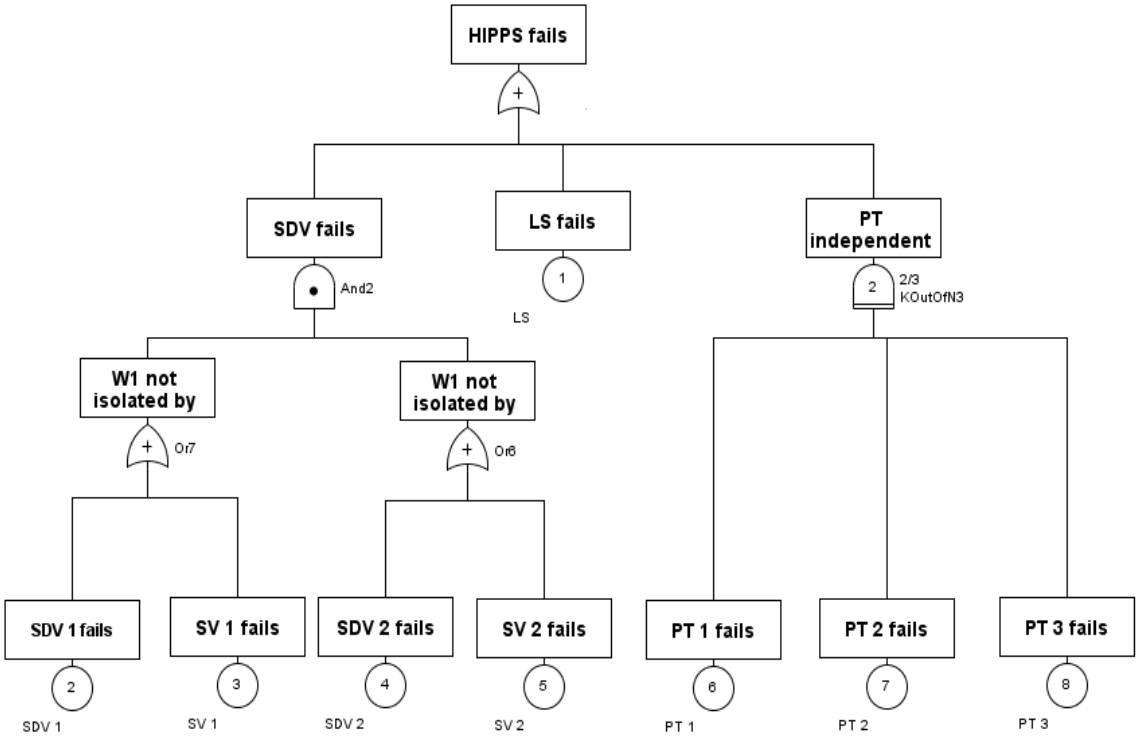


Figure 4.3 : Arbre de défaillance du HIPPS sans considération des DCCs.

La figure 4.4 représente le tracé de la courbe de fiabilité et de défaillance relatives au HIPPS.

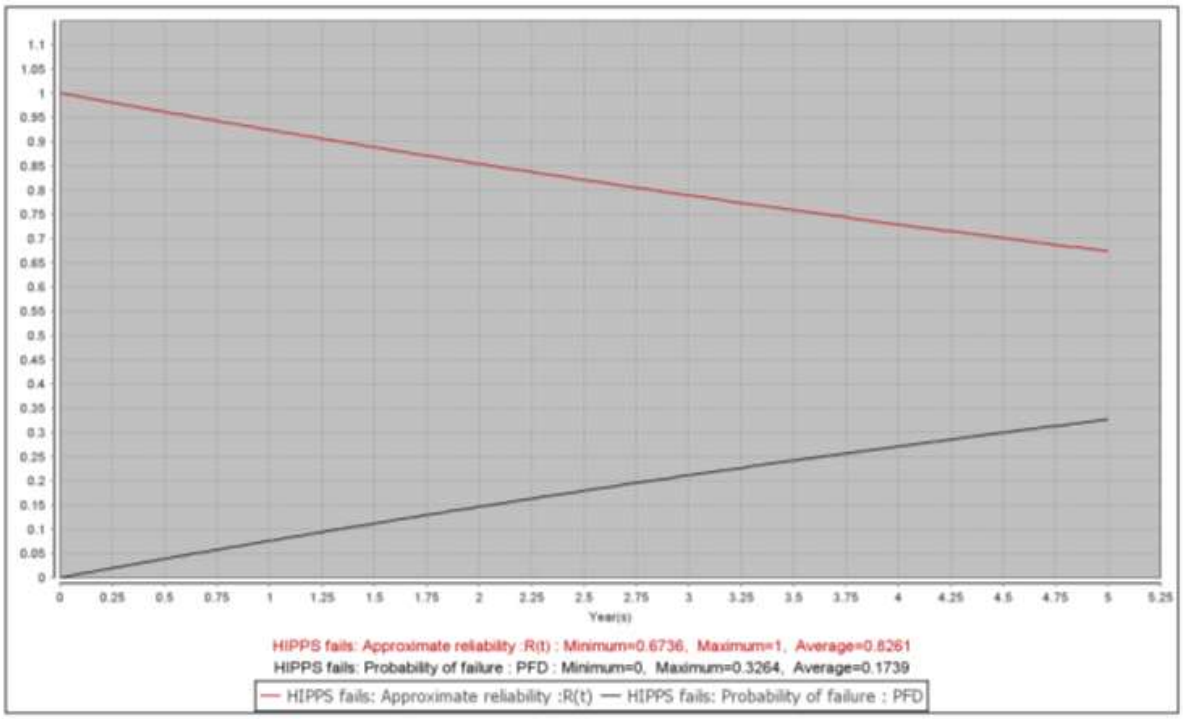


Figure 4.4 : Fonction de fiabilité et la fonction cumulée de défaillance relative au HIPPS par l'analyse dysfonctionnelle.

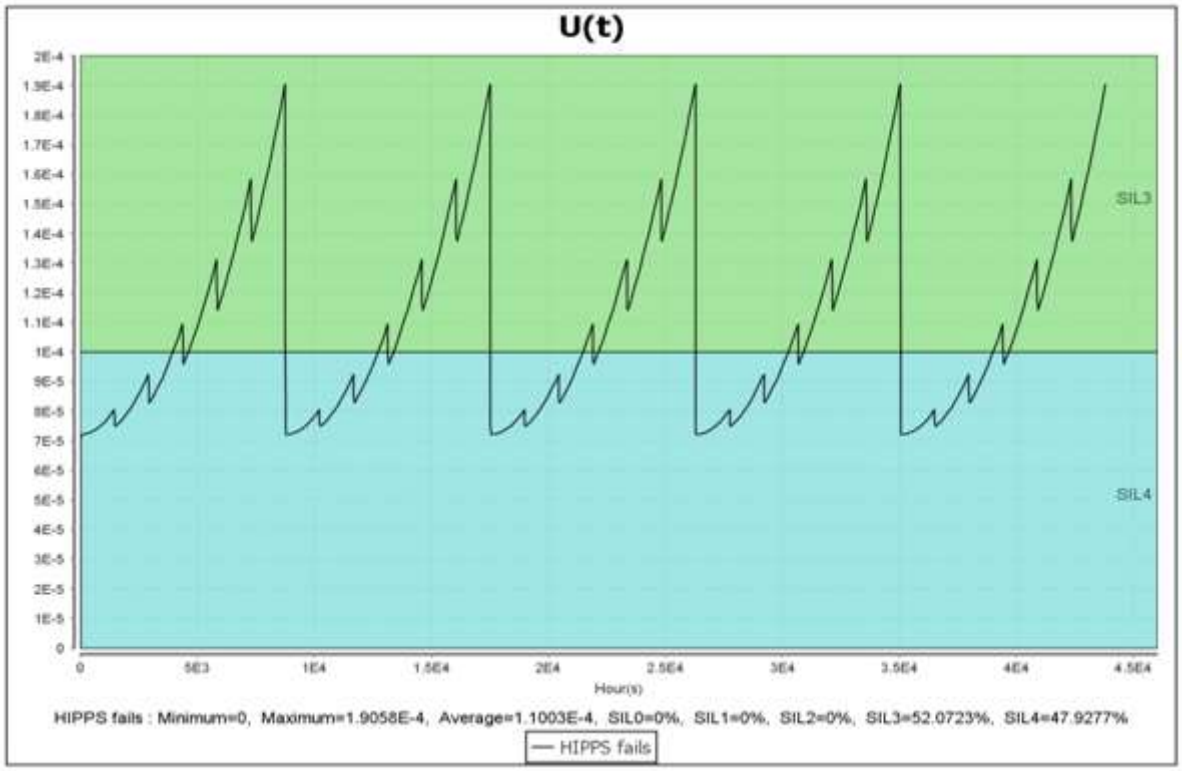


Figure 4.5 : Fonction cumulée de l'indisponibilité instantanée (SIL) par AdD.

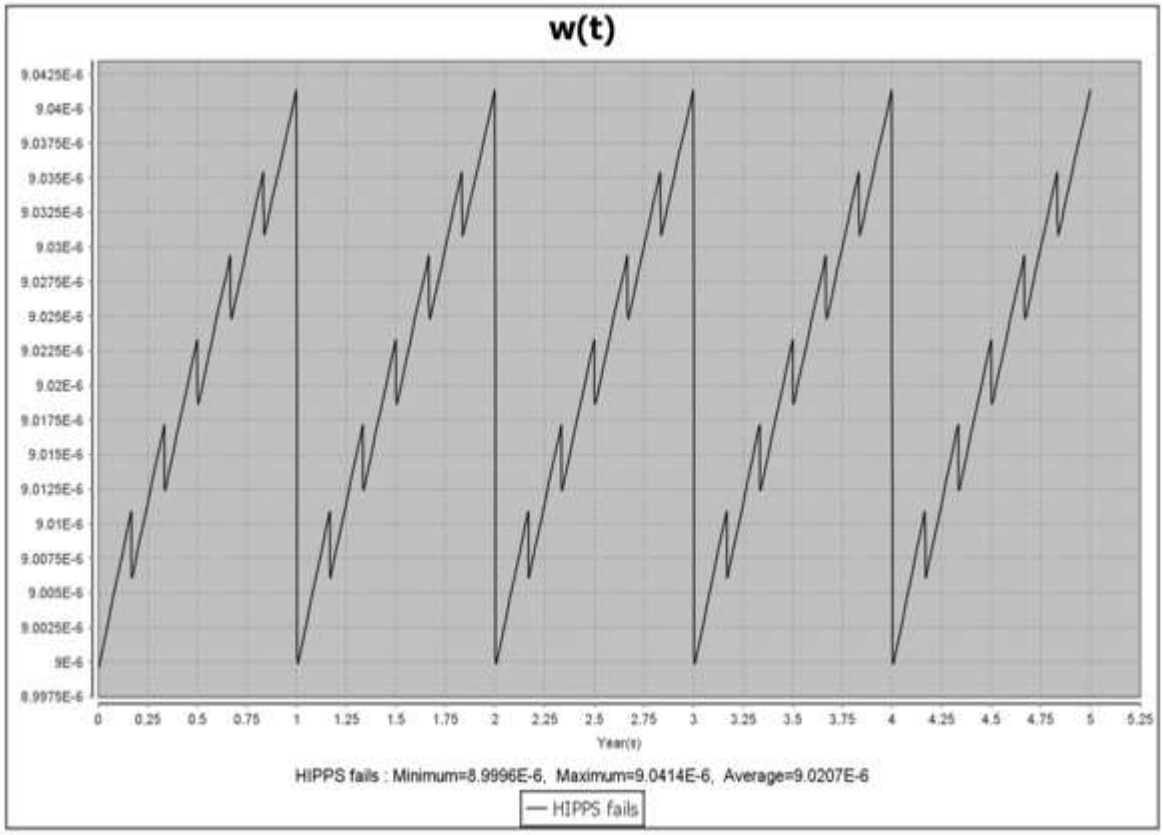


Figure 4.6 : Evolution de la fréquence cumulée de défaillance pour l'évènement sommet.

-La figure 4.5 représente l'évolution de l'indisponibilité instantanée ou la variation du niveau d'intégrité de sécurité (SIL) pour le HIPPS.

-La figure 4.5 montre que 52% de U(t) sont dans la zone du SIL3, 47.9% de la courbe sont dans la zone SIL4, et la moyenne du SIL 1.003E-4 qui correspond au SIL3.

-La figure ci-dessous 4.6 représente l'évolution de la fréquence de défaillance de notre système, avec une valeur moyenne de 9.0207E-6 h^{-1}.

Le tableau 4.3 présente la collecte des valeurs moyennes pour les paramètres : R(t), F(t), U(t), et W(t)

Tableau 4.3 : Probabilités et fréquences de défaillance au sommet de l'AdD.

Technique : AdD	**System**	**HIPPS fails**		
Probabilités/Fréquences	**$R(t)_{avg}$**	**$F(t)_{avg}$**	**$U(t)_{avg}$**	**$W(t)_{avg}$**
Valeur	**0.8261**	**0.1739**	**1.1003E-4**	**9.0207E-6h^{-1}**

La valeur moyenne de fiabilité : **R(t)avg=82,61%, et le SIL_{avg} =1.1003E-4,** qui correspond au SIL3. Ce qui nous informe que le HIPPS répond aux exigences de sûreté.

Dans le tableau 4.4, on montre le calcul de la métrique : MTTF, MTBT, MDT, et MUT. La surveillance de cette métrique éliminera les conjectures et donnera aux responsables de la maintenance les données concrètes et nécessaires aux prises de décisions.

Tableau 4.4 : Métrique du HIPPS par AdD

Technique :AdD	**System**	**HIPPS fails**		
Métrique :	**MTTF**	**MDT**	**MUT**	**MTBF**
Valeur	**1.1084E5h**	**12.1973h**	**1.1084E5h**	**1.1086E5h**

D'après le tableau 4.4, **Le MTTF= le MUT=110840 heures** ce qui est équivalent approximativement à 12 ans, qui représente la durée de vie du HIPPS. Donc notre système peut fonctionner 12 ans avant l'occurrence de la première défaillance. La MTTF est une mesure très basique de la fiabilité. **Un MTTF=12 ans**, signifie une continuité de fonctionnement, absence des temps d'arrêt et des interruptions.

Un MUT =12 ans représente un temps moyen de disponibilité. Le HIPPS à une grande probabilité de disponibilité opérationnelle.

Le MDT=12.1973 heures, cette faible valeur signifie que la maintenabilité du système est très rapide, et aussi l'existence d'une une grande efficacité de réparation. Le MDT mesure l'indisponibilité du HIPPS, qui comprend : la détection de la panne, la réparation et la remise on service. On cherche toujours à réduire la MDT avec une équipe de maintenance bien soutenue par les ressources, les outils, les pièces de rechange et les logiciels nécessaires.

La MTBF= 110860 heures qui mesure la fiabilité et la disponibilité du HIPPS est approximativement équivalent à 13 ans. Cette mesure indique que le HIPPS peut fonctionner longtemps avant la prochaine panne non planifiée. Plus le MTBF est très élevé plus le fonctionnement du système est assurer pour une période temporelle très importante avant de tomber en panne.

On remarque que l'égalité : $MTBF = MUT + MDT$ est vérifiée, la MDT est faible devant la MUT, ce qui rend le MTBF et le MTTF très proches.

Le tableau 4.4 sont présentés les calculs des coupes minimales, on constate l'existence de **8 Coupes Minimales une coupe d'ordre1 et les autres d'ordre 2.**

La coupe d'ordre 1 : l'unité de traitement (LS) signifiait qu'une simple défaillance au niveau de ce sous-système va entraîner l'évènement sommet.

Les coupes d'ordres 2 : signifiait qu'une paire de défaillance au niveau des composants indiqués dans le tableau 4.5 et qui se produisant en même temps vont entraîner l'évènement redouté.

Tableau 4.5 : Coupes minimales du HIPPS via l'AdD.

PRODUCTS			
Type=PRODUCTS, Nom=HIPPS fails			
Ordre	**La Coupe**	**Probabilité (Coupe)**	**Fréquence (Coupe)**
1	**LS**	**7.1995E-5**	**8.9983E-6**
2	**SDV1, SDV2**	**9.1963E-5**	**2.0866E-8**
2	**SDV1, SV2**	**1.2593E-5**	**9.9648E-9**
2	**SDV2, SV1**	**1.2593E-5**	**9.9648E-9**
2	**SV1, SV2**	**1.7243E-6**	**2.3377E-9**
2	**PT1, PT2**	**5.76E-12**	**1.4397E-12**
2	**PT1, PT3**	**5.76E-12**	**1.4397E-12**
2	**PT2, PT3**	**5.76E-12**	**1.4397E-12**

La figure 4.7 présente un classement des coupes minimales selon leurs probabilités d'occurrences.

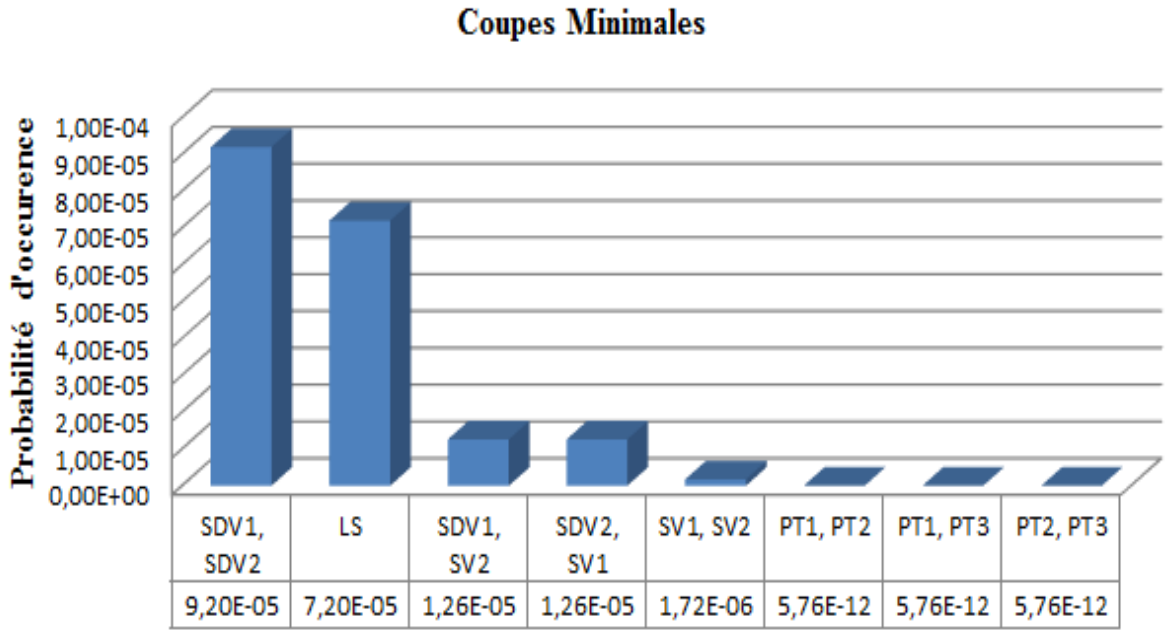


Figure 4.7 : Coupes minimales en fonction de leurs probabilités d'occurrence.

La figure 4.8 représente un classement des coupes minimales selon leurs fréquences d'occurrence.

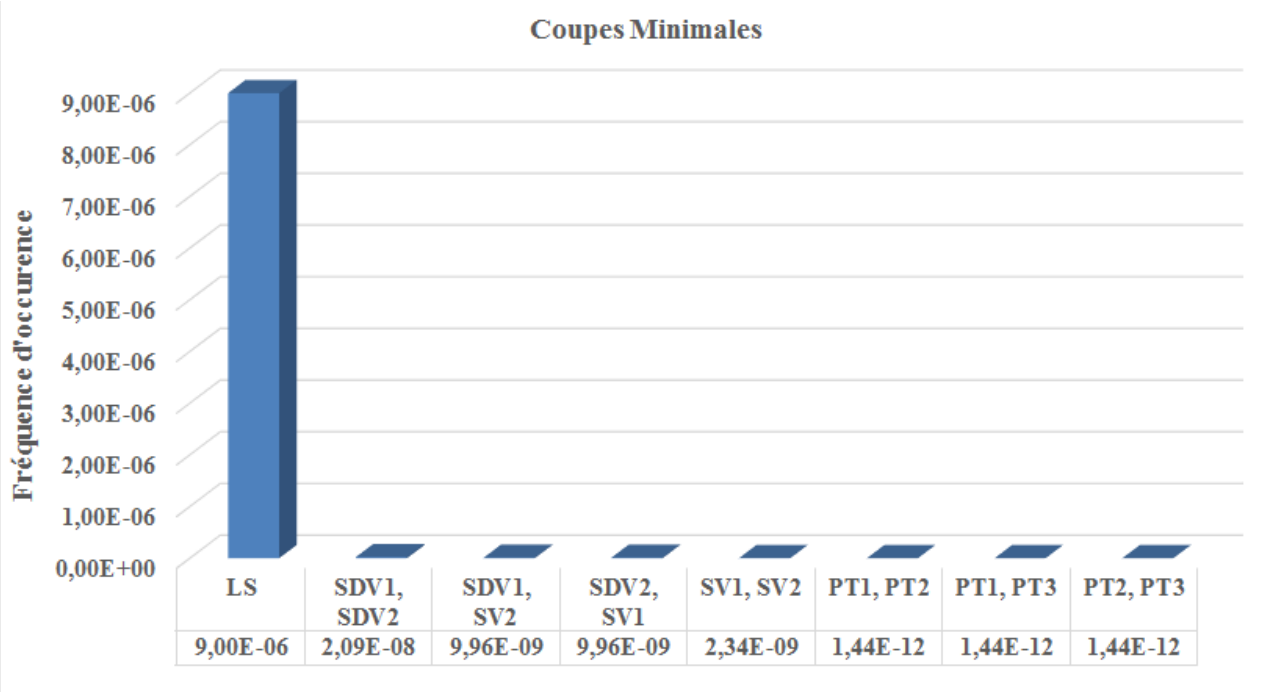


Figure 4.8 : Coupes minimales en fonction leurs fréquences d'occurrence.

4.3.1.1 Mesure des facteurs d'importances

4.3.1.1.1. Mesure de Birnbaum (Marginal Important Factor (MIF))

Le MIF représente une mesure de sensibilité de fiabilité du HIPPS suivant l'état du composant en question. Autrement dit si on veut augmenter la fiabilité du système il faut commencer par améliorer la fiabilité du composant qui a le plus grand facteur d'importance marginal [21].

4.3.1.1.2. Mesure de Lambert (Critical Important Factor (CIF))

Le CIF évalue l'importance du composant en question en fonction de sa participation à la mise en panne du système, donc il est utile en cas de défaillance, pour identifier les composants à réparer en priorité, c'est-à-dire ceux dont la mise en marche est la plus susceptible de restaurer le fonctionnement du système. Ce facteur a un grand intérêt dans l'optimisation de la maintenance, il indiquera sur quels composants il est intéressant d'exécuter une maintenance préventive, et ceux sur lesquels la maintenance corrective suffit [25].

4.3.1.1.3. Mesure de Fussel Vesely (Diagnostic Important Factor (DIF))

Le DIF est un indicateur très utile pour le diagnostic des causes de défaillance du système, d'où son appellation : facteur de diagnostic, il est très précieux dans la phase de conception de n'importe quel système [36]. Là où les modifications importantes de fonctionnements et/ou

design peuvent intervenir, et faire varier le risque associé au système avec de grandes proportions. Dans notre analyse le MIF et le CIF donnent presque les mêmes résultats de simulation ce qui En parfait accord avec la théorie [26]

4.3.1.1.4. Mesure de Facteur augmentation de risque (Reliability Achievement Word (RAW))

Le RAW est un indicateur de l'importance qu'il y a à maintenir le niveau de fiabilité du composant en question pour maintenir la fiabilité du système globale. Autrement dit ce facteur quantifie l'accroissement maximum de la fiabilité du système généré par le composant en question. Un RAW élevé reflète une mauvaise immunité du système vis-à-vis la défaillance du composant [27][28].

4.3.1.1.5. Mesure de Facteur réduction de risque (Reliability Achievement Word (RRW))

Le RRW ce facteur évalue les dommages éventuels causés au système par le composant en question. Il représente la réduction maximale du risque, que l'on peut espérer en améliorant la fiabilité du composant en question. Ce facteur est intéressant pour repérer les composants dont l'amélioration de la fiabilité est plus susceptible d'augmenter celle du système globale. Il est utile pour déterminer les composants à fiabiliser en priorité dans le cadre d'une maintenance préventive [27][28].

4.3.1.1.6. Mesure de facteur de Barlow et Proschan (PB)

Le facteur de Barlow et Proschan donne des probabilités pour la contribution de chacun des composants dans la mise en défaillance du système globale. Il montre la probabilité que la panne du composant coïncide avec la défaillance du système globale, ou le système est défaillant parce-que la coupe minimale contenant le composant en question est défaillante, d'une autre manière, il indique le poids respectif de chaque coupe minimale dans leur contribution à la défaillance du système. Le composant ayant le PB le plus élevé a une grande influence sur la fiabilité globale du système. Théoriquement la somme de tous les valeurs BP pour tous les composants d'un système donne l'unité. Cet indicateur a un intérêt dans le développement et l'implémentation de la maintenance [29].

Les tableaux 4.6, 4.7, 4.8, 4.9, 4.10 et 4.11, illustrent les différents Facteurs d'importances pour chacun des composants au niveau du HIPPS.

Tableau 4.6: Mesure de Birnbaum (MIF)

Type=MIF, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	0.9999	LS
8.76E3	0.0109	SDV1
8.76E3	0.0109	SDV2
8.76E3	0.0108	SV1
8.76E3	0.0108	SV2
8.76E3	4.7991E-6	PT1
8.76E3	4.7991E-6	PT2
8.76E3	4.7991E-6	PT3

Tableau 4.7 : Mesure de Lambert (CIF)

Type=CIF, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	0.5472	SDV1
8.76E3	0.5472	SDV2
8.76E3	0.3777	LS
8.76E3	0.0743	SV1
8.76E3	0.0743	SV2
8.76E3	6.0434E-8	PT1
8.76E3	6.0434E-8	PT2
8.76E3	6.0434E-8	PT3

Tableau 4.8: Mesure de Fussel Vesely DIF

Type=DIF, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	0.5516	SDV1
8.76E3	0.5516	SDV2
8.76E3	0.3778	LS
8.76E3	0.0755	SV1
8.76E3	0.0755	SV2
8.76E3	2.4604E-6	PT1
8.76E3	2.4604E-6	PT2
8.76E3	2.4604E-6	PT3

Tableau 4.9: Mesure du facteur augmentation de risque (RAW)

Type=RAW, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	5.247E3	LS
8.76E3	57.5152	SDV1
8.76E3	57.5152	SDV2
8.76E3	57.5152	SV1
8.76E3	57.5152	SV2
8.76E3	1.0252	PT1
8.76E3	1.0252	PT2
8.76E3	1.0252	PT3

Tableau 4.10: Mesure du facteur de reduction de risque (RRW)

Type=RRW, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	2.2085	SDV1
8.76E3	2.2085	SDV2
8.76E3	1.607	LS
8.76E3	1.0803	SV1
8.76E3	1.0803	SV2
8.76E3	1	PT1
8.76E3	1	PT2
8.76E3	1	PT3

Tableau 4.11: Mesure du facteur de Barlow et Proschan

Type=BP, System=HIPPS fails		
Time	**Value**	**Component**
8.76E3	0.9952	LS
8.76E3	1.3104E-3	SDV1
8.76E3	1.3104E-3	SDV2
8.76E3	1.0722E-3	SV1
8.76E3	1.0722E-3	SV2
8.76E3	1.5924E-7	PT1
8.76E3	1.5924E-7	PT2
8.76E3	1.5924E-7	PT3

Les figures 4.9, 4.10, 4.11, 4.12, 4.13 et 4.14 illustrent un classement de différentes mesures d'importances par ordre décroissant.

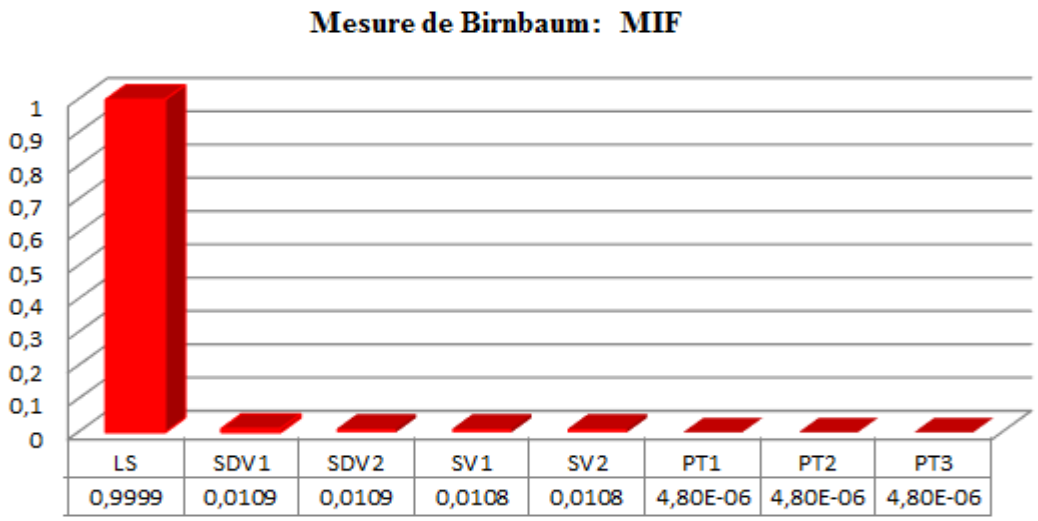


Figure 4. 9 : Classement des composants selon le MIF

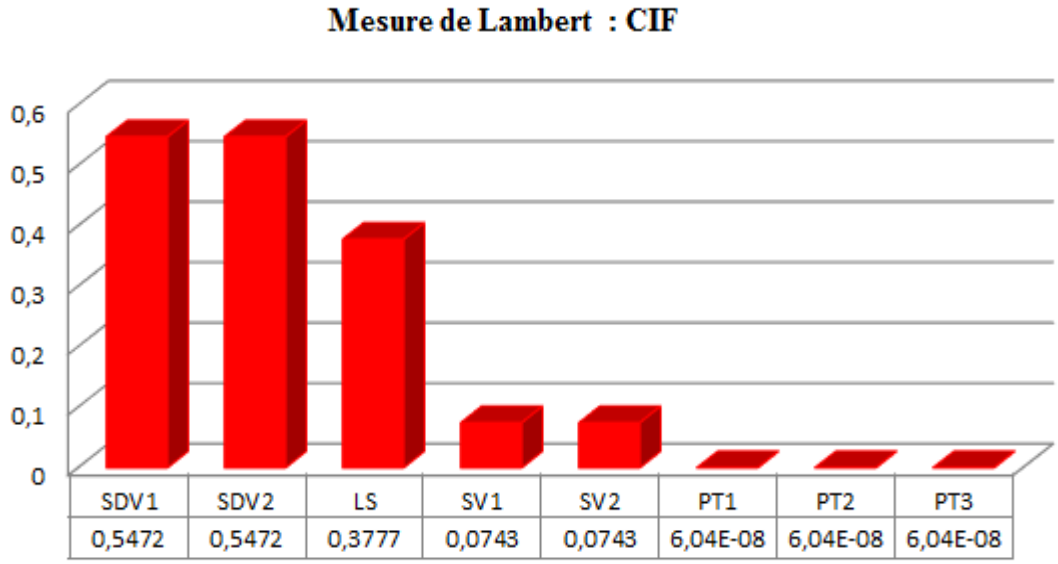


Figure 4.10 : Classement des composants selon le CIF.

