REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université Hadj-Lakhdar, Batna
Institut d'Hygiène et Sécurité Industrielle
Département de Sécurité Industrielle
Laboratoire de Recherche en Prévention Industrielle (LRPI)

MEMOIRE

Présenté pour l'obtention du diplôme de

MAGISTER

EN HYGIÈNE ET SÉCURITÉ INDUSTRIELLE

Option : Gestion du Risque

Par

Hafed TOUAHAR

Ingénieur d'Etat en Hygiène et Sécurité Industrielle

Thème :

Maintenance des Systèmes Instrumentés de Sécurité (SIS): Etude de cas.

Soutenu le 23 Mai 2015 devant le jury d'examen :

M.	**Abdallah TAMRABET,**	Professeur à l'Univ. de Batna	**Président**
M.	**Rachid NAIT-SAID,**	Professeur à l'Univ. de Batna	**Rapporteur**
M.	**Mourad KORICHI,**	Maître de Conférences A à l'Univ. de Ouargla	**Co-Rapporteur**
M.	**Noureddine SETTOU,**	Professeur à l'Univ. de Ouargla	**Examinateur**
Mme.	**Nouara OUAZRAOUI,**	Maître de Conférences B à l'Université de Batna	**Membre invité**

2015

A ma famille

A mes collègues

A tous les miens

Remerciements

Je tiens à exprimer mes sincères remerciements et toute ma gratitude à Monsieur **NAIT-SAID Rachid**, Professeur à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté de diriger ce travail, pour son soutien permanent, son aide constante et ses encouragements inconditionnés durant tout ce travail.

Je tiens à remercier vivement Monsieur **KORICHI Mourad**, Maître de Conférences A à l'Univ. de Ouargla d'avoir accepté le Co-encadrement de ce travail et pour ses remarques pertinentes ainsi que son soutien continu qui sont concrétisés par l'achèvement de ce travail dans les meilleurs conditions.

Je présente mes vifs remerciements aux membres du jury de soutenance de ce mémoire de Magistère, à savoir :

- Monsieur **TAMRABET Abdallah,** Professeur à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté de présider le jury de soutenance.

- Monsieur **SETTOU Noureddine,** Professeur à l'Université de Ouargla d'avoir accepté d'évaluer ce travail.

- Madame **OUAZRAOUI Nouara,** Maître de Conférences B à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté l'invitation.

J'exprime, également, ma profonde gratitude à tous les personnels de l'entreprise SONATRACH, division de production d'In Amenas, pour leur aide et fourniture des données sur l'unité RGTE (Récupération des Gaz Torchés *du champ **E**djelet).*

Enfin, nos derniers remerciements vont à l'ensemble de la famille enseignante de l'institut d'hygiène et sécurité industrielle de l'Université Hadj Lakhdar de Batna. A tous ceux qui de près ou de loin, ont contribué à la réalisation de ce mémoire.

Table des matières

Abréviations, acronymes

AdD	Arbre des Défaillances
BPCS	Basic Process Control System (système de commande de processus de base)
CEI	Commission d'Electrotechnique Internationale
C_{STR}	Coût lié au taux de déclenchement intempestif
DCC	Défaillance de Cause Commune
E/E/EP	Electrique / Electronique / Electronique Programmable
EN	European Norm (Norme Européenne)
ESD	Emergency Shutdown Systems (systèmes d'arrêt d'urgence)
EUC	Equipment Under Control (équipement à protéger)
GGFR	Global Gas Flaring Reduction Initiative (Partenariat Mondiale de la réduction des gaz torchés)
IPL	Independant Protection Layers (Couches de Protection Indépendante)
ISA	Instrument Society of America
ISO	International Organisation for Standardization (Organisation Internationale de Normalisation).
KooN	K out of N (K parmi N)
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection)
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance)
PFD	Probability of Failure on Demand (probabilité de défaillance à la demande)
PFH	Probability of Failure per Hour (probabilité de défaillance par heure)
RGTE	**R**écupération des **G**az **T**orchés du champ d'**E**djelet
SFF	Safe Failure Fraction (proportion des défaillances en sécurité)
SIF	Safety Instrumented Function (fonction instrumentée de sécurité)
SIL	Safety Integrity Level (niveau d'intégrité de sécurité)
SIS	Safety Instrumented System (système instrumenté de sécurité)
SO	Spurious Operation (Opération intempestive)
STL	Spurious Trip Level (niveau de déclenchement intempestif)
STR	Spurious Trip Rate (taux de déclenchement intempestif)
λ	Taux de défaillance aléatoire du matériel,
λ_D	Taux de défaillance aléatoire dangereuse du matériel,
λ_{DD}	Taux de défaillance aléatoire dangereuse du matériel détectée,

λ_{DU}	Taux de défaillance aléatoire dangereuse du matériel non détectée
λ_{S}	Taux de défaillance aléatoire en sécurité du matériel,
λ_{SD}	Taux de défaillance aléatoire en sécurité du matériel détectée,
λ_{SU}	Taux de défaillance aléatoire en sécurité du matériel non détectée
λ_{STD}	Taux de défaillance intempestive du matériel détectée,
λ_{STU}	Taux de défaillance intempestive du matériel non détectée,
λ_{NONC}	Taux de défaillance non critique du matériel,
λ_{SO}	Taux de défaillance d'une opération intempestive,
T_1	Durée entre deux tests périodiques.
$MTTR_{SD}$	Durée moyenne de réparation d'une défaillance sûre (détectée).
β_{D}	Facteur correspondant aux défaillances de causes communes dangereuses
β_{SD}	Facteur correspondant aux défaillances de causes communes intempestives détectées
β_{SU}	Facteur correspondant aux défaillances de causes communes intempestives non détectées

Liste des figures

Liste des tableaux

Introduction

Les établissements industriels deviennent techniquement de plus en plus complexes et le potentiel de danger s'accroît en conséquence si les flux de danger ne sont pas convenablement contrôlés. Lorsque les systèmes industriels présentent des risques potentiels pour les personnes, l'environnement ou les biens, la gestion de ces risques nécessite de mettre en place des mesures de maitrise des risques aussi communément appelées barrières de sécurité. Celles-ci participent soit à la prévention en minimisant la probabilité d'apparition du risque, soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés pour assurer la sécurité fonctionnelle des installations, *i.e.* la réduction des risques à un niveau inférieur ou égal au risque tolérable.

L'activation des SIS dans les processus industriels est effectuée après l'occurrence des déviations spécifiques (situation dangereuse) par rapport au fonctionnement normal (situation normale), mais dans certains cas les SIS sont activés en absence des déviations ou de demandes : il s'agit des activations intempestives.

Les activations intempestives des SIS sont caractérisées en terme de fréquence par un taux de déclenchement intempestif (STR : *Spurious Trip Rate*). Plusieurs formules analytiques liées à l'estimation du STR sont présentées dans la littérature et selon différentes approches. Une étude bibliographique permet d'examiner l'ensemble de ces formules. La détermination du STR d'un SIS installé dans un processus industriel a une signification en termes de coûts liés aux pertes de production imputables aux déclenchements intempestifs.

Pour les industriels, il est donc incontestable de réduire au maximum possible ce type de déclenchements. La minimisation de ces déclenchements implique un investissement en matière de coûts d'où l'intérêt d'un tel objectif qui sera traité dans ce travail.

Le présent mémoire a un double objectif : d'une part, il vise l'évaluation quantitative du taux de déclenchement intempestif (STR : Spurious Trip Rate) d'un système instrumenté de sécurité (SIS) installé dans un processus industriel opérationnel (en phase d'exploitation), par application de la méthode de l'arbre de défaillance et par d'autre formules analytiques trouvées dans la littérature et d'autre part, la minimisation de ce taux sous contraintes de coûts de maintenance à des valeurs adéquates aux seuils prédéfinis par les concepteurs des SIS.

Le présent mémoire est scindé en quatre chapitres :

Au niveau du premier chapitre seront présentés, dans un premier temps, quelques concepts et définitions liés à la sécurité. Nous évoquerons ensuite l'organisation de la norme CEI 61508 qui constitue le document de référence pour la mise en œuvre des SIS. Puis, nous définirons les systèmes instrumentés de sécurité, leur fonctionnement et organisation.

Le deuxième chapitre représente la base de ce travail, il permet de clarifier la typologie des défaillances liées aux SIS et, d'apprécier la nature des activations intempestives et d'examiner l'ensemble de formulations analytiques de l'estimation du taux de déclenchement intempestif (STR) selon ce qui est retrouvé dans la littérature.

Au début du troisième chapitre, une présentation des installations choisis comme champ d'application est donnée. Puis, nous présenterons le SIS, objet d'étude de notre travail. Ce système est décrit selon son architecture réelle. La modélisation du STR et son évaluation sont faite moyennant la méthode de l'arbre de défaillance (AdD). De plus, et dans un but de comparaison, d'autres approches ont été utilisées à savoir les travaux de M. A Lundteigen, et M.Rausand, l'approche présentée par ISA, l'approche proposée par l'organisme norvégien SINTEF, les formules présentées dans le rapport de la société TOTAL et l'approche basée sur l'application des chaines de Markov.

Le quatrième et dernier chapitre sera consacré à la minimisation du STR évalué. Un ensemble de contraintes en termes de coûts de maintenance est prendre en considération. Ces contraintes impliquent implicitement des stratégies de maintenance qui permet de minimiser le STR à des valeurs adéquates et acceptable.

Ce mémoire sera clos par une conclusion générale résumant le travail réalisé et donnant les difficultés rencontrées.

Chapitre 1

Systèmes Instrumentés de Sécurité (SIS)

1.1.Introduction

Les industries ne se préoccupent plus uniquement des performances des systèmes en termes de qualité et de rentabilité mais aussi en termes de sécurité puisque ces systèmes peuvent présenter des risques dommageables. La réduction de ces risques à un niveau jugé tolérable est indispensable, elle est souvent obtenue par l'interposition successive de plusieurs barrières de sécurité entre la source de danger, qui peut être un procédé industriel, et les cibles potentielles que sont les personnes, les biens et l'environnement. Ces barrières incorporent souvent des systèmes instrumentés de sécurité (SIS*: Safety Instrumented System)* utilisés pour exécuter des fonctions de sécurité nécessaires à la mise en sécurité de l'équipement à protéger (EUC *: Equipment Under Control*).

Au début de ce premier chapitre, une définition précise pour les termes omniprésents dans ce mémoire est donnée, tels que système, danger, risque et réduction du risque, sécurité et sécurité fonctionnelles puis, nous présentons le cadre normatif des SIS (précisément la norme CEI 61508 et ses normes filles « sectorielles ») ensuite, nous donnons une synthèse sur les concepts relatifs au système instrumenté de sécurité, leur fonctionnement (dysfonctionnement) et leur organisation et, enfin, nous rappelons l'objectif du chapitre pour conclure.

1.2.Principaux concepts de sécurité

1.2.1 Notion de système

Plusieurs définitions ont été proposées pour le mot système. La plus générale est celle proposée par J. L. Le Moigne [**26**], qui considère un système comme : " *un objet doté de finalité qui, dans un environnement, exerce une activité et voit sa structure interne évoluer au fil du temps, sans qu'il perde pourtant son identité "*. Selon cet auteur, un système peut être vu donc comme :

- Quelque chose (n'importe quoi présumé identifiable),
- Qui fait quelque chose (activité, fonctionnement),
- Dans quelque chose (environnement),
- Pour quelque chose (finalité, projet),
- Par quelque chose (structure = support de l'activité),
- Et qui se transforme dans le temps (évolution).

1.2.2 Notion de danger

Selon Desroches [**03**] et la norme CEI 61508 [**38**], *le danger désigne une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes. Les dangers peuvent avoir une incidence directe sur les personnes, par des blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens ou l'environnement.*

Selon la norme OHSAS 18001 [**41**] : "*un danger est une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments "*. Les dangers liés à un système sont inhérents au fonctionnement ou au dysfonctionnement du système, soit extérieur au système.

Plusieurs auteurs et dictionnaires confondent le terme danger au terme risque, ce qui explique l'utilisation indifférente de ces deux termes par plusieurs personnes.

1.2.3 Notion de risque et de réduction du risque

Le risque peut être considéré comme une certaine quantification du danger associant une mesure de l'occurrence d'un événement redouté à une estimation de la gravité de ses conséquences [**16**]. Cette définition est proche de celle proposée par A. Villemeur, *" Le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences."* [**08**].

La définition suivante est rencontrée souvent pour caractériser le sens du mot risque: *" La combinaison de la probabilité d'occurrence d'un dommage et la gravité de ce dernier."* [**21**].

Le terme combinaison est généralement matérialisé par opération de multiplication, se qui nous permet la formulation suivante : *Risque* (*R*) = *Probabilité* (*P*) × *Gravité* (*G*).

La représentation graphique de cette relation est une droite ou une courbe décroissante. Elle dérive de la courbe dite de *Farmer* [**17**] et permet d'illustrer la partition de l'espace du risque en deux sous-ensembles disjoints, correspondant respectivement au domaine du risque acceptable et à celui du risque inacceptable (figure 1.1).