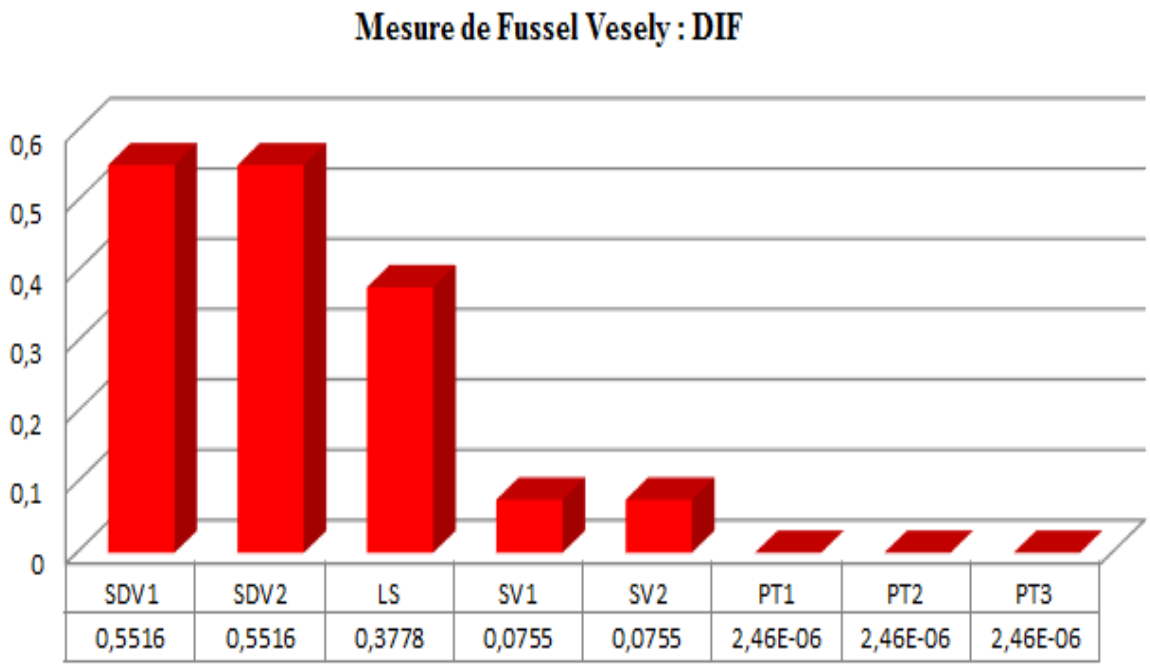


Figure 4.11 : Classement des composants selon le DIF.

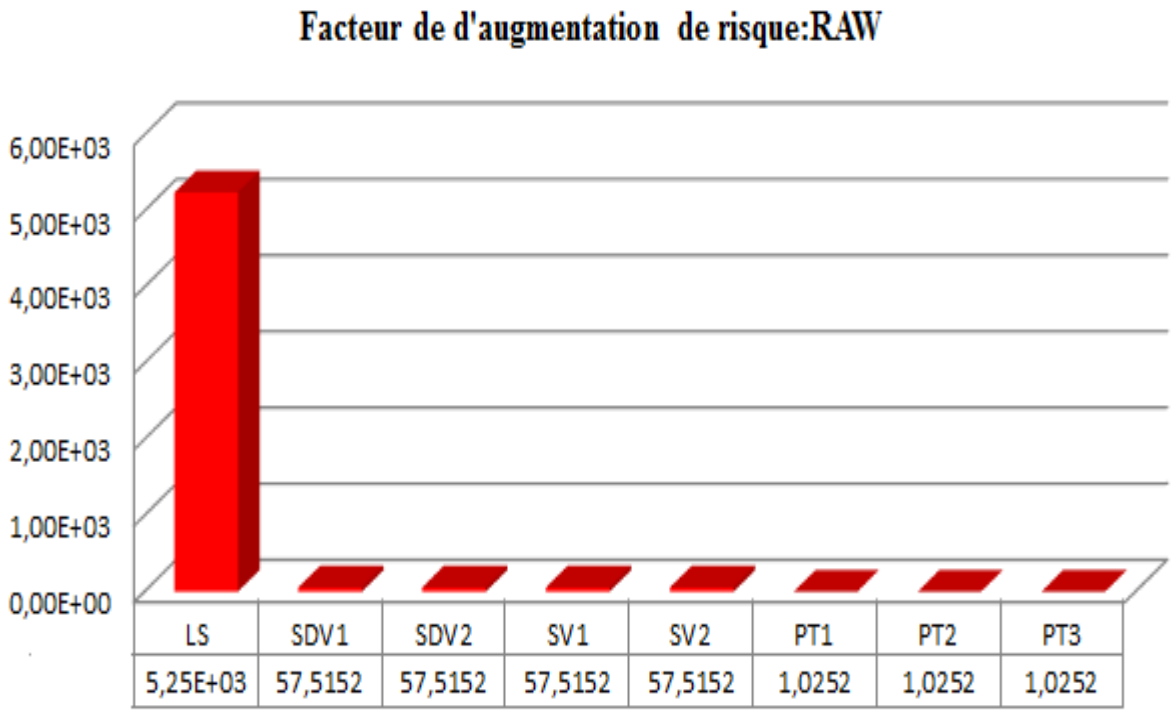


Figure 4.12 : Classement des composants selon le RAW.

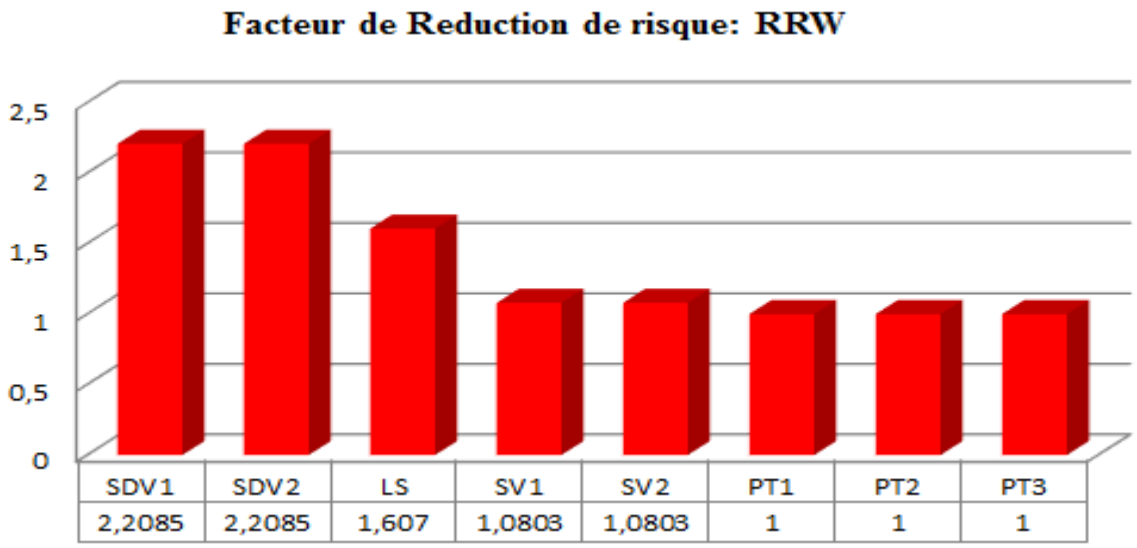


Figure 4.13 : Classement des composants selon le RRW.

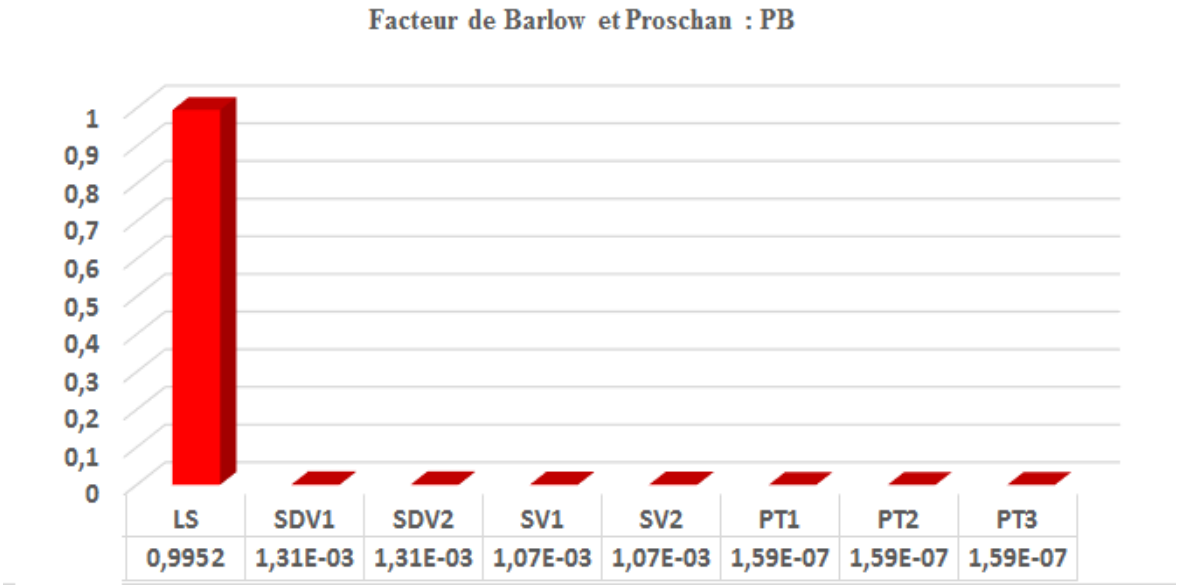


Figure 4.14 : Classement des composants selon le facteur de Barlow et Proschan : BP

Le tableau 4.12 présente le classement des différents composants selon leurs facteurs d'importances.

Tableau 4.12 : Classement des composants selon leurs facteurs d'importance via l'AdD.

MIF	CIF	DIF	RAW	RRW	BP
LS	SDV1=SDV2	SDV1=SDV2	LS	SDV1=SDV2	LS
SDV1=SDV2	LS	LS	SDV1=SDV2	LS	SDV1=SDV2
SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2
PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3

4.3.2. Modélisation fonctionnelle par la méthode Blocs de Fiabilité (BdFs)

La figure 4.15 illustre le BdF du HIPPS, qui est basé sur une découpe partition fonctionnelle pour le HIPPS, ce qui définit les différentes interactions logiques nécessaires pour avoir le fonctionnement du système. La détermination des différents indicateurs de sûreté de fonctionnement pour le système, nécessite tout d'abord de connaître la loi de fiabilité ou de défaillance de chacun des composants intervenant dans notre système d'étude. Pour cela, chaque bloc du BdF est configuré et les données sont fournies pour chacun des composants (taux de défaillance λ, taux de réparation μ, et test périodique). Une analyse qualitative est effectuée par le calcul des coupes minimales, une analyse quantitative complémentaire est réalisée ensuite en calculant les différents paramètres de Sûreté de fonctionnement R(t), F(t), U(t), et W(t) à la sortie du HIPPS, ainsi que la métrique MTTF, MTBF, MUT, et la MDT.

Le BdF permet de suivre l"état de fonctionnement du HIPPS et l'analyse qualitative et quantitative, nous permet de surveiller l'évolution d'une anomalie, d'optimiser la maintenance, ainsi de garantir la qualité et la capacité de production.

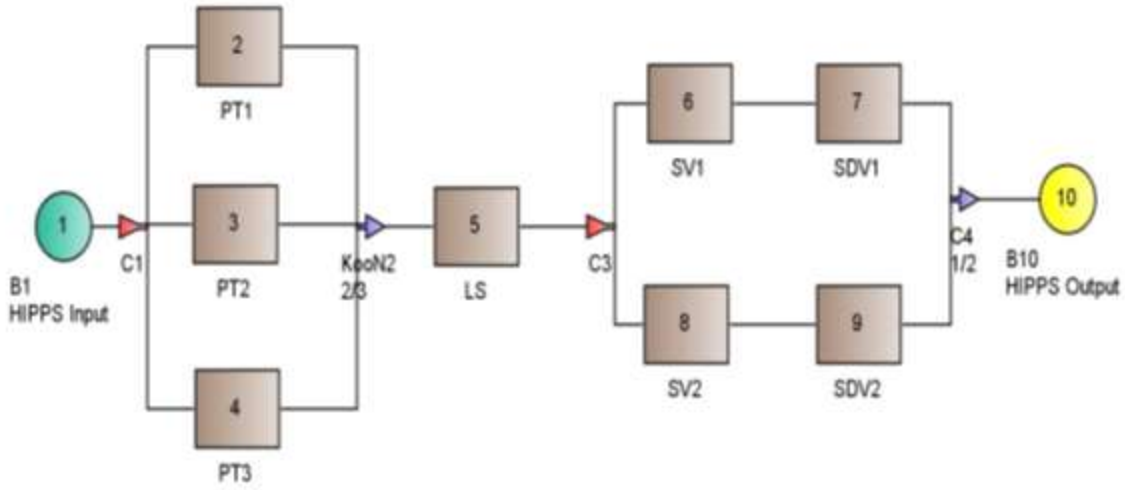


Figure 4.15 : Bloc diagramme de fiabilité sans considération des DCCs relatif au HIPPS.

Les figures 4.16, 4.17, 4.18 représentent l'évolution des différents paramètres R(t), F(t), U(t), et W(t), pour une séquence temporelle de 5 ans.

D'après la figure 4.16 on constate que la fiabilité est toujours une courbe monotone décroissante à l'inverse de la fonction cumulée de défaillance qui est une courbe croissante au court du temps.

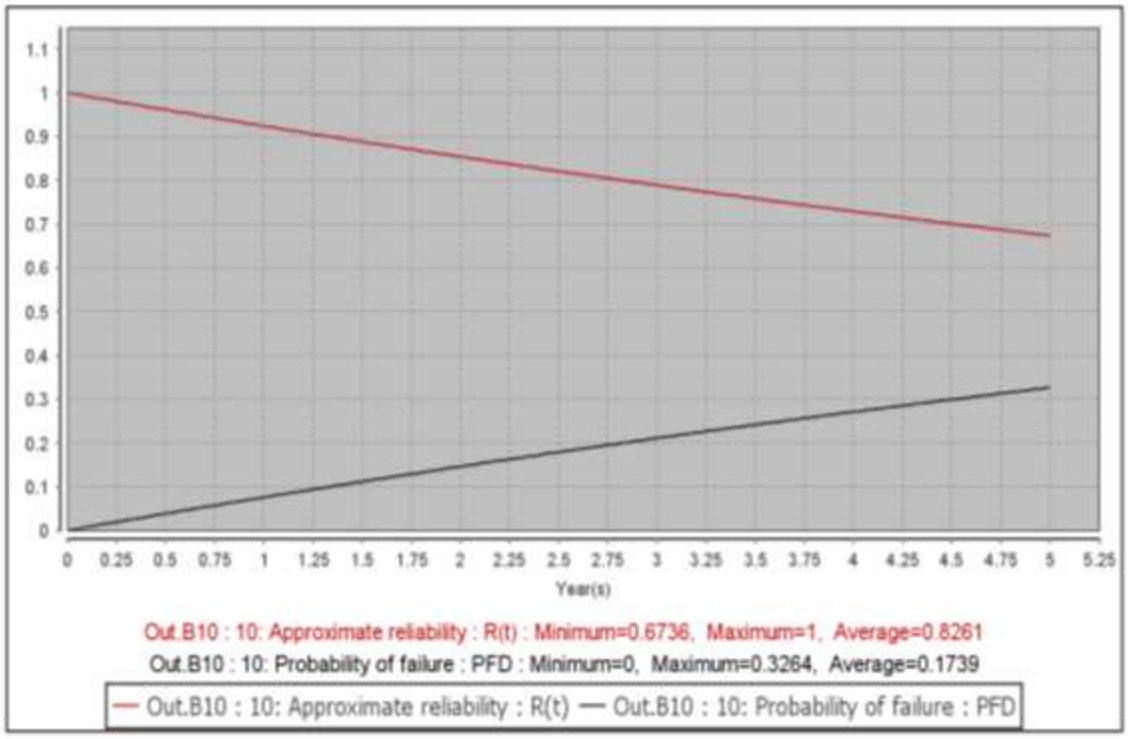


Figure 4.16 : Fonction de fiabilité et la fonction cumulée de défaillance relative au HIPPS par l'analyse fonctionnelle.

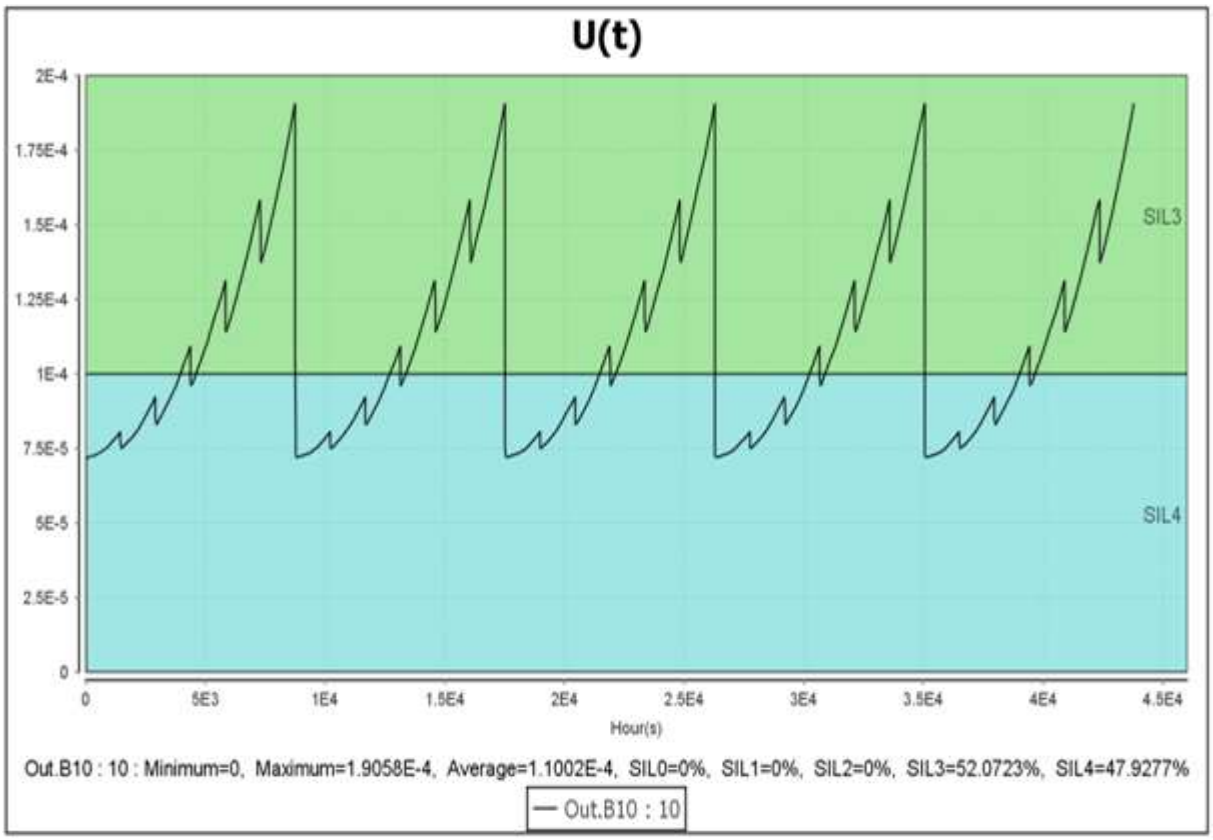


Figure 4.17 : Évolution de temporelle l'indisponibilité instantanée du HIPPS (SIL) par BdF.

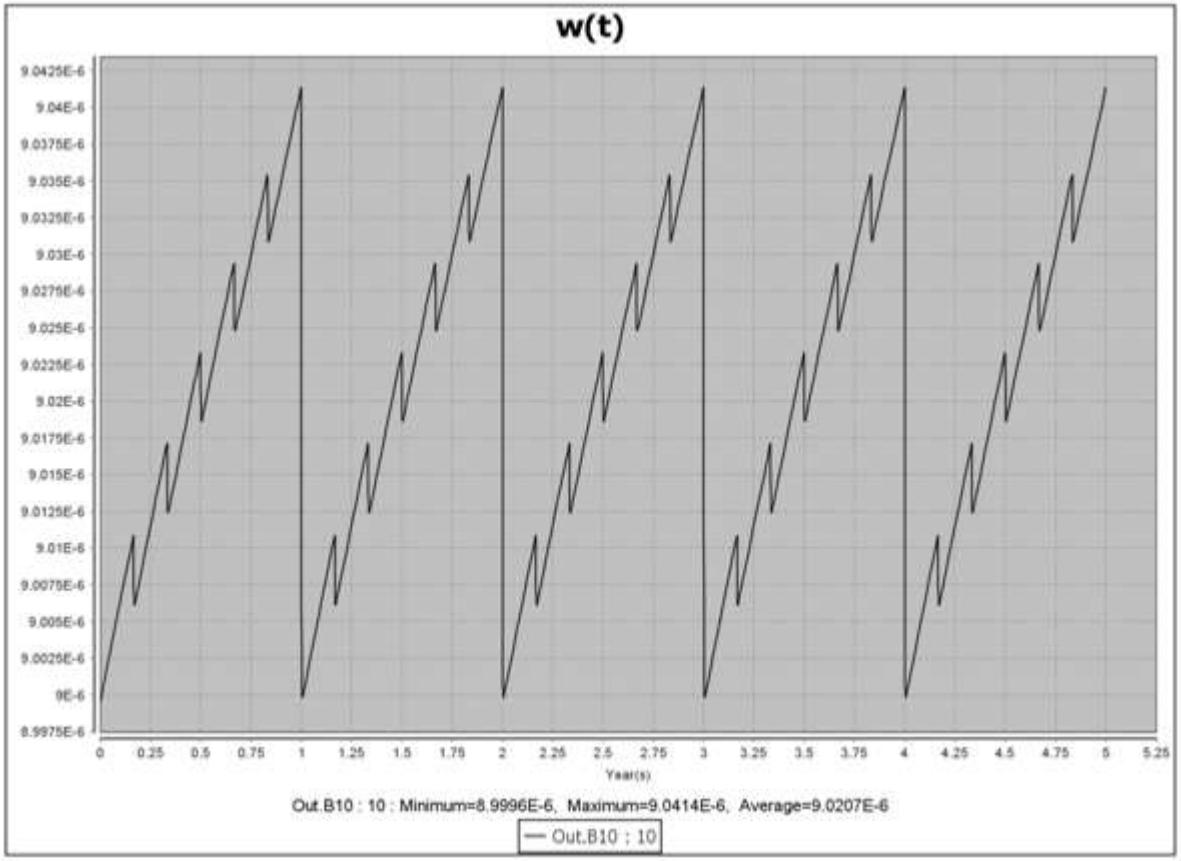


Figure 4.18 : Évolution de la fréquence cumulée de panne à la sortie du HIPPS par BdF.

Le Tableau 4.13 présente les valeurs moyennes des différents paramètres de la sûreté de fonctionnement relatifs au HIPPS.

Tableau 4.13 : Probabilités et fréquence de défaillance à la sortie du HIPPS

Technique :BdF	**System**	**HIPPS Output.B10**		
Probabilités/Fréquences	**$R(t)_{avg}$**	**$F(t)_{avg}$**	**$U(t)_{avg}$**	**$W(t)_{avg}$**
Valeur	**0.8261**	**0.1739**	**1.1003^{E}-4**	**9.0207^{E}-$6h^{-1}$**

Le tableau 4.13 montre les mêmes résultats contenu dans le tableau 4.3

Le tableau 4.14 présente le calcul de la métrique du HIPPS en unité d'heure.

Tableau 4.14: Métrique du HIPPS par le BdF

Technique :BdF	**System**	**HIPPS Output.B10**		
Temps Moyen	**MTTF**	**MDT**	**MUT**	**MTBF**
Valeur	**1.1084E5h**	**12.1971h**	**1.1084E5h**	**1.1086E5h**

Les résultats de la métrique du HIPPS illustrés dans le tableau 4.14 sont similaires aux résultats obtenus par la méthode AdD montrés dans le tableau 4.4

Le Tableau 4.15 présente les combinaisons nécessaires et suffisantes pour la mise en défaillance du système considéré.

La connaissance de l'ensemble des coupes minimales permet d'établir qualitativement la liste des composants critiques au niveau du HIPPS d'après une organisation fonctionnelle du système.

Tableau 4.15 : Coupes Minimales du HIPPS via le BdF.

PRODUCTS			
Type=PRODUCTS, Nom=HIPPS fails			
Ordre	**Coupes**	**Probabilité (Products)**	**Fréquence (Products)**
1	LS	7.1995E-5	8.9994E-6
2	SDV1, SDV2	9.1963E-5	2.0895E-8
2	SDV1, SV2	1.2593E-5	1.005E-8
2	SDV2, SV1	1.2593E-5	1.005E-8
2	SV1, SV2	1.7243E-6	2.3605E-9
2	PT1, PT2	5.76E-12	1.44E-12
2	PT1, PT3	5.76E-12	1.44E-12
2	PT2, PT3	5.76E-12	1.44E-12

D'après le tableau 4.15 la méthode BdF nous donne les mêmes coupes minimales calculées par la méthode AdD avec les mêmes ordres, mais il y en a quelques différences très futiles dans les probabilités et les fréquences d'occurrence de ces coupes. Les tableaux 4.16, 4.17, 4.18, 4.19, 4.20, et 4.21 montrent le calcul des mesures d'importances de chaque composant dans le HIPPS par la méthode Bloc de diagramme de fiabilité.

Tableau4.16: Mesure de Birnbaum (MIF) par le BdF

Type=MIF, System=HIPPS Output.B10		
Time	**Value**	**Component**
8.76E3	0.9999	LS
8.76E3	0.0109	SDV1
8.76E3	0.0109	SDV2
8.76E3	0.0108	SV1
8.76E3	0.0108	SV2
8.76E3	4.7991E-6	PT1
8.76E3	4.7991E-6	PT2
8.76E3	4.7991E-6	PT3

Tableau4.17: Mesure de Lambert (CIF) par le BdF

Type=CIF, System=HIPPS Output.B10		
Time	**Value**	**Component**
8.76E3	0.5472	SDV1
8.76E3	0.5472	SDV2
8.76E3	0.3777	LS
8.76E3	0.0743	SV1
8.76E3	0.0743	SV2
8.76E3	6.0434E-8	PT1
8.76E3	6.0434E-8	PT2
8.76E3	6.0434E-8	PT3

Tableau4.18: Mesure de Fussel Vesely (DIF) par le BdF.

Type=DIF, System=HIPPS Output.B10		
Time	**Value**	**Component**
8.76E3	0.5516	SDV1
8.76E3	0.5516	SDV2
8.76E3	0.3778	LS
8.76E3	0.0755	SV1
8.76E3	0.0755	SV2
8.76E3	2.4604E-6	PT1
8.76E3	2.4604E-6	PT2
8.76E3	2.4604E-6	PT3

Tableau4.19: Mesure du facteur augmentation de risque (RAW) par le BdF.

Type=RAW, System=HIPPS Output.B10		
Time	**Value**	**Component**
8.76E3	5.247E3	LS
8.76E3	57.5152	SDV1
8.76E3	57.5152	SDV2
8.76E3	57.5152	SV1
8.76E3	57.5152	SV2
8.76E3	1.0252	PT1
8.76E3	1.0252	PT2
8.76E3	1.0252	PT3

Tableau4.20: Mesure du facteur de reduction de risque (RRW) par le BdF

Type=RRW, System=HIPPS Ouput.B10		
Time	**Value**	**Component**
8.76E3	2.2085	SDV1
8.76E3	2.2085	SDV2
8.76E3	1.0803	SV1
8.76E3	1.0803	SV2
8.76E3	1.607	LS
8.76E3	1	PT1
8.76E3	1	PT2
8.76E3	1	PT3

Tableau4.21: Mesure du facteur de Barlow et Proschan par le BdF

Type=BP, System=HIPPS Output.B10		
Time	**Value**	**Component**
8.76E3	0.9952	LS
8.76E3	1.3104E-3	SDV1
8.76E3	1.3104E-3	SDV2
8.76E3	1.0722E-3	SV1
8.76E3	1.0722E-3	SV2
8.76E3	1.5924E-7	PT1
8.76E3	1.5924E-7	PT2
8.76E3	1.5924E-7	PT3

Le tableau 4.22 affiche le classement des composants selon leurs facteurs d'importances

Tableau 4. 22 : Classement des composants du HIPPS selon leurs facteurs d'importances par le BdF.

MIF	CIF	DIF	RAW	RRW	BP
LS	SDV1=SDV2	SDV1=SDV2	LS	SDV1=SDV2	LS
SDV1=SDV2	LS	LS	SDV1=SDV2	LS	SDV1=SDV2
SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2	SV1=SV2
PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3	PT1=PT2=PT3

Le tableau 4.22 affiche le même ordre de classement que le tableau 4.12 obtenus par la méthode arbre de défaillance.

4.3.3 Discussion des résultats de simulation de la phase diagnostic

Basés sur les résultats de simulation fournit dans cette étape de diagnostic, présentés par les différents figures (4.4-4.18) et tableaux (4.3-4.22), on peut dire que les deux méthodes BdF et AdD donnent les mêmes résultats de simulation que ce soit sur les paramètres de sûreté de fonctionnement du HIPPS R(t) F(t), U(t), W(t), ou la métrique MTTF MTBF MUT, et la MDT. Ainsi que le calcul des différents facteurs d'importances. Ils conservent le même classement des composants selon leurs facteurs d'importances.

D'après les tableaux 4.12 et 4.22, le MIF est un indicateur de fiabilité, donc pour augmenter la fiabilité du HIPPS, il est nécessaire de fiabiliser : l'automate programmable LS en première position, ensuite en considérant les vannes d'arrêt d'urgence SDV1, SDV2 et les solénoïdes vannes SV1, SV2 en troisième place.

Le CIF utilisé pour détection des composants concernés par une maintenance préventive, et ceux qui font l'objet d'une maintenance corrective. Selon le tableau 4.21 les vannes d'arrêt d'urgence SDV1, SDV2 sont les éléments à surveiller en première lieu, le deuxième composant à considérer le :

LS, en vue de l'existence d'une seule unité de traitement donc sa panne va provoquer la défaillance globale du HIPPS. Ensuite les solénoïdes vannes SV1, SV2 qui fonctionnent d'une manière séquentielle avec les SDV1, SDV2 .Les éléments finales à considérer sont les transmetteurs PT1, PT2, PT3.

En conclusion : les vannes SDV1, SDV2, l'unité de traitement LS, et les solénoïdes SV1, SV2 font l'objet d'une maintenance préventive systématique ou conditionnelle. Tandis que les transmetteurs PT1, PT2, PT3, sont concernés par une maintenance corrective, car l'intervention est effectuée après la défaillance, puisque leurs pannes n'aurait pas assez d'influence.

Pour le DIF, et d'après les tableaux 4.17 et 4.18 on constate que le CIF et le DIF donnent les mêmes classements, et mêmes résultats de simulation, en particulier pour les composants les plus vulnérables unité de traitement (LS), les vannes d'arrêt d'urgence (SDV1, SDV2) et les vannes solénoïdes (SV1, SV2).

D'après le classement des composants dans le tableau 4.19, le RAW nous permet d'extraire les éléments à probabilité de défaillance faible, mais dont la perte de la mission se traduit par une forte augmentation du risque.

Selon le tableau 4.20, le RRW nous permet de sélectionner les composants qui sont les meilleurs candidats pour les efforts visant à améliorer la fiabilité du HIPPS.

Pour le facteur de Barlow et Proschan (BP), les composants ayant un BP élevé ont un effet significatif sur les performances globales du système étudié. D'après le tableau 4.22 le LS aura une grande influence sur la fiabilité du HIPPS. Le BP, MIF, et CIF donnent le même ordre de classement, alors ils sont des critères de base pour la planification et l'orientation de la maintenance du HIPPS.

Dans cette phase de diagnostic les deux approches AdD et BdF fournissent les mêmes résultats de simulation que ce soit pour les différents paramètres de la sûreté de fonctionnement R(t), F(t) U(t), W(t), ou pour la métrique MTTF, MTBF, MUT, et MDT. Les deux approches fournissent un classement similaire de mesure d'importances.

Le calcul des différents facteurs MIF, CIF, DIF, RAW RRW, et BP, constituent un outil très efficace d'aide à la conception et d'aide précieuse au diagnostic des pannes. Dans notre analyse, le MIF RAW et DIF, nous permet d'identifier les composants sur lesquels il faudrait agir afin d'améliorer les performances du HIPPS à moindre coût et moindre effort, donc il faut les utilisés au stade de conception. Tandis que pour le CIF RRW et BP, nous permet d'identifier les composants responsables à la mise en défaillance du HIPPS. Ces facteurs contribuent à réduire le temps de localisation des pannes, et sont des critères essentiels pour la planification de la maintenance, ce qui impose leurs usages au stade d'exploitation.

4.4. Analyse des performances du HIPPS par considération des DCCs via le modèle Beta.

4.4.1. Modélisation dysfonctionnelle du HIPPS par Arbre de Défaillance (AdD)

Dans cette deuxième phase, on traite l'implémentation du HIPPS, par les deux techniques précédentes : bloc de fiabilité et arbre de défaillance avec la prise en compte des DCCs.

L'arbre de défaillance illustré dans la Figure 4.18, illustre une démarche structurée et descendante de l'aspect dysfonctionnelle du HIPPS. Nous calculons les mêmes paramètres de sûreté de fonctionnement que dans la phase précédente. Objectif est de quantifier l'effet du DCCs sur les performances globales du HIPPS. En étape de discussion nous effectuons une étude comparative entre les résultats de simulation réalisés en première phase et celles de la deuxième phase. Les DCCs ont été implémenté via le modèle Beta, puisque c'est le modèle recommandé par la norme CEI61508 et 615011. Les DCCS ont été inclus au niveau :

- Des Transmetteurs de pression PT1, PT2, PT3 avec un taux de 15% du facteur Beta [6]
- Des Vannes d'arrêt d'urgence SDV1, SDV2 et les solénoïdes vannes SV1, SV2, avec un

Taux de 12% du coefficient Beta [6]

On fixe la séquence temporelle de calculs des différents indicateurs à 5 ans.

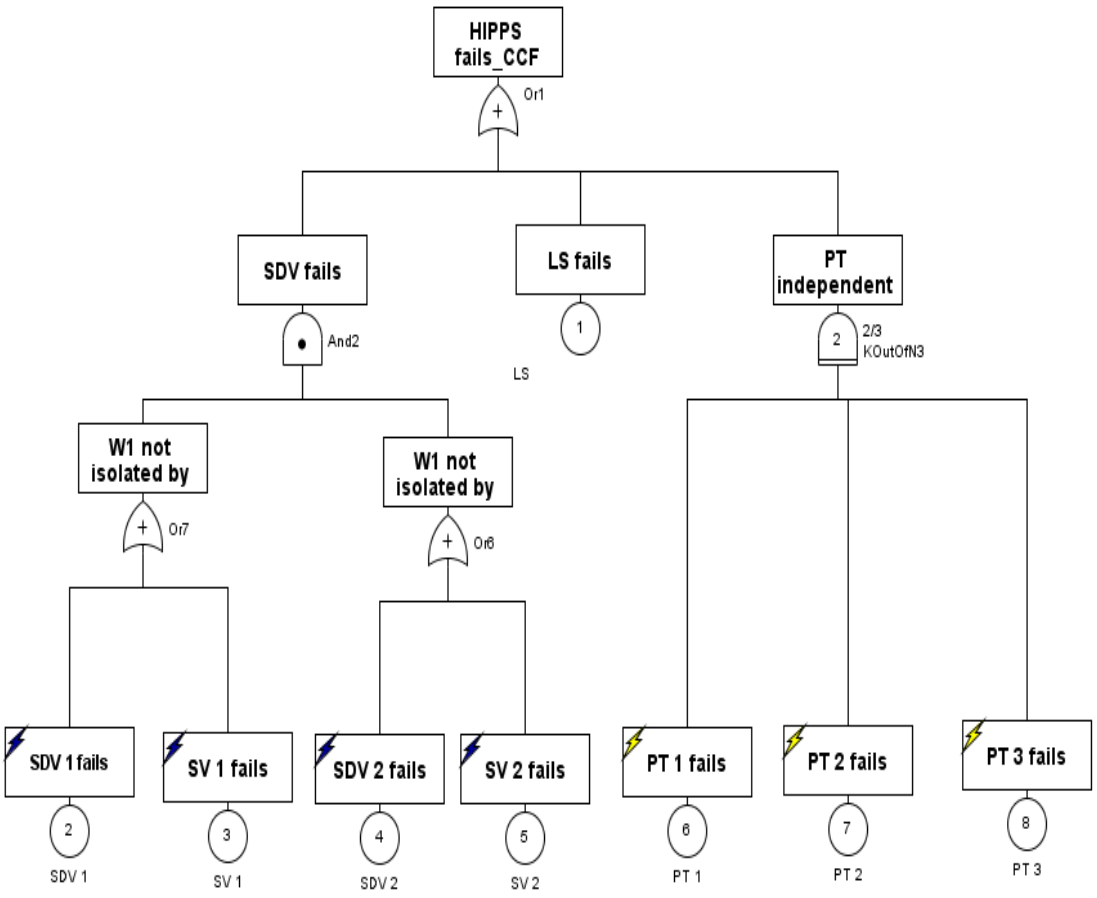


Figure 4.19 : Arbre de défaillance du HIPPS en considérant les DCCs

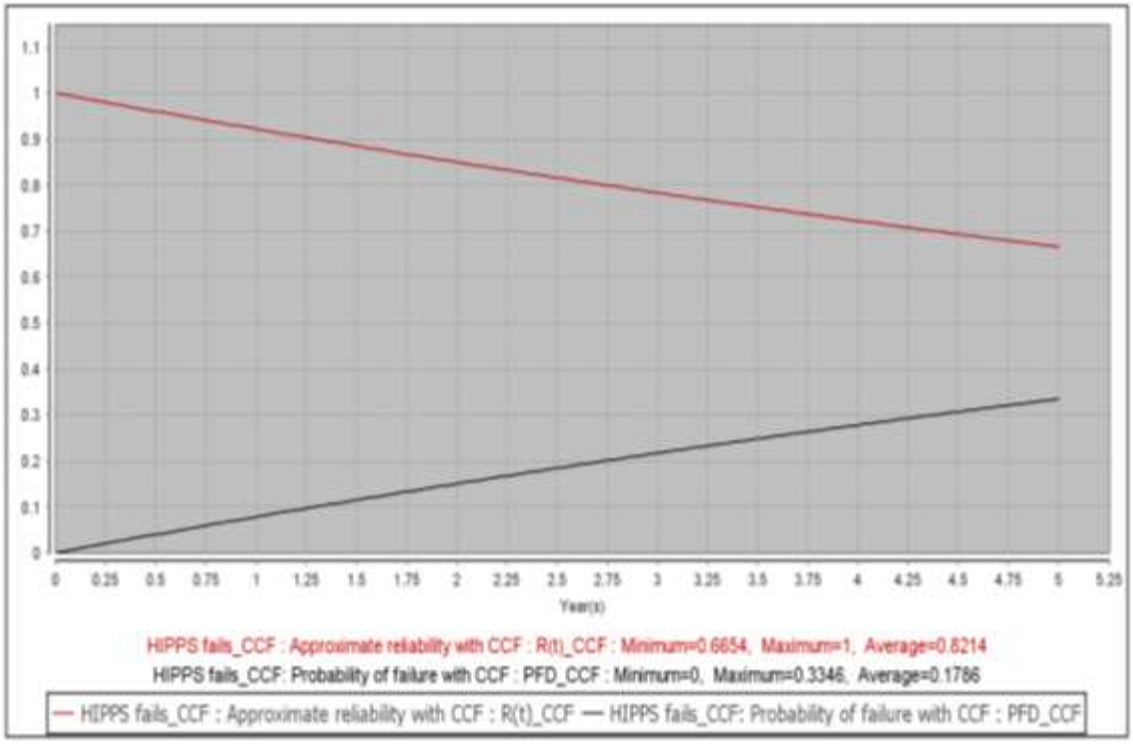


Figure 4.20 : Fonction de fiabilité et fonction cumulée de défaillance en considération des DCCs par AdD.

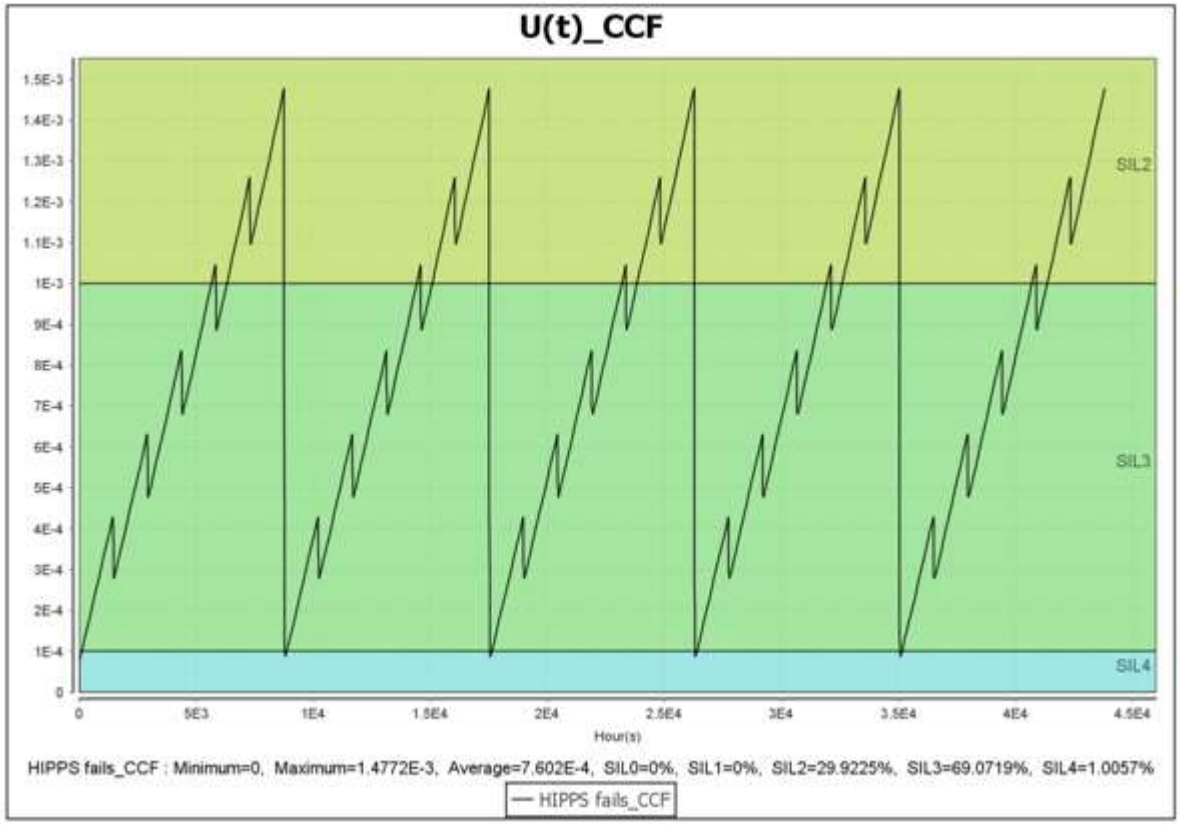


Figure 4.21 : Evolution du SIL en considération des DCCs par AdD.

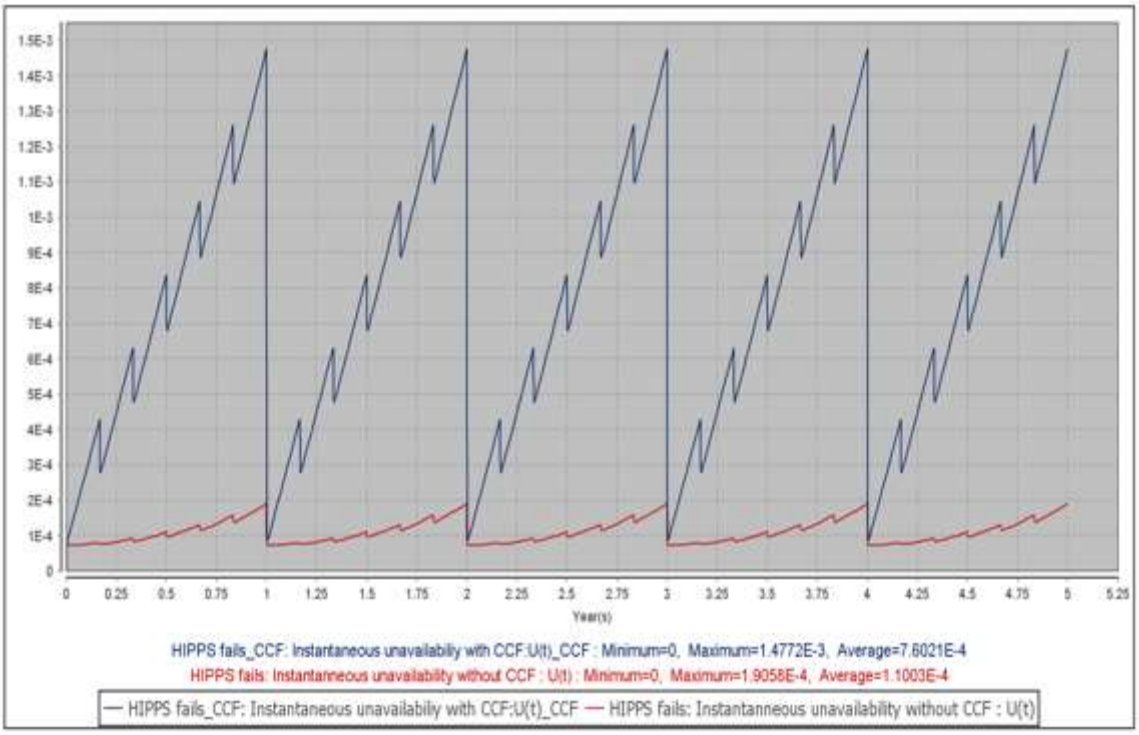


Figure 4.22 : Comparaison entre le SIL avec et sans DCCs par AdD.

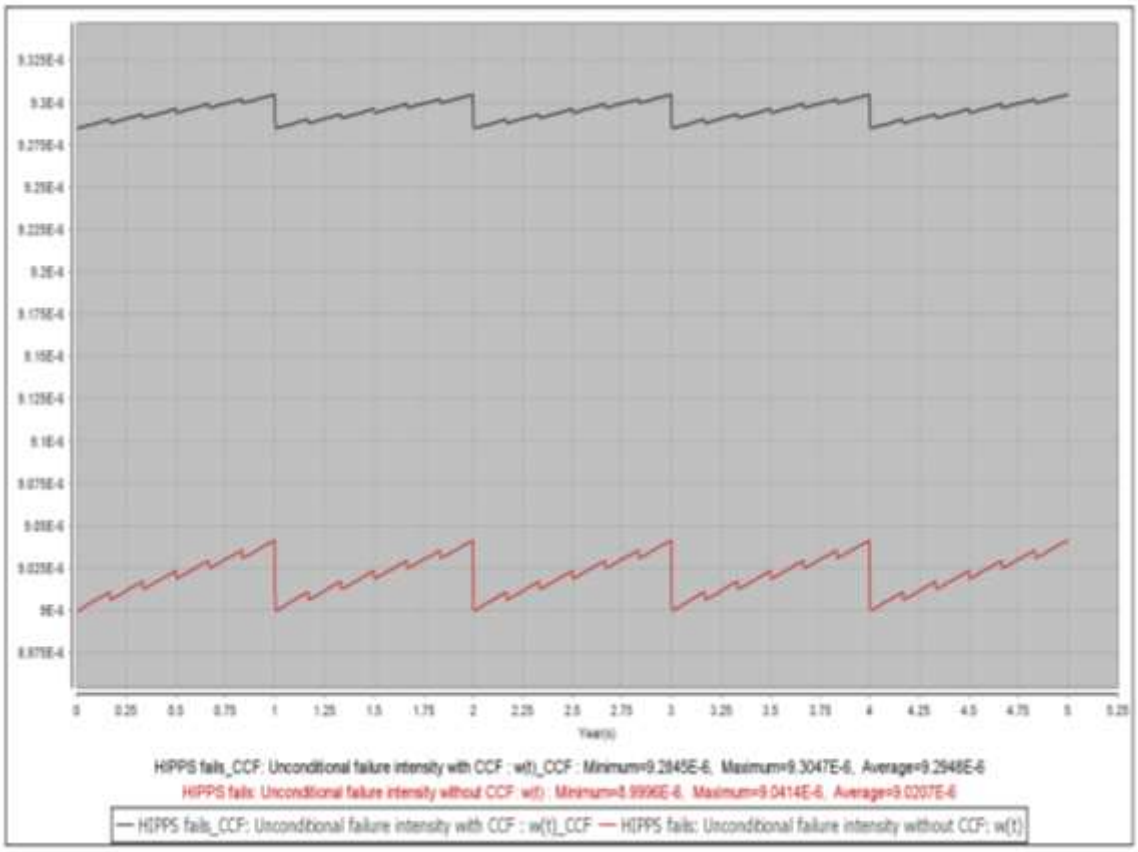


Figure 4.23 : Comparaison entre les fréquences de panne avec et sans DCCs par AdD.

Le tableau 4.23 présente les valeurs moyennes de tous les paramètres calculés dans la première et la deuxième phase via la méthode arbre de défaillance.

Tableau 4.23 : Comparaison entre les différents paramètres du HIPPS avec et sans DCCs.

Méthode: AdD							
$R(t)_{avg}$	$R(t)_{avg}$_DCC	$F(t)_{avg}$	$F(t)_{avg}$_DCC	$U(t)_{avg}$	$U(t)_{avg}$_DCC	$W(t)_{avg}$	$W(t)_{avg}$_DCC
0.8261	0.8214	0.1739	0.1786	1.1003E-4	7.6021E-4	9.0207E-6	9.2948E-6

D'après le tableau 4.23 on constate que les DCCs ont pour effet de réduire la valeur moyenne de la fiabilité R(t), d'augmenter la valeur moyenne de la fonction défaillance F(t), et aussi de réduire la valeur moyenne de l'indisponibilité instantanée U(t), avec une importance portion, qui représente réellement la dégradation du niveau du SIL pour le HIPPS, tandis que une augmentation très légère au niveau de la fréquence de défaillance W(t).

Tableau 4.24 : Comparaison entre la métrique du HIPPS avec et sans DCCs.

Technique: AdD				
Indicateur	MTTF	MDT	MUT	MTBF
Indicateur sans DCCs	1.1084E5h	12.1973h	1.1084E5h	1.1086E5h
Indicateur avec DCCs	1.0751E5h	81.7895h	1.0751E5h	1.0759E5h

Le tableau 4.24 présente les différents indicateurs de la métrique du HIPPS avec et sans prise en considération des DCCs. Ces mesures ont une importance vitale pour confirmer si le HIPPS répond aux exigences de la sûreté. Selon ce tableau les DCCs réduit le MTTF, le MUT par **3330** heures ce qui équivaut à **138.75** jours, et le MTBF par **3270 heures**, ou **136.25 jours**, mais augmente le MDT par **69,59 heures**, qui est approximativement **3jours.**

4.4.2. Modélisation fonctionnelle du HIPPS par blocs de fiabilité (BdFs)

Le module Bloc de Fiabilité (Reliability Bloc Diagram : RBD), nous offre :

- Une facilité et une rapidité d'élaboration de l'aspect fonctionnelle du HIPPS.
- Il est très adapté à notre système d'étude (HIPPS), puisque il nous donne une découpe technique très proche de la découpe fonctionnelle du HIPPS.
- Il permet de visualiser directement les redondances et génère et regroupe les blocs avec les mêmes DCCs
- Permet l'implémentation du modèle Beta pour une évaluation exacte des défaillances de la cause communes, comme il est illustré à la figure 4. 24.

Le taux des DCCs pour les transmetteurs est de 15% du facteur Beta [6].

Et pour les vannes est de 12% de taux Beta [6].

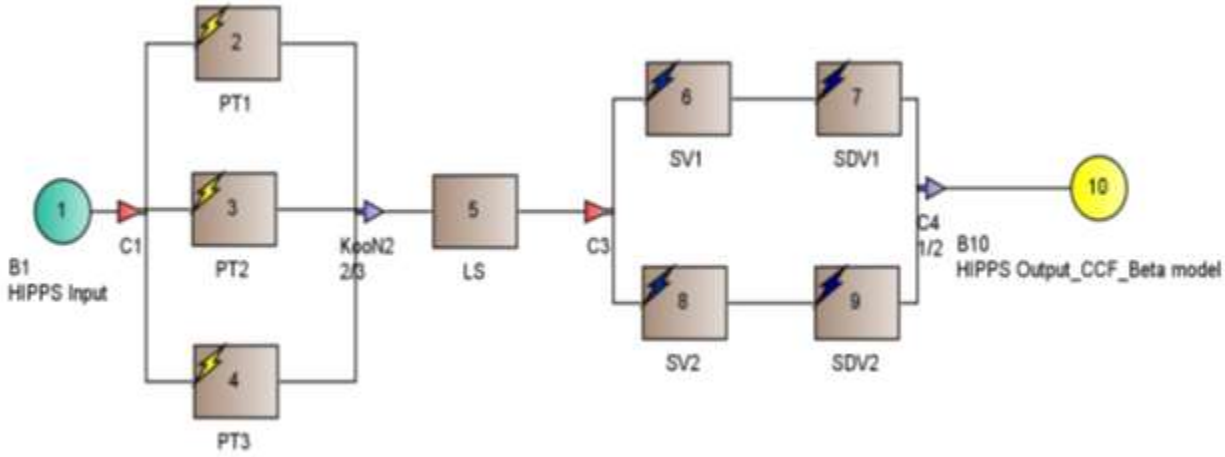


Figure 4.24 : Bloc diagramme de fiabilité relatif au HIPPS en prise en compte des DCCs.

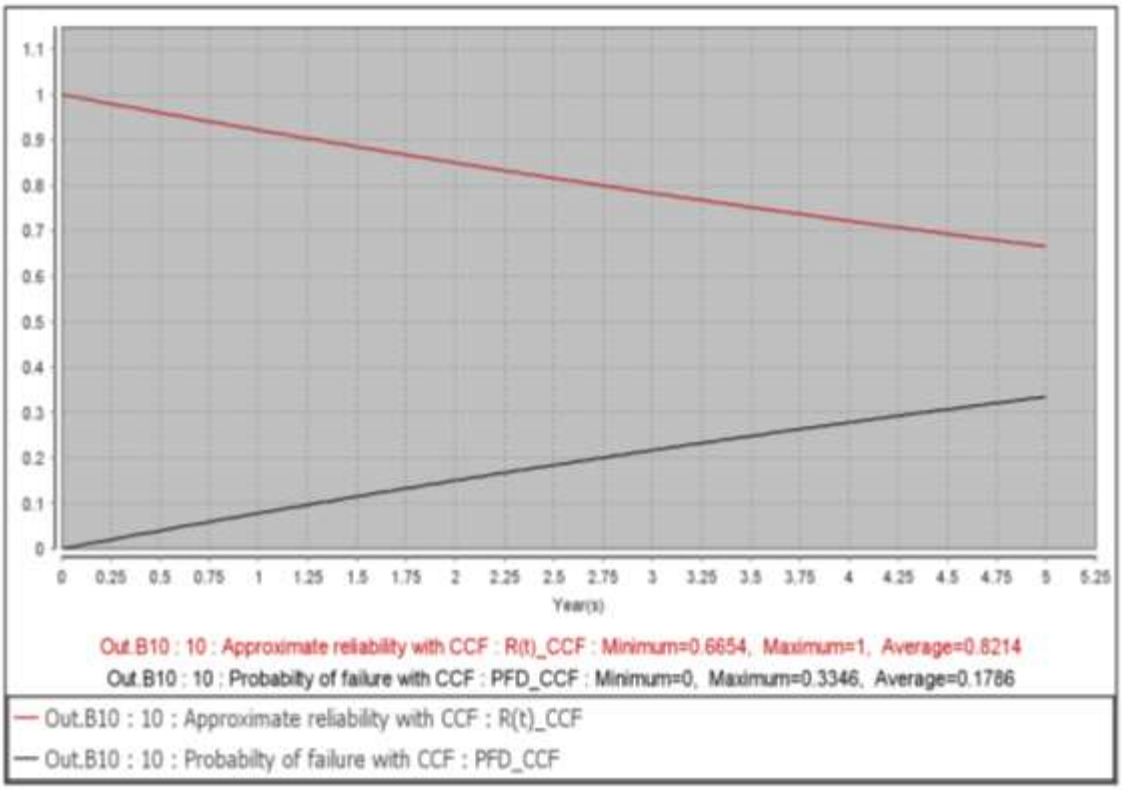


Figure 4.25 : Fonction cumulée de fiabilité et de défaillance relative au HIPPS avec DCCs par le BdF.

La figure 4.26 affiche l'évolution du niveau d'intégrité (SIL), pour le HIPPS en présence des DCCs.

La figure 4.27 affiche l'évolution des deux courbes SIL, en présence et en absence des DCCs pour l'objectif de mise en évidence de l'effet du DCCs.

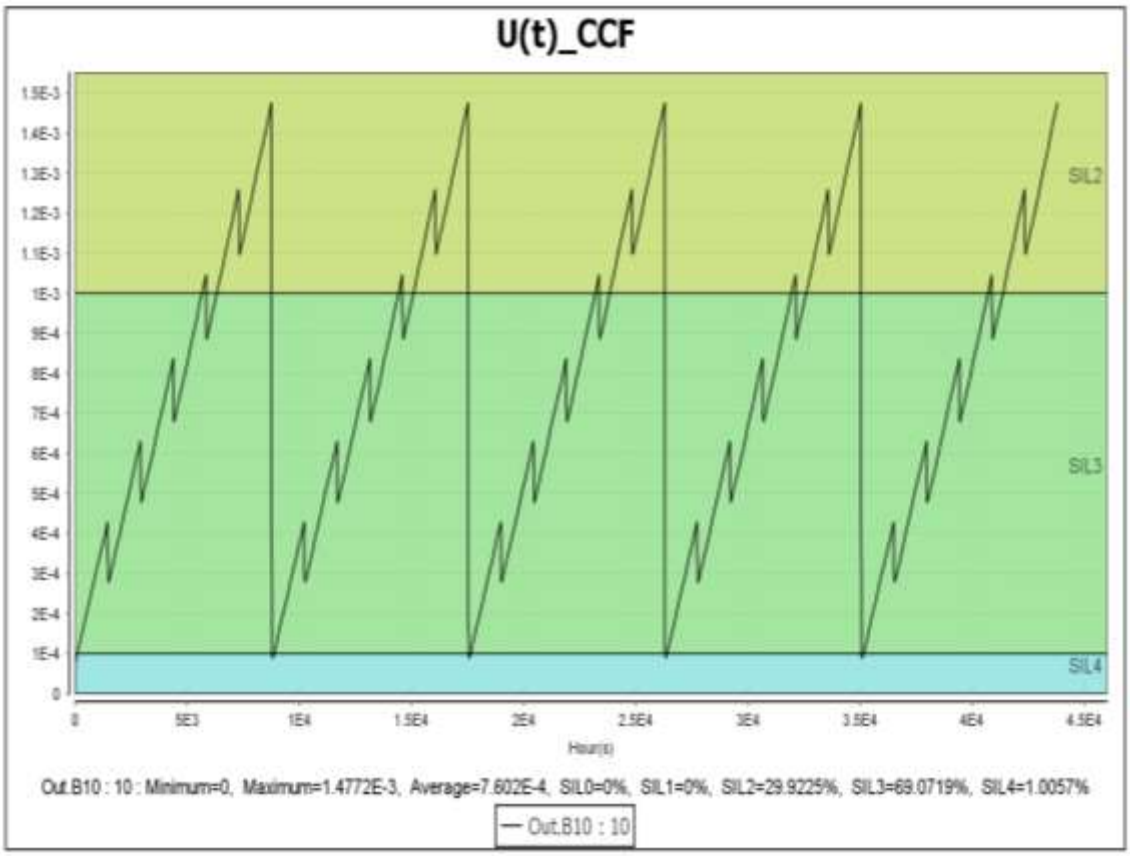


Figure 4.26 : Evolution du SIL par la prise en compte des DCCs par le BdF.

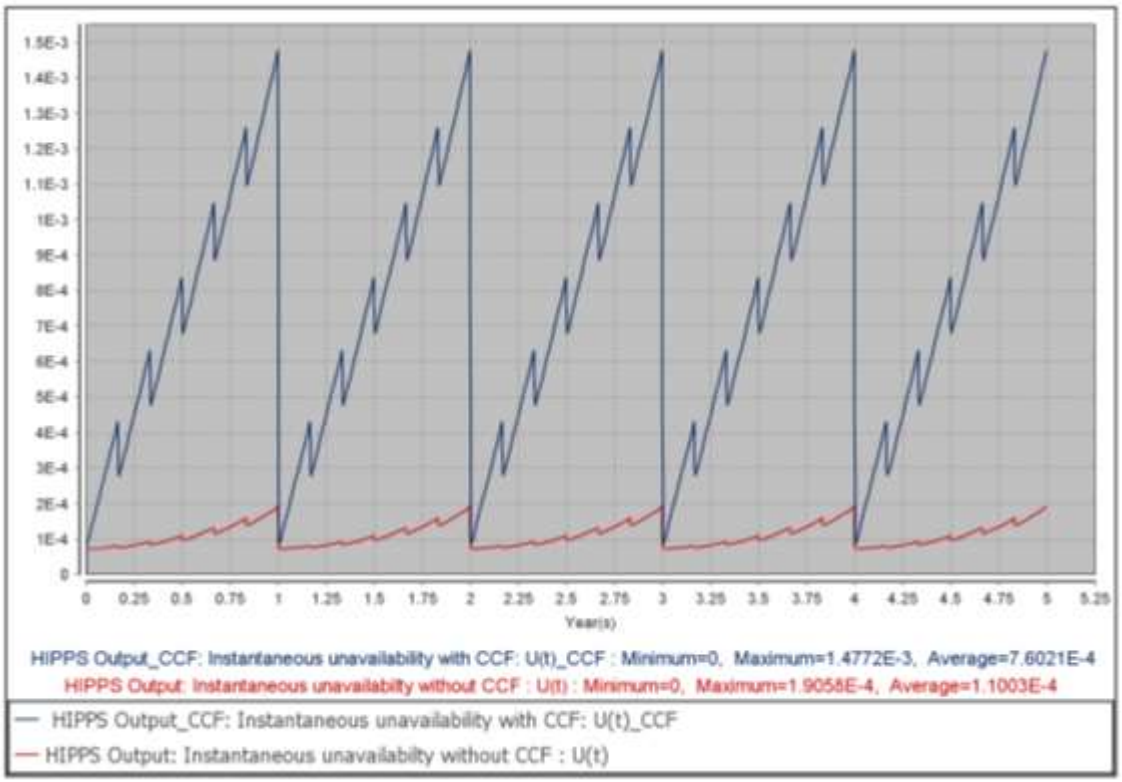


Figure 4.27 : Comparaison ente le SIL avec et sans DCCs par le BdF.