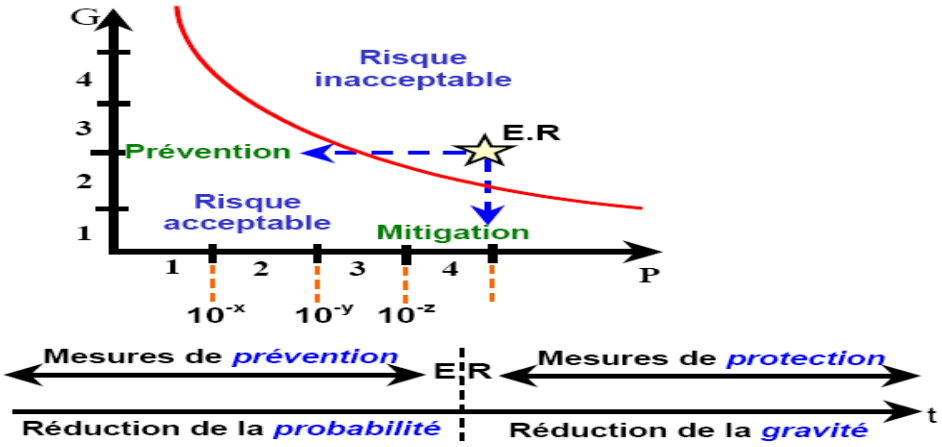


Figure 1.1 : L'espace du risque. ***[16]***

Réduction du risque : La réduction du risque doit être considérée dès lors que le risque considéré est jugé inacceptable. Il s'agit d'identifier les barrières nécessaires pour ramener le niveau de risque des différents scénarios d'accidents, en agissant le plus en amont possible de leur développement (principe d'élimination à la source), à un niveau acceptable. La réduction du risque peut être obtenue de deux manières différentes (figure1.1).

- ***La protection :*** elle regroupe les mesures prises pour limiter les conséquences de la survenue d'un accident en diminuant ainsi sa gravité. Par exemple : une cuvette de rétention assurant le non épandage d'un liquide, un système d'extinction automatique permettant de réduire les effets d'un incendie, les plans de secours et les procédures d'urgence pouvant réduire largement les dommages susceptibles d'être occasionnés, etc.

- ***La prévention :*** elle a pour but la réduction de sa probabilité (ou fréquence) d'occurrence. La prévention désigne donc les mesures préalables mises en place pour empêcher la survenue d'un accident. Cela peut être assuré par une conception sûre de l'installation ou par l'ajout de systèmes assurant la sécurité de l'installation en cas de dérive. Ainsi, pour protéger une installation contre les surpressions, les mesures de prévention peuvent consister en une soupape de sécurité, un disque de rupture ou encore en un système automatique d'arrêt d'urgence.

Par ailleurs, les risques assumés, résiduels, doivent être contrôlés et gérés par :

- La sensibilisation et la communication sur ces risques. A ce titre, les exploitants sont tenus pour responsables et sont suspectés s'ils n'ont pas communiqué de manière suffisamment transparente sur les risques qui dépendent de leur autorité.
- Le maintien et le contrôle des mesures de réduction mises en place.
- La gestion financière et assurances.

1.2.4 Notion de sécurité

La sécurité est généralement définie par l'absence de phénomènes dangereux, de risque inacceptable, d'accident ou de situations catastrophiques. D'après le guide ISO/CEI 73[**22**], la sécurité est " *l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement*. ".

La sécurité d'un système peut être définie en termes d'aptitude, les deux définitions suivantes précisent cet aspect : " *La sécurité d'un système est son aptitude à fonctionner ou à dysfonctionner sans engendrer d'événement redouté à l'encontre de lui-même et de son environnement, notamment humain.*" [**16**], Et " *La sécurité est l'aptitude d'une entité à éviter de faire apparaitre, dans des conditions données, des événements critiques ou catastrophiques.* " [**07**].

Dans le cadre des systèmes industriels, la sécurité consiste à mettre en œuvre des moyens évitant l'apparition de dangers. Elle s'énonce par l'absence de risque inacceptable [**38**].

1.2.5 Sécurité fonctionnelle

La sécurité fonctionnelle a pour objet de contrôler les risques inacceptables qui pourraient provoquer des accidents dangereux. Elle couvre les systèmes mettant en œuvre des solutions de protection appliquées dans plusieurs domaines mécanique, électrique, électronique, électronique programmable, hydraulique, optique, . . .

La norme CEI 61508 [**38**] dans sa partie 4 définit la *sécurité fonctionnelle* comme un sous ensemble de la sécurité globale qui se rapporte au système commandé (*EUC, Equipement Under Control*) et qui dépend du fonctionnement correct du système

électrique, électronique programmable E/E/EP relatif à la sécurité, des systèmes relatifs à la sécurité basées sur une autre technologie et des dispositifs externes de réduction de risque.

La norme CEI 61511 [**39**] définit la *sécurité fonctionnelle* comme un sous-ensemble de la sécurité globale qui se rapporte au processus et au système de commande de processus de base (*BPCS, Base Process Control System*) et qui dépend du fonctionnement correct du système instrumenté de sécurité et d'autres couches de protection. Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

1.3. Normes relatives aux Systèmes Instrumentés de Sécurité

L'instrumentation doit réellement être utilisée pour réaliser des fonctions instrumentées de sécurité, donc il est essentiel qu'elle présente des niveaux minimums de qualité et de performance. En conséquence, un grand travail a été effectué mettant en question les performances des systèmes relatifs à la sécurité de type instrumenté, considérés comme complexes, par le développement des normes qui favorisent l'évaluation, la validation et la certification systématique de ces systèmes. Parmi ces différents documents normatifs, la norme CEI 61508 [**38**] développée et publiée par la Commission d'Electrotechnique Internationale (CEI), cette dernière développe aussi des normes relatives à des secteurs bien précis, ce qui sera présenté dans la suite de cette section.

1.3.1 Norme CEI 61508

La CEI 61508 [**38**] est une norme internationale qui a été conçue comme une norme générique contenant un ensemble d'informations et de lignes directrices visant à l'amélioration de la sécurité via l'utilisation des systèmes électriques, électroniques programmables E/E/PE que sont les SIS. Elle s'inscrit dans une approche globale de la sécurité que l'on peut comparer aux systèmes ISO 9000 et ISO 14000 qui concernent respectivement les domaines de la qualité et de l'environnement. Elle propose une démarche opérationnelle permettant de mettre en place un système E/E/PE à partir de l'étude des exigences de sécurité issues notamment d'une analyse et d'une évaluation des risques, et ce, en prenant en compte toutes les étapes de son cycle de vie. Un des objectifs visés lors de sa conception était (et est toujours) qu'elle serve de document de référence

facilitant l'élaboration de normes sectorielles qui devraient alors former un ensemble doté d'une certaine cohérence.

La CEI 61508 [**38**] est un ensemble des règles et des recommandations permettant l'amélioration de la sécurité par l'utilisation des systèmes E/E/EP. Cette norme orientée performances, propose une démarche opérationnelle permettant de mettre en place un système E/E/EP à partir de l'étude des exigences de sécurité issues notamment d'une analyse des risques. L'avantage de cette norme est qu'elle propose des moyens de justification sur l'ensemble du cycle de vie d'un produit en fonction du niveau de sécurité que l'on souhaite atteindre.

La norme CEI 61508 [**38**] se compose de sept volets comme suit :

- 61508-1 présente les définitions des prescriptions générales.
- 61508-2 traite les prescriptions spécifiques aspect matériel des systèmes E/E/EP.
- 61508-3 dédiée à la présentation des prescriptions spécifiques, aspect logiciel, des systèmes E/E/EP. Elle est développée dans la troisième partie de norme.
- 61508-4 présente les définitions et les abréviations utilisées.
- 61508-5 donne des exemples de méthode pour la détermination des niveaux d'intégrité de sécurité.
- 61508-6 fournit les guides d'application des parties 2 et 3 de la norme.
- 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

La complexité de la norme CEI 61508 a conduit ses concepteurs à développer des normes relatives à des secteurs bien précis (ex : machines, processus industriels, ferroviaire, centrales nucléaires . . .). La figure 1.2 montre la norme CEI 61508 générique ainsi que ses normes filles selon le secteur d'activité concerné. Elle influence le développement des systèmes E/E/EP et les produits concernés par la sécurité dans tous les secteurs.

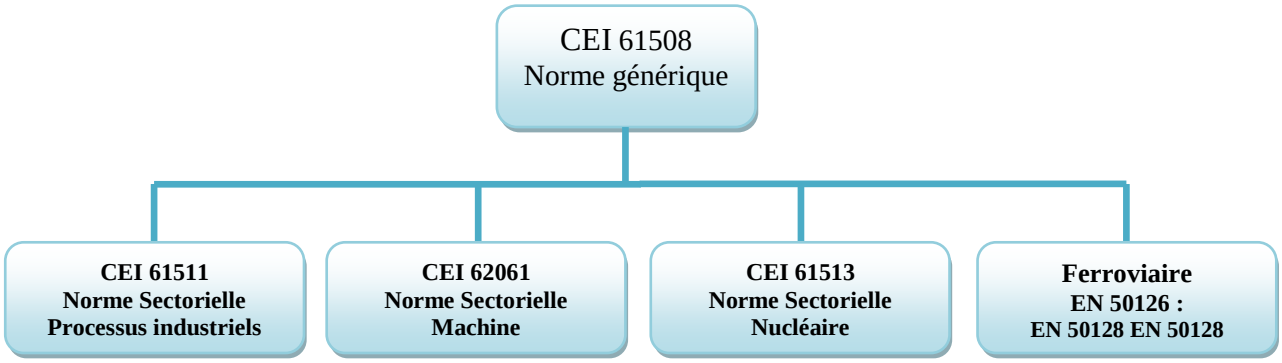


*Figure 1.2 : Les normes sectorielles de la CEI 61508. [**51**]*

1.3.2 Norme CEI 61511

La CEI 61511[**39**], s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie des procédés continus. Cette norme est composée de trois grandes parties :

- 61511-1 présente les définitions et les exigences des systèmes (matériel et logiciel).
- 61511-2 traite les lignes directrices pour l'application de la première partie de la norme.
- 61511-3 fournit des conseils pour la détermination des niveaux d'intégrité de sécurité.

La CEI 61511 [**39**] détaille les définitions et les prescriptions relatives au cycle de vie en sécurité contenant la spécification, la conception, l'exploitation et la maintenance d'un système instrumenté de sécurité, afin de maintenir le procédé dans une position de sécurité convenable.

La norme CEI 61511 est l'une des déclinaisons de la norme CEI 61508. Les SIS constituent l'objet principal de ces deux normes, mais ils y sont considérés différemment selon les métiers auxquels elles s'adressent (figure 1.3).

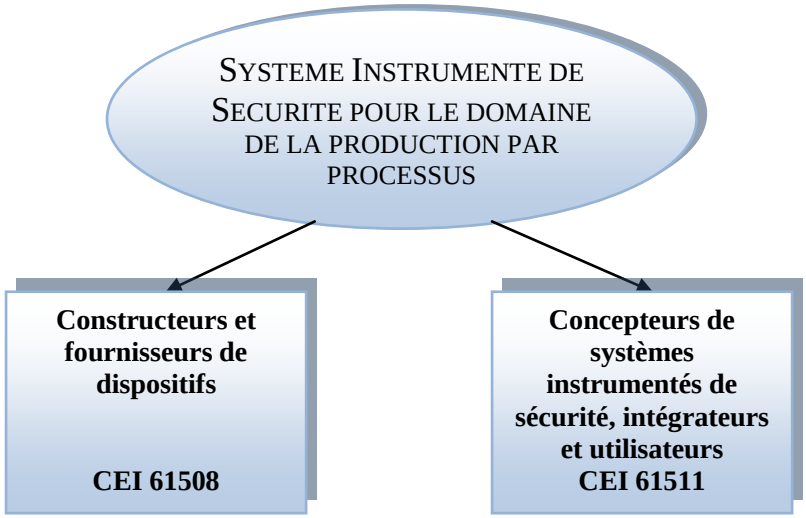


*Figure 1.3 : Relations entre la 61508 et la 61511. [**39**]*

La CEI 61508 est une norme complexe, difficile à mettre en œuvre, elle est destinée surtout aux fabricants et fournisseurs de systèmes E/E/EP, alors que la norme CEI 61511 est plus facile à utiliser, elle présente une simplification de la CEI 61508, en se limitant aux éléments nécessaires pour l'industrie de *process*. [**37**]

1.3.3 Norme CEI 62061

La CEI 62061 repose sur les mêmes concepts que ceux de la CEI 61508. Elle est destinée à être utilisée par les concepteurs de machines et les fabricants de systèmes de commande électroniques relatifs à la sécurité de machines. Elle concerne la spécification des prescriptions et fait des recommandations pour la conception, l'intégration et la validation de ces systèmes. [**51**]

1.3.4 Norme CEI 61513

La CEI 61513 [**40**] concerne le secteur de la sureté des centrales nucléaires. Elle présente les prescriptions relatives aux systèmes de contrôle commande utilisés pour accomplir les fonctions de sécurité des centrales nucléaires. La conception des systèmes de contrôle commande peuvent être réalisés à l'aide d'une combinaison de composants traditionnels câblés à des composants informatiques. La conformité à la CEI 61513 facilite la compatibilité avec les exigences de la CEI 61508 telles qu'elles ont été interprétées dans l'industrie nucléaire.