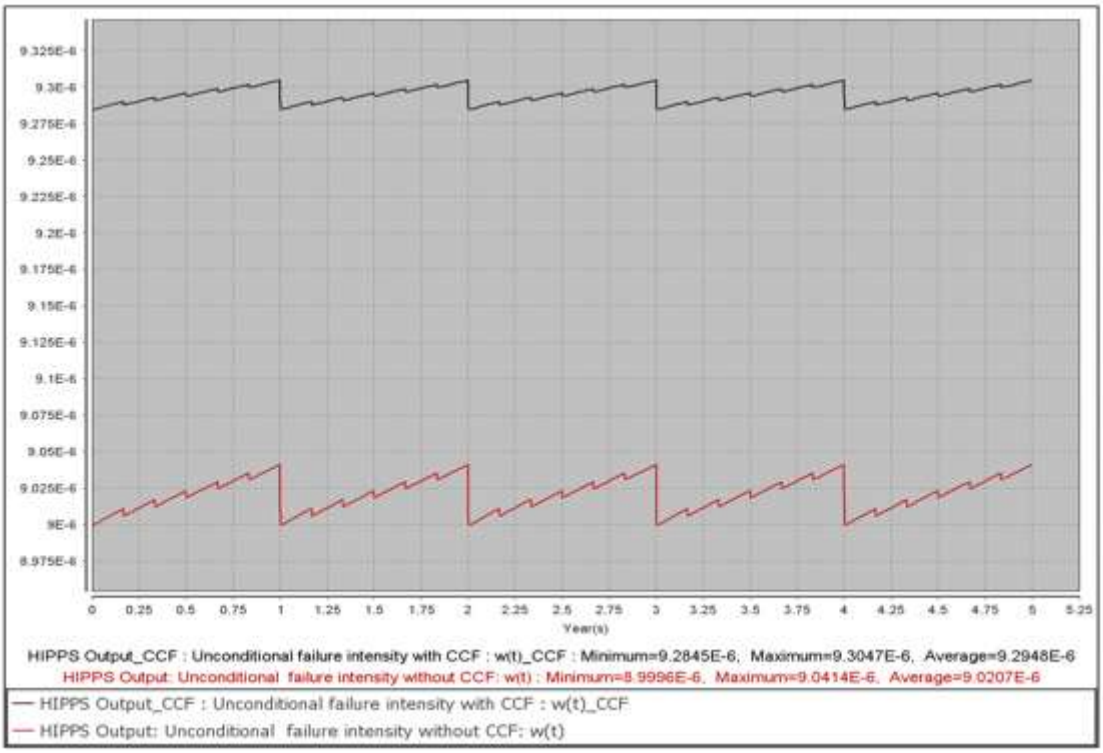


Figure 4.28 : Comparaison entre les fréquences de panne avec et sans DCCs par le BdF.

Le tableau 4.25 illustre une comparaison entre les différents paramètres de sûreté avec et sans la prise en compte des DCCs fournit par la méthode BdF.

Tableau 4.25 : Comparaison entre les différents paramètres du HIPPS avec et sans DCCs par le BdF.

Technique : BdF							
$R(t)_{avg}$	$R(t)_{avg\_DCC}$	$F(t)_{avg}$	$F(t)_{avg\_DCC}$	$U(t)_{avg}$	$U(t)_{avg\_DCC}$	$W(t)_{avg}$	$W(t)_{avg\_DCC}$
0.8261	0.8214	0.1739	0.1786	1.1003E-4	7.6021E-4	9.0207E-6	9.2948E-6

Le tableau 4.26 montre les paramètres de la métrique du HIPPS avec et sans considération des DCCs, obtenus par l'analyse fonctionnelle du système.

Tableau 4.26 : Comparaison entre la métrique du HIPPS avec et sans DCCs par le BdF.

Technique : RBD				
Indicateur	**MTTF**	**MDT**	**MUT**	**MTBF**
Indicateur sans DCCs	1.1084E5h	12.1971h	1.1084E5h	1.1086E5h
Indicateur avec DCCs	1.0751E5h	81.7893h	1.0751E5h	1.0759E5h

D'après les tableaux 4.25, et 4.26 , on constate que les DCCs ont un effet négatif sur les performances du HIPPS, puisque il ya une influence négative sur la fiabilité **R(t)**, sur la fonction de probabilité de défaillance **F(t)**, ainsi que l'indisponibilité instantanée **U(t)**, et la fréquence de l'évènement indésirable W(t). Cette influence négative concerne également la métrique : **MTTF, MTBF, MUT**, et le **MDT**. D'après le tableau 4.26, on remarque que les DCCs diminue le **MTTF** de

3330 heures ce qui équivalent à **138.75 jours**, de même pour le **MUT**, tandis que le **MTBF** diminue de **3270 heures**, ou **136.25 jours**. Cependant on constate que les DCCs augmentent le **MDT** de **69. 59 heures**, ce qui est correspond à **3 jours.** Car le **MDT** est le temps moyen dont le HIPPS est en arrêt de fonctionnement, ceci inclue tous les temps moyens de logistiques (détection de la défaillance et en plus l'arrivée des moyens humaines et matériels), et les temps moyens techniques de réparation pour la maintenance préventive et corrective.

le MDT est très négligeable devant le MUT. $MDT \ll MUT$. Ce qui est théoriquement vérifié pour de nombreux systèmes.

Pour prouver l'efficacité et la robustesse des deux méthodes BdF et AdD, on a effectué les calculs des différents paramètres précédents pour les séquences temporelles suivantes : **25,** et **50 ans.**

Le tableau 4.27 présente les résultats de simulation avec et sans la prise en compte des DCCs pour les séquences temporelles : **5, 25 et 50 ans.** Ces résultats montrent que le BdF et l'AdD fournissent les mêmes résultats de simulation pour tous les paramètres de la sûreté de fonctionnement qui concerne le HIPPS , la valeur moyenne de fiabilité $R(t)_{avg}$, la valeur moyenne de l'indisponibilité $U(t)_{avg}$, et la valeur moyenne de la fréquence $W(t)_{avg}$ pour les séquences de temps 5, 25 et 25 ans. Notons que la fréquence préserve une seule valeur moyenne de 5 à 50 ans.

Il est constaté que: $\mathbf{MTTF = MUT}$ dans les deux phases d'étude avec et sans prise en compte des DCCs, par l'usage des deux approches et durant les différents séquences temporelle de 5, 25, et 50 ans. Ce qui signifie que lorsque le HIPPS est remis en service après la défaillance, tous ses éléments défaillants ont été réparés. Ce qui montre une grande rentabilité et une meilleure maintenabilité pour le système étudié [1].

Le tableau 4.27 montre également la réduction de la fiabilité du HIPPS dans la phase de diagnostic de **82.61% à 24.62%** le long de 50 ans, et de **82.14% à 24.13%** dans la phase d'évaluation des DCCs. Ce qui explique les dégradations physiques (matérielles) des différents composants du système.

Notons par ailleurs que la fiabilité se dégrade faiblement durant la même séquence temporelle. Le HIPPS demeure donc fiable dans les deux phases d'études, en utilisant les deux approches.

Le tableau 4.28 présente les temps moyens en unité de l'heure, et calculés par le BdF et l'AdD durant les deux phases d'études.

Tableau 4.27 : Collection des résultats de simulation de l'implémentation du HIPPS pour les séquences temporelles 5, 25 et 50 ans par l'AdD et BdF.

Approches	*Technique: Arbre de Défaillance*						*Technique : Bloc diagramme de Fiabilité*					
Etudes	*Etude sans CCFs*			*Etude avec DCCs*			*Etude sans DCCs*			*Etude avec DCCs*		
Paramètre / *Iterations*	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)_{\_avg}$ (h^{-1})	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)_{\_avg}$ (h^{-1})	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)_{\_avg}$ (h^{-1})	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)_{\_avg}$ (h^{-1})
5 -ans	*0.8261*	*1.1003E-4*	*9.0207E-6*	*0.8214*	*7.6021E-4*	*9.2948E-6*	*0.8261*	*1.1003E-4*	*9.0207E-6*	*0.8214*	*7.6021E-4*	*9.2948E-6*
25- ans	*0.436*	*1.1047E-4*	*9.0207E-6*	*0.4269*	*7.6076E-4*	*9.2948E-6*	*0.436*	*1.1046E-4*	*9.0207E-6*	*0.4269*	*7.6074E-4*	*9.2948E-6*
50 -ans	*0.2462*	*1.1088E-4*	*9.0207E-6*	*0.2413*	*7.611E-4*	*9.2948E-6*	*0.2482*	*1.1086E-4*	*9.0207E-6*	*0.2413*	*7.6108E-4*	*9.2948E-6*

Tableau 4.28 : Collection de la métrique du HIPPS pour les séquences temporelle 5, 25 et50 ans par l'AdD et le BdF.

Approches	***Technique Arbre de Défaillance***								***Technique :Bloc diagramme de Fiabilité***							
Etudes	***Etude sans DCCs***				***Etude avec DCCs***				***Etude sans DCCs***				***Etude avec DCCs***			
Indicateur / Iterations	**MTTF**	**MDT**	**MUT**	**MTBF**	**MTTF**	**MDT**	**MUT**	**MTBF**	**MTTF**	**MDT**	**MUT**	**MTBF**	**MTTF**	**MDT**	**MUT**	**MTBF**
5- ans	1.1084E5	12.1973	1.1084E5	1.1086E5	1.0751E5	81.7895	1.0751E5	1.0759E5	1.1084E5	12.1791	1.1084E5	1.1086E5	1.0751E5	81.7893	1.0751E5	1.0759E5
25- ans	1.1084E5	12.2468	1.1084E5	1.1086E5	1.0751E5	81.8479	1.0751E5	1.0759E5	1.1084E5	12.2448	1.1084E5	1.1086E5	1.0751E5	81.8464	1.0751E5	1.0759E5
50- ans	1.1084E5	12.292	1.1084E5	1.1086E5	1.0751E5	81.8843	1.0751E5	1.0759E5	1.1084E5	12.2899	1.1084E5	1.1086E5	1.0751E5	81.8828	1.0751E5	1.0759E5

La figure 4.29 représente la comparaison de l'effet des DCCs sur la fiabilité du HIPPS à travers les séquences temporelles de 5, 25 et 50 ans.

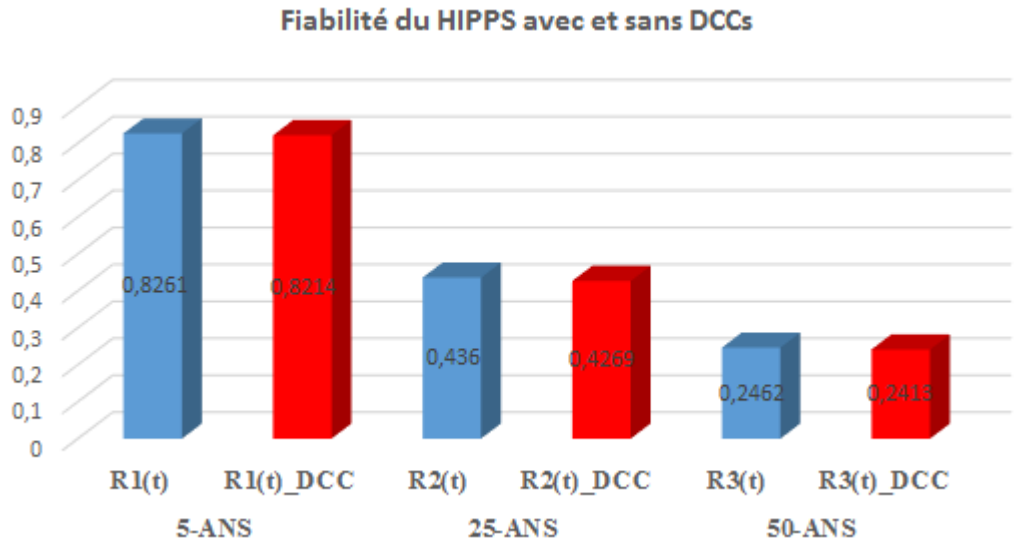


Figure 4. 29 : Variation de la fiabilité du HIPPS avec et sans la prise en compte des DCCs à travers les séquences temporelle de 5, 25 et 50 ans.

La figure 4.30 représente la comparaison de l'effet des DCCs sur la probabilité de défaillance du HIPPS à travers les séquences temporelles de 5, 25 et 50 ans.

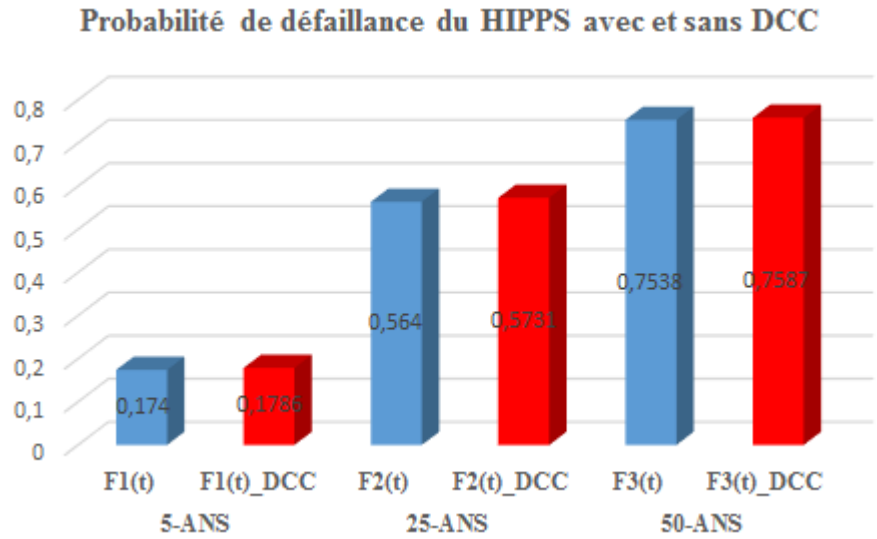


Figure 4.30 : Variation de la probabilité de défaillance du HIPPS avec et sans la prise en compte des DCCs à travers les séquences temporelle de 5, 25 et 50 ans.

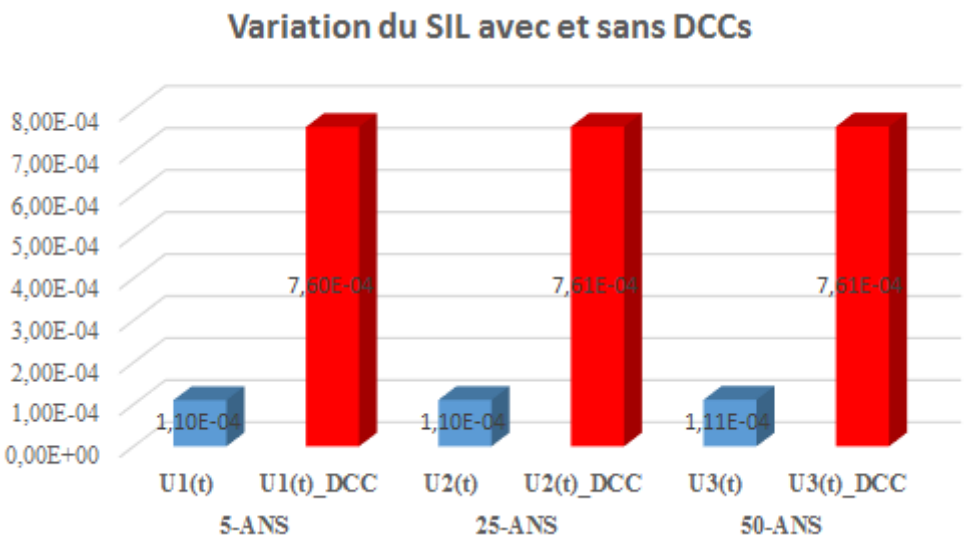


Figure 4.31 : Effet des DCCs sur le niveau d'intégrité de sécurité (SIL) à travers les séquences temporelle de 5, 25 et 50 ans.

D'après la figure 4.31, le SIL du HIPPS varié au court du temps et les DCCs ont une grande influence sur la diminution du niveau d'intégrité de sécurité.

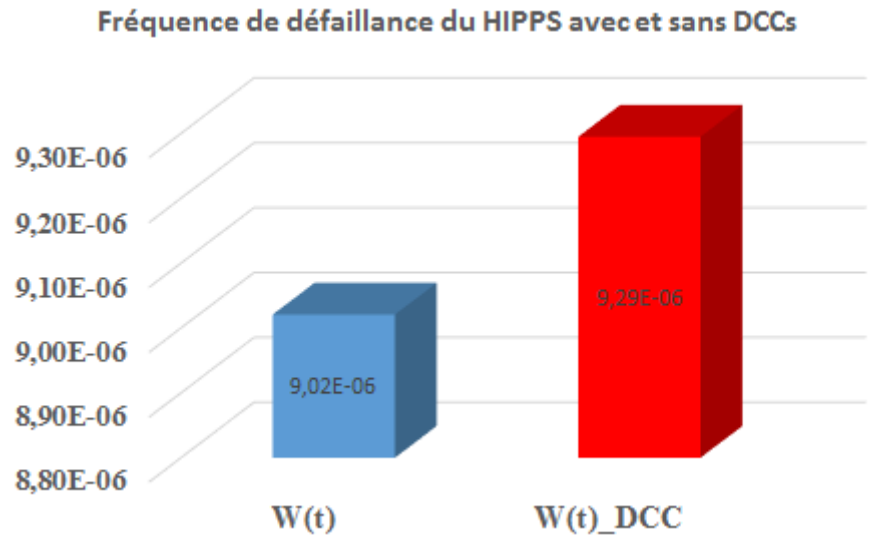


Figure 4. 32 : Effet des DCCs sur la fréquence de défaillance relative au HIPPS.

D'après la figure 4.32, la fréquence de défaillance du HIPPS est presque invariable dans les deux phases d'études (avec et sans DCCs), pour les différentes séquences de temps.

W(t) =9.02E-06 h^{-1} ce qui est équivalent à 79E-06 an^{-1} et W(t)_DCC=9.29E-06, ce qui est équivalent à 81.38 E-06 an^{-1}. Donc les DCCs ont un peu d'influence pour provoquer plus de défaillances critiques au niveau du système.

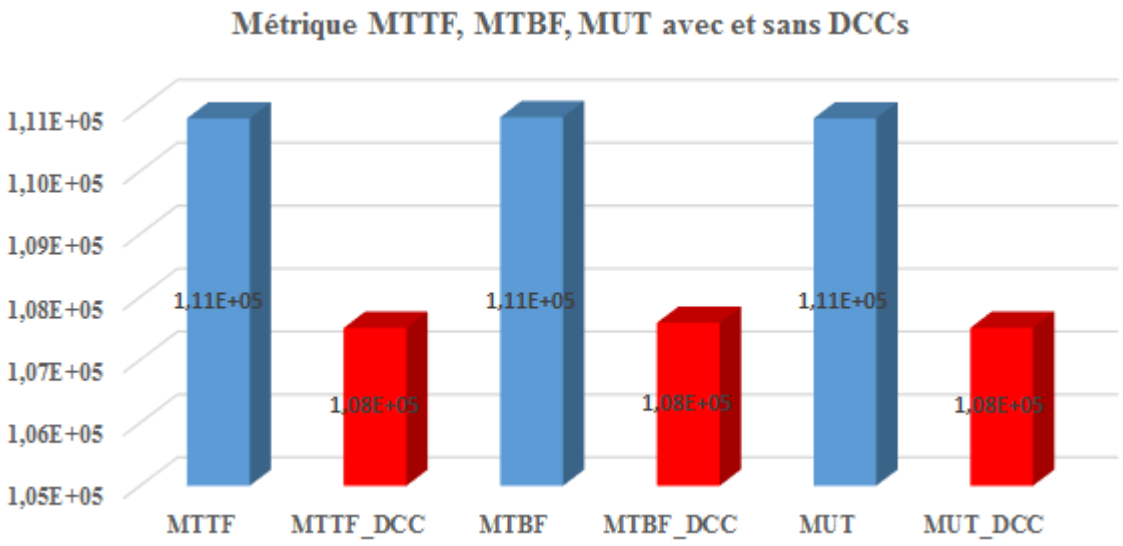


Figure 4.33 : Effet des DCCs sur la métrique : MTTF, MTBF et MUT relatives au HIPPS.

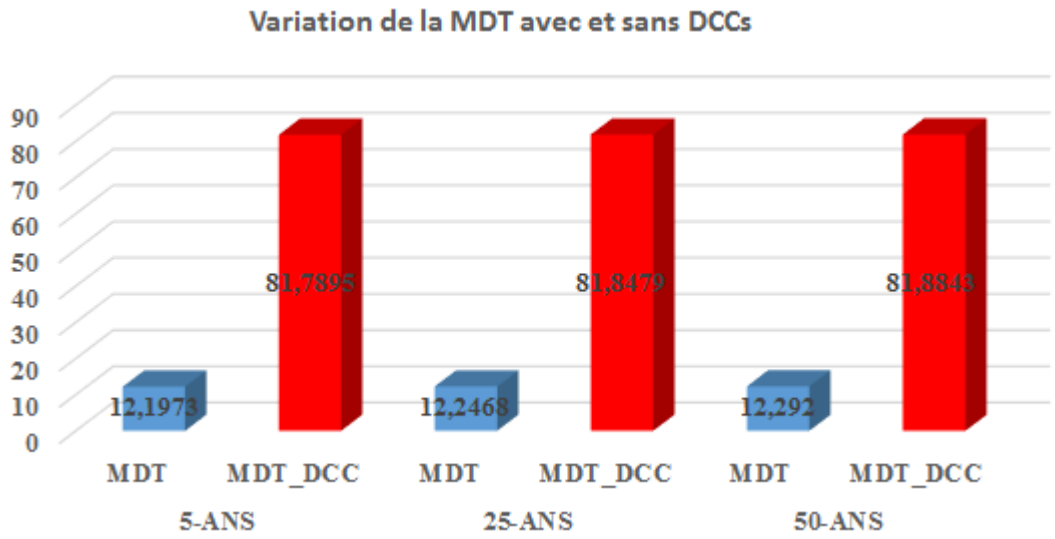


Figure 4.34 : Effet des DCCs sur la MDT du HIPPS à travers les séquences temporelle de 5, 25 et 50 ans.

Les DCCs augmentent le temps Moyen de panne (MDT) avec une grande proportion, ce qui traduit l'augmentation du temps moyen de détection de la panne, et de la durée d'intervention, la durée de réparation et la durée de remise en service. Cela a pour effet de prolonger le temps des actions de maintenance préventive et corrective et dégrade la capacité de production de l'installation industrielle.

Le tableau 4.28 montre que les temps moyens suivant : MTTF MUT et MTBF préserve une seule valeur de 5 à 50 ans, ce qui nous informe que le HIPPS répond aux exigences de sûreté de fonctionnement.

Mais la MDT augmente avec un facteur acceptable de 5 à 50 ans, ce qui indique une bonne robustesse du HIPPS contre les DCCs.

D'après les tableaux 4.27 et 28, on résume que les égalités suivantes sont vérifiées, dans les deux phases d'études.

$$MTTF = MUT = \frac{1}{W(t)_{avg}} \qquad et \qquad MTTF_{DCC} = \quad MUT_{DCC} = \frac{1}{W(t)_{avg\_DCC}}$$

Qui est un critère sur les bonnes caractéristiques de fiabilité, et de disponibilité de notre système considéré en présence et en absence des DCCs.

Le tableau 4.29 affiche les différents facteurs de l'effet des DCCs sur les paramètres de sûreté de fonctionnement suivant : R(t), U(t), W(t), MTTF, MTBF, MUT, et la MDT, obtenus par les deux méthodes.

Tableau 4.29 : Calcul du facteur effet des DCCs résidus par les deux approches AdD et BdF.

Paramètre / **Iterations**		$\frac{R(t)_{avg}}{R(t)_{avg\_DCC}}$	$\frac{U(t)_{avg\_DCC}}{U(t)_{avg}}$	$\frac{W(t)_{avg\_DCC}}{W(t)_{avg}}$	$\frac{MTTF}{MTTF_{DCC}}$	$\frac{MTBF}{MTBF_{DCC}}$	$\frac{MUT}{MUT_{DCC}}$	$\frac{MDT_{DCC}}{MDT}$
5 - ans	**AdD**	**1.0057**	**6.9091**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.7055**
	BdF	**1.0057**	**6.9091**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.7155**
25- ans	**AdD**	**1.021**	**6.8865**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.6832**
	BdF	**1.021**	**6.8870**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.6841**
50- ans	**AdD**	**1.020**	**6.8641**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.6615**
	BdF	**1.028**	**6.8652**	**1.0303**	**1.0309**	**1.0303**	**1.0309**	**6.6626**

On constate que le facteur de réduction de fiabilité augmente légèrement de **1.0057 à 1.028 durant 5 à 50 ans.**

Notons que pour les paramètres suivants, **W(t), le MTTF, le MTBF, et le MUT**, le facteur du DCCs demeure approximativement constant **(environ 1.03)**. Donc il est évident que le HIPPS préserve ces performances de sûreté de fonctionnement en présence des DCCs.

Pour l'indisponibilité instantanée **U(t)**, le facteur du DCCs est d'environ 6.9 qui sont un facteur de dégradation acceptable pour le niveau d'intégrité de sécurité (SIL). Dans cette phase, il est montré que le HIPPS préserve son SIL avec **69% dans la zone SIL3**, **1% dans la zone SIL4**, et **29.9 % dans la zone SIL2**. On remarque presque le même facteur DCCs pour **le MDT** qui est d'environ **6.7**. Ces indices prouvent la capacité du HIPPS de préserver ces performances en présence du DCCs.

D'après le tableau 4.29 les deux méthodes illustrent les facteurs du DCCs pour chacun des paramètres dans une même séquence de temps. Ce qui prouve la robustesse, l'exactitude, l'adéquation de la méthodologie utilisée dans l'évaluation des DCCs.

4.4.3. Discussion des résultats de simulation en considérant les DCCs

Dans cette deuxième phase nous avons abordé la modélisation des DCCs au niveau des transmetteurs PT_1, PT_2, PT_3 et au niveau des vannes SV_1, SV_2, SDV_1, SDV_2 via le modèle Beta, puisque c'est le modèle recommandé par la norme IEC61508 et 61511. Nous avons illustré par figures et tableaux l'effet négatif de ce type de défaillances sur les performances du HIPPS. Nous avons prouvé la similarité des résultats obtenus par les deux approches dans la rangé des paramètres R(t), F(t), U(t), et W(t), ainsi que la métrique MTTF, MTBF, MUT, et MDT pour les séquences temporelles 5, 25, et 50 ans. Le BdF et l'AdD montrent une évaluation exacte des différents facteurs de l'effet du DCCs d'après les tableaux 4.27, 4.28 et 4.29. D'après les résultats de simulation les DCCs ont un effet néfaste sur les performances suivantes Fiabilité, le niveau du SIL, la fréquence, et la capacité de production.

Après l'analyse qualitative qui inclus l'identification des parties concernées par les DCCs, le calcul des coupes minimales MCS, et l' analyse quantitative qui provoque le calcul des probabilités et les fréquences des différents évènements, et le calcul de la métrique de sûreté de fonctionnement pour les différents séquences temporelles, nos résultats prouvent que les deux formalismes BdF et l'AdD sont robustes, et puissantes pour l'implémentation des DCCs, au niveau du HIPPS, qui est un système instrumenté de sécurité fortement utilisé dans les installations pétrole et gaz, donc il doit être périodiquement testé pour relever les défaillances afin de le protéger contre les pannes

4.5. Conclusion

L'objectif de ce chapitre est l'analyse de la fiabilité, la disponibilité, et la maintenabilité d'un HIPPS existant en plateforme on-shore de la raffinerie de Skikda. On se basant sur une analyse qualitative et quantitative à travers deux phases : une première phase de diagnostic sans la prise en compte des DCCs, et une deuxième phase par la prise en considération des DCCs, et s'accordant en trois séquences temporelle : 5, 25 et 50 ans, par l'usage d'une analyse fonctionnelle et dysfonctionnelle respectivement par les deux formalismes BdF et AdD.

Dans la phase de diagnostic six facteurs d'importances sont implémentés : MIF, CIF, DIF, RAW, RRW, et BP. Généralement les composants possédant des valeurs élevés de mesure

d'importances ont un effet considérable sur les performances du HIPPS, tandis ceux qui ont des valeurs faibles ont une influence négligeable. La mesure d'importance est nécessaire pour l'optimisation du programme de maintenance. Ces mesures sont employées pour l'identification des composants critiques qui font l'objet d'une maintenance préventive qui nécessite des coûts élevés et des périodes considérablement prolongés pour le rétablissement en service. D'après nos résultats on a classé LS ou l'automate programmable, les vannes d'arrêts d'urgence : SDV_1, SDV_2 et les solénoïdes vannes : SV_1, SV_2 pour une maintenance préventive systématique ou conditionnelle. Mais les transmetteurs : PT_1, PT_2, PT_3 font l'objet d'une maintenance corrective. Nous avons montré par tableaux que les deux approches BdF et AdD donnent le même classement des composants du HIPPS selon leurs facteurs d'importance. Dans cette première phase l'analyse de la sûreté de fonctionnement du HIPPS a été effectué par le calcul des paramètres suivants : R(t), F(t), U(t) W(t), les coupes minimales : MCS, les temps moyens : MTTF, MTBF, MUT, et MDT. Après une étude comparative des résultats précédents illustrés par figures et tableaux nous avons confirmé que les deux méthodes fournissent les mêmes résultats qualitatifs et quantitatifs durant les différentes séquences temporelles, Cette phase vise la détection de la criticité et la vulnérabilité des composants pour une meilleure localisation des barrières de sécurité. Les méthodes BdF et AdD ont été utilisées dans la phase opérationnelle pour comprendre et corriger les erreurs de fonctionnement.

Pour la deuxième phase nous avons effectué une étude comparative entre les résultats obtenus par les deux approches avec la prise en compte des DCCs, par illustration de l'influence négative de ce type de défaillance sur les performances globales du HIPPS. Influence que nous résumons comme suit :

- Réduction de fiabilité R(t).
- Augmentation de probabilité de défaillance F(t), et de la fréquence de l'évènement redouté W(t).
- Augmentation de l'indisponibilité U(t), ou la dégradation du SIL.
- Réduction des temps moyens : MTTF, MTBF, et MUT.
- Augmentation de la MDT, ce qui provoque la réduction de la capacité de production.

Nous pouvons conclure, en se Basant sur notre analyse que le HIPPS considéré demeure fiable dans la phase d'évaluation des DCCs, ce qui prouve une capacité de persistante contre ce type de défaillances néfastes. Le choix d'un HIPPS avec des performances fiables éprouvées nous assurent une exploitation sûre et fiable de notre installation industrielle.