1.3.5 Norme EN 50126

La norme EN 50126 [**13**] s'intéresse essentiellement aux applications ferroviaires. Elle permet de spécifier les principaux concepts de la sureté de fonctionnement des systèmes tels que : la fiabilité, la disponibilité et la sécurité,…Cette norme est constituée de deux normes filles. L'EN 50128 [**14**] est destinée à la partie logicielle des systèmes de protection ferroviaire. L'EN 50129 [**15**] concerne les systèmes électroniques de sécurité pour la signalisation.

1.4. Définitions et concepts relatifs aux SIS

1.4.1 Définitions

La norme CEI 61508 [**38**] définit les systèmes relatifs aux applications de sécurité par : *"un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité."*

La norme CEI 61511 [**39**] définit les systèmes instrumentés de sécurité de la façon suivante : *" système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité(SIF). Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux)."*

Les systèmes suivants sont des exemples des systèmes instrumentés de sécurité :

- Système d'arrêt d'urgence (*ESD : Emergency Shutdown Systems*), utilisé, par exemple, dans les industries chimique et pétrochimique.
- Système d'arrêt automatique de train (*ATS : Automatic Train Stop*), utilisé dans le domaine ferroviaire.
- Système de freinage de l'automobile.
- Airbag.
- Système de détection de surface d'un avion.
- Equipements médicaux critiques de traitement et de surveillance.

Un SIS se compose de n'importe quelle combinaison de :

- ***Sous-système S (Sensor)* :** il est constitué d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, débit, niveau…). Si au moins un de ces paramètres dévie au-delà d'une valeur de consigne et s'y maintient, cette déviation constitue ce qui a été appelé demande ou sollicitation émanant du procédé, de l'EUC. Elle est détectée par les capteurs concernés qui envoient un signal au sous-système LS.
- ***Sous-système LS (Logic Solver)* :** ce sous-ensemble d'éléments logiques réalise le processus de prise de décision qui s'achève par l'activation du troisième sous-système FE. Le sous-système LS peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques.

- ***Sous-système FE (Final Element)* :** ces éléments agissent directement (vannes d'arrêt d'urgence) ou indirectement (vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système à l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité [**38**].

La figure 1.4 représente un exemple d'un SIS :

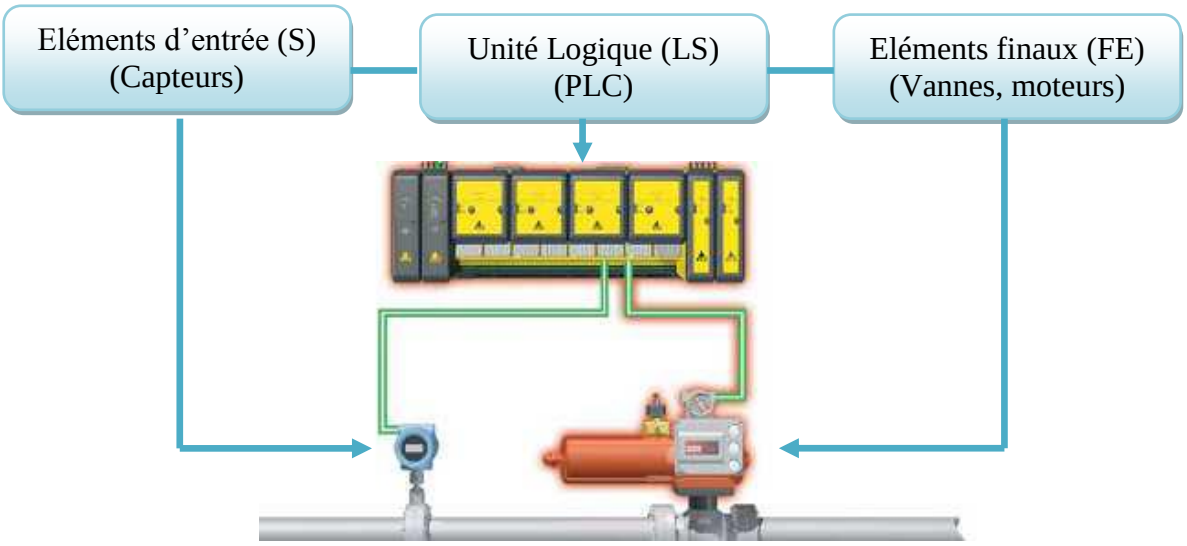


*Figure 1.4 : Un exemple de SIS. [**38**]*

Une fonction instrumentés de sécurité (SIF, *Safety Instrumented Function*) est une fonction à réaliser par un SIS prévue pour assurer ou maintenir un état de sécurité de l'équipement à protéger (EUC) par rapport à un événement dangereux spécifique.

Une fonction instrumentée de sécurité (SIF) est utilisée pour décrire les fonctions de sécurité implémentées par un système instrumenté de sécurité. Une fonction instrumentée de sécurité peut être considérée comme une barrière de protection fonctionnelle lorsque le système instrumenté de sécurité est considéré comme un système réalisant cette barrière de sécurité [**50**].

Un SIS peut implémenter une ou plusieurs SIF. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger.

L'architecture fonctionnelle d'un SIS est un ensemble de SIF qui comprend trois fonctionnalités de base, la détection (ou la mesure), le traitement (ou la décision) et l'actionnement.

1.4.2 Intégrité de sécurité d'un SIS

La référence [**38**] la définit comme suit : "*probabilité pour qu'un système relatif à la sécurité (SRS) exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et pour une période de temps spécifiée*". Elle indique également que cette définition est centrée sur la fiabilité des *SRS* dans l'exécution de leurs fonctions de sécurité.

Cette même référence, précise que l'intégrité de sécurité comprend l'intégrité de sécurité du matériel ainsi que l'intégrité de sécurité systématique. Elles sont définies ci-après.

- *Intégrité de sécurité du matériel :* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité liée aux défaillances aléatoires du matériel en mode de défaillance dangereux.
- *Intégrité de sécurité systématique :* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux, en précisant que l'intégrité systématique ne peut normalement, ou précisément, être quantifiée, mais simplement considérée d'un point de vue qualitatif.

Les deux types de défaillances, aléatoires du matériel et systématiques, définis par la norme CEI 61508 seront explicités au début du prochain chapitre.

Les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux *SIS* sont spécifiées en termes de niveau d'intégrité de sécurité (*SIL*) : niveau discret parmi quatre possibles, le *SIL* 4 possède le plus haut degré d'intégrité de sécurité. Sa détermination dépend du mode de fonctionnement du *SIS*. Ce point est évoqué dans ce qui suit.

1.4.3 Modes de fonctionnement des SIS et paramètres cibles de défaillances

- **Fonctionnement en faible demande,** Un SIS est en mode de fonctionnement à faible demande lorsque la fréquence de sollicitation est inférieure à une fois par an (1*/an*) ou inférieure au double de la fréquence des tests périodiques auxquels il est soumis. [**38**]

Probabilité moyenne de défaillance à la demande, notée *PFDavg* (*Average Probability of Failure on Demand*). Elle n'est pas définie dans le volume 4 de la norme CEI 61508, malgré son utilisation dans plusieurs définitions et abréviations. Cette probabilité représente tout simplement l'indisponibilité moyenne d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité. [**16**]

- **Fonctionnement en forte demande ou demande continue,** Un SIS en mode de fonctionnement continu ou à forte demande implique une forte sollicitation du SIS. Il est considéré lorsque la fréquence de sollicitation est élevée ou continue, c'est-à-dire qu'elle est supérieure à une fois par an (1*/an*) ou supérieure à deux fois la fréquence des tests périodiques.[**47**]

  Probabilité de défaillance dangereuse par heure, notée *PFH (Probability of a dangerous Failure per Hour),* est parfois appelée " fréquence des défaillances dangereuses ", ou " taux de défaillances dangereuses ", ou " nombre de défaillances dangereuses par heure ". La probabilité de défaillance par heure n'est pas aussi citée dans la partie 4 de la norme CEI 61508-4 destinée aux définitions. Elle est indiquée dans le tableau 1.1 pour le mode de fonctionnement continu ou à demande élevée. **[51**]

- **Notion de niveau d'intégrité de sécurité (SIL)**

Les normes de sécurité fonctionnelle CEI 61508 et CEI 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque. Plus le SIL a une valeur élevée plus la réduction du risque est importante.

Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle de un à quatre niveaux (Tableau 1.1). Les SILs sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme CEI 61508. Le SIL "4" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "1" désigne l'exigence la plus faible.

Niveau d'intégrité de sécurité (SIL)	Mode de fonctionnement à faible sollicitation (PFD_{moy})	Mode de fonctionnement continu ou à forte sollicitation (PFH)
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$

*Tableau 1.1 Les différents niveaux de SIL définis par la norme CEI 61508. [**38**]*

L'utilisation des niveaux SIL permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel, menant aux événements dangereux identifiés pendant l'analyse de risque. Les SILs sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances.

La norme CEI 61508 détaille les prescriptions nécessaires pour répondre aux exigences de chaque niveau d'intégrité de sécurité. Ces prescriptions deviennent plus rigoureuses à mesure que le niveau de SIL s'élève en vue d'obtenir la probabilité d'une défaillance dangereuse de plus en plus faible.

1.5. Conclusion

Au cours du premier chapitre nous avons d'abord rappelé les définitions des termes fondamentaux du domaine de la sécurité afin de lever, si possible, toute ambiguïté quant à la signification que nous leur accordons dans la suite de ce mémoire. Nous avons ensuite présenté l'ensemble des normes qui discutent les systèmes instrumentés de sécurité (norme CEI 61508 et ses normes sectorielles). Il convient à cet effet de rappeler que la CEI 61508 de même que ses normes filles sont actuellement devenues la référence par excellence pour la mise en œuvre de ce type de systèmes. Puis nous avons donné une synthèse sur les concepts et définitions relatifs aux SIS.

Ceci, est considéré comme une initiation pour passer vers un encadrement sur les concepts des activations intempestives des SIS qu'on va essayer de les entourer suite à une recherche exhaustive qui va être résumée au cours du prochain chapitre.

Chapitre 2

Activation Intempestives des Systèmes Instrumentés de Sécurité

2.1. Introduction

L'objectif premier assigné à un système instrumenté de sécurité (SIS) est la détection des situations dangereuses (augmentation de température ou de pression, fuite de gaz…) pouvant mener à un accident (incendie, explosion, rejet d'un produit dangereux…) et de mettre ensuite en œuvre un ensemble de réactions (fonctions de sécurité) nécessaires pour atteindre un état de sécurité.

L'activation des SIS dans les processus industriels est effectuée donc après l'occurrence des déviations spécifiques (situation dangereuse) par rapport au fonctionnement normal (situation normale), mais dans certains cas les SIS sont activés en absence des déviations ou de demandes : il s'agit des activations intempestives qui représentent le noyau de ce chapitre.

Au début de ce deuxième chapitre, nous exposons la typologie des défaillances liée aux systèmes instrumentés de sécurité selon deux approches différentes. Ceci permet de bien apprécier la nature des activations (défaillances) intempestives puis nous présentons les concepts de base relatifs aux activations intempestives des SIS (définitions, classification,…), précisons et discutons ses causes, et présentons un ensemble de formulations analytiques, qui concernent l'estimation du taux de déclenchement intempestif (STR) selon ce qui est retrouvé dans la littérature.

2.2. Classification des défaillances des SIS

2.2.1 Classification retenue dans la norme CEI 61508

- ***Classification des défaillances selon leurs causes***

La norme CEI 61508 [**38**] adopte une classification qui contient deux catégories de défaillances : les défaillances physiques (aléatoires du matériel) et les défaillances fonctionnelles (systématiques).

La définition des défaillances aléatoires du matériel donnée par cette norme est la suivante : *«défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradations au sein du matériel»*. Une telle défaillance rend donc le système incapable de remplir sa fonction suite à sa dégradation physique. Il est important de noter que la dégradation physique du système à deux causes principales :

- *Vieillissement du matériel*. Les défaillances dues au vieillissement sont appelées *défaillances naturelles ou primaires*.
- *Exposition aux contraintes excessives* : ces contraintes peuvent être induites par des facteurs externes ou par des erreurs humaines. Ces défaillances sont appelées *défaillances secondaires*.

Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives à cette catégorie de défaillances sont, dans la plupart du temps, disponibles.

La défaillance systématique est définie par la même norme comme étant *« défaillance reliée 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»*. Lors de l'occurrence d'une telle défaillance, le système ne remplit plus la fonction qui lui est demandée, mais il ne présente aucune dégradation physique. C'est la raison pour laquelle ces défaillances sont qualifiées de non physiques ou de fonctionnelles (par exemple : l'opérateur ferme une vanne par erreur, la vanne dans ce cas n'est pas dégradée physiquement). Les défaillances systématiques peuvent être divisées en deux catégories :

- *Défaillances de conception* : ces défaillances sont introduites lors de l'une des phases du cycle de vie du système. Elles existent à l'état latent, se révèlent lors du fonctionnement du système et ne peuvent généralement être éliminées que par une modification de la conception ou du processus de fabrication. Des exemples typiques de ces défaillances sont les défauts de conception du logiciel et du matériel.

- *Défaillances d'interactions* : ces défaillances sont initiées par les erreurs humaines lors de l'exploitation, la maintenance,…

La norme CEI 61508 [**38**] considère que les défaillances du logiciel sont toutes systématiques. Par opposition aux défaillances aléatoires du matériel, les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles.

Cette classification de défaillances est résumée à la figure 2.1 :

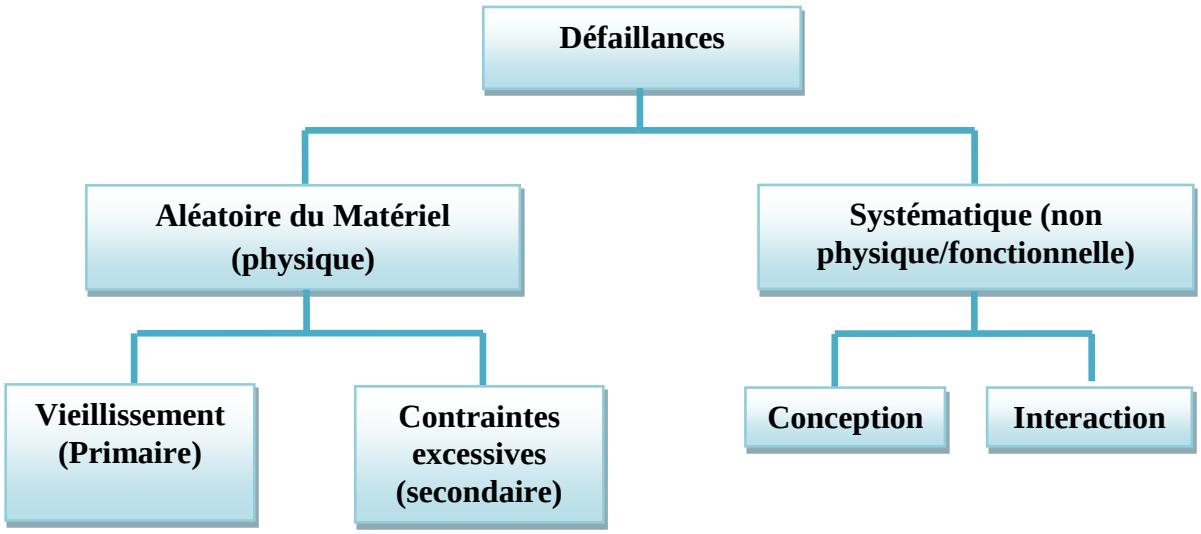


*Figure 2.1: Classification des défaillances selon leurs causes. [**47**]*

➢ ***Classification des défaillances selon leurs effets sur la fonction de sécurité***

Toutes les défaillances (aléatoires du matériel et systématiques), selon leurs effets, peuvent être classées dans l'une des deux catégories suivantes : *défaillances en sécurité* (*safe failures*) ou *défaillances dangereuses* (*dangerous failures*).

Suivant cette dernière classification, seules les défaillances aléatoires du matériel sont prises en compte dans ce qui suit. Dans ces conditions, les définitions de ces deux catégories selon la norme CEI 61508 [**38**] sont données ci-après :

- *Défaillance dangereuse* : «*défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction* ».
- *Défaillance en sécurité* : *« défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction»*.

En nous situant donc dans le contexte de la CEI 61508, une défaillance dangereuse est une défaillance qui tend à inhiber la fonction de sécurité en cas de demande émanant de l'*EUC* qui sera alors dans un état dangereux. Une défaillance sûre est une défaillance qui tend à anticiper le déclenchement de la fonction de sécurité, en l'absence de toute demande, en conduisant effectivement l'EUC dans un état sûr. C'est-à-dire tel que l'occurrence de tout événement dommageable n'y est plus possible.

Compte tenu de cette décomposition, le taux de défaillance aléatoire du matériel de chaque canal (λ) comporte deux composantes :

$$\lambda = \lambda_S + \lambda_D \qquad (2.1)$$

Avec :

λ_S : taux de défaillance aléatoire en sécurité du matériel,

λ_D: taux de défaillance aléatoire dangereuse du matériel.

Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne (tests de diagnostic). Les premières sont dénommées défaillances détectées (*detected failures*) et les secondes, qui ne peuvent être révélées que lors des tests périodiques hors ligne ou lors de la sollicitation du *SIS* par le système surveillé, sont dénommées défaillances non détectées (*undetected failures*). Le schéma suivant est classiquement présenté pour résumer cette double partition [**16**].

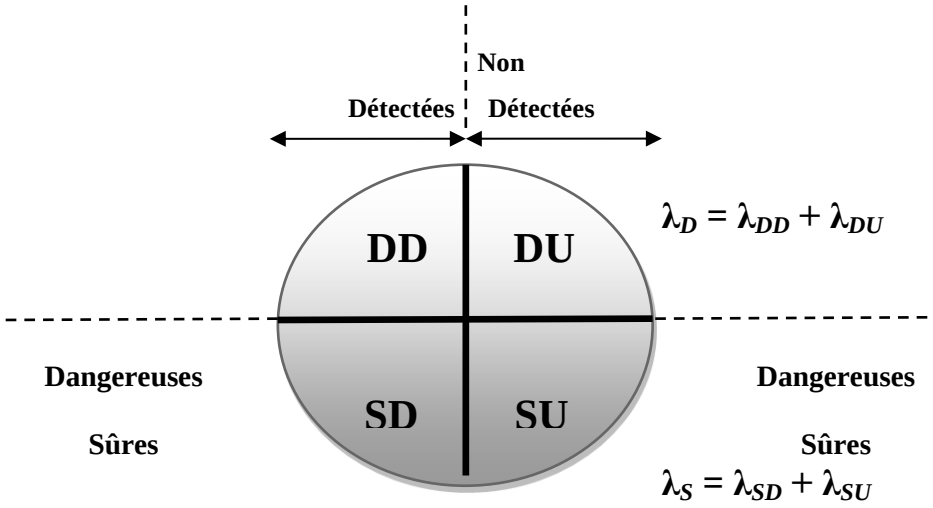


*Figure 2.2 : Typologie des défaillances selon la norme CEI 61508. [**16**]*

2.2.2 Classification proposée par SINTEF

Cet organisme propose, dans son manuel [**48**], une classification plus fine et plus réaliste que la précédente, puisqu'elle prend en compte les défaillances intempestives et les défaillances non-critiques qui sont définies ci-après. Cette classification est résumée par l'arborescence suivante :

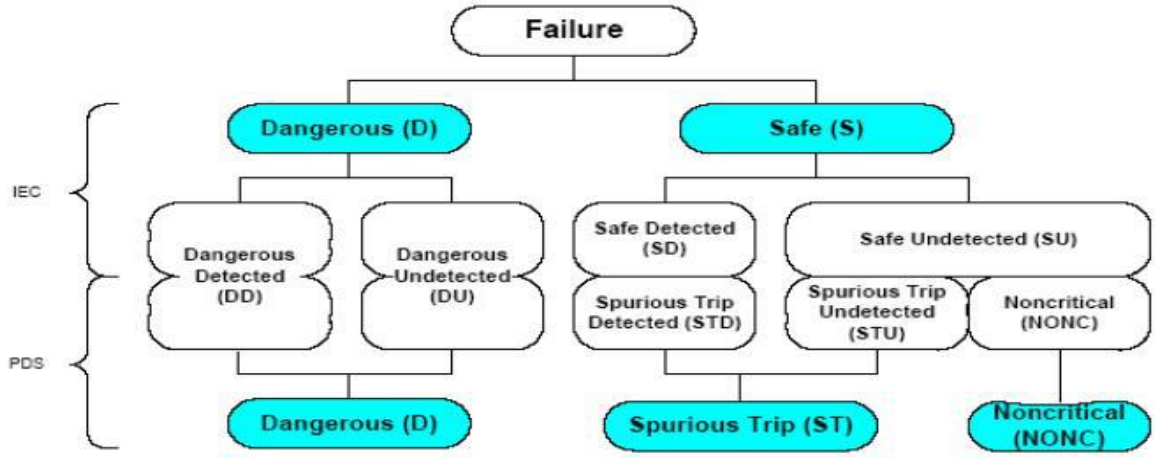


*Figure 2.3 : Classification des défaillances selon SINTEF. [**48**]*

Pour résumer, la méthode PDS de SINTEF considère, au niveau des composants, trois types de défaillances : dangereuses, intempestives et non-critiques.

- Les défaillances dangereuses sont celles de la norme et se divisent donc en défaillances détectées (λ_{DD}) et non-détectées (λ_{DU}).
- Les défaillances intempestives sont un sous-ensemble des défaillances sûres et se divisent également en défaillances détectées (λ_{STD}) et non-détectées (λ_{STU}).
- Les défaillances non-critiques (λ_{NONC}) sont celles qui n'ont aucune incidence sur les deux fonctions principales du système EUC, c'est-à-dire son aptitude à produire (disponibilité de production) et son aptitude à ne pas engendrer d'événements redoutés (sécurité).

A partir de cette classification, il a été déduit une classification des taux de défaillance résumée ci-dessous [**16**] :

- λ_{DD} et λ_{DU} sont ceux définis dans la norme.
- λ_{STD} est le taux de défaillance intempestive détectée. Il correspond au λ_{SD} de la norme.
- La somme ($\lambda_{STD} + \lambda_{NONC}$) correspond au λ_{SU} de la norme.
- La somme ($\lambda_{D} + \lambda_{STD} + \lambda_{STU}$) est appelée $\lambda crit$.

Commentaire : Les défaillances intempestives ne sont même pas citées dans la classification retenue dans la norme CEI 61508, alors que la classification SINTEF considère ces défaillances comme une sous-classe des défaillances sûres. Les exemples, souvent évoqués, du déclenchement intempestif d'un airbag ou de l'inversion intempestive du flux de poussée d'un réacteur en plein vol suffisent à montrer que cette classification est pour le moins réductrice [**16**].

2.3. Définitions et classification des activations intempestives des SIS

2.3.1 Définitions

La première étude *monothématique* qui traite le sujet des défaillances intempestives des SIS est celle présentée par M.A. Lundteigen et M. Rausand [**30**]. Dans cet article, les auteurs utilisent le terme collectif : activation intempestive (*spurious activation*). Dans ce qui suit de ce mémoire, nous utilisons le même terme comme générique. Le terme '**activation'** indique qu'il y a une certaine transition d'un état vers un autre et le terme '**intempestive'** indique que les causes du déclenchement sont fausses, incorrects et non-réels [**30**]. Dans un processus industriel, les activations intempestives des SIS peuvent provoquer des arrêts partiels ou complets des installations, donc il est nécessaire de réduire son nombre d'apparition pour :

(1) éviter les pertes de production suite aux arrêts,

(2) éviter les risques qui peuvent apparaitre durant la phase de redémarrage.

2.3.2 Classification des activations intempestives

Selon la référence [**30**], il existe trois différents types des activations intempestives des systèmes instrumentés de sécurité qui sont :

- **L'opération intempestive (*Spurious operation*) :** une opération intempestive SO est une activation d'un élément du SIS individuellement en absence d'un processus spécifié la demande d'activation (des déviations réelles).

Exemples :

(1) Un faux signal sur un niveau élevé émet par un détecteur du niveau dû à une défaillance interne du détecteur.

(2) Une alarme est émet à partir d'un transmetteur de niveau sans que le niveau de liquide ait dépassé la limite supérieure, en raison de l'échec à distinguer la mousse par rapport au niveau réel du liquide dans un séparateur.

- **Le déclenchement intempestif (*Spurious trip*) :** un déclenchement intempestif est une activation d'un ou plus d'éléments du SIS sachant que la fonction instrumenté de sécurité (SIF) est effectuée en absence d'un processus spécifié la demande d'activation (des déviations réelles)

Exemples :

(1) deux détecteurs de flamme dans une configuration 2oo3 (le système fonctionne si au moins 2 composants fonctionnent parmi les 3) donnent un faux signal sur le feu ce qui provoque le déclenchement des éléments finaux et l'activation de la fonction instrumenté de sécurité (SIF).

(2) La fermeture d'une vanne d'arrêt d'urgence (ESV) dans une configuration 1oo2 (le système fonctionne si au moins 1 composant fonctionne parmi les 2) des éléments finaux suite à une défaillance interne.

- **L'arrêt intempestif (*Spurious shutdown*) :** un arrêt intempestif est un arrêt partiel ou complet des systèmes en absence d'un processus spécifié la demande d'activation (des déviations réelles).