Conclusion générale et perspectives

La norme CEI 61508 représente un document normatif central pour la conception et l'exploitation des systèmes instrumentés de sécurité (SIS). Cette norme met en œuvre, en tant que cadre technique un modèle de cycle de vie de sécurité globale et adopte le concept de niveau d'intégrité de sécurité (SIL) qui spécifie les exigences (qualitatives et quantitatives) sur la fonction de sécurité implémenté au niveau des SISs. Les exigences quantitatives d'intégrité de sécurité (intégrité de sécurité du matériel) doivent être traduites en mesures cibles de défaillances. Ces derniers s'identifient à la probabilité moyenne de défaillance à la demande du SIS (PFD_{moy}) pour un système instrumenté de sécurité fonctionnant en « faible demande » et à sa probabilité de défaillance dangereuse par heure (PFH : probability of failure per hour) s'il est appelé à fonctionner en mode « demande élevée ou continu »

Les systèmes instrumentés de sécurité constituent une ligne défensive primordiale dans le processus, la chose qui nous a attiré pour réaliser une analyse justificative des indicateurs de performance d'un système de protection contre les surpressions de haute fiabilité (HIPPS). La vérification de l'aptitude du HIPPS à l'exécution correcte de ses fonctions constitue une étape très importante pour sa validation et son efficacité. Cet objectif fait l'objet de notre travail, pour cela nous avons organisé cette thèse comme suit :

Au niveau du premier chapitre nous avons d'abord présentés les éléments clés relatifs à la sûreté de fonctionnement puis la méthodologie utilisée dans l'analyse de risque et le diagnostic des pannes. Des mesures d'importances ont finalement été développées en termes de définition et de calcul probabiliste.

Le second chapitre a été consacré à la présentation des systèmes instrumentés de sécurité en termes de définition, constitution, architectures, et leurs différents paramètres de performances (PFD, PFH, SIL, SIF, SFF…). Le deuxième volet de ce chapitre était réservé aux différents détailles des HIPPS (types, SIL, fonction instrumenté de sécurité, rôle et justification, principe de fonctionnement…).

Le problème des Défaillances de Cause Commune (DCCs) a été détaillé au niveau du troisième chapitre. A ce titre nous avons défini les différents types de modélisations implicites et explicites des DCCs et par la suite nous avons exposé les modèles existant dans la littérature parmi lesquelles le modèle implicite du facteur Beta exploité dans notre analyse.

La défectuosité d'un HIPPS, peut sérieusement affecter le fonctionnement des installations, l'environnement et le personnel. La conception d'un HIPPS devrait être fondée sur des solides arguments techniques et économiques et des perspectives à long terme. Le rôle primordial de ces systèmes nous a amené à élaborer une analyse fonctionnelle et dysfonctionnelle d'un HIPPS existant à la plateforme onshore de la raffinerie de Skikda (RA1K) dans notre quatrième chapitre. L'analyse fonctionnelle a été élaborée par la méthode bloc diagramme de fiabilité (BdF), tandis que l'analyse dysfonctionnelle a été réalisée par la technique déductive arbre de défaillance (AdD). Notre analyse a été divisée en deux phases :

Une première phase de diagnostic sans la prise en compte des défaillances de cause commune. A travers cette phase nous avons calculé les différents attributs : fiabilité : R(t) probabilité de défaillance F(t), indisponibilité instantanée U(t) , et la fréquence de l'évènement redouté W(t), au bout d'une séquence temporelle de 5 ans . Une mesure d'importance a été ajoutée par la quantification des paramètres suivants : facteur de Birubaum (MIF), le facteur de Lambert (CIF), facteur de Fussel Vesely (DIF), le facteur d'augmentation de risque(RAW), le facteur de réduction de risque (RRW) et le facteur de Barlow et Proschan (BP). L'intérêt de ces mesures d'importances est double , ils servent d'aide à la conception (identification des points faibles)pour le système au stade de conception, et d'aide au diagnostic de pannes pour les systèmes au stade d'exploitation par génération d'une liste de contrôle ou, par une planification d'une stratégie de maintenance pour les composants constitutif du système.

Une seconde phase d'évaluation de l'effet des défaillances de cause commune sur les différents indicateurs de performances du HIPPS. Dans cette phase les DCCs ont été modélisé via le modèle Beta recommandé par la norme CEI 61508, les différents paramètres sont recalculés avec prise en compte des DCCs pour l'objectif d'effectuer une comparaison avec ceux calculés en première phase. Les résultats ont montré l'effet néfaste de ce type de défaillances sur les performances du HIPPS, à savoir réduction de la fiabilité, augmentation de la probabilité de défaillance, augmentation de l'indisponibilité instantanée et de la fréquence de l'évènement indésirable, diminution du SIL, diminution de MTTF, MTBF, et de MUT ainsi que l'augmentation de MDT, sans oublier la réduction de la capacité de production du complexe.

Notre analyse a été effectuée sur des séquences temporelles plus larges de 25 à 50 années dans l'objectif de tester l'exactitude, la robustesse, et la conformité de la méthodologie utilisée pour l'estimation des DCCs. Les résultats de simulation illustrent la capacité du HIPPS considéré en terme de maintenir ses caractéristiques fiabilistes en présence des DCCs. Les deux approches donnent les mêmes résultats de simulation à travers les deux phases d'études et le long de toutes les séquences temporelles (5, 25 et 50ans)

Dans cette thèse nous avons exploités, Les Blocs diagrammes de fiabilité et les arbres de défaillances respectivement pour l'analyse fonctionnelle et dysfonctionnelle d'un HIPPS utilisé en industrie pétrole et gaz. À travers les résultats obtenus, nous avons confirmé que les deux méthodes, AdD et BdF sont parmi les méthodes puissantes et robustes pour la modélisation du HIPPS en présence et en absence des DCCs. Nos résultats de simulation prouvent la conformité des deux approches pour l'implémentation des DCCs au niveau des unités redondantes (transmetteurs et vannes). D'une manière quantitative nous avons montré l'effet néfaste de ce type de défaillances sur les différents paramètres fiabilistes, ainsi qu'une capacité pour le HIPPS utilisé à maintenir le niveau d'intégrité de sécurité (SIL3) en présence des DCCs. Les résultats fournis par les deux approches nous permettent à optimiser les délais de programmation de la maintenance préventive et corrective pour le HIPPS.

Comme future travail de recherche et perspectives, nous nous proposons d'aborder la modélisation des systèmes instrumentés de sécurité par arbre de défaillance floue ou par les arbres de défaillances dynamiques et/ou par les blocs de fiabilité dynamiques. Ainsi que le développement les systèmes tolérants aux fautes par la prise en compte du facteur temporel.

Références bibliographiques

[1] Rausand, M.and Hoyland, S. System reliability theory : models and applications. (2004) Wiley Hoboken, NJ. ISBN : 0-471-47133-X

[2]www.techniques-ingénieur.fr/base-documentaire/genie-industriel-th6/qualité-et-sécurité-des-systèmes-industriels.Septembre2020.

[3] IEC 61508 (2010). Functional Safety of Eletrical/Electronic/Programmable Electronic Safety-Related Systems, part 1-7, 2nd, Ed, International Electrotechnical Commission, Geneva.

[4] IEC 61511 (2003). Functional Safety : Safety Instrumented Systems for Process Industry Sector, part 1-3 ; International Electrotechnical Commission, Geneva.

[5] Lundteigen, M.A. Safety instrumented systems in oil and gas industry : concepts, and methods for safety and reliability assessment in design, and operation''. These de doctorat (2008).Trondheim, université de la Norvège.

[6] Hauge, S. Hoem, A.S. Hohstad, P. Habrekke, S. and Lundteigen, M.A. Common cause failures in safety instrumented systems, Beta factors and equipment specific checklists based on operational experience. SINTEF report (2015), reference number 102001186. ISBN : 978-82-14-05953-3.

[7] Abdelhak Mkhida. Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence ". Thèse de doctorat, institut National Polytechnique de Lorraine, 2008.

[8] www.Claire Pagetti –EMSSIHT- module sûreté de fonctionnement.html. / 10-Mai-2017.

[9] Amel Demri. Contribution à l'évaluation de la fiabilité d'un système mécatronique par modélisation fonctionnelle et dysfonctionnelle, Thèse de doctorat 2009, Université d'Angers.

[10] Ouahiba Tebbi, '' estimation des lois de fiabilité en mécanique par les essais accélérés ''. Thèse de doctorat (2005), université d'Angers. France

[11] Villemeur, « Sûreté de fonctionnement de systèmes industriels, fiabilité, facteurs humains, information ». Collection de la direction des études et recherche d'électricité de France. Ed. Eyrolles (1998), Paris.

[12] Loubna Chergui, « Diagnostic des défaillances et optimisation des architectures des systèmes instrumentes de sécurité ». Thèse de Magistère (2010), Universite El-Hadj Lakhdar, Batna.

[13] Pierre David, ''Management des Risques Industriels''. Thèse de doctorat (2011, université de Grenoble, France.

[14] Hasan, O. and Ahmed, W, Tahar, S. and Salah Hamdi, M. Reliability blocks diagrams based analysis : A survey. Preceeding of International Conference on Numerical Analysis and Applied Mathematics (ICNAAM-2014), Greece (2014). AIP Conf. Pro.1648, 850129-1850129-4, https://doi.org/10.1063/1.4913184. ISBN : 978073541287307354128 71.

[15] Rausand, M. Risk assessment theory, methods and applications''. (2011), Wiley Hoboken, NJ. ISBN : 978-0-470-637647

[16] Roberts, N.H. and Vesely, W.E. Fault Tree, Handbook.(1981). NUREG-0492.

[17]Thomas Philippe. Contribution à l'approche booléenne de la sûreté de fonctionnement » l'atelier logiciel Workshop. Thèse de doctorat(2002), université de Bordeaux1. Ecole doctorale de science physique et de l'ingénieur. Bordeaux, France.

[18] Mohamed Sallak. Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitude et aide à la conception : Application aux systèmes instrumentés de sécurité ». Thèse de doctorat (2007), Université Nancy.
[19] Benaicha Halima, « Analyse des stratégies de maintenance des systèmes de production industrielle ». Thèse de doctorat (2015), université des sciences et technologie d'Oran. Algérie.
[20] Basilio, A. Safety instrumented systems manual for plant engineering and maintenance. (2015), 4th édition. ISBN : 978-8894208702.
[21] Birnbaum, Z.W. On the importance of components in a multicomponent system, in multivariate analysis, (1969). P.R.Krishanaial. Ed. Academic Press, vol.2, pp.581-592.
[22] Kuo, W. and Zhu, X. Some recent advances on importance measures in reliability, (2012). IEEE Transactions on reliability. Vol.61. No.2, pp.344-360. https://doi.org/10.1109/TR.2012.2194196. ISSN : 1558-1721.
[23] Kuo, W. and Zhu, X. Relations and generalizations of importance measures in reliability. (2012). IEEE Transactions on reliability Vol.61, no.3,pp.659-674.https://doi.org/ 10.1109/TR.2012.2208302. ISSN : 1558-1721.
[24] Kuo, W. and Zhu, X. (2012). Importance measures in reliability and risk optimization: principles and applications. (2012). W, S, Ltd, Ed Wiley&Sons Ltd, Chichester, UK. ISBN: 9781119993445.
[25] Lambert, H.E. Fault tree for decision making in system analysis. PhD (1975). Dissertation, Lawrence, Livermore Laboratory-university of California.
[26] Vesely, W.E, Davis, T.C, Dening, R.S. and Saltos, N. Measures of risk importance and their applications. Technical report reference number : NUREG/GR-3385 BMI-2103. (1986).
[27] Levitin, G, Podofillini, L. and Zio, E. (2003), Generalised importance measures for multi-state elements based on performance level restrictions. (2003).Journal of reliability engineering & safety. Vol.82. No.3, pp.287-298, https://doi.org./10.1016/S0951-83205 (03)00171-6. ISSN : 0951-8320.
[28] Wang, N, Zahao, J.B, et al. Reliability optimization of systems with component improvement cost based on importance measure, (2018). Journal of advances in mechanical engineering. Vol.10, No.11, pp.1-15, https://doi.org/ 10.1177/1687814018809781. ISSN : 1687-8140.
[29] Iyer, S. (1992), the Barlow-Proschan importance and its generalizations with dependent components. Journal of stochastic processes and their applications, (1992). Vol.42, No.2. pp. 353-359. https://doi.org./10.1016/0304-4149(92)90046-S. ISSN : 0304-4149.
[30] ISA-TR84.00.02-2002. The Instrumentation Systems and Automation society, ''Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation''. Technique Part 2 : Determining the SIL of a SIF via Simplified Equations». Technical report, (2002).
[31] Fares, Innal. Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performance : analyse critique de la norme CEI 61508''. Thèse de doctorat, (2008). Université de Bordeaux1. France
[32] Dutuit, Y, Rauzy, A. and Signoret, J.P. A snapshort of methods and tools to assess safety integrity levels of high integrity protection systems, (2008). Proceedings of the Institution of Mechanical Engineers, Part0: Journal of Risk and Reliability 222:371-379, https://doi.org/10.1243/1748006XJRR147. ISSN : 1748006X.
[33] Mokveld valves. Safety instrumented system – HIPPS. www.mokveld.com. Juin 2020
[34] Severn Glocon. High Integrity Pressure Protection Systems (HIPPS) for oil & gas installations. www.severnglocon.com. Juin 2020

[35] Angela E. Summers. High Integrity Pressure Protection Systems (HIPPS), Chemical Engineering Progress.Volume 3, November 2000. www.SIS-Tech.com (page consultée le 20 Aout 2020).

[36] Emerson Process Management. Fundamentals of Safety Instrumented Systems, FISHER. September 2005. www.Fisher.com. Septembre 2020.

[37] Hauge, S, Lundteigen, M.A, et al. (2010), reliability prediction method for safety-instrumented systems- PDS-example, (2010) édition. SINTEF report. ISBN : 978-82-14-05080-6.

[38] Lundteigen M.A, Rausand M. Common cause failure in safety instrumented systems on oil and gas installations : implementing defence measures through function testing, (2007). International journal of Loss Prevention in process industries. Vol20, pp.218-229, https://doi.org/10.1016/J.Jlp.2007.03.007. ISSN: 0950-4230.

[39] Fleming, K. (1974), a reliability model for common mode failures in redundant systems. Technical report.

[40] Anne Brros, Antoine Grall and Dominique Vasseur. Estimation of common cause failure parameters with periodic tests. (2008). International journal of Engineering and Design (Elsevier). Vol 239(4), pp. 761-768, https://doi.org/10.1016/j.nucengdes.2008.12.013.

[41] SIL verification report Skikda refinery construction project. (2014) –Algérie.

[42] GRIF Workshop (2019),''graphical interface for reliability forecasting, software, available at: http://grif-workshop.com.

[43] Triconex operating manual Tristation. (2010), V.4.7.

[44] Hassina, Metatla and Rouainia Mounira. (2022), Functional and dysfunctional analysis of a safety instrumented system (SIS) through the common cause failures (CCFs) assessment. Case of High Integrity Protection Pressure System (HIPPS). International journal of systems Assurance Engineering and Management. Vol 13(4), pp. 1932-1954. https://doi.org/10.1007/s13198-021-01608-8.

Annexe A Normes relatives aux systèmes instrumentés de sécurité

1. Systèmes relatifs aux applications de sécurité

Un système E/E/EP (électrique/électronique/électronique programmable de sécurité) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la function de sécurité. C'est –à-dire, depuis le capteur, en passant pa la logique de contrôle et les systèmes de communication, jusqu'à l'actionneur final tout en incluant les actions critiques de l'opérateur. Les systèmes de sécurité sont définis en termes d'absencede risqué inacceptable de blessure ou de prejudice à la santé des personnes. Les dommages peuvent être directs ou indirects comme des dommages aux biens ou à l'environnement par exemple certains systèmes peuvent être principalement conçus pour prémunir contre des pannes ayant des implications économiques majeurs. Ceci signifie que dans l'esprit à objectifs technique comparables ou idantiques, il n'ya pas de difference entre un système de sécurité et un système de contrôle de commande. L'IEC 61508 [IEC61508, 2002] et l'IEC61511 [IEC61511, 2003] peuvent être utilisées pour developer n'importe quell système E/E/EP comportant des fonctions critiques, tells que la protection des équipements, des biens ou de la productivité.

2. Norme IEC 61508 et ses normes filles

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme Internationale relative à la sécurité. Cette norme CEI 61508 [3] est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP; relies à la sécurité elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CEI 61508. La norme CEI 61508 repose sur deux concepts qui sont fondamentaux vis-à-vis de son application: le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties, afin de couvrir les multiples aspects des systèmes (E/E/PE):

- 61508-1 : Prescriptions générales.
- 61508-2 : Prescriptions propres aux systèmes (E/E/PE).

- 61508-3 : Prescriptions relatives au logiciel.
- 61508-4 : Définitions et abréviations.
- 61508-5 : Exemples de méthodes pour déterminer le niveau d'intégrité de la sécurité.
- 61508-6 : Guides pour l'application des parties 2 et 3 de la norme.
- 61508-7 : Tour d'horizon des techniques et des mesures.

La norme CEI 61508 est la base d'autres normes sectorielles (ex: machines, procédés continus, ferroviaire, nucléaire) ou de produits (ex: variateurs de vitesse). Elle influence donc le développement des systèmes E/E/PE et des produits concernés par la sécurité à travers tous les secteurs. La figure montre la norme CEI 61508 générique et ses normes filles par secteur d'activité.

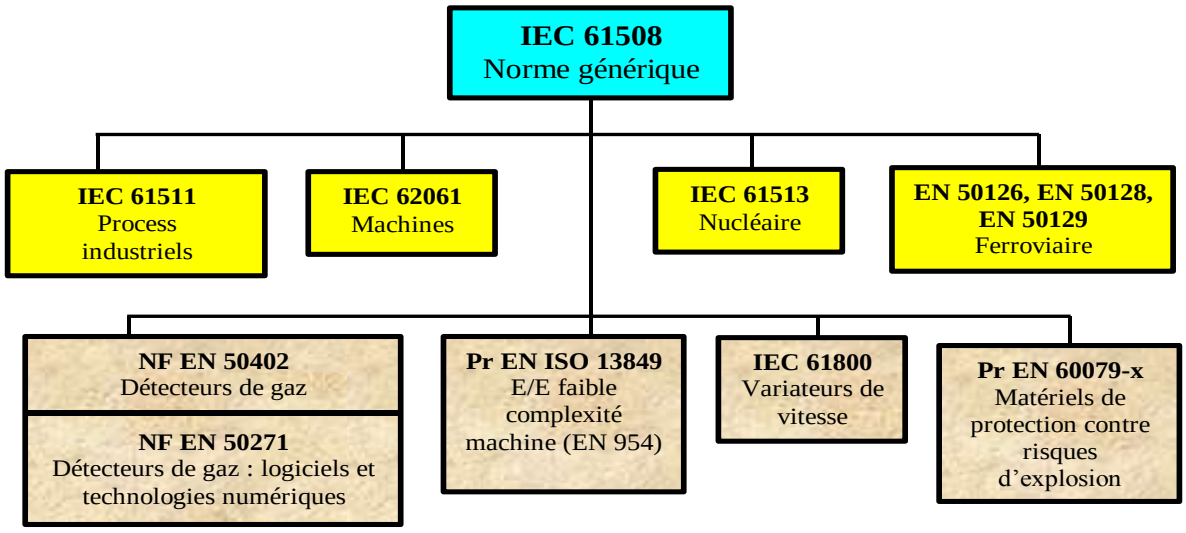


Figure 1. Norme CEI 61508 et normes dérivées [4].

L'IEC 61508 [3] a pour but de:

- ❖ Fournir le potentiel des technologies E/E/PE pour améliorer à la fois les performances économiques et de sécurité.
- ❖ Elle fournit une méthode de développement pour réaliser la sécurité fonctionnelle des systèmes relatifs à la sécurité.
- ❖ Elle définit des niveaux d'intégrité de sécurité (SIL) des systèmes E/E/PE relatifs à la sécurité.
- ❖ Elle décrit une approche basée sur l'analyse de risque pour déterminer les niveaux d'intégrité de sécurité (SIL) à atteindre pour un risque donné.
- ❖ Elle fixe des objectifs quantitatifs de défaillances dangereuses des systèmes de sécurité en fonction des niveaux d'intégrité de sécurité.
- ❖ Elle décrit les principes, techniques et mesures pour la réalisation de la sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité.
- ❖ Elle concerne toutes les phases du cycle de vie des matériels et du logiciel (depuis la conceptualisation, en passant par la conception, l'installation, l'exploitation, la maintenance, jusqu'à la mise hors service).
- ❖ Permettre des développements technologiques dans un cadre global de sécurité.
- ❖ Fournir une approche système, techniquement saine, suffisamment flexible pour le futur.

- ❖ Fournir une approche basée sur le risque pour déterminer les performances des systèmes concernés par la sécurité.
- ❖ Fournir une norme générique pouvant être utilisée par l'industrie, mais qui peut également servir à développer des normes sectorielles (par exemple : machines, usines chimiques, ferroviaires ou médicales) ou des normes produit (par exemple : variateurs de vitesse),
- ❖ Fournir les moyens aux utilisateurs et aux autorités de réglementation d'acquérir la confiance dans les technologies basées sur l'électronique programmable.
- ❖ Fournir des exigences basées sur des principes communs pour faciliter :

  - Une compétence améliorée de la chaîne d'approvisionnement des fournisseurs de sous-systèmes et de composants à des secteurs variés.
  - Des améliorations de la communication et des exigences (c'est-à-dire de clarifier ce qui doit être spécifié).
  - Le développement de techniques et de mesures pouvant être utilisées par tous les secteurs, augmentant de ce fait la disponibilité des ressources.
  - Le développement des services d'évaluation de la conformité si nécessaire.

3. Norme CEI 61511

La norme sectorielle CEI 61511 concerne les systèmes instrumentés de sécurité pour le secteur des processus industriels. Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente. Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité intrinsèques, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Elle comprend trois parties :

1. Cadre, définitions, exigences pour le système, le matériel et le logiciel,
2. Lignes directrices pour l'application de la CEI 61511-1.
3. Conseils pour la détermination des niveaux exigés d'intégrité de sécurité.

Cette norme permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état de sécurité.

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [2][4].

Annexe B | Production scientifique

Publications

Intitulé de la 1ère Publication: ***« Assessment of Common Cause Failure (CCFs) Effect on Safety Instrumentes System (SIS) by using the Fault Tree Analysis (FTA) Method ».***
Intitulé de la revue: ***Algerian Journal o Signals and Systems (AJSS).***
Vol.5, Issue.2, June-2021, ISSN: 2543-3792-EISSN: 2676-1548, pp.118-129.
Intitulé de la 2ème Publication: ***« Functional and Dysfunctional Analysis of a Safety Instrumented System (SIS) Assessment. Case of High Integrity Protection Pressure System (HIPPS).***
Intitulé de la revue: ***International journal of Sytem Assurance Engineering and Management (IJSAEM)***
Publised online: 04 January 2022. Vol.13, Issue.4, August-2022, Print-ISSN: 09756809, EISSN: 09764348.
Url de la revue/article: ***https://doi.org/10.1007/s13198-021-01608-8***

Communications

1. ***Metatla Hassina,*** *Rouainia Mounira « Impact Measure of the Common Cause Failure (CCFs) using the Fault Tree Analysis (FTA) Method » ,2nd International Conference On Advanced Engineering in Petrochemical Industry (ICAEPI, November, 2019), Skikda-Algeria.*
2. ***Metatla Hassina,*** *Rouainia Mounira « Impact Measure of the Common Cause Failure (CCFs) using the Reliability Blocks Diagram (RBD) Method » ,2nd International Conference On*

   Advanced Engineering in Petrochemical Industry (ICAEPI, November, 2019), Skikda-Algeria.
3. ***Metatla Hassina,*** *Rouainia Mounira « Common Cause Failure (CCF) Assessment By the Reliability Blocks Diagram (RBD) Method » ,8th International Symposium on Hydrocarbons and Chimistry (ISHC8, April, 2019), Boumlerdes-Algeria.*

4. ***Metatla Hassina,*** *Rouainia Mounira « Measure of the Importance Factors by Reliability Reliability Blocks Diagram (RBD) Method » 3rd International Conference On Electromechanical Engineering (ICEE, November, 2018), Skikda-Algeria.*
5. ***Metatla Hassina,*** *Rouainia Mounira « Common Cause Failure (CCFs) Assessment By using the Fault Tree Analysis (FTA) Method » ,3rd International Conference On Technological Advances in Electrical Engineering (ICATEE, December, 2018), Skikda-Algeria.*
6. ***Metatla Hassina,*** *Rouainia Mounira « Application de la Méthode FMD dans la politique de Maintenance sur la turbine à gaz MS5002C » 4 éme Conférence Internationale sur la Maintenance et la sécurité Industrielle (CIMSI, Novembre, 2017), Skikda-Algeria.*
7. ***Metatla Hassina,*** *Rouainia Mounira « Dependability Assessment by Reliability Blocks Diagram (RBD) Method » First International Conference On Advanced Engineering in Petrochemical Industry (ICAEPI, November, 2017), Skikda-Algeria.*
8. ***Metatla Hassina,*** *Rouainia Mounira « Analyse des Systèmes Instrumentés de Sécurité (SIS)» International Conference : Rencontre des Femmes Scientifiques Méditerranéennes (REFSCIME, Avril, 2013), Skikda-Algeria.*

Comité d'organisation de Conférence

1. ***Metatla Hassina,*** *participated in the 3rd International Conference On Advanced Engineering in Petrochemical Industry (ICAEPI, November, 2021), Skikda-Algeria, as a member of the Organisation Committee.*
2. ***Metatla Hassina,*** *participated in the 2nd International Conference On Advanced Engineering in Petrochemical Industry (ICAEPI, November, 2019), Skikda-Algeria, as a member of the Organisation Committee.*

Int J Syst Assur Eng Manag (August 2022) 13(4):1932–1954
https://doi.org/10.1007/s13198-021-01608-8

ORIGINAL ARTICLE

Functional and dysfunctional analysis of a safety instrumented system (SIS) through the common cause failures (CCFs) assessment. Case of high integrity protection pressure system (HIPPS)

H. Metatla[1] · **M. Rouainia**[2]

Received: 20 June 2021 / Revised: 12 December 2021 / Accepted: 17 December 2021 / Published online: 4 January 2022

Abstract In oil & gas industrial plants, High Integrity Pressure Protection Systems (HIPPS) are widely used as barrier between high pressure and low pressure sections. Hence, it is necessary to optimize its reliability, availability and, maintainability to help in the implementation of HIPPS maintenance planning from a quantitative point of view. The objective of our work is included in this concept. Where a comparative study on HIPPS dependability with and without considering common cause failures (CCFs) is realized, through the quantification of CCFs effects on overall performances by considering HIPPS reliability reduction, HIPPS Safety Integrity Level degradation, and the decrease of HIPPS Mean Down Time, and production capacity. Beta factor is used to model the CCFs on HIPPS and, the reliability block diagram RBD is used for functional aspects and fault tree analysis FTA technique is used for dysfunctional aspects. The obtained simulation results show the effectiveness of the HIPPS, in keeping its safety and reliability characteristics in presence of the CCFs, the robustness, accuracy, and the suitability of the used methodology in CCFs assessment.

Keywords HIPPS · CCFs · Beta factor model · FTA · RBD · SIL

1 Introduction

The safety instrumented systems (SISs) are vital safety barriers, widely used in industrial plants to reduce the probability of hazardous situations such as: gas leakages and fires explosions. A SIS may assure the control of many Safety Instrumented Functions (SIFs) (IEC 61508 2010). In the recent years several safety standards are presented, the most known are IEC 61,508 and IEC 61,511. Oil and gas companies have to align their operation and maintenance according to requirements in IEC 61,508 and IEC 61,511. IEC standard covers the SIS operation and maintenance through the handling of CCFs, and the supervision of SIS safety integrity performance (Hauge et al. 2016). According to IEC 61,508 standard each safety instrumented function (SIF) corresponds to predefined safety integrity level (SIL). This standard prescribes four safety integrity levels, where SIL4 is the highest, or the most reliable level, and SIL1 is the lowest requirements, or is the least reliable one, IEC 61,508 prescribes two reliability measures to allocate a SIL for each SIF, the average probability of failure on demand (PFD) for low demand SISs and the probability of failure per hour (PFH) for high demand or continuous mode SISs. The differences between low demand system and high demand system is not limited to the frequency of failure on demand, but also the methods used to analyze the SIS reliability (IEC 61508 2010). Table 1 includes the values of PFD and PFH with the corresponding SIL.

✉ H. Metatla
metatla.hassina@yahoo.fr; h.metatla@univ-skikda.dz

M. Rouainia
rouainia_m@yahoo.fr; mounira.rouainia@univ-skikda.dz

[1] LGCES Research Laboratory, Department of Petrochemistry and Process, University 20Août 1955, Skikda, Algeria

[2] LGCES Research Laboratory, Department of Petrochemistry and Process Engineering, University 20Août 1955, Skikda, Algeria

Table 1 Safety integrity level (SIL) according to PFD_{avg} and PFH (IEC 61508 2010)

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

Several methods are used to analyze the SIS reliability, among them: Risk graph, Layer Of Protection Analysis (LOPA), Markov method, Fault Tree Analysis (FTA) and Reliability Block Diagrams (RBD) (Birnbaum 1969; Dutuit et al. 2008).

Risk graph is an approach suitable for the SIL determination of low-demand systems (IEC 61511 2003. part3), it allows the evaluation of the following hazard factors: the consequences severity, time exposed to danger, possibility to avoid the danger and probability of undesirable occurrences in absence of safety functions (Beugin et al. 2006). Even it is eseay to be implemented, many papers have highlighted some shortcomings of this technique, particularly due to its subjective idea and the big limitation, is that the method more suitable for series configuration (Di Bona et al. 2020). While LOPA is a semi quantitative risk assessment method introduced by the Center for Chemical Process Safety in 1993 (CCPS 1993), whose primary purpose is to determine whether, or not there are sufficient layers of protection (A.Lassen 2008). LOPA is a tool that can be used after a qualitative hazards analysis, generally the HAZOP (Hazard and Operability Analysis), but before using FTA technique, or any quantitative risk analysis where: the consequences identified in HAZOP are listed and classified respectively as impact events and severity level, the initiating causes are listed for each impact event, likelihoods estimated for each initiating cause, the Independent Protection Layers (IPLs) are determined, including: process design, basic process control system, alarms and procedures, safety instrumented system, and additional mitigation, each IPL is assigned a probability of failure on demand (PFD), a mitigated event likelihood is then calculated by multiplying the initiating cause likelihood by the PFDs for applicable IPLs, an the mitigated event likelihood is then compared to a criterion linked to the corporation criteria for unacceptable risk levels, and additional IPLs can be added to reduce the risk. Finally the mitigated event likelihoods are summed to give an estimate of the risk for the whole process. The weaknesses of this technique: it is suitable for low demand system and used only for series configurations (Di Bona et al. 2020). Markov method includes qualitative and quantitative aspects; it is suitable for small systems and is not recommended for complex systems with dynamic properties. Markov method is suitable only for high demand systems (Rausand and Hoyland 2004; Rausand 2011; Lundteigen 2008).

FTA was developed by Bell Telephone Laboratories in 1962 for U.S.Air Force to use with Minuteman systems; it was later adopted and extensively applied by the Boeing Company (Roberts et al. 1981). It is one of the prominent techniques used in oil and gas industries and supported by a wide range of software tools. FTA is a top-down logic diagram, which is formed by logic gates to display the relationship between the events in a system. The basic events are located at the lowest level, generally depicts component failure, human error, or environment conditions. This technique can be qualitative in terms of the determination of Minimal Cut Sets (MCS), and quantitative in terms of the calculation of probabilities and frequencies of hazardous events. It is often carried out in four steps (1) definitions of the system problem and, boundary conditions of analysis, (2) construction of FT, (3) identification of MCS, (4) qualitative and quantitative analysis of FT. This model displays cause-consequence relationships, and combines hardware, software, environment, and human interaction,this methodology also utilizes Boolean algebra, probability and reliability theory, logic, and follows the laws of physics, chemistry and engineering (Ruijters and Stoelinga 2015). In contrast to Markov method FTA is not suitable for analyzing dynamic systems, however it should mention that FTA has been widely used in many application areas, particularely to analyze large and complex systems (Rausand and Hoyland 2004; Lundteigen 2008; ISO/TR 2013; Roberts 1981).

Finally the RBD method performs system reliability and availability analysis for large and complex systems. The structure of reliability block diagram defines logical interaction between system components to ensure reliable operation. The fundamental concept of RBD starts from an input located at the left side of the diagram, and it will follow a series, or parallels arrangement of blocks to reach an output node at the right side of the diagram. The RBD is a network connection of different structures such as parallel, series, K out of N, or mixed. A successful operation system requires at least one maintained path between the system input and the system output (Rausand 2004). Boolean algebra expressions are used to describe the minimum combination of failures required to cause a system failure. RBD is a graphical and calculation tool used to model industrial processes, it enables us to evaluate the impact of component failures on global system reliability and safety, it is widely used for assessing the trade-offs of various preceding structures at the system design phase. We summarize RBD steps as follows: (1) partitioning the given system segments, and constructing its equivalent

RBD, (2) evaluating the reliability of the individual segments, (3) assessing different dependability parameters for the complete system (Hasan et al. 2014).

In this paper FTA and RBD techniques are used to model both functional and dysfunctional aspects with and without consideration of CCFs of a low demand SIS. The study uses a High Integrity Pressure Protection System (HIPPS), in oil and gas industry. The considered FTA and RBD techniques will help in the quantification of Importance Measures (IMs) for the HIPPS's components. These IMs were first introduced by Birnbaum in 1969 (Birnbaum 1969), they provide a numerical rank to determine the more critical components for system reliability improvement (Bozoudis et al. 2018).

The IMs for any component should depend on three factors: (1) the component location in the system, (2) unreliability/unavailability of the component in question, (3) the system structure (Amrutkar and Kamalja 2017).

The authors in (Liu and Lundteign 2015), have computed five IMs, of a HIPPS channels, using the average PFD as reliability performance measure, and Markov method in order to link the failures rates of the system channels. In our work six IMs**: Birnbaum measure: MIF** (Birnbaum 1969)**, Lambert measure: CIF** (Lambert 1975)**, Fussel Vesely measure: DIF** (Vesely 1970)**, Risk Achievement Worth: RAW** (Fusell 1975)**, Risk Reduction Worth: RRW** (Levitin et al. 2003; Meng 2009)**, and Barlow and Proschan measure: BP** (Basilio et al. 2015; Hweng 2005; Lyer 1992), are calculated by the proposed methodology. Main purpose of those IMs, is to identify weaknesses or the most vulnerable parts in our considered HIPPS, and may serve as resource allocation factors for scheduled HIPPS maintenance in order to minimize its down time and cost-efficient operation of our system. In the present work we calculate these IMS, only in the diagnostic stage (study without considering of the CCFs).

The HIPPS is a reactive barrier designed in accordance with the IEC 61,508, and IEC 61,511 standards to stop or mitigate the consequences of the chain events following a hazardous situations, it is one of the best choices to protect the plants and to increase safety. The most important aspects of HIPPS are safety, economy, and environmental considerations, it is used in oil and gas industry such as in liquefied natural gas (LNG) facilities, transport, and storage,piplines, ships, and process package (Lundteign et al. 2008). Its shutdowns and failures cause a total break of production. The HIPPS safety integrity level (SIL) also, defines a required probability of failure on demand (PFD) for the complete functional loop and architectural constraints for loop and its elements (Liu and Lundteign 2015). HIPPS is specified for compliance with SIL 3 performances requirement as provided in IEC 61,508 (IEC 61508 2010). This target SIL is equivalent to a probabilty of failure on demand in the range of 1E-4–1E-3. Its high availability requirements drive the choices made for the device integrity: diversity, redundancy, voting, protection against CCFs, dignostic, maintenance strategies, and testing frequency (Bozoudis et al. 2018; Lundteigen and Rausand 2010). Therefore, it is necessary to periodically monitor and control the HIPPS SIL, and to assure that the HIPPS meets its depandability requirements.

Our proposed HIPPS is basically composed of simplex or redundant unit of treatment or logic solver, two solenoid valves (SV1, SV2), and two safety shutdown valves (SDV1, SDV2), working on 1oo2 logic, and three pressure transmitters working on 2oo3 logic. The authors in (Liu et al. 2021) have modeled the degradation of HIPPS final elements by considering the intermediate degraded state between the working and failed states. Numerical examples are presented to provide clues in selection of optimal maintenance strategies for final 1oo2 HIPPS elements by using muti-phases Markov process. However in this article using the FTA and RBD, we check the overall HIPPS dependability parameters: Reliability: **R(t)**, Unavailability: **U(t)**, or HIPPS Safety Integrity Level: **SIL**, the accident frequency: **W(t)**, and the metrics: **MTTF**, **MTBF**, **MUT**, **MDT** for three different sequences times of **5**, **25**, **50** years, and we demonstrate high availability of our system to better perform on the required specifications of HIPPS in onshore application since it maintains its target SIL in the range of 1E-4 to 1E-3 (SIL 3).

The Redundancy introduced in the HIPPS is a common practice engineering tool used to improve its availability, and reliability (Lundteigen and Rausand 2007). The CCFs are simultaneous failures of multiple components within a system, due to a common-cause or a shared root cause. These dependent failures can significantly contribute to the overall HIPPS unreliability. Until now it has been impossible to avoid the CCFs but, by a good risk assessment we can reduce its influence on global system reliability. It has received considerable attention in the recent decades, and more recently the standard IEC 61,508 for oil and gas industry (IEC 61508 2010) has pointed out the importance of controlling these failures in order to maintain the integrity of safety instrumented functions (SIFs) (Lundteign and Rusand 2007). There are two methods to model CCFs: explicit modeling and implicit modeling. We use the first one (**Explicit modeling**), when the specific causes of CCFs can be identified, and the latter one: when the causes of CCFs are difficult, or impossible to be identified. The Beta factor model belongs to implicit modeling, and it is the simplest and widely used model. This model was originally developed for two components, later extended to larger systems, it is based on notion that the components failures can be divided into two groups: independent failures, and dependent failures of all components. The IEC

61,508 recommends this model to assess SIS reliability, the Beta rate may be determined by: expert judgment, checklists and use of historical data (Lundteigen and Rausand 2007; Hauge et al. 2016; Hokstad and Rausand 2008; Jin et al. 2011; Fleming 1974; Basilio et al. 2015). Oil and gas industry design engineers are focusing on CCFs in the design phase of SIS, whearas less attention is given in the operational phase (Hauge et al. 2016). In the design phase CCFs causes may be the result of inadequate understanding of failure mechanisms and responses, improper selection of hardware components, and so forth. In operational phase, CCFs causes may be introduced due to improper testing, human errors during operation and maintenance, and environmental stresses, that are generally systematic failures, and are observed as CCF potential of causes, or dominating factor for providing this type of failures (Rausand and Hoyland 2004; Lundteigen 2008).

By the presented work we target the assessment of real onshore HIPPS dependability, with and without consideration of CCF, using FTA and RBD methods.And demonstrating the suitability of these techniques to model functional and dysfunctional aspects of our system. In this study a comparison between the results fournished by RBD and FTA is highlighted, and we have illustrated the similarity of results given by Both methods in overall stages of study (with and without CCFs), besides giving an illustration by quantification of HIPPS dependability parameters in the objectif to demonstrate the negative effect of CCFs on the global HIPPS reliability.

The remaining sections of of the paper are organized as follows: in Sect. 2, HIPPS functional loop and CCFs are presented; Sect. 3 is reserved to HIPPS diagnostic stage by the HIPPS implementation through the RBD and FTA techniques without account of CCFs. Then in Sect. 4 after, computing the different HIPPS parameters and the illustration of the various results by figures and tables, the first stage simulation results are discussed. Section 5 is dedicated to HIPPS reliability analysis by considering CCFs. In the objective to compare performances of both techniques, the obtained simulation results of the CCFs assessment are interpretated in the last section followed by a conclusion.

2 HIPPS functional loop and common cause failures (CCFs)

2.1 HIPPS functional loop

As a case study we have considered a real HIPPS, which is a SIS system used in oil and gas industry. In our case the system is used, to protect a Liquefied Petrol Gas (LPG) bullet (600-S-156) from high pressure phenomenon. The bullet is located in SKIKDA Refinery-ALGERIA. Figure 1 shows implementation of HIPPS as it is indicated in the unit's, Piping & Instrumentation Diagram (P&ID) showing HIPPS subsystems:

Sensors: three pressure transmitters with Tags PT-7504 A/B/C connected following a 2oo3 voting architecture.

Logic Solver: is TMR (Triple Modular Redundant) PLC from -TRICONEX-, Here the interlock is described using the tag I-7504 (Triconex manual 2010).

Final elements: are solenoid valves (ROV-2524 A and ROV-2524 B) each final element comprises a solenoid

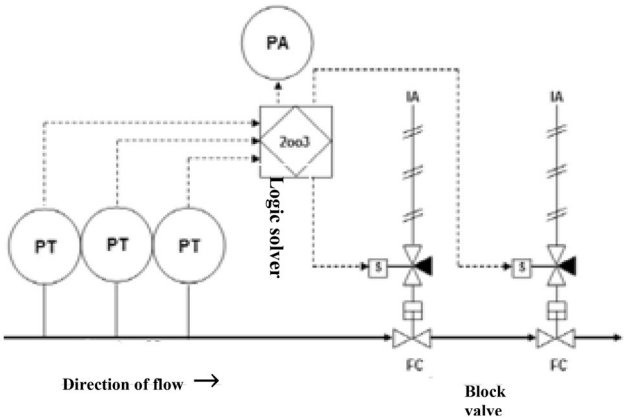


Fig. 2 Simplified illustration of the HIPPS

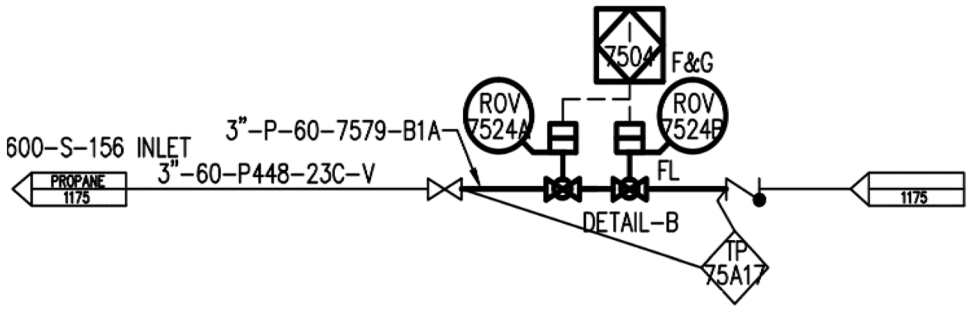


Fig. 1 HIPPS I-7504 implementation (P&ID Skikda refinery)

(SV1, SV2), and safety shutdown valves (SDV1, SDV2) in 1oo2 architecture. The Figs. 2 and 3, summarizes the function of our HIPPS.

A basic HIPPS is illustrated in Fig. 2, redundant 2003 voted pressure transmitters detects high pressure and gives a signal to the logic solver. The 2003 voting offers both a level of redundancy and fault tolerance. The logic solver sends signals to solenoid valves to close and acts as barriers against high pressure. SV1, SV2 are Solenoid Valves, SDV1and SDV2: are Safety Valves, or the barriers valves that are the final elements of HIPPS. They close and act as barriers to protect against over-pressure. HIPPS valves have a failure-proof design, meaning that any loss of electric or hydraulic power will cause the valves to close. SDV1 and SDV2 are installed in series with a 1002 voting to meet the requirements of IEC-61508. Valve closing is devised to prevent pressure built up in low rated zone (IEC 61508 2010). HIPPS is installed to perform a safety instrumented functions (SIFs), which operated in low demand mode, and its availability must be quantified by using the average probability of failure on demand PFD_{avg}, and must be periodically function tested every 12 months to ensure that it meets safety integrity requirements. Short test intervals will improve the system's PFD but is very expensive. A test scheme needs to be made to meet SIL 3 requirements. In order to understand HIPPS potential failures, it is important to have a good understanding of various functions of each functional block. HIPPS' various functions are devised by asking how to accomplish HIPPS function. For this system function to be accomplished the pressure has to be measured, which must be evaluated to stop the flow. In order to do this, the pressure must be observed, and converted to an electrical signal. The signal must also be transmitted for evaluation.

2.2 HIPPS CCFs

Because of these redundancies, HIPPS may be influenced by CCFs, which are defined by NUREG/GR6268 as dependent failures in which two or more component fault states exists simultaneously, within a short time interval, and are a direct result of shared cause. It occurs when the components are all from the same manufacturer, or are the same type, and are affected by common factors: dirty environment, manufacturing, fault maintained incorrectly, missed calibration….etc. They are serious threats to HIPPS reliability because they can increase HIPPS probability of failure on demand (PFD_{avg}).

The reasons for CCFs at the level of HIPPS include:

Separation: the degree that can affect similar units by a single environmental effect, for example: a single failure may result in the loss of two power supplies.

Similarity: the degree of similarly designed equipment that manufactured maintained or operated.

In this paper we have used two formalisms FTA and RBD to assess HIPPS reliability with and without taking account of CCFs in the objective to compare the results obtained from both methods. During HIPPS reliability assessment with CCFs, these are modeled using the Beta factor approach. This model assumes that CCFs rate is fixed in proportion to the individual item failure rate, which is typically between **2** and **15%** (Hauge et al. SINTEF 2015), depending on competency, type of equipment, and quality of installation and site conditions. The CCFs have been included for:

Pressure transmitters (PT_i): 2out of 3 arrangements to obtain HIPPS trigger, with **15%** of beta rate (Hauge et al. SINTEF 2015). Solenoid valves (SV1, SV2), and safety shutdown valves (SDV1, SDV2): activating solenoid and safety shutdown valves (SDV1, SV1), or (SDV2, SV2) in a 1 out of 2 arrangements, **12%** of beta rate (Hauge et al. SINTEF 2015).

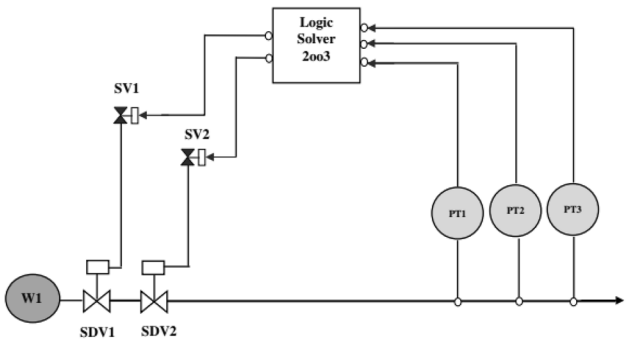


Fig. 3 HIPPS functional loop

3 HIPPS reliability analysis without considering CCFs: diagnostic stage

For HIPPS implementation using FTA and RBD approaches, all simulation data is collected from the reference (Skikda refinery project 2014). All following simulation results are obtained using GRIF software (GRIF 2019). Main objective of this paper is to make a comparative study between RBD and FTA method to quantify HIPPS reliability R(t), unavailability U(t), HIPPS unreliability F(t), various HIPPS metrics: MTTF, MTBF, MUT, MDT, and the accident frequency: W(t) of HIPPS implementation with and without considering CCFs, and to study how CCFs influences the value of all preceding parameters, and to give an illustrative results that both methods are very, powerful and robust, for assessing HIPPS CCFs and are similar, or present same simulation results in overall HIPPS studies. In the first part we show the simulation results of the HIPPS implementation using the FTA, and the RBD

approaches without considering CCFs, or to make a diagnostic study by computing: HIPPS MCS, and the HIPPS IMs: Marginal Importance Factor: MIF, Critical Importance Factor: CIF, Diagnostic Importance Factor: DIF, RAW, and RRW, for each HIPPS components, as well as quantification of all previous HIPPS parameters.

3.1 HIPPS dysfunctional modeling using FTA method

HIPPS functional loop is presented in the Fig. 3, we firstly present HIPPS implementation by FTA method, and after that, an assessment of probabilities and frequencies of HIPPS failure, to analyze HIPPS reliability. FT reproduced in Fig. 4 was constructed starting with top event (HIPPS fails), which was then successively broken down via various possible intermediate failures using AND and, OR logic gates, so as finally to yield basic failure events at the lowest levels: PT_i failures, SV_i failures, and SDVi failures. Each basic failure events depicted by circles should be described using time for distribution failure or for proper configuration, and the data is provided for each one, for calculating system reliability measures. In the first part, we give all simulation results for a sequence time of **5** years.

- Figures 5 and 6 are respectively the tracing of the HIPPS unavailability, or HIPPS SIL evolution, and the HIPPS frequency.
- Figure 5 depicts that about **52%** of U(t) are in **SIL3 zone**, and **47.9%** are in **SIL4 zone**. So HIPPS is reliable, because its average value **1.1003E-4** corresponds to **SIL3**.
- The appearance of different peaks, in the precedents, and in all subsequent curves refers to the effect of periodic proof test applied on safety shutdown valves and solenoid valves: SDV_i and SV_i.
- According to the simulation results, we present in Table 2 the average value of: HIPPS reliability R(t), unreliability F(t), also HIPPS unavailability U(t), and frequency in the top event provided by FTA method.
- According to the Table 2, average HIPPS reliability is about **82.61%,** and HIPPS unavailabilty average, representing SIL of HIPPS is equal to **1.1003E-4**, this value corresponds to **SIL 3**. So the HIPPS has its significant industry applications.
- Table 3 shows calculation of HIPPS mean times, here we discuss mean time to failure (MTTF), mean time between failures (MTBF), mean down time (MDT), and mean up time (MUT), always measuring in hours.
- Table 4 presents calculation of HIPPS Minimal Cut Sets (MCS), or minimum number of failures that can cause failure of HIPPS. According to Table 4, they are **8 MCS**, **only one order 1,** and **two other orders.**
- So reducing failures probabilities of MCS is very interesting, and a good way to improve overall HIPPS reliability. Tables 5, 6, 7, 8, 9, 10 give values of different IMs for each component given by FTA method.
- In the precedent Tables 5, 6, 7, 8, 9, 10, these IMs factors quantify the impact of HIPPS components

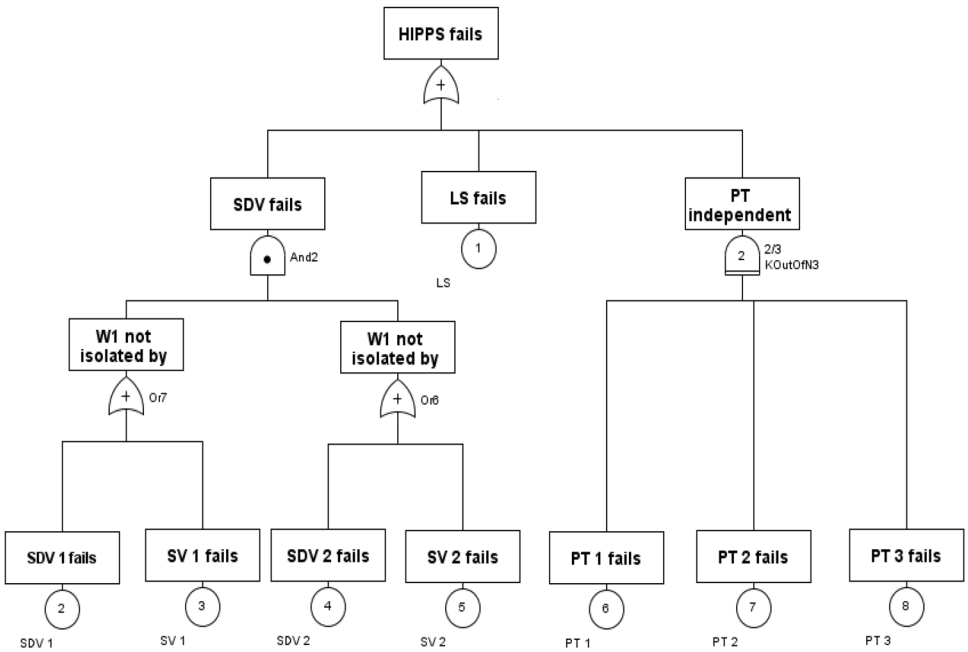


Fig. 4 HIPPS FTA without CCFs

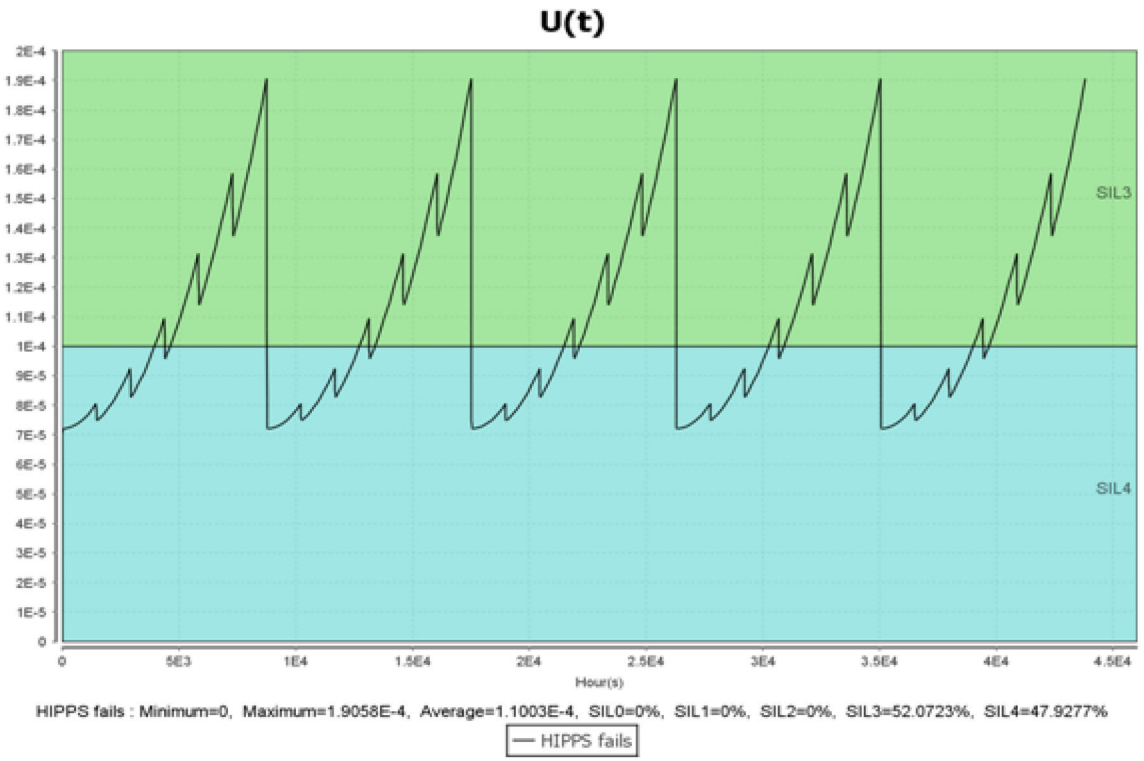


Fig. 5 Time evolution of the HIPPS instantaneous unavailability (HIPPS SIL) without CCFs

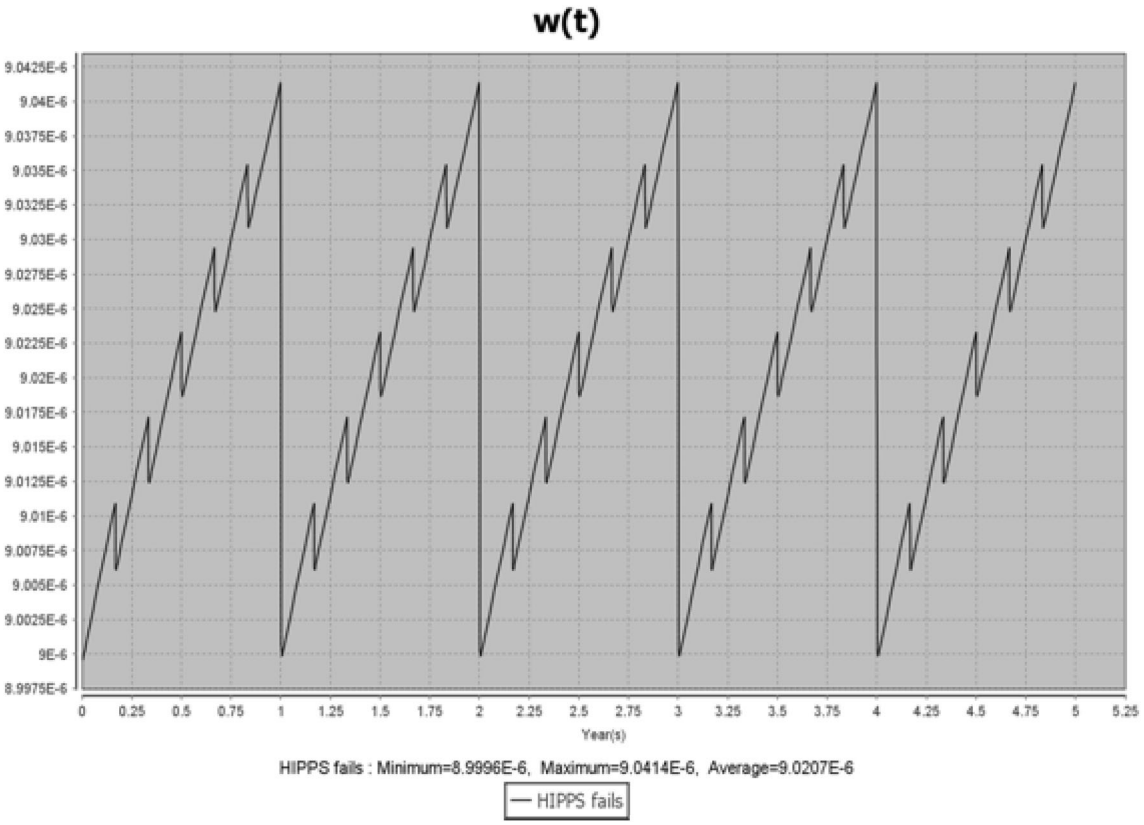


Fig. 6 HIPPS frequency in the top event without CCFs in hour(s)$^{-1}$

Table 2 Probabilities and frequencies in the top event

FTA method	System HIPPS fails			
Probabilities/Frequencies	$R(t)_{avg}$	$F(t)_{avg}$	$U(t)_{avg}$	$W(t)_{avg}$
Value	0.8261	0.1739	1.1003E-4	9.0207E-6 h^{-1}

Table 3 HIPPS dependability metrics

FTA method	System HIPPS fails			
Dependabilitymetrics	MTTF	MDT	MUT	MTBF
Value	1.1084E5h	12.1973 h	1.1084E5h	1.1086E5h

Table 4 Minimal cuts set of HIPPS

PRODUCTS			
Type = PRODUCTS, Name = HIPPS fails			
Order	Products	Probability (Products)	Frequency (Products)
1	LS	7.1995E-5	8.9983E-6
2	SDV1, SDV2	9.1963E-5	2.0866E-8
2	SDV1, SV2	1.2593E-5	9.9648E-9
2	SDV2, SV1	1.2593E-5	9.9648E-9
2	SV1, SV2	1.7243E-6	2.3377E-9
2	PT1, PT2	5.76E-12	1.4397E-12
2	PT1, PT3	5.76E-12	1.4397E-12
2	PT2, PT3	5.76E-12	1.4397E-12

Table 5 Birnbaum measure (MIF)

Type = MIF, System = HIPPS fails		
Time	Value	Component
8.76E3	0.9999	LS
8.76E3	0.0109	SDV1
8.76E3	0.0109	SDV2
8.76E3	0.0108	SV1
8.76E3	0.0108	SV2
8.76E3	4.7991E-6	PT1
8.76E3	4.7991E-6	PT2
8.76E3	4.7991E-6	PT3

Table 6 Lambert measure (CIF)

Type = CIF, System = HIPPS fails		
Time	Value	Component
8.76E3	0.5472	SDV1
8.76E3	0.5472	SDV2
8.76E3	0.3777	LS
8.76E3	0.0743	SV1
8.76E3	0.0743	SV2
8.76E3	6.0434E-8	PT1
8.76E3	6.0434E-8	PT2
8.76E3	6.0434E-8	PT3

failures, and delivers an information about the 'hierarchy' of HIPPS components. The elements: LS, SDVi, SV_i will have a bigger influence on global HIPPS dependability, because those have higher value of IMs measures. But the PT_i will have a negligiable effect on overall HIPPS reliability, since those have low value of IMs measures.

– Table 11 presents ranking of HIPPS components in accordance with their importance measures.

3.2 HIPPS functional modeling using RBD approach

Figure 7 illustrates HIPPS RBD, it is defining logical interactions of functioning items in the system that is required to sustain HIPPS operation. HIPPS RBD starts from an input node located at the left side of the diagram, this node flows to arrange three parallel blocks of pressure transmitters with 2 out of 3 votings, which must be readied by one logic solver, and then the formation must be sent to final elements that are safety shutdown valves (SVi, SDVi),

Table 7 Fussel vesely measure (DIF)

Type = DIF, System = HIPPS fails		
Time	Value	Component
8.76E3	0.5516	SDV1
8.76E3	0.5516	SDV2
8.76E3	0.3778	LS
8.76E3	0.0755	SV1
8.76E3	0.0755	SV2
8.76E3	2.4604E-6	PT1
8.76E3	2.4604E-6	PT2
8.76E3	2.4604E-6	PT3

Table 8 Reliability achievement worth (RAW)

Type = RAW, System = HIPPS fails		
Time	Value	Component
8.76E3	5.247E3	LS
8.76E3	57.5152	SDV1
8.76E3	57.5152	SDV2
8.76E3	57.5152	SV1
8.76E3	57.5152	SV2
8.76E3	1.0252	PT1
8.76E3	1.0252	PT2
8.76E3	1.0252	PT3

Table 9 Reliability reduction worth (RRW)

Type = RRW, System = HIPPS fails		
Time	Value	Component
8.76E3	2.2085	SDV1
8.76E3	2.2085	SDV2
8.76E3	1.607	LS
8.76E3	1.0803	SV1
8.76E3	1.0803	SV2
8.76E3	1	PT1
8.76E3	1	PT2
8.76E3	1	PT3

with 1oo2 voting. Finally we conclude the outputs node at the right side of diagram. In this HIPPS RBD every block is configured properly, and the data is provided for each one. Different HIPPS dependability parameters can be calculated: R(t), F(t), U(t), W(t), and the HIPPS mean times: such as: MTTF, MTBF, MUT, and MDT.