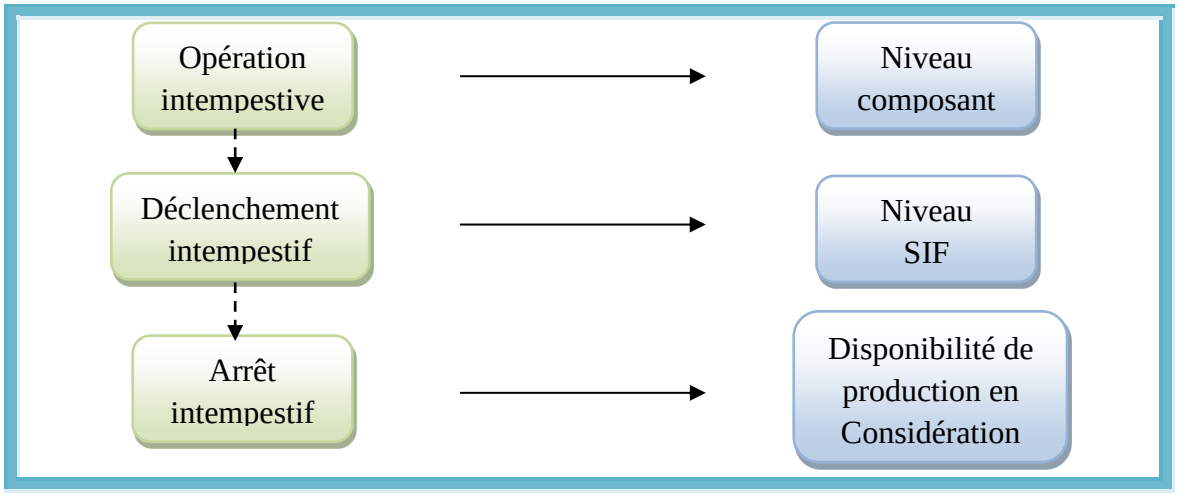


Figure 2.4 : les différents types des activations intempestives.

Selon les définitions précédentes, les différents types des activations intempestives se réalisent *'en absence d'un processus spécifié la demande d'activation '* ce qui nous permet de penser que ces activations des SIS ne concernent que le mode de fonctionnement faible demande. Cette restriction n'a pas de justification, si ce n'est le fait que le domaine de la demande continue, et la *PFH* qui lui est associée, ont été moins largement étudiés que celui de la faible demande et de son indicateur caractéristique, la PFD_{moy}. [**16**]

La définition suivante est plus étendue que les précédentes : «*Une défaillance intempestive ne peut se définir que par rapport à une fonction de sécurité spécifiée. Elle a pour résultat, soit de déclencher la réalisation de cette fonction de sécurité en l'absence de toute demande, soit d'annihiler l'effet protecteur de cette fonction après son déclenchement réussi*». [**16**] On remarque que le premier volet de cette définition concerne le mode de fonctionnement faible demande des SIS qui assurent la fonction de sécurité, et que le second concerne le mode de fonctionnement continu.

Autre point à souligner : l'activation intempestive des SIS peut être considérée comme sûre (peut être temporairement), tandis qu'elle est dangereuse. Autrement dit, cela nous conduit à nouveau à affirmer que *les activations intempestives ne constituent pas un sous-ensemble des défaillances sûres, ni d'ailleurs des défaillances dangereuses.* [**16**]

2.4. Causes des activations intempestives

Des relations de causalité peuvent liées les différents types des activations intempestives des systèmes instrumentés de sécurité tel que :

- Une opération intempestive peut être l'une des nombreuses causes d'un déclenchement intempestif.
- Un déclenchement intempestif peut-être l'une des causes d'un arrêt intempestif. Ces relations sont illustrées dans la Figure 2.5 par des flèches en pointillés.

La figure 2.5 illustre les causes principales des activations intempestives représentées dans un diagramme de fluence (*influence diagram*).

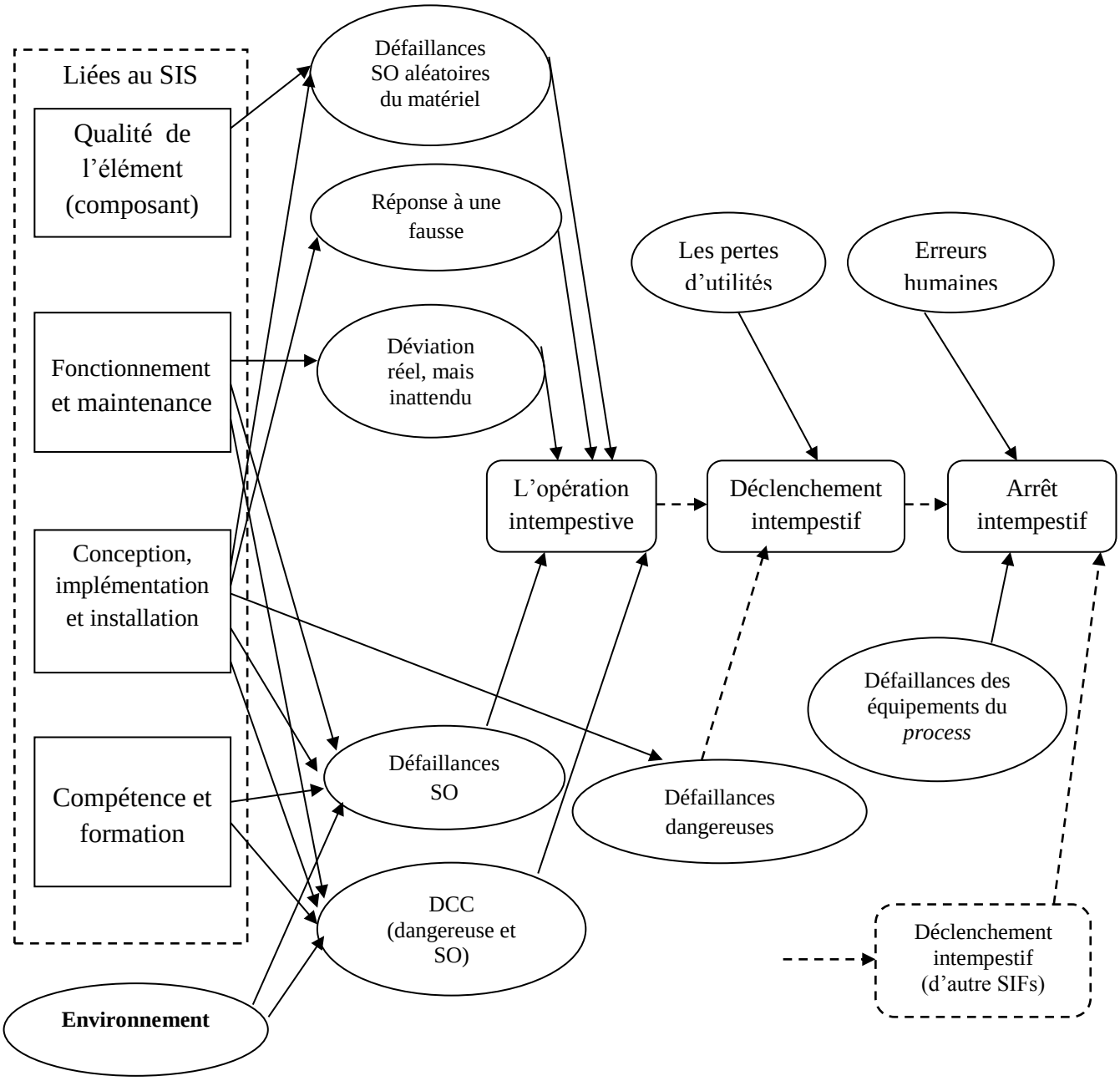


*Figure 2.5 : les décisions et les facteurs influençant les activations intempestives. [**30**]*

Discussion :

L'opération intempestive SO, le déclenchement intempestif, et l'arrêt intempestif sont présentés comme nœuds de performance (rectangles arrondis), puisque leurs taux d'occurrence sont des mesures de performance qui nous voulons de les minimiser afin de réduire les pertes de production. [**31**]

Les nœuds de chance (cercles) représentent les facteurs qui influencent les taux des activations intempestives. Nous ne sommes pas en mesure de contrôler ces facteurs directement, mais nous pouvons les influencer indirectement par un ensemble de décisions.

Une décision peut être de choisir un élément avec une fiabilité supérieure à celle spécifiée. Autre décision peut être d'investir davantage dans la formation et la compétence du personnel, afin de réduire les erreurs humaines en cours de fonctionnement et d'entretien. Les décisions pertinentes sont illustrées dans la figure comme des nœuds de décision (rectangles). Les flèches indiquent les relations entre les décisions, les facteurs influençant, et les mesures de performance. Les flèches en pointillés sur la figure 2.5 indiquent que la liaison est présente, sous certaines conditions, par exemple, pour une configuration matérielle donnée. Plus de détaille dans ce qui suit.

2.4.1 Causes des opérations intempestives

Pour les opérations intempestives SO, on trouve deux causes principales d'activation des éléments du SIS tel que :

(1) Une défaillance interne de l'élément (ou son support) conduit à une Opération Intempestive.

(2) L'élément d'entrée répond à une fausse déviation.

Les défaillances SO* dues à des défaillances internes sont souvent considérées comme *défaillances en sécurité* car ils ne gênent pas le SIS á l'exécution en demande. Cependant, toutes les défaillances en sécurité ne conduit pas forcément à des défaillances SO, et il est donc nécessaire d'étudier les modes de défaillance en sécurité pour chaque élément pour déterminer quelles ceux qui sont pertinents pour les défaillances SO.

Les défaillances SO (figure 2.5) sont distinguées en :

- Défaillances SO aléatoires du matériel dus principalement aux dégradations normales des éléments du SIS et,
- Des défaillances SO systématique dus aux erreurs de conception, l'insuffisance des procédures,…

La qualité des éléments du SIS influence sur le taux des défaillances SO aléatoires du matériel (illustré par une flèche en figure 2.5). Une matière bien définie peut, par exemple, supporter des hautes températures et des pressions élevées plus qu'une autre matière. Ou bien un principe de détection utilisé pour un capteur de niveau peut être plus vulnérable à une

* Représente les défaillances liées aux opérations intempestives.

condition de fonctionnement spécifique qu'un autre. Les procédures d'exploitation et d'entretien, les outils, et les méthodes de travail, la conception, l'implémentation et l'installation des procédures, les compétences et la formation, ainsi que l'exposition á l'environnement peuvent influer sur la probabilité de défaillances systématiques (figure 2.5). La vérification, la validation et les tests peuvent réduire le taux d'apparition des défaillances systématiques. Des moyens de vérification (par exemple, des essais ou des révisions) pour vérifier et confirmer que la conception mis en œuvre est conforme aux spécifications, bien que des moyens de validation pour évaluer également la pertinence du modèle choisi. Dans la phase d'exploitation, le taux des défaillances systématiques peut être réduit par la vérification et la validation des tests par exemple, des procédures d'inspection visuelles,… La compétence et la formation sont aussi importantes pour réduire les erreurs humaines lors des fonctions de tests.

Les conditions environnementales influencent sur l'apparition des défaillances systématiques si ces conditions ne conforme pas aux conditions de conception. Cependant, dans la plupart des cas, il n'est pas possible d'influer sur les conditions environnementales. La contribution de l'environnement est donc illustrée par un nœud de chance dans la figure 2.5.

Les défaillances de causes communes (DCC) peuvent être aussi l'une des causes des opérations intempestives (figure 2.5). Non seulement les DCC dangereuses qui conduit á des opérations intempestives, mais il est également nécessaire de tenir compte les défaillances SO de causes communes DCC-SO. Ces derniers n'ont pas les mêmes causes que les DCC dangereuses. La norme CEI 61508 [**38**] recommande que les DCC dangereuses soient modélisés par un modèle de facteur beta β, et la partie 6 de la norme inclut une procédure pour estimer une valeur spécifique du paramètre β pour les DCC dangereuses. Comme ces derniers ont une nature différente des DCC-SO intempestives, la procédure présentée dans la partie 6 de la norme CEI 61508 n'est pas adapté pour estimer le paramètre β^{SO} pour les DCC-SO intempestives.

Les fausses déviations sont des causes importantes qui conduisent aux opérations intempestives des éléments du SIS. Une fausse déviation partage souvent certaines caractéristiques (par exemple, l'aspect visuel et composition) avec une déviation réelle, alors il peut être difficile pour l'élément d'entrée du SIS de distinguer les deux. Un rayon de la lumière du soleil peut être, par exemple, vue comme une petite flamme sur certains angles, et un détecteur de flamme peut donc le lire comme une flamme.

Il n'est pas possible de réduire l'apparition des fausses déviations, mais nous pouvons influencer la façon de réponse de l'élément d'entrée du SIS. On ne peut pas, par exemple, de supprimer la lumière du soleil ou de modifier la densité de la mousse, mais nous pouvons sélectionner les éléments qui visent à mieux distinguer entre faux et vrai exigences du processus, ou nous pouvons déplacer les éléments pour les rendre moins vulnérables aux fausses déviations.