Table 10 Barlow and proschan importance factor (BP)

Type = BP, System = HIPPS fails		
Time	Value	Component
8.76E3	0.9952	LS
8.76E3	1.3104E-3	SDV1
8.76E3	1.3104E-3	SDV2
8.76E3	1.0722E-3	SV1
8.76E3	1.0722E-3	SV2
8.76E3	1.5924E-7	PT1
8.76E3	1.5924E-7	PT2
8.76E3	1.5924E-7	PT3

- We present tracing of these parameters with their average values for a sequence time of **5 years**, in figures and tables given in the following steps.
- Figures 8 and 9 display same curves with same averages value given by previous Figs. 5 and 6.
- Table 12 shows collection of probabilities, and frequencies in HIPPS output provided by RBD method.
- Following step is calculation of basic metrics of reliability that are the measurements of mean times in HIPPS output provided by RBD method in the unit of hours shown in Table 13.
- RBD qualitative aspect are the calculation of MCS, which is shown in Table 14 indicating which combinations of component failures lead to HIPPS failures.

They point out the existence of 8 minimal cuts: **7** of order **2** and **1** of order **1**. The critically path are the safety valves (SDV1, SDV2), the second path is LS: logic solver, the third paths (SDV1, SV2), (SDV2, SV1), then the solenoid valves (SV1, SV2), and the minimum cuts sets are: (PT1, PT3), (PT1, PT2), (PT2, PT3). We notice that these products are the same Minimal Cuts Sets given by FTA method, with approximately the same probabilities and frequencies of occurrence.

- The Tables 15, 16, 17, 18, 19, 20 present the calculations of HIPPS IMs for each components given by RBD method.
- Table 21 presents resulting classification
- Overall figures and tables given by HIPPS RBD implementation show same results of previous tables and figures given by HIPPS FTA implementation.

Table 11 Ranking of HIPPS components according to their importance factors

MIF	CIF	DIF	RAW	RRW	BP
LS	SDV1 = SDV2	SDV1 = SDV2	LS	SDV1 = SDV2	LS
SDV1 = SDV2	LS	LS	SDV1 = SDV2	LS	SDV1 = SDV2
SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2
PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3

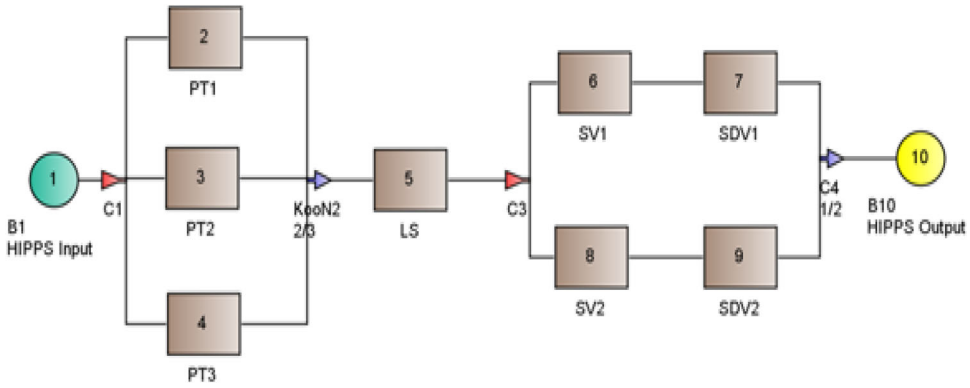


Fig. 7 HIPPS RBD without CCFs

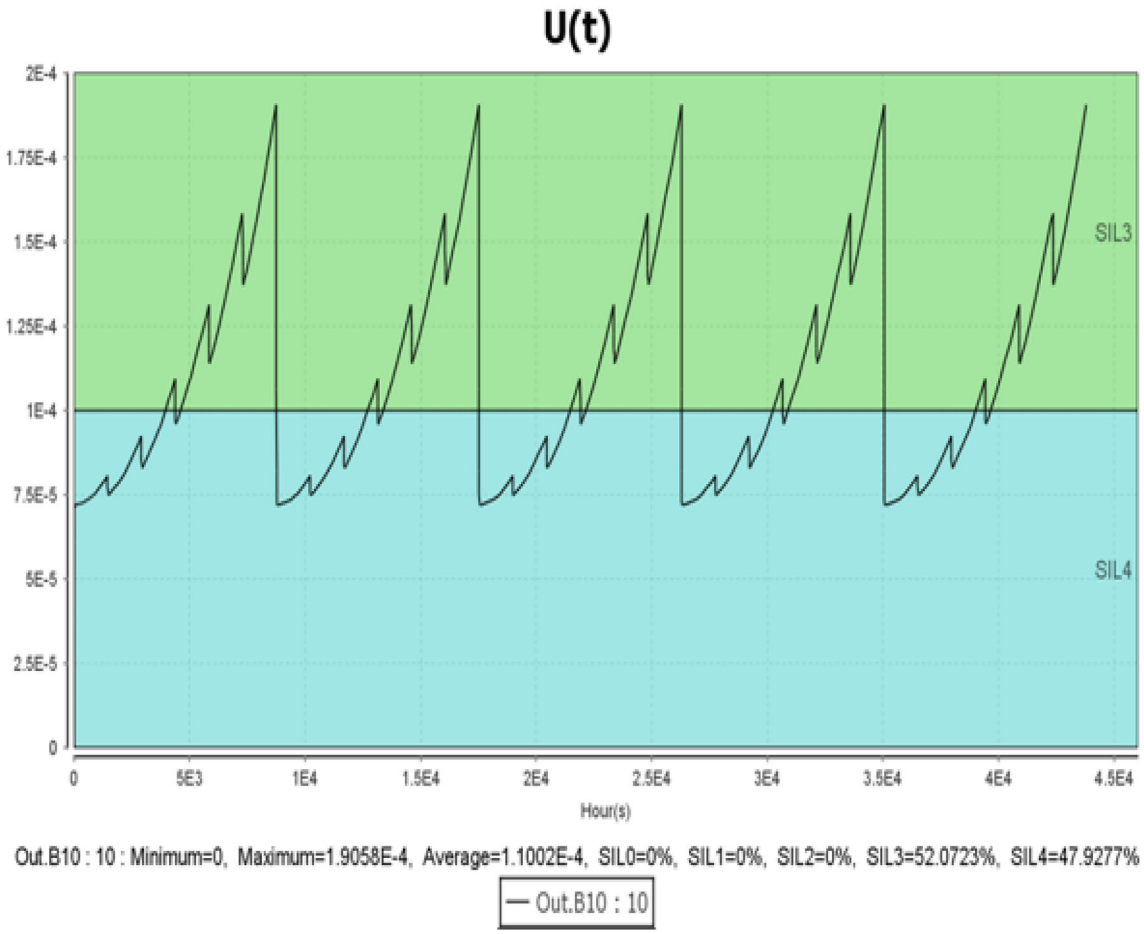


Fig. 8 Time evolution of HIPPS instantaneous unavailability without CCFs

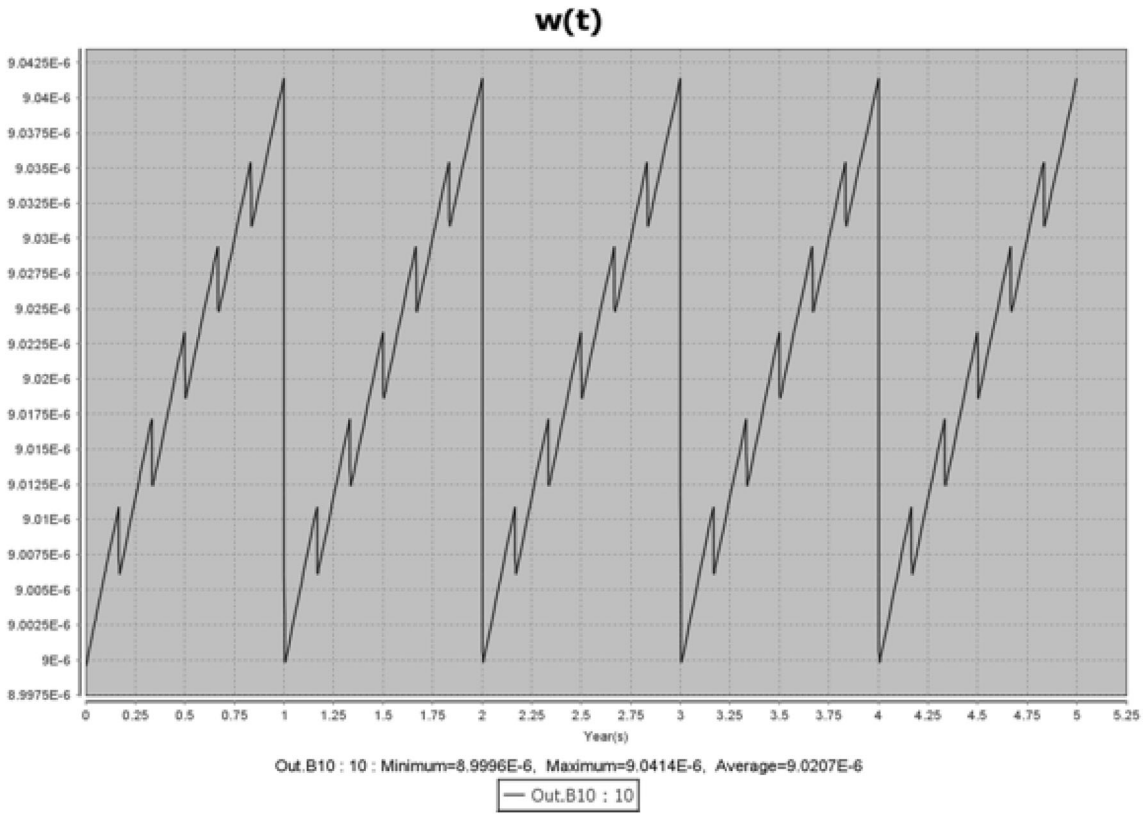


Fig. 9 HIPPS output frequency without CCFs in hour(s)$^{-1}$

Table 12 Probabilities and frequencies

RBD method	System HIPPS Output.B10			
Probabilities/Frequencies	$R(t)_{avg}$	$F(t)_{avg}$	$U(t)_{avg}$	$W(t)_{avg}$
Value	0.8261	0.1739	1.1003E-4	9.0207E-6 h^{-1}

Table 13 HIPPS dependability metrics

RBD method	System HIPPS Output.B10			
Dependabilitymetrics	MTTF	MDT	MUT	MTBF
Value	1.1084E5h	12.1971 h	1.1084E5h	1.1086E5h

Table 14 Minimal cuts set of HIPPS

PRODUCTS			
Type = PRODUCTS, Name = HIPPS Output.B10			
Order	Products	Probability (Products)	Frequency (Products)
1	LS	7.1995E-5	8.9994E-6
2	SDV1, SDV2	9.1963E-5	2.0895E-8
2	SDV1, SV2	1.2593E-5	1.005E-8
2	SDV2, SV1	1.2593E-5	1.005E-8
2	SV1, SV2	1.7243E-6	2.3605E-9
2	PT1, PT2	5.76E-12	1.44E-12
2	PT1, PT3	5.76E-12	1.44E-12
2	PT2, PT3	5.76E-12	1.44E-12

Table 15 Birnbaum measure (MIF)

Type = MIF, System = HIPPS Output.B10		
Time	Value	Component
8.76E3	0.9999	LS
8.76E3	0.0109	SDV1
8.76E3	0.0109	SDV2
8.76E3	0.0108	SV1
8.76E3	0.0108	SV2
8.76E3	4.7991E-6	PT1
8.76E3	4.7991E-6	PT2
8.76E3	4.7991E-6	PT3

Table 16 Lambert measure (CIF)

Type = CIF, System = HIPPS Output.B10		
Time	Value	Component
8.76E3	0.5472	SDV1
8.76E3	0.5472	SDV2
8.76E3	0.3777	LS
8.76E3	0.0743	SV1
8.76E3	0.0743	SV2
8.76E3	6.0434E-8	PT1
8.76E3	6.0434E-8	PT2
8.76E3	6.0434E-8	PT3

Table 17 Fussel vesely measure (DIF)

Type = DIF, System = HIPPS Output.B10		
Time	Value	Component
8.76E3	0.5516	SDV1
8.76E3	0.5516	SDV2
8.76E3	0.3778	LS
8.76E3	0.0755	SV1
8.76E3	0.0755	SV2
8.76E3	2.4604E-6	PT1
8.76E3	2.4604E-6	PT2
8.76E3	2.4604E-6	PT3

Table 18 Reliability achievement worth (RAW)

Type = RAW, System = HIPPS Output.B10		
Time	Value	Component
8.76E3	5.247E3	LS
8.76E3	57.5152	SDV1
8.76E3	57.5152	SDV2
8.76E3	57.5152	SV1
8.76E3	57.5152	SV2
8.76E3	1.0252	PT1
8.76E3	1.0252	PT2
8.76E3	1.0252	PT3

Table 19 Reliability reduction worth (RRW)

Type = RRW, System = HIPPS Ouput.B10		
Time	Value	Component
8.76E3	2.2085	SDV1
8.76E3	2.2085	SDV2
8.76E3	1.607	LS
8.76E3	1.0803	SV1
8.76E3	1.0803	SV2
8.76E3	1	PT1
8.76E3	1	PT2
8.76E3	1	PT3

Table 20 Barlow and proschan importance factor (BP)

Type = BP, System = HIPPS Output.B10		
Time	Value	Component
8.76E3	0.9952	LS
8.76E3	1.3104E-3	SDV1
8.76E3	1.3104E-3	SDV2
8.76E3	1.0722E-3	SV1
8.76E3	1.0722E-3	SV2
8.76E3	1.5924E-7	PT1
8.76E3	1.5924E-7	PT2
8.76E3	1.5924E-7	PT3

4 Discussion of HIPPS diagnostic stage

Based on the simulation results (Tables 11 and 21), we can say that RBD and FTA methods yield the similar results in the diagnostic stage. The two approaches conserve the same raking of the HIPPS components according to their importance factors.

Tables 11 and 21 shows, that MIF measures behavior of global HIPPS reliability thus, to increase reliability of HIPPS it is necessary to begin by improving reliability of logic solver (LS) above all, After that we consider the

Table 21 Ranking of HIPPS components according to their importance factors

MIF	CIF	DIF	RAW	RRW	BP
LS	SDV1 = SDV2	SDV1 = SDV2	LS	SDV1 = SDV2	LS
SDV1 = SDV2	LS	LS	SDV1 = SDV2	LS	SDV1 = SDV2
SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2	SV1 = SV2
PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3	PT1 = PT2 = PT3

reliability improvement for safety shutdown valves (SDV1, SDV2), and solenoid valves (SV1, SV2) in third place.

CIF is used to identify HIPPS weaknesses, or critical HIPPS components, to get maintenance optimization, or for selection of components for preventive maintenance, and those on which corrective maintenance is enough. The components ranking in Table 21 shows that emergency shutdown valves (SDV1, SDV2) are the elements to supervise first and foremost. The second critical element to consider is the logic solver (LS), as there is one single treatment unit in the considered system, since it can cause total fault of HIPPS, and the solenoid valves (SV1, SV2), which work in sequential way with SDV1, SDV2 in the third step. The ultimate elements to consider are the transmitters PT1, PT2, and PT3. Therefore for the most critical components: safety valves (SDV1, SDV2), logic solver (LS), solenoid valves (SV1, SV2) are the object of a systematic or conditional preventive maintenance. While the transmitters PT_i are objects of a corrective maintenance, where intervention is effected only after fault, since their breakdown would not have enough influence.

For DIF, this factor is very interesting in design stage (Vesely 1970). From the results indicated in Tables 16 and 17, we can notice that CIF and DIF give same classifications, and same simulation values using both techniques, especially, for most critical elements (LS, SDV1, SDV2, SV1, and SV2).

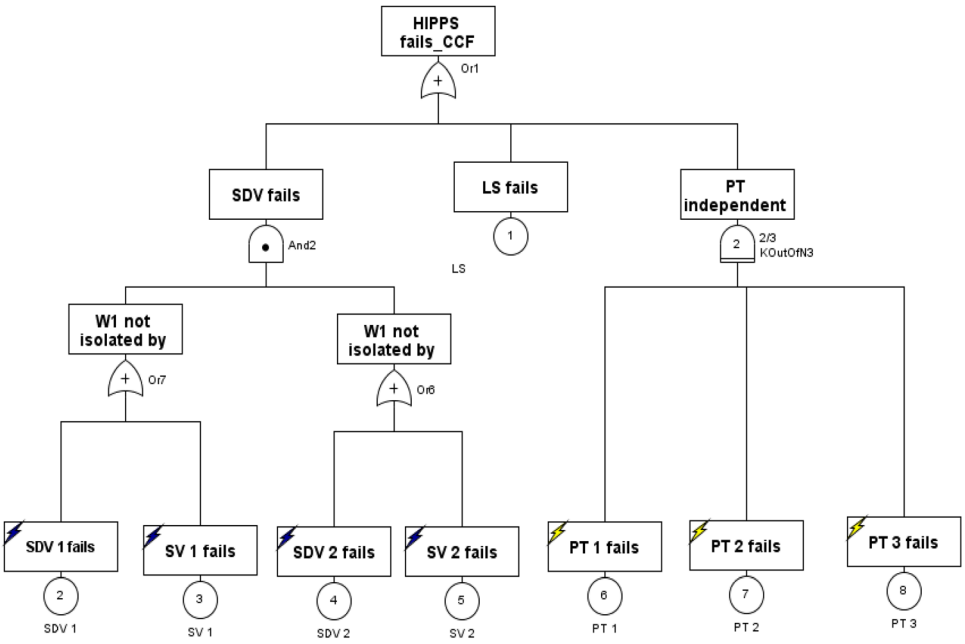
Classification of components given in Table 18, informs us that RAW, has allowed extraction of elements which are translated by a strong increase of risk, because it quantifies maximum possible percentage of system reliability increase generated by the component in question, otherwise the components with a high value of RAW will have a significant effect on overall HIPPS reliability.

According to Table 19, for RRW the classification gives a selection of the components which are the best candidates for efforts aiming to improve total HIPPS reliability, SDV_i and LS that expresses relative decrease of HIPPS unreliability for components they have a high value in case of perfect functionning. RRW, CIF, and DIF give the same order of classification. They contribute to the diagnostics of HIPPS breakdown.

Finally for BP factor: HIPPS components with a high-BP value have a significant effect on global system reliability, so any change at the level of LS reliability will have a big change at HIPPS performance level, which is very interesting in implementation of HIPPS maintenance optimization. It gives the same components ' order of classification as that of MIF and RAW. We notice that the sum of all HIPPS components importance on BP measure is unity. MIF, RAW, and BP, are used for detection of the significant components influencing global HIPPS reliability.

In this diagnostic stage, the RBD and FT correspond to the physical arrangement of HIPPS components. These methods enable us to calculate a range of IMs that are: MIF, CIF, DIF, RAW, RRW, and BP which provide elements that might help to make decision for improving HIPPS working, these IMs are also known as a sensitivity analysis of our system. MIF, RAW, and DIF are used for estimating the risk significance of HIPPS components, so their use must be in design phase (Liu and Lundteign 2015; Vesely 1970), but CIF, RRW, and BP are used to help prioritizing the effort of testing and maintenance, to assure their use in operational phase (Liu and Lundteign 2015; Lyer 1992). We find that is necessary to pay attention to these following parts of components: LS, SDV_i and SV_i RBD and FTA methods respectively provide a "static picture" of HIPPS function and fault, knowing that the most fundamental difference between the two approaches is: the RBD focus on success combinations, but the FTAs focus on failure combinations, and are able to capture all HIPPS dependability parameters, which are shown by previous simulation results, and give same simulation results for the overall HIPPS dependability properties measures: **R(t), F(t), MCS, HIPPS SIL, and W(t)**, and IMs measures.

Fig. 10 HIPPS FTA with CCFs



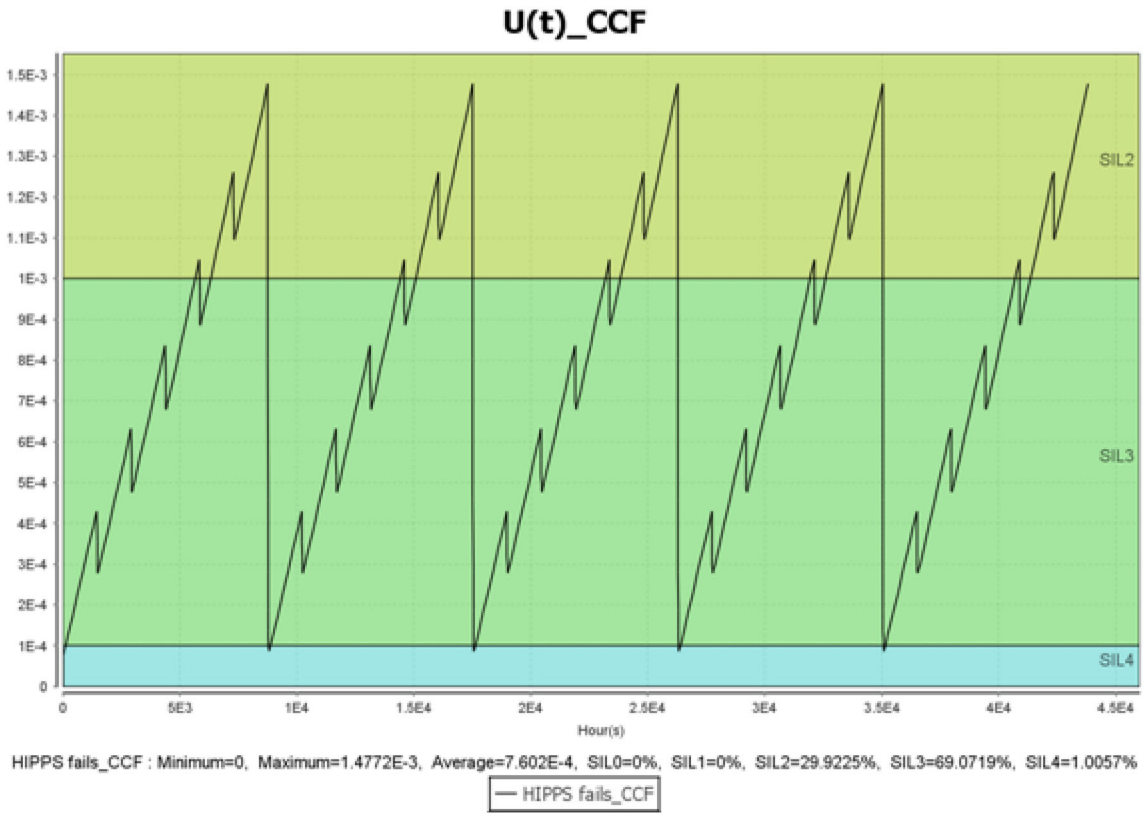


Fig. 11 Time evolution of the HIPPS instantaneous unavailability with CCFs

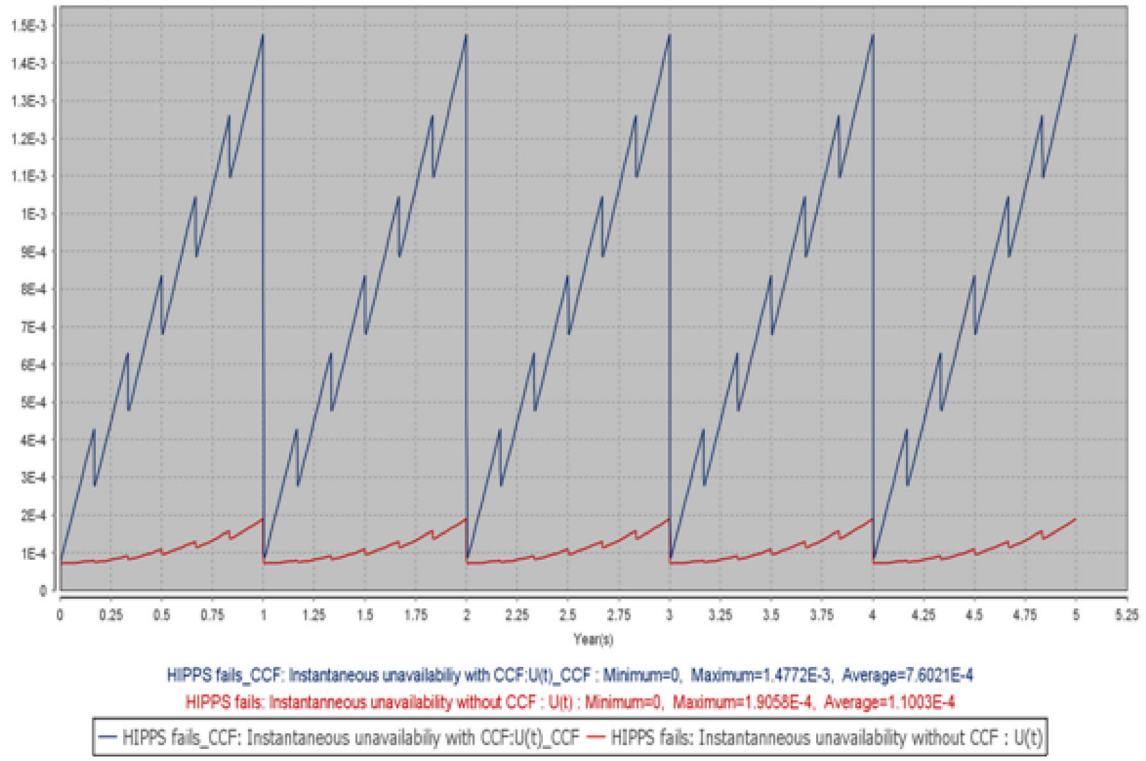


Fig. 12 Time evolution of instantaneous unavailability (HIPPS SIL) with and without CCFs

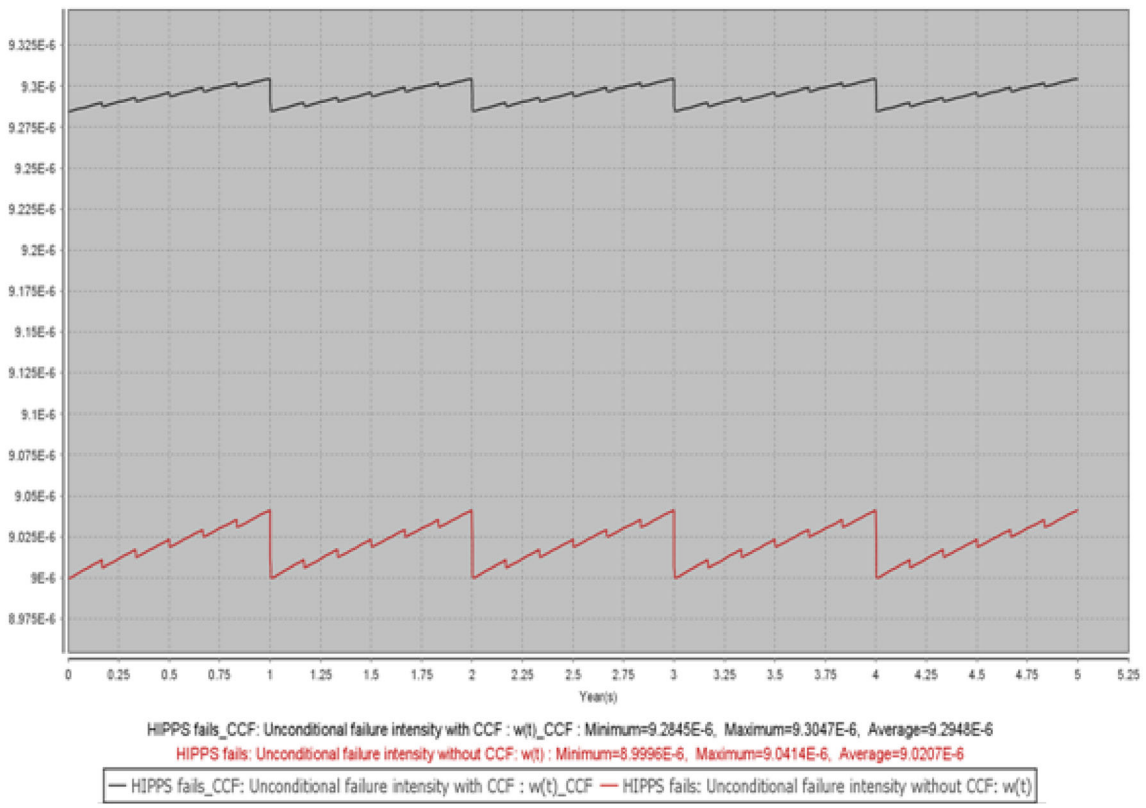


Fig. 13 HIPPS frequency in the top event in hour(s)$^{-1}$ with and without CCFs

5 HIPPS reliabilty analysis with considering CCFs by using beta factor model

5.1 HIPPS FTA implementation

In this second stage, we show HIPPS implementation with consideration of CCFs by using Beta factor model as shown in Fig. 10, we also calculate same dependability parameters, by using both formalisms. In the third part we make a comparison between simulation results given in earlier two stages and to present appropriate interpretation. Wherein all simulation results, always for a sequence time of **5** years in this overall study are also provided.

- Figure 11 shows that about **69%** of U(t)_CCF are in **SIL3 zone**, **29.9%** are in **SIL2 zone**, and about **1%** in **SIL4 zone**. So CCFs decrease HIPPS **SIL** value, by comparing Fig. 11 with Fig. 5**.**
- Figure 12 is the tracing of HIPPS unavailability with and without account of CCFs: U(t)_CCF, and U(t).
- Following Fig. 13 shows the tracing of HIPPS frequency: W(t), with and without CCFs.
- Table 22 presents the collection of various simulation results given by FTA method in both studies.
- As shown in the Table 22 CCFs reduce average reliability: R(t), and increase average probability of failure:F(t), average unavailability: U(t), and frequency: W(t).We observe a low differences between frequency $W(t)_{avg}$, and $W(t)_{avg\_CCF}$ but big difference between $U(t)_{avg}$, and $U(t)_{avg\_CCF}$ because they represent the value of SIL. So CCFs decrease **HIPPS SIL value.**
- Table 23 shows the calculation of HIPPS dependability metrics with and without CCFs given by FTA method. These measures are vital to determine if the HIPPS meets its dependability requirements. It is observed that CCFs reduce MTTF, MUT by **3330 h** or **138.75 days**, and MTBF, by **3270 h** or **136.25 days**, but increase MDT by **69.59 h**, which is approximatively **2.89 days** or **3 days**.

5.2 HIPPS RBD implementation

The RBD module generates, and groups blocks with the same CCFs, also includes a special Beta-factor, for an accurate evaluation of their effects, as shown in Fig. 14.

- Following Figs. 15, 16 and 17 give the same curves, with the same average value shown respectively in the Figs. 11, 12 and 13, in FTA CCFs assessment stage.