Quelques fausses déviations sont provoquées par l'homme, ce qui signifie que nous sommes en mesure d'influencer la façon dont ils se produisent souvent en améliorant les procédures d'exploitation et de maintenance et les processus des travaux.

Si nous voulons, par exemple, éviter la réponse du détecteur de flamme á la soudure, nous devons assurer que le détecteur ne voit pas ces flammes par des couverts ou d'autres barrières. Ceci est illustré par une flèche de « fonctionnement et maintenance » au nœud de chance « Déviation réel, mais inattendu » sur la figure 2.5.

2.4.2 Causes des déclenchements intempestifs

L'un des principaux contributeurs aux déclenchements intempestifs est évidemment les opérations intempestives SO des éléments du SIS. SO peut conduire à un déclenchement intempestif si le nombre d'éléments activés correspond au nombre d'éléments nécessaires à l'exécution de la fonction de sécurité. La configuration matérielle choisie détermine donc si les opérations intempestives SO peuvent conduire à un déclenchement intempestif ou non. Cette «condition » est illustrée par des flèches en pointillés sur la figure 2.5.

Il existe plusieurs d'autres causes des déclenchements intempestifs, par exemple:

- Les pertes d'utilités ; comme pneumatique, hydraulique ou l'alimentation électrique : ces pertes d'utilités peuvent directement conduire á des déclenchements intempestifs.

- Défaillances dangereuses détectées (DD) : Dans certains cas, les systèmes instrumentés de sécurité peuvent intempestivement réaliser la fonction de sécurité (SIF) attendue même en présence des défaillances dangereuses détectées (DD) qui arrêtent la réalisation du SIF en présence de demande. Dans une configuration 2oo3, la fonction de sécurité peut réaliser en présence d'une seule défaillance DD, mais ce n'est pas le cas en présence de deux défaillances DD.

2.4.3 Causes des arrêts intempestifs

Un déclenchement intempestif peut généralement, mais pas toujours, conduire à un arrêt intempestif du processus. Si la fonction instrumentée de sécurité (SIF) du SIS n'a pas un effet direct sur le processus (par exemple, activer d'autres SIFs), le processus peut être en dépit de l'arrêt suite au déclenchement intempestif. Une flèche en pointillé est donc utilisé pour indiquer qu'un déclenchement intempestif peut (mais pas toujours) conduire à un faux arrêt. La figure 2.5 indique également (par des flèches en pointillés et nœud) que les différents types de SIFs peuvent conduire à des arrêts intempestifs.

Un arrêt intempestif peut aussi être causé par des défaillances (arrêts) des équipements du processus (équipements ne sont pas des éléments du SIS) comme des vannes de commande ou des pompes…. Une fermeture intempestive d'une vanne de régulation ou un arrêt intempestif d'une pompe peut être dû aux défaillances internes d'éléments, d'erreurs humaines ou les erreurs du système de contrôle automatique. Dans la figure 2.5, les défaillances des équipements du processus (non SIS) et les défaillances du système de contrôle automatique sont illustrées par un nœud de chance « défaillances des équipements de processus », et les erreurs humaines en tant que nœud de chance "erreurs humaines".

2.5. Taux de déclenchements intempestifs (STR)

2.5.1 Définition du taux de déclenchement intempestif

Le taux de déclenchements intempestifs STR est défini comme le nombre moyen des activations intempestives de la fonction instrumentée de sécurité (SIF) par une unité de temps. [**43**]

2.5.2 Formules analytiques relatives aux STR

La littérature offre pas mal de travaux qui présentent des formules analytiques relatives au taux de déclenchements intempestifs STR ; Avant de les présenter, Nous allons, dans ce qui suit, donner une description de quelques architecture typique à la configuration des SIS de type *K*oo*N* (le système fonctionne si au moins K composants fonctionnent parmi les N) regroupées dans le tableau suivant (2.1).

Architecture (*KooN*)	**Description**
1oo1	Une architecture de base, 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 opération intempestive conduit à l'exécution de cette fonction en absence de demande.
1oo2	Cette architecture se compose de deux canaux identiques fonctionnant en redondance : 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, l'opération intempestive de l'un ou l'autre des deux canaux conduit à l'activation de la fonction de sécurité. Toutes les architectures de type 1*ooN* ont le même principe de fonctionnement.
1oo3	Cette architecture est composée de trois canaux connectés en parallèle, fonctionnant en redondance active. C'est-à-dire que ce système restera opérationnel, vis-à-vis des défaillances dangereuses, tant qu'au moins un de ces canaux le sera. Cela dit, une opération intempestive de l'un des trois canaux provoque l'activation de la fonction de sécurité.
2oo2	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 une opération intempestive.
2oo3	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 [**32**]. 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.

*Tableau 2.1 : description de quelques architectures K*oo*N usuelles.*

D'une manière générale, pour une architecture *KooN*, (***N – K+1)*** représente le nombre de défaillances dangereuses dont l'occurrence induit la perte de la fonction de sécurité et ***K*** représente le nombre des opérations intempestives dont l'occurrence conduit à l'activation intempestive de cette même fonction.

Le taux de déclenchements intempestifs (STR) d'une fonction de sécurité bien définie, assurée par un SIS donné, est déterminé par le calcul et la combinaison du STR de ses trois sous-systèmes (*S*, *LS* et *FE*). Cela peut être exprimé par la formule générale suivante :

$$STR_{moy}^{SIS} = STR_{moy}^{S} + STR_{moy}^{LS} + STR_{moy}^{FE} \quad (2.2)$$

Bien évidemment, chacun de ces trois sous-systèmes est représenté par une architecture *KooN*. Voyons à présent les différentes formules mathématiques du STR retrouvées dans la littérature pour les architectures de type *KooN*.

Travaux de M. A Lundteigen, et M.Rausand

Les formules proposées par ces auteurs [**30**] sont basées sur un modèle binomial. Ces formules sont liées directement aux causes principales du déclenchement intempestif des SIS (rappelons qu'il y a trois causes principales : l'opération intempestive, les défaillances dangereuses détectées et les pertes d'utilités).

- **Opération intempestive ;** comme on a déjà vu (Paragraphe 2.3.2), les opérations intempestives dus essentiellement à des défaillances internes d'un ou plusieurs éléments du SIS (dépond de sa configuration), ou à une fausse déviation.

Défaillances internes ; soit $\lambda_{SO\,j}$ le taux de l'opération intempestive (SO) d'un élément du SIS de type *j*. Pour une architecture *1ooN* (i.e. Système parallèle) de N *éléments indépendants* identiques de type *j*, supposons que cette configuration fait partie d'un SIS (par exemple éléments d'entrées ou finaux) et n'importe quelle défaillance de type 'opération intempestive SO' provoque un déclenchement intempestif. Le STR due à des défaillances internes de cette architecture est donné par :

$$STR_{1J} = N\,\lambda_{SO\,j}. \quad (2.3)$$

Si les éléments sont exposés à des défaillances de causes communes (DCC) modélisées par le modèle de facteur-beta avec un taux $\beta_j^{SO}\,\lambda_{SOj}$ (β_j^{SO} est un nouveau facteur proposé par les auteurs pour les DCC intempestives de l'élément du SIS de type *j*), le STR de l'architecture 1ooN devient :

$$STR_{1J} = N\,(1-\beta_j^{SO})\,\lambda_{SOj} + \beta_j^{SO}\,\lambda_{SOj}$$

$$= N\,\lambda_{SOj} - (N-1)\,\beta_j^{SO}\,\lambda_{SOj} \quad (2.4)$$

Pour une architecture *KooN* ($N \geq K \geq 2$),

$$STR_{1J}\,(KooN) \approx N\,(1-\beta_j^{SO})\,\lambda_{SOj}\left[\sum_{m=K-1}^{N-1}\binom{N-1}{m}p^m(1-p)^{N-1-m}\right]+\beta_j^{SO}\,\lambda_{SOj} \quad (2.5)$$

Avec ; $p = N\,(1-\beta_j^{SO})\,\lambda_{SOj}MDT_j$; MDT est le temps moyen d'indisponibilité.

Fausse déviation ; le STR d'un SIS causé par des déviations fausse est donné par

$$STR_{2J} = (\lambda_F + \lambda_{SF})\,(1-PFD) \quad (2.6)$$

Avec ; λ_F est le taux d'une déviation non réelle, mais elle a quelques caractéristiques et propriétés similaire à une déviation réelle.

λ_{SF} est le taux d'une déviation réelle, mais la réponse à cette déviation est empêché comme par exemple une soudure n'est pas détectée par un détecteur de flamme.

- **Défaillances dangereuses détectées (DD) ;** le STR de l'architecture *KooN* de éléments de SIS de type *j* due à des défaillances dangereuses détectées est donné par :

$$STR_{3J}\,(KooN) \approx N\,(1-\beta_j^{DD})\lambda_{DDj}\left[\sum_{m=N-K}^{N-1}\binom{N-1}{m}(p')^m(1-p')^{N-1-m}\right]+\beta_j^{DD}\,\lambda_{DDj} \quad (2.7)$$

Avec ; λ_{DDj} est le taux de défaillances dangereuses détectées. Ces dernières peuvent être indépendantes ou de causes communes (DCC), donc on doit utiliser le modèle de facteur-beta pour les DCC avec un taux de $\beta j^{DD}\,\lambda_{DDj}$

$p' = (1-\beta_j^{DD})\,\lambda_{DDj}\,MDT_j'$. MDT_j' est le temps moyen d'indisponibilité suite aux actions de réparation après l'occurrence des défaillances dangereuses détectées.

- **Pertes d'utilités ;** les pertes des utilités peuvent directement conduit à un déclenchement intempestif avec le taux suivant ;

$$STR_{4J} = \lambda_{ULj} \quad (2.8)$$

Avec ; λ_{ULj} est le taux des pertes d'utilités associé aux éléments de type *j* du SIS.

Remarque : STR total, STR_T est obtenu par la somme des taux cités dans cette partie (2.5, 2.6, 2.7 et 2.8) selon ses contributions dans les cas étudiés.

Approche ISA

La partie 2 du rapport technique ISA-TR 84.00.02 [**20**] regroupe les formules analytiques du *STR* de plusieurs architectures du type *K*oo*N* (*1oo1*, *1oo2*, 1oo3, *2oo2*, *2oo3* et *2oo4*). Ces formules incluent la contribution des défaillances systématiques. Nous n'incluons pas, dans ce qui suit et pour des raisons d'homogénéité, ces contributions dans les expressions *STR* (*K*oo*N*)

données par l'ISA, d'autant plus, que dans les autres approches présentées dans ce mémoire, les défaillances systématiques sont considérées comme négligeables. L'ensemble des formules du STR proposées par ISA sont regroupées dans le tableau 2.2.

Architectures	***STR***
1*oo*1	$\lambda_S + \lambda_{DD}$
1*oo*2	$2\cdot[\lambda_S + \lambda_{DD}] + \beta\ (\lambda_S + \lambda_{DD})$
1*oo*3	$3\cdot[\lambda_S + \lambda_{DD}] + \beta\ (\lambda_S + \lambda_{DD})$
2*oo*2	$2\cdot\lambda_S\ [\lambda_S + \lambda_{DD}]\cdot MTTR + \beta\ (\lambda_S + \lambda_{DD})$
2*oo*3	$6\cdot\lambda_S\ [\lambda_S + \lambda_{DD}]\cdot MTTR + \beta\ (\lambda_S + \lambda_{DD})$

Tableau 2.2 : Formules relatives aux STR des architectures KooN selon ISA.

- Les défaillances sûres, quelles qu'elles soient, sont supposées détectées en ligne !
- Les défaillances dangereuses détectées sont intégrées aux calculs de déclenchement intempestif quand elles amènent le canal concerné d'un système redondant ou le système lui-même, quand il n'est pas redondant, dans un état sûr (*safe state*). Si ce n'est pas le cas, ces défaillances dangereuses détectées ne sont pas prises en compte.

Approche SINTEF

L'organisme norvégien SINTEF [**49**] propose les formules analytiques du *STR* regroupées dans le tableau 2.3.

Architectures	***STR***
1*oo*1	λ_{SU}
1*oo*2	$2\ \lambda_{SU}$
1*oo*3	$3\ \lambda_{SU}$
2*oo*2	$\beta\ \lambda_{SU}$
2*oo*3	$C_{2oo3}\ \beta\ \lambda_{SU}$
1ooN; N= 1, 2, 3,…	$N\ \lambda_{SU}$
MooN $\mathbf{2 \le M \le N;\ N = 2, 3,...}$	$C_{(N-M+1)\ ooN}\ \beta\ \lambda_{SU}$

Tableau 2.3 : Formules relatives aux STR des architectures KooN (M=K) selon SINTEF

L'organisme SINTEF n'utilise pas le modèle du facteur β pour les défaillances de cause commune. Il met en œuvre un nouveau modèle, dénommé facteur β généralisé, moins

pessimiste que celui utilisé par la CEI 61508. La contribution des défaillances de cause commune dans une architecture *KooN* est estimée par $C_{MooN}\ \beta$ et Les facteurs C_{MooN} relatifs aux architectures *KooN (M=K)* sont donnés ci-après (tableau 2.4) :

M \ N	N = 2	N = 3	N = 4	N = 5	N = 6	N = 7	N = 8
M = 1	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.21$	$C_{1oo6} = 0.17$	$C_{1oo7} = 0.15$	$C_{1oo8} = 0.15$
M = 2	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.7$	$C_{2oo6} = 0.4$	$C_{2oo7} = 0.27$	$C_{2oo8} = 0.15$
M = 3	-	-	$C_{3oo4} = 2.9$	$C_{3oo5} = 1.8$	$C_{3oo6} = 1.1$	$C_{3oo7} = 0.8$	$C_{3oo8} = 0.6$
M = 4	-	-	-	$C_{4oo5} = 3.7$	$C_{4oo6} = 2.4$	$C_{4oo7} = 1.6$	$C_{4oo8} = 1.1$
M = 5	-	-	-	-	$C_{5oo6} = 4.3$	$C_{5oo7} = 3.0$	$C_{5oo8} = 2.1$
M = 6	-	-	-	-	-	$C_{6oo7} = 4.8$	$C_{6oo8} = 3.5$
M = 7	-	-	-	-	-	-	$C_{7oo8} = 5.3$

*Tableau 2.4 : C_{MooN} relatifs aux architectures KooN (M=K). [**48**]*

Rapport TOTAL

Pour une architecture KooN , la formule du STR proposée par les auteurs du rapport de la société française TOTAL [**12**] est basée sur une approche binomiale. Cette formule est donnée par :

$$\text{STR}\ (KooN) \approx A_N^K \cdot \lambda_{Sind}^K \cdot \left[\prod_{i=1}^{K-1} MDTS_i\right] + \left[\beta\ \lambda_{SU} + \beta_D\ \lambda_{SD}\right] \qquad (2.9)$$

Avec:

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

$\lambda_S = \lambda_{SU} + \lambda_{SD}$

$\lambda_{Sind} = (1- \beta_{SU})\ \lambda_{SU} + (1- \beta_{SD})\ \lambda_{SD}$

$MDTS_{1ooi} = \frac{\lambda_{SU}}{\lambda_S} \cdot \left(\frac{T_1}{i+1} + MTTR_{SD}\right) + \frac{\lambda_{SD}}{\lambda_S} \cdot MTTR_{SD}$

T_1 : durée entre deux tests périodiques.

$MTTR_{SD}$: durée moyenne de réparation d'une défaillance sûre (détectée).

Approche basée sur l'application des chaines de Markov

Le tableau 2.5 suivant regroupe l'ensemble des formules du STR déterminé à l'aide des chaines de Markov. [**47**]

Architecture	*STR*
1*oo*1	$\lambda_{SU} + \lambda_{SD}$
1*oo*2	$2 \cdot \left((1- \beta_{SD})\, \lambda_{SD} + (1- \beta_{SU})\, \lambda_{SU}\right) + \beta_{SD}\, \lambda_{SD} + \beta_{SU}\, \lambda_{SU}$
1*oo*3	$3 \cdot \left((1- \beta_{SD})\, \lambda_{SD} + (1- \beta_{SU})\, \lambda_{SU}\right) + \beta_{SD}\, \lambda_{SD} + \beta_{SU}\, \lambda_{SU}$
2*oo*2	$2 \cdot (\lambda_{SD} + \lambda_{SU})\left((1- \beta_{SD}) \cdot \lambda_{SD} \cdot MTTR_{SD} + (1- \beta_{SU}) \cdot \lambda_{SU} \cdot \left[\frac{T_1}{2} + MTTR_{SD}\right]\right) + \lambda_{SDCC}$
2*oo*3	$3 \cdot \left[(2-\beta_{SD}) \cdot \lambda_{SD} + (2-\beta_{SU}) \cdot \lambda_{SU}\right] \cdot \left[(1- \beta_{SD}) \cdot \lambda_{SD} \cdot MTTR_{SD} + (1- \beta_{SU}) \cdot \lambda_{SU} \cdot \left[\frac{T_1}{2} + MTTR_{SD}\right]\right) + \lambda_{SDCC}$

Tableau 2.5: Formules du STR des architectures KooN à l'aide de chaines de Markov.

En plus des approches citées au préalable, elle existe d'autres approches qu'on peut les résumées dans ce qui suit :

- Les auteurs Lu and Jiang [**29**] proposent une approche basée sur un modèle binomial. Cependant, leur objectif est d'estimer les activations intempestives sous différentes stratégies de maintenances. Cette approche prend uniquement les défaillances SO indépendantes.

- Les auteurs Andrews et Bartlett [**23**] utilisent un algorithme pour modéliser la contribution des activations intempestives dans une architecture *KooN*. Leur algorithme a pour objectif d'optimiser la sélection de K et N (*KooN*) pour minimiser les couts.

- Les auteurs Cho et Jiang [**46**] proposent le modèle markovien pour estimer le STR mais ne considèrent pas la contribution des défaillances de causes commune (DCC).

2.6. Conclusion et Résumé

Au cours du chapitre, nous commençons par une exposition de la typologie des défaillances liée aux systèmes instrumentées de sécurité selon deux approches différentes (norme CEI 61508 et SINTEF), puis nous avons présenté les concepts de base relatifs aux activations intempestives des SIS et discuté ses causes et enfin, nous avons présenté un ensemble de formulations analytiques, qui concernent l'estimation du taux de déclenchement intempestif (STR) selon différentes approches (travaux de M. A Lundteigen, et M.Rausand, formules présentées par ISA, formules proposées par l'organisme norvégien SINTEF, formules présentées dans le rapport TOTAL et des formules basée sur l'application des chaines de Markov). Le chapitre suivant est consacré à l'estimation du STR d'un SIS installé dans un processus industriel opérationnel par application des différentes formules ainsi que par application de la méthode Arbre des défaillances.

Chapitre 3

Modélisation et Estimation du taux de déclenchement intempestif d'un système d'arrêt d'urgence ESD

3.1. Introduction

La modélisation et l'estimation du taux de déclenchements intempestifs STR d'un système instrumenté de sécurité installé dans un processus industriel opérationnel (en phase d'exploitation) est l'objet de ce troisième chapitre.

Le chapitre débute par une présentation des installations choisis comme champ d'application. Il s'agit des installations de récupération des gaz torchés au niveau des centres de séparation de pétrole brut. Ces installations sont équipées de plusieurs systèmes instrumentés de sécurité, parmi ces derniers, nous choisissons comme exemple d'application, un système d'arrêt d'urgence (*ESD : Emergency Shutdown Systems*) d'une partie de processus globale pour des raisons de leur importance et de disponibilité des informations et données.

Le système d'arrêt d'urgence *choisi* est décrit dans la suite de ce chapitre et son architecture est déterminée, puis nous précisons les cas qui nécessitent son activation afin de modélisé le STR relatif, par la méthode de l'arbre de défaillance AdD, et d'estimé sa valeur par son traitement d'une part, et par l'application des différentes formules analytiques d'une autre part. Après cette estimation, une discussion comparative des résultats obtenus sera évoquée. Et enfin, nous rappelons l'objectif du chapitre pour conclure.

3.2. Présentation des installations RGTE

L'unité RGTE (***R***écupération des ***G***az ***T***orchés du champ d'***E***djelet[*]), mise en service en Mars 2005, a pour but la récupération, la compression, la déshydratation et le transport des gaz habituellement torchés (brulés dans des torchère) au niveau des dix (10) centres de séparation de pétrole brut du champ d'Edjelet. Les gaz récupérés seront utilisés pour assurer le *gas-lift* injecté dans des puits de pétrole qui nécessitent une *activation* (par le *gas-lift*) pour augmenter la production de brut ou dans des cas pour obtenir un débit stable des puits.

En plus des objectifs précités, l'unité RGTE contribue à la réduction de la pollution de l'environnement pour être conforme aux termes du Partenariat Mondiale de la réduction des gaz torchés (*GGFR : Global Gas Flaring Reduction Initiative*) dont l'Algérie est partie prenante.

[*] Situé dans le bassin d'Illizi, à environ 70 Km au sud-est d'In Amenas et 2000 Km au sud-est d'Alger.

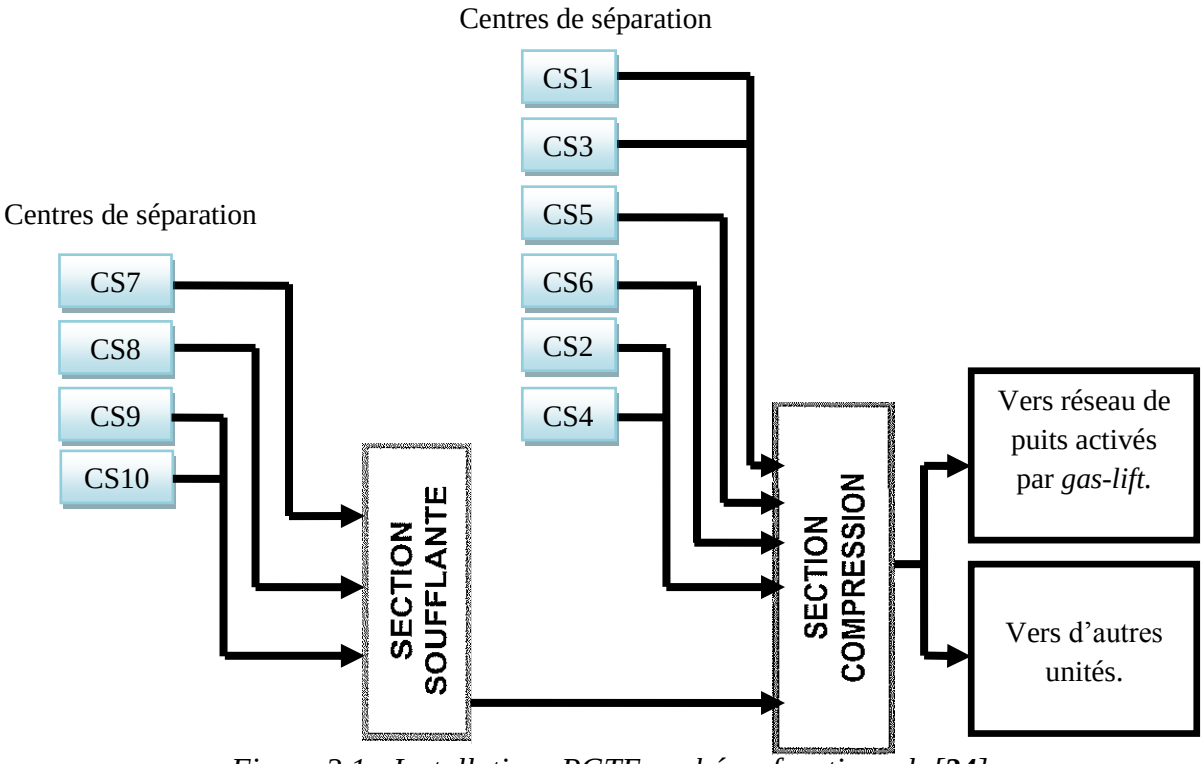


*Figure 3.1 : Installations RGTE ; schéma fonctionnel. [**34**]*

L'unité RGTE possède un autre rôle économique puisque elle participe à la production totale du pétrole brut du champ Edjelet avec un apport total estimé à environ 15 tonne/heure. Les installations RGTE comprend principalement deux (02) parties essentielles : une section soufflante et une autre de compression. La figure 3.1 présente le schéma fonctionnel de l'unité et précise ses deux parties.

3.2.1 Centres de séparation

Le champ Edjelet comporte dix (10) centres de séparation ; le pétrole et les gaz des puits sont distribués vers des ballons de séparation. Les pressions de service des ballons sont de 0.30 à 0.60 barG*. Les gaz de torche récupérés de chaque centre de séparation sont transportés à la section soufflante et de compression à travers les canalisations enterrées de collecte à basse pression. Les diamètres nominaux de ces canalisations de collecte sont optimisés de manière à maintenir la pression de gaz au moins à 0.1 barG aux aspirations de la soufflante de compression (11-K-001) et du compresseur de *gas-lift* (20-K-001). Le gaz total récupéré des (10) centres de séparation est estimé à environ $1.372 \cdot 10^6$ Std m^3/jour. [**35**]

* unité utilisée par les anglo-saxons qui représente le bar de la jauge ou manomètre / 0 barG = 1 bar atmosphérique.

- ✓ **Vers la section soufflante**; les gaz récupérés des quatre (04) centres de séparation CS7, CS8, CS9 et CS10 (figure 3.1) sont collectés par les canalisations enterrées de collecte à basse pression et transportés au manifold d'entrée de la section soufflante. Ensuite, le gaz comprimé est envoyé à la section de compression par la canalisation de collecte à basse pression de 18''.

- ✓ **Vers la section de compression** ; les gaz récupérés des six (06) centres de séparation CS1, CS2, CS3, CS4, CS5 et CS6 (figure 3.1) et le gaz comprimé provenant de la section soufflante sont collectés par les canalisations enterrées de collecte à basse pression et transportés au manifold d'entrée de la section de compression.