Table 22 Comparison between various HIPPS parameters with and without CCFs

$R(t)_{avg}$	$R(t)_{avg}$_CCF	$F(t)_{avg}$	$F(t)_{avg}$_CCF	$U(t)_{avg}$	$U(t)_{avg}$_CCF	$W(t)_{avg}$	$W(t)_{avg}$_CCF
0.8261	0.8214	0.1739	0.1786	1.1003E-4	7.6021E-4	9.0207E-6	9.2948E-6

Table 23 Comparison of HIPPS dependability metrics with and without CCFs

FTA method				
Indicator	MTTF	MDT	MUT	MTBF
Indicator without CCFs	1.1084E5h	12.1973 h	1.1084E5h	1.1086E5h
Indicator with CCFs	1.0751E5h	81.7895 h	1.0751E5h	1.0759E5h

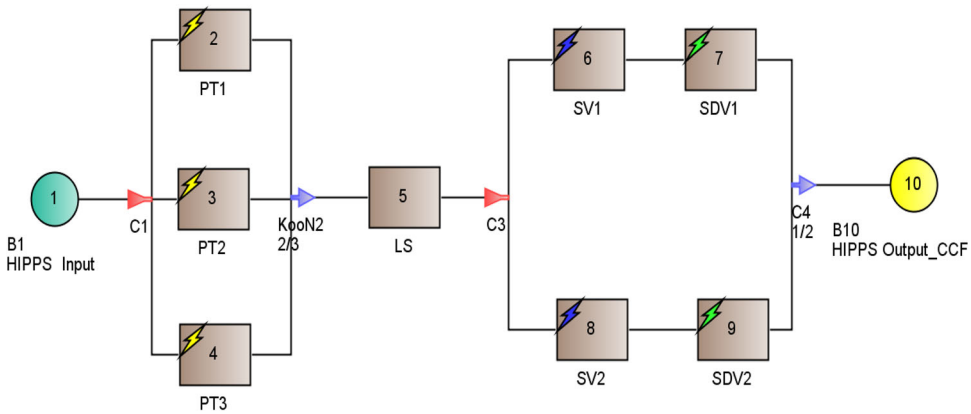


Fig. 14 HIPPS RBD with CCFs

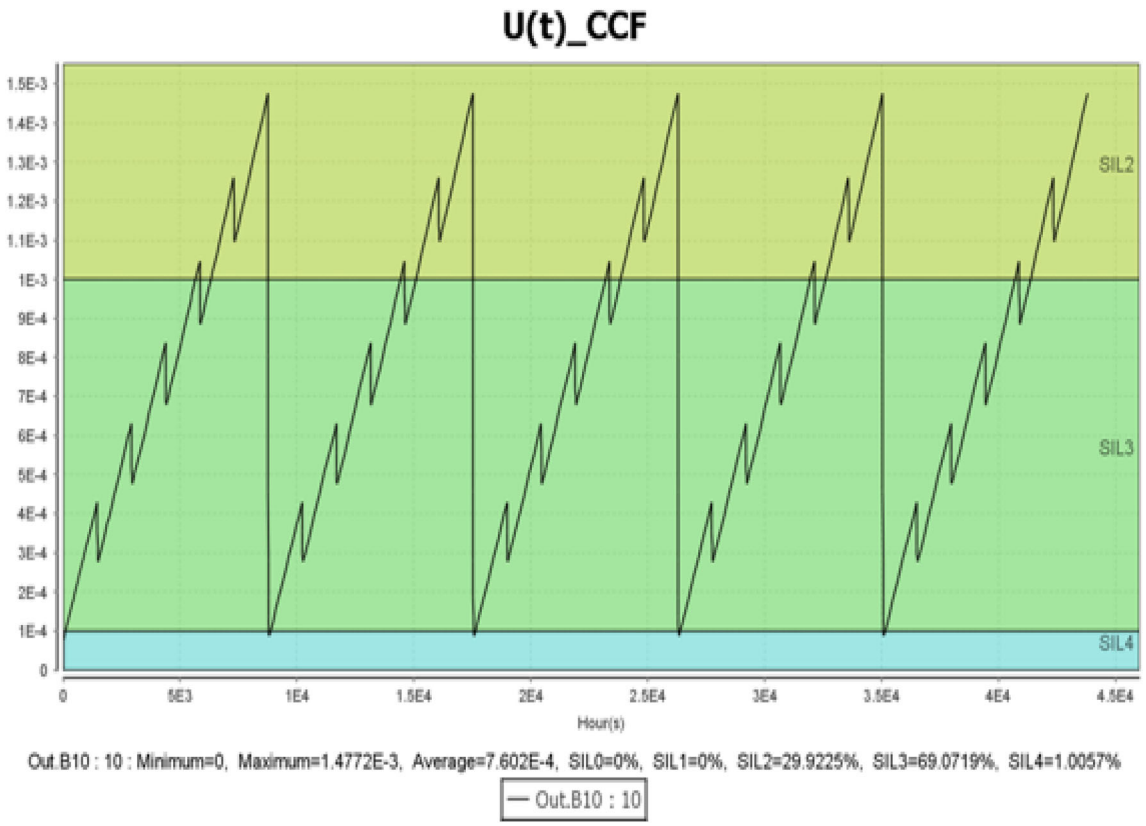


Fig. 15 Time evolution of HIPPS instantaneous unavailability with CCFs

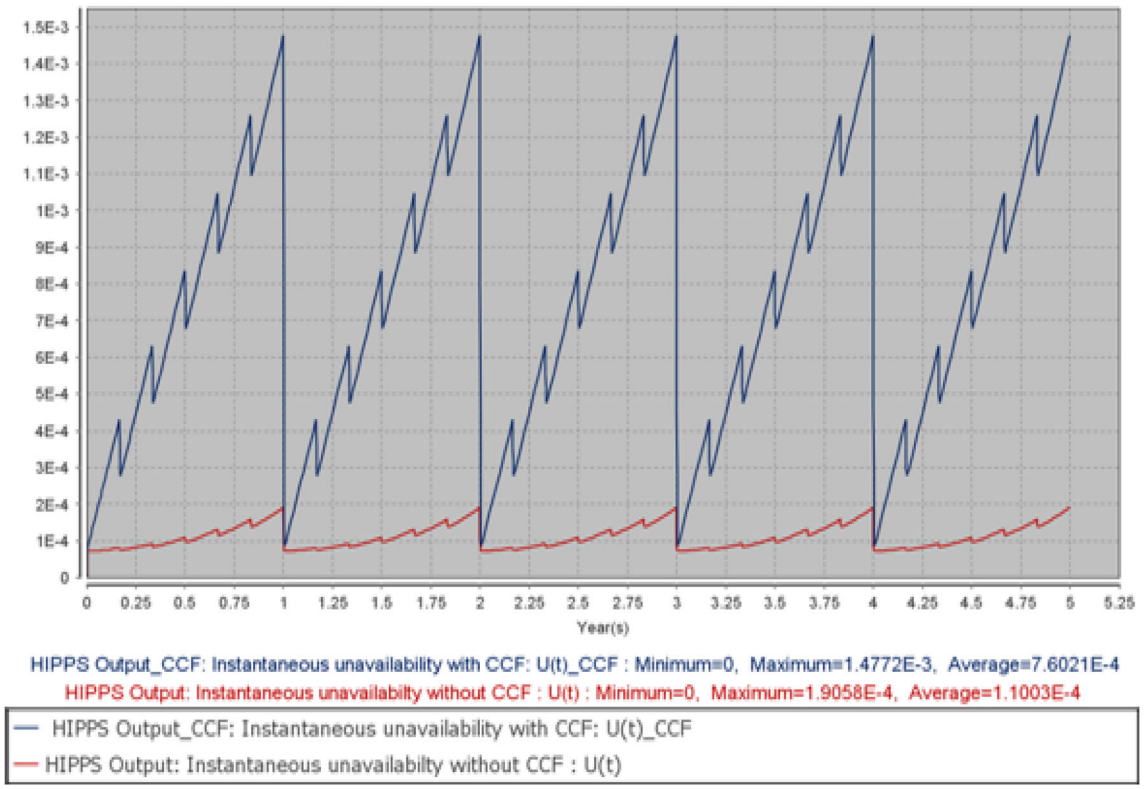


Fig. 16 Time evolution of instantaneous unavailability with and without CCFs

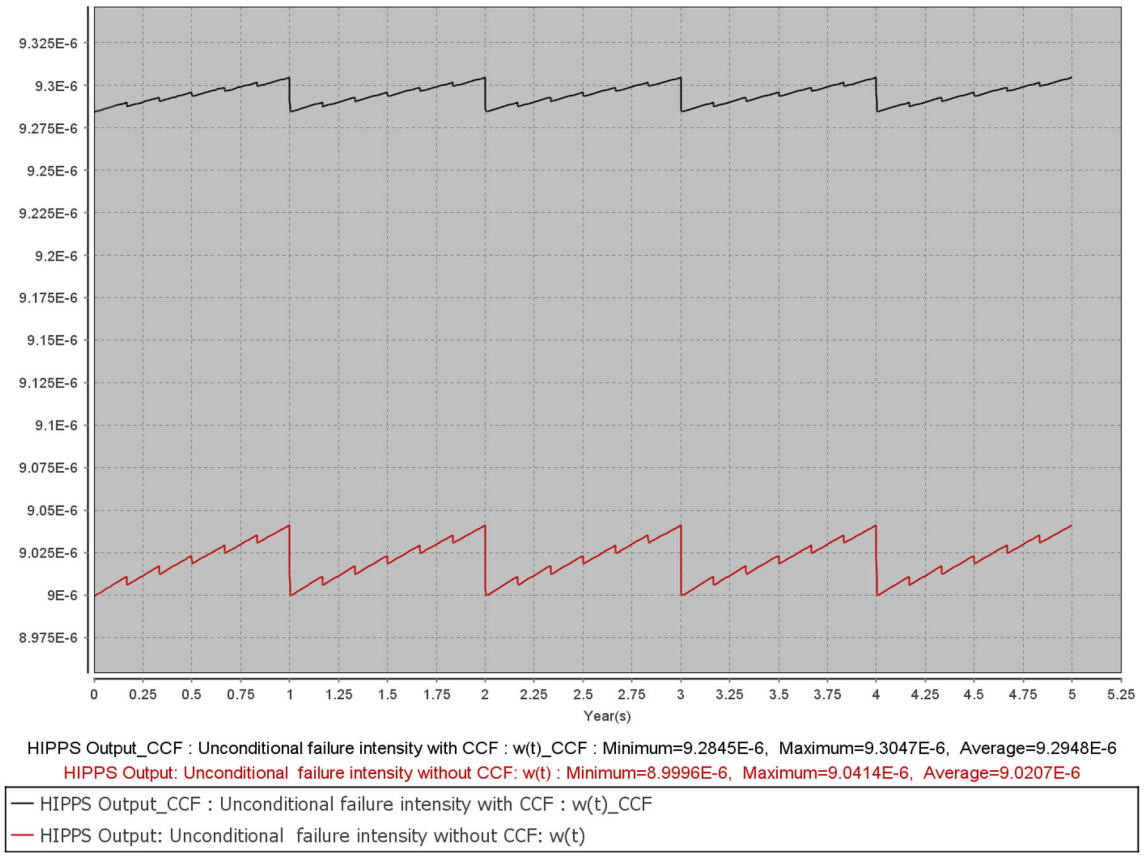


Fig. 17 Frequency in HIPPS output in hour(s)$^{-1}$ with and without CCFs

Table 24 Comparison of various HIPPS parameters with and without CCF

RBD method							
$R(t)_{avg}$	$R(t)_{avg\_CCF}$	$F(t)_{avg}$	$F(t)_{avg\_CCF}$	$U(t)_{avg}$	$U(t)_{avg\_CCF}$	$W(t)_{avg}$	$W(t)_{avg\_CCF}$
0.8261	0.8214	0.1739	0.1786	1.1003E-4	7.6021E-4	9.0207E-6	9.2948E-6

Table 25 Comparison of the HIPPS dependability metrics with and without CCF

RBD method				
Indicator	MTTF	MDT	MUT	MTBF
Indicator without CCFs	1.1084E5h	12.1971 h	1.1084E5h	1.1086E5h
Indicator with CCFs	1.0751E5h	81.7893 h	1.0751E5h	1.0759E5h

- Table 24 presents the collection of various simulation results given by RBD method with and without CCFs.
- Table 25 shows the calculation of HIPPS dependability metrics with and without CCFs given by RBD method.
- According to Tables 24 and 25 we can say that CCFs have a negative effect on global HIPPS basic measures of reliability, since it influences on value of reliability R(t), unreliability F(t), unavailability U(t), and frequency W(t). Without forgetting HIPPS dependability metrics, or HIPPS mean times, those indicators are tools and engineering techniques to identify equipment failures. Looking to Table 25, we notice that CCFs decrease MTTF by **3330 h** or **138.75 days,** the same thing for MUT, and MTBF is decreased by **3270 h** or **136.25 days**, but it increases the mean down time MDT by **69.59 h** that is equivalent to **2.89 days** (or **3 days**), as it is the mean time that a HIPPS is not usable, this include all repair times, corrective and preventive maintenance.
- It is noticed that overall simulation results given in this part, or by using HIPPS RBD implentation with

consideration of CCFs are similar with them given by the HIPPS FTA implementation with account of CCFs.

- For more illustrations about the effectiveness and robustness, of both techniques we carried out simulation for three separate time's sequences: **5**, **25**, and **50** years. Following Table 26 presents the collection of simulation results with and without consideration of CCFs for sequence times of 5, **25** and, **50** years.
- As shown in Table 26, the two techniques gives the same simulation results in the full dependability parameters: the average reliability $R(t)_{avg}$, the average unavailability $U(t)_{avg}$, and the average unconditional failure intensity $W(t)_{avg}$, for the all sequence times but the frequency: $W(t)_{avg}$ preserve only one value from 5 to 50 years in the both stages of study.
- According to this table, we notice: **MTTF** = **MUT**, in both stages (with and without considering CCFs), by using two approaches through various sequences time (5, 25 and, 50 years).
- We also notice that the reliability decreases through **5** years from **82.61** to **43, 60%** for **25** years, and to **24, 62%** for **50** years in the first stage without considering CCFs. And in second stage (with CCFs) it decreases through **5** years **from 82.14%** to **42.69%** for **25** years, and to **24, 13%** for **50** years**.** That explains the physical degradation of hardware HIPPS components, but HIPPS reliability decreases with very very low factor through the same sequence time, so the HIPPS remains reliable in the two stages of studies, by using the both methods.
- Following Table 27 is the collection of HIPPS means times in hours given by both approaches.
- According to Table 27, following HIPPS mean times: MTTF, MUT, and MTBF keeps its value from 5 to 50 years in the both studies, that is an indicator, that our proposed HIPPS meets its dependability requirements, but MDT increases slightly from 5 to 50 years, which is a very good indicator.
- From Tables 26 and 27 we, also noticed: MTTF = MUT = $\frac{1}{W(t)_{avg}}$ and $MTTF_{CCF}$ = $MUT_{CCF} = \frac{1}{W(t)_{avg\_CCF}}$, This is one criterion that HIPPS keeps a higher performances of reliability and availability in both studies by using the two techniques.
- Following Table 28 presents the calculation of CCFs factors'effect for each HIPPS parameter dependability.
- As shown in Table 28, the factor of CCFs reliability reduction increases slowly from **1.0057** to **1.028** in the time range from **5** to **50** years.
- For the average frequency $W(t)_{avg}$., the CCFs factor remains canstant for over **50** years, same thing for the MTTF MTBF, and MUT with very low value, that is

Table 26 Collection of HIPPS simulation results for sequence times of 5, 25 and 50 years

Approaches	FTA method						RBD method					
Studies	Study without CCFs			Study with CCFs			Study without CCFs			Study with CCFs		
Parameters Iterations	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)\_{avg}$	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)\_{avg}$	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)\_{avg}$	$R(t)_{avg}$	$U(t)_{avg}$	$W(t)\_{avg}$
5-years	0.8261	1.1003E-4	9.0207E-6 h^{-1}	0.8214	7.6021E-4	9.2948E-6 h^{-1}	0.8261	1.1003E-4	9.0207E-6 h^{-1}	0.8214	7.6021E-4	9.2948E-6 h^{-1}
25-years	0.436	1.1047E-4	9.0207E-6 h^{-1}	0.4269	7.6076E-4	9.2948E-6 h^{-1}	0.436	1.1046E-4	9.0207E-6 h^{-1}	0.4269	7.6074E-4	9.2948E-6 h^{-1}
50-years	0.2462	1.1088E-4	9.0207E-6 h^{-1}	0.2413	7.611E-4	9.2948E-6 h^{-1}	0.2482	1.1086E-4	9.0207E-6 h^{-1}	0.2413	7.6108E-4	9.2948E-6 h^{-1}

Table 27 Collection of HIPPS means times results for the sequence time of 5, 25 and 50 years

Approaches	FTA method							RBD method						
Studies	Study without CCFs				Study with CCFs			Study without CCFs				Study with CCFs		
Indicator Iterations	MTTF	MDT	MUT	MTBF	MTTF	MDT	MUT	MTBF	MTTF	MDT	MUT	MTBF	MTTF	MDT	MUT	MTBF
5-years	1.1084E5	12.1973	1.1084E5	1.1086E5	1.0751E5	81.7895	1.0751E5	1.0759E5	1.1084E5	12.1791	1.1084E5	1.1086E5	1.0751E5	81.7893	1.0751E5	1.0759E5
25-years	1.1084E5	12.2468	1.1084E5	1.1086E5	1.0751E5	81.8479	1.0751E5	1.0759E5	1.1084E5	12.2448	1.1084E5	1.1086E5	1.0751E5	81.8464	1.0751E5	1.0759E5
50-years	1.1084E5	12.292	1.1084E5	1.1086E5	1.0751E5	81.8843	1.0751E5	1.0759E5	1.1084E5	12.2899	1.1084E5	1.1086E5	1.0751E5	81.8828	1.0751E5	1.0759E5

approximately constant (about **1.03)** through **5–50** years. So it is evident that HIPPS meets its dependability requirements in presence of CCFs.

- For the CCFs factor of the unavailability increase of about (**6.9**) is an acceptable facor for HIPPS SIL reduction, as mentionned in this section. HIPPS keep its SIL value with **69%** in **SIL3 zone**, **1%** in **SIL4** zone, and **29.9%** in **SIL2** zone, same thing for the factor of MDT increase that is about **(6.7)**. All these are good criterion and, prove the HIPPS ability in keeping its safety and reliability performance in presence of the CCFs.
- According Table 28 both techniques give approximatively same value of CCFs factor for the same HIPPS dependability parameter in overall sequences times. These displays robustness, accuracy, and suitability of the used methodology for CCFs evaluation.

6 Discussion of the HIPPS CCFs assessment stage

The RBD and FTA can modelize CCFs. In this article we use beta factor model, since it is easy to understand get adequate results, and accurate evaluation of HIPPS CCFs effects. But regarding the results RBD, and FTA methods gives same simulation results in the stage of CCFs assessment for overall parameters: R(t), F(t), U(t), W(t), and the mean times: MTTF, MUT, MDT, MTBF, for different sequences times 5, 25, and 50 years. So we conclude by comparing overall HIPPS parameters in the second stage that FTA and RBD give an accurate evaluation of CCFs effects as per the results given in Tables 26, 27 and 28.

The simulation results show that CCFs is a part of dependent failure which occurs in redundant HIPPS components (transmitters and valves), and it is a serious threat to global HIPPS reliability. This kind of failure contributes to a lot of major negative impacts: reduction of global HIPPS reliability, increasing $F(t)_{avg}$, and the HIPPS unavailability: U(t), and accidente frequency: W(t). After achieving this comparative study between the stages with and without CCFs, we suggest that FTA and RBD formalisms as a practical and strength approaches for the HIPPS CCFs assessment, that is safety instrumented system operates in low demand mode, so it must be periodically tested to reveal failures and improve HIPPS reliability by protecting and tacking care against CCFs. Lastly after this qualitative analysis that include, HIPPS parts of common cause failure, identification of HIPPS minimal cut sets (MCS), and for the quantitative aspect containing computing of the HIPPS failure probabilities and frequencies, the HIPPS dependability metrics for

Table 28 Calculation CCFs effect factor through overall sequence times using both appraoches

Time	CCFs factor	$\frac{R(t)_{avg}}{R(t)_{avg\_CCF}}$	$\frac{U(t)_{avg\_CCF}}{U(t)_{avg}}$	$\frac{W(t)_{avg\_CCF}}{W(t)_{avg}}$	$\frac{MTTF}{MTTF_{CCF}}$	$\frac{MTBF}{MTBF_{CCF}}$	$\frac{MUT}{MUT_{CCF}}$	$\frac{MDT_{CCF}}{MDT}$
5 years	FTA_ factor	1.0057	6.9091	1.0303	1.0309	1.0303	1.0309	6.7055
	RBD_factor	1.0057	6.9091	1.0303	1.0309	1.0303	1.0309	6.7155
25 years	FTA_factor	1.021	6.8865	1.0303	1.0309	1.0303	1.0309	6.6832
	RBD_factor	1.021	6.8870	1.0303	1.0309	1.0303	1.0309	6.6841
50 years	FTA_factor	1.020	6.8641	1.0303	1.0309	1.0303	1.0309	6.6615
	RBD_factor	1.028	6.8652	1.0303	1.0309	1.0303	1.0309	6.6626

following sequences: 5, 25 and, 50 years, we can say that these models are oriented graph, are more comprehensive, accurate and very powerful for CCFs implementation and HIPPS diagnostic stage. since the both techniques assign the calculation of range of IMs for each HIPPS component, by taking jointly into account its.

7 Conclusion

The aim of this paper is to check the reliability, availability, and maintainability of a real onshore HIPPS, based on qualitative and quantitative aspects, through two stages: the first one without consideration of CCFs, or the diagnostic phase, and the second with consideration of CCFs according the following three sequences times: 5, 25, and 50 years, by using functional and dysfunctional analysis respectively by RBD and FTA techniques. In the diagnostic stage, six IMs were considered: MIF, CIF, DIF, RAW, RRW, and BP, generally the components with very low importance value had negligible effects on global HIPPS reliability, while the higher importance value of components had a big influence on HIPPS performances. These ranges of measures are very interesting for optimizing the HIPPS maintenance planning, in particular the IMS were used for the identification of the critical components in HIPPS which were concerned by the preventive maintenance, which typically incured high costs and considerably lengthy times to return the system to service. These measures help us to identify HIPPS weakest areas, and moreover they give hints to modification which will improve HIPPS dependability. From the simulation results, we have found that the Logic Solver: LS, Safety Shutdown Valves: SDVi and, the Solenoid Valves: SVi need the subject of a systematic or conditional preventive maintenance, but the transmitters PT_i were concerned by a corrective maintenance. In the diagnostic phase using RBD, and FTA the HIPPS dependability analysis has been achieved by computing following parameters: reliability: R(t), unreliability: F(t), HIPPS unavailability: U(t), that presents HIPPS safety integrity level: (SIL), frequency: W(t), minimal cut sets: MCS, mean times, the two approaches give the same simulation results and the same ranking of HIPPS components, in the objective to evaluate maintenance strategies by detecting criticality and vulnerability, and to determine best location of safety devices (weak links). This methodology is used in operation phase to understand and correct the errors in HIPPS functioning. Bisides this, we illustrate using comparison beteween simulation results, that both approaches give same quantitative results for the full range of parameters in different precedent sequences time.

For the second stage of study, we made a comparative study between results fournished by both techniques, tacking in account the effect of CCFs, and to study how the CCFs influence on the value of HIPPS properties measures. The results show that CCFs have the following negative impacts on global HIPPS performance:

- Decreasing HIPPS reliability: R(t)
- Increasing HIPPS: unreliability: $F(t)_{avg}$, and frequency of the feared accident: W(t).
- Increasing HIPPS unavailability $U(t)_{avg}$, or, decreasing the HIPPS SIL.
- Decreasing HIPPS mean times: MTTF, MTBF, and MUT, or decreasing HIPPS availability.
- Increasing HIPPS MDT, thus decreasing HIPPS production capacity.

Based on our analysis the designed and proposed HIPPS remained reliable in the case of CCFs assessment, which indicate highest HIPPS performance.

The obtained simulation results of proposed HIPPS show that the results fournished by both techniques in overall stages of study, for sequences times 5, 25, 50 years, are similar (according to Tables 26, 27 and 28). Thus FTA and RBD are strong accurate, and more suitable to assess the effects of CCFs. This paper evaluated the effect of CCFs on global HIPPS reliability, and the degradation of the HIPPS safety level, the CCFs were modeled implicitly using beta factor with defined structure and rigorous methodology, thus we can say, that RBD and FTA are from the most prominent, and powerful techniques, which are widely used in oil and gas industries. The limitations of the used methodology, are basically static, and require binary

states of all components and will not be able to model any degraded operation.

In practice the reduction of CCFs effect was achieved by decreasing beta factor to an acceptable level through right implementations of certain items such as: physical separation of redundant units, use of different types of equipment that responds differently to a common stressor, the robustness in hardware and software parts of the system, and the environmental control.

Further work will focus on the estimation of CCFs by the dynamic reliability blocks diagram, and the dynamic Fault tree analysis methods for effective and better treatment of this problem, or we can also propose as future research the estimation of CCFs by fuzzy FTA technique.

Funding All authors certify that they have no financial interest in the publication of this article.

Declarations

Conflict of interest All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

Human or animal rights The authors certify that this research does not involving Human Participants and/or Animal.

References

Amrutkar KP, Kamalja KK (2017) An overview of various importance measures of reliability system. Int J Math Eng Manag Sci 2:150–171. https://doi.org/10.33889/IJMEMS.2017.2.3-014

Basilio A, Glissente L, Tino Vande C (2015) Safety instrumented systems manual for plant and maintenance, 4th edn. publisher GM international. ISBN-10: 8894208702, ISBN-13:978-8894208702

Beugin J, Renaux D, Cauffriez L (2006) A SIL quantifcation approach based an operating situations model for safety evaluation in complex guided transportation systems. Int J Reliab Eng Saf Syst 92:1686–1700. https://doi.org/10.1016/j.ress.2006.09.022.ISSN:0951-8320

Birnbaum ZW (1969) On the importance of components in a multicomponent system. In: Krishanaial PR (ed) Multivariate analysis. Academic Press, pp 581–592

Bozoudis M, Lappas I, Kottas A (2018) Use of cost-adjusted importance measures for aircraft system maintenance optimization. J/Aerosp/ 5:68. https://doi.org/10.3390/aerospace5030068

CCPS (1993) Guidelines for safety automation of chemical processes. Center for chemical process safety. American institute of chemical engineers, New York, NY, USA

Di Bona G, Forcina A, Falcone D, Silvestri L (2020) Critical risk methods (CRM): a new safety allocation approach for critical infrastructure. Sustainability 12:4949. https://doi.org/10.3390/su12124949

Dutuit Y, Rauzy AB, Signoret JP (2008) A snapshort of methods and tools to assess safety integrity levels of high integrity protection systems. Proc Instit Mech Eng Part 0 Int J Risk Reliability 222:371–379. https://doi.org/10.1243/1748006XJRR147

Fleming K (1974) A reliability model for common mode failures in redundant systems. Technical report.

Fusell JB (1975) How to hand calculate system reliability and safety characteristics. IEEE Trans Rel R-24:169–174. https://doi.org/10.1109/TR.1975.5215142

GRIF Workshop (2019) Graphical interface for reliability forecasting, software, available at: http://grif-workshop.com

Hasan O, Ahmed W, Tahar S, Hamdi M.S (2014) Reliablity blocks diagrams based analysis: a survey. Preceeding of international conference on Numerical analysis and applied mathematics (ICNAAM-2014), Greece. AIP Conf. Pro.1648, 850129–1850129–4, Doi: https://doi.org/10.1063/1.4913184

Hauge S, Hokstad P, Habrekke S, Lundteigen MA (2016) Common cause failures in safety instrumented systems: using field experience from petroleum industry. Int J Reliability Eng Syst Saf 151:34–45. https://doi.org/10.1016/j.ress.2015.09.018.ISSN:0951-8320

Hauge S, Hoem AS, Hohstad P, Habrekke S, Lundteigen MA (2015) Common cause failures in safety instrumented systems, Beta factors and equipment specific checklists based on operational experience. SINTEF report, reference number 102001186

Hokstad P, Rausand M (2008) Common cause failure modeling: status and trends. In: Misra KB (ed) Handbook of performability engineering. Springer, London, pp 621–640

Hwang FK (2005) A hierarchy of importance indices. IEEE Trans Rel 54:169–172. https://doi.org/10.1109/TR.2004.841707

IEC 61508 (2010) Functional safety of eletrical/electronic/programmable electronic safety-related systems, part 1–7, 2nd edn. International Electrotechnical Commission, Geneva

IEC 61511 (2003) Functional safety: safety instrumented systems for process industry sector, part 1–3. International Electrotechnical Commission, Geneva

Iyer S (1992) The Barlow-Proschan importance and its generalizations with dependent components. J Stoch Processe Appl 42:353–359. https://doi.org/10.1016/0304-4149(92)90046-S

Jin H, Lundteigen MA, Rausand M (2011) Reliability performance of safety instrumented systems: a common approach for both low- and high demand mode of operation. Int J Reliab Eng Syst Safe 96:365–373. https://doi.org/10.1016/j.ress.2010.11.007

Lambert HE (1975) Fault tree for decision making in system analysis. PhD. Dissertation, Lawrence, Livermore Laboratory-university of California

Lassen CA (2008) Layer of protection analysis (LOPA) for determination of safety integrity level (SIL). Technical report Snarøya, 19.06.2008. Norwiegian University of Science and Tachnology, Departement of Production and Quality Engineering

Levitin G, Podofillini L, Zio E (2003) Generalised importance measures for multi-state elements based on performance level restrictions. Int J Reliab Eng Saf 82:287–298. https://doi.org/10.1016/S0951-83205(03)00171-6

Liu Y, Lundteign MA (2015) Reliability importance of the cannels in safety instrumented systems. Int J Ind Eng Manag Sci Appl 349:1041–1054. https://doi.org/10.1007/978-3-662-47200-2_108

Liu Y, Zhang A, Srivastav H, Barros A (2021) Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state. Int J Reliab Eng Syst Safe 209:107393. https://doi.org/10.1016/J.ress.2020.107393

Lundteigen MA, Rausand M (2007) Common cause failure in safety instrumented systems on oil and gas installations: implementing defence measures through function testing. Int J Loss Prev Process Ind 20:218–229. https://doi.org/10.1016/J.Jlp.2007.03.007

Lundteigen MA, Rausand M (2010) Reliability of safety instrumented systems: where to direct future research? Wiley onev line library (wileyonlinelibrary.com). Proc Safe Prog 29:372–379. https://doi.org/10.1002/prs.10390

Lundteigen MA (2008) Safety intrumented systems in oil and gas industry: concepts, and methods for safety and reliability assessment in design, and operation. PhD Thesis, University of Norwegian

Lundteign MA, Rausand M, Bouwer UI (2008) Developpement of safety instrumented systems-RAMS engineering and management from producer perspective. Int J Reliab Eng Syst Safe 5:7491

Meng FC (2009) On some structural importance of system components. J Data Sci 7:277–283. https://doi.org/10.6339/JDS.2009.07(2).472

Petroleum, petrochemical, and naturel gas industries-reliability modeling and calculation of safety systems. (2013), Technical report. Reference number ISO/TR 12489/2013(E)

Rausand M (2011) Risk assessment theory, methods and applications. Wiley Hoboken, NJ

Rausand M, Hoyland S (2004) System reliability theory: models and applications. Wiley Hoboken, NJ

Roberts NH, Vesely WE (1981) Fault tree, handbook. NUREG-0492. U.S. Government printing office: 1992–318–277/60129

Ruijters E, Stoelinga M (2015) Fault tree analysis: a survey of the state-of-the-art in modeling analysis and tools. Int J Comput Sci Rev. https://doi.org/10.1016/j.cosrev.2015.03.001

Sonatrach-company of oil and gas -Algeria- Skikda refinery rehabilitation and adaptation project. SIL verification report 2014

Triconex operating manual Tristation (2010). Ver.4.7, Available at: http://www.triconex.com

Vesely WE (1970) A time dependent methodology for fault tree evaluation. Nucl Eng Des 13:337–360. https://doi.org/10.1016/0029-5493(70)90167-6