Chaque centre de séparation possède une unité d'injection d'inhibiteur de corrosion. L'inhibiteur est injecté en aval de la vanne de contrôle de pression à l'aide d'une pompe à plongeur.

3.2.2 Section soufflante

Les gaz collectés aux centres de séparation CS7, CS8, CS9 et CS10 sont à basse pression (entre 0.30 et 0.40 barG). Pour assurer qu'ils arrivent à la section principale de production de *gas-lift* (section de compression), ces gaz collectés passent, dans un premier temps, par la section soufflante qui comporte les équipements principaux suivants :

- Equipements de *process* :
  - Un (01) ballon de séparation pour soufflante de *boosting* (11-B-001).
  - Une (01) soufflante de *boosting* (11-K-001).
  - Un (01) post-refroidisseur (Aéroréfrigérant) pour soufflante de *boosting*(11-E-001).

- Equipements des *utilités* :
  - Deux (02) compresseurs d'air instrument (11-K-002A/B).
  - Une (01) unité de séchage d'air instrument (11-V-002).
  - Un (01) package de générateur de secours (11-V-003).
  - Une (01) unité d'inhibiteur de corrosion (11-V-002).
  - Un (01) bourbier 'Burn Pit'(11-F-002).

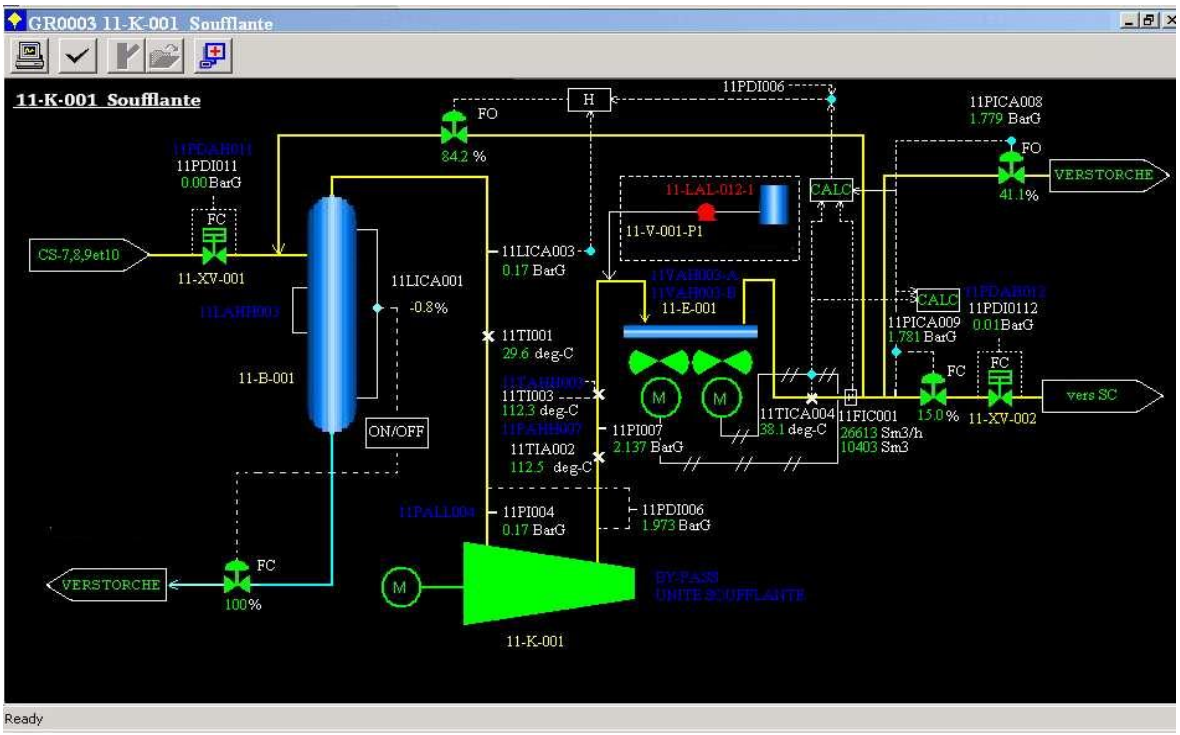


*Figure 3.2 : Section soufflante. [**53**]*

Les gaz provenant des centres de séparation CS7, CS8, CS9 et CS10 sont comprimés (*boosted up*) par la soufflante de compression (11-K-001) de 0.1 barG à 2.3 barG de manière à maintenir la pression des gaz comprimés à un niveau suffisant à l'aspiration de la section de compression.

Dès l'arrivée du gaz au manifold d'entrée de la section soufflante, Il achemine vers un dispositif antibuée qu'il est le ballon de séparation (11-B-001). Ce dernier est un séparateur de type vertical qu'il peut recueillir des particules de liquide qui pourraient être amènes à travers la ligne de collecte d'aspiration ou les condensats éventuellement présents. Le drain liquide et/ou les liquides sont envoyés vers le bourbier 'Burn Pit' (11-F-002).

Le flux de gaz est ensuite acheminé vers l'aspiration du compresseur (11-K-001) afin d'être comprimé d'environ 0,1 barG et 16,8 °C (25 °C en été et 10 °C en hiver) à une moyenne de 2,3 barG et 109 °C (2,1 barG, 105 °C en été et 2,8 barG, 114 °C en hiver). Il s'agit d'un compresseur centrifuge électrique Mitsubishi d'une puissance de 1284 kilowatts. Au refoulement du compresseur, un inhibiteur de corrosion (11-V-001-P1) est injecté dans le flux de gaz qui est refroidi dans des Aéroréfrigérants (11-E-001) entre 55 et 60 °C. Le flux de gaz est ensuite exporté vers la section compression principale qu'on doit la présentée dans la partie suivante. [**34**]

3.2.3 Section de compression

La section de compression est la partie principale des installations RGTE ; le gaz provenant de la section soufflante et des centres de séparation CS1, CS2, CS3, CS4, CS5 et CS6 sera comprimé d'environ 0.10 barG jusqu'à 65 barG, de façon à ce que ce gaz puisse être envoyé comme *gas-lift* aux puits qui nécessitent l'activation.

Dès l'arrivée du gaz au manifold d'entrée de la section de compression (32''), Il achemine vers un premier ballon tampon (20-B-001) puis il sera comprimé dans un compresseur (20-K-001) centrifuge à quatre étages. Les pressions et les températures d'aspiration- refoulement de chaque étage de compresseur (20-K-001) sont indiquées dans le tableau 3.1. Le flux de gaz est refroidi par des aéroréfrigérants et les fluides sont récupérés dans des ballons tampons après chaque étage de compression. Les drains liquides dans les ballons sont envoyés vers un bourbier 'Burn Pit' sous le contrôle du niveau.

Etage du compresseur	**Aspiration**		**Refoulement**	
	Pression	**Température**	**Pression**	**Température**
1	0.10 barG	15 °C	02.6 barG	118 °C
2	01.9 barG	55 °C	07.8 barG	116 °C
3	07.1 barG	55 °C	23.9 barG	133 °C
4	23.0 barG	55 °C	65.0 barG	140 °C

*Tableau 3.1 : Conditions d'exploitation du compresseur 20-K-001. [**33**]*

Après le quatrième étage de compression, le flux de gaz est acheminé vers une unité de déshydratation afin d'enlever l'eau contenu pour la protection contre la corrosion et éviter la formation des hydrates dans le réseau de canalisations qui transporte le *gas-lift*.

Chaque un des deux sections constituant les installations RGTE (soufflante et de compression) est menu d'un système d'arrêt d'urgence qui consiste à protéger ces installations en cas d'anomalies. Le système ESD de la section soufflante fait l'objet d'un exemple d'application dans ce qui suit.

3.3. Système d'arrêt d'urgence ESD de la section soufflante

La présence de toutes anomalies ayant pour résultat une perte immédiate de contrôle des opérations de la section soufflante, avec la possibilité de mettre en danger la vie des personnes et d'endommager les équipements, doivent être considérées comme celles qui nécessitent une action corrective et immédiate. Cette action est assurée par l'activation du système d'arrêt d'urgence (*ESD).*

3.3.1 Description du système ESD

Le système ESD installé dans la section soufflante est un type de SIS fonctionnant en faible demande qui assure, en cas d'activation, l'arrêt total automatique de la section pour minimiser le risque de dommage consécutif. Il est constitué d'un ensemble d'éléments d'entrée (transmetteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé de la section soufflante (température, pression, niveau). Si au moins un de ces paramètres dévie au-delà d'une valeur de consigne et s'y maintient, cette déviation constitue ce qui a été appelé demande ou sollicitation. Elle est détectée par les capteurs concernés qui envoient un signal au l'unité logique qui est un automate programmable contrôleur d'un niveau d'intégrité de sécurité SIL 3 de type *Triconex Trident Controller*.

L'architecture de l'unité logique est basée sur une redondance appelée *Triple-Modular Redundant* (*TMR*). Elle est constituée de trois modules de traitement identiques, parallèles et isolés avec l'exécution de diagnostique par une seule carte qui en cas de déviation, donne l'ordre pour réaliser des actions automatiquement. Ces actions sont les suivantes :

- Arrêt de la 11-K-001 ;
- Fermeture de la vanne d'isolement aspiration du 11-K-001 :11-XV-001 ;
- Fermeture de la vanne d'isolement refoulement du 11-K-001 : 11-XV-002 ;
- Ouverture de la vanne de mise à l'air libre du 11-K-001 : 11-PV-008 ;
- Ouverture de la vanne d'anti-pompage du 11-K-001 : 11-FV-001 ;

L'ensemble des éléments constituant le système ESD de la section soufflante est regroupé dans le tableau 3.2 avec la présentation de l'architecture (de type *KooN*) de chaque un de ces élément ainsi que la définition de ses fonctions dans le procédé.

N°	Elément	Désignation	Type	Architecture	Fonction en procédé
1	11-LSHH-003	L1	Contacteur de niveau à flotteur	1oo1	Détecter le niveau de liquide du ballon de séparation 11-B-001
2	11-LSLL-262	L2	Contacteur de niveau à flotteur	1oo1	Détecter le niveau d'huile d'étanchéité dans le réservoir
3	11-PT-004	P1	Transmetteur de pression *différentiel*	1oo1	Détecter la pression d'aspiration en amont de la soufflante 11-K-001
4	11-PT-007	P2	Transmetteur de pression	1oo1	Détecter la pression du *refoulement* de la soufflante
5	11-PT-502	P3	Transmetteur de pression	1oo1	Détecter la pression d'air instrument
6	11-PS-256	P4	Manocontact (pressure Switch)	1oo1	Détecter la pression d'huile de lubrification
7	11-TT-003	T1	Transmetteur de température à résistance	1oo1	Détecter la température de refoulement en aval de la soufflante 11-K-001
8	11-TE-302A	T2	Détecteur de température	1oo3 A, B, C	Détecter la température de refoulement en aval de la soufflante 11-K-001
9	11-TE-302B	T3			
10	11-TE-302C	T4			
11	11-TE-303A	T5	Détecteur de température	1oo3 A, B, C	Détecter la température de bobinage du moteur 11-KM-001
12	11-TE-303B	T6			
13	11-TE-303C	T7			
14	11-TE-300A	T8	Détecteurs de température à résistance	2oo2 A, B	Détecter la température du palier de la soufflante 11-K-001
15	11-TE-300B	T9			
16	11-TE-301A	T10		2oo2 A, B	
17	11-TE-301B	T11			
18	11-TE-310A	T12		2oo2 A, B	
19	11-TE-310B	T13			
20	11-TE-311A	T14		2oo2 A, B	
21	11-TE-311B	T15			
22	11-TE-312A	T16		2oo2 A, B	
23	11-TE-3128	T17			
24	11-TE-313A	T18		2oo2 A, B	
25	11-TE-313B	T19			
26	11-TE-320A	T20		2oo2 A, B	
27	11-TE-320B	T21			
28	11-TE-321A	T22		2oo2 A, B	
29	11-TE-321B	T23			
30	11-TE-330A	T24		2oo2 A, B	
31	11-TE-330B	T25			
32	11-TE-331A	T26		2oo2 A, B	
33	11-TE-331B	T27			
34	11-TE-332A	T28		2oo2 A, B	
35	11-TE-332B	T29			
36	11-TE-333A	T30		2oo2 A, B	
37	11-TE-333B	T31			
38	MP1	MP1	Modules de traitement	1oo3 A, B, C	Récoltent l'information de la partie détection, réalisent le processus de prise de décision et le transmit aux actionneurs.
39	MP2	MP2			
40	MP3	MP3			
41	11-XV-001	V1	Vanne d'isolement aspiration	1oo1	Fermer pour arrêter l'arrivé du gaz à l'entrée de la section soufflante
42	11-XV-002	V2	Vanne d'isolement refoulement	1oo1	Fermer pour arrêter le retour du gaz à la sortie de la section soufflante

Tableau 3.2 : Les éléments du système ESD

3.3.2 Architecture du système ESD

La figure 3.3 suivante représente l'architecture des éléments du système ESD de la section soufflante :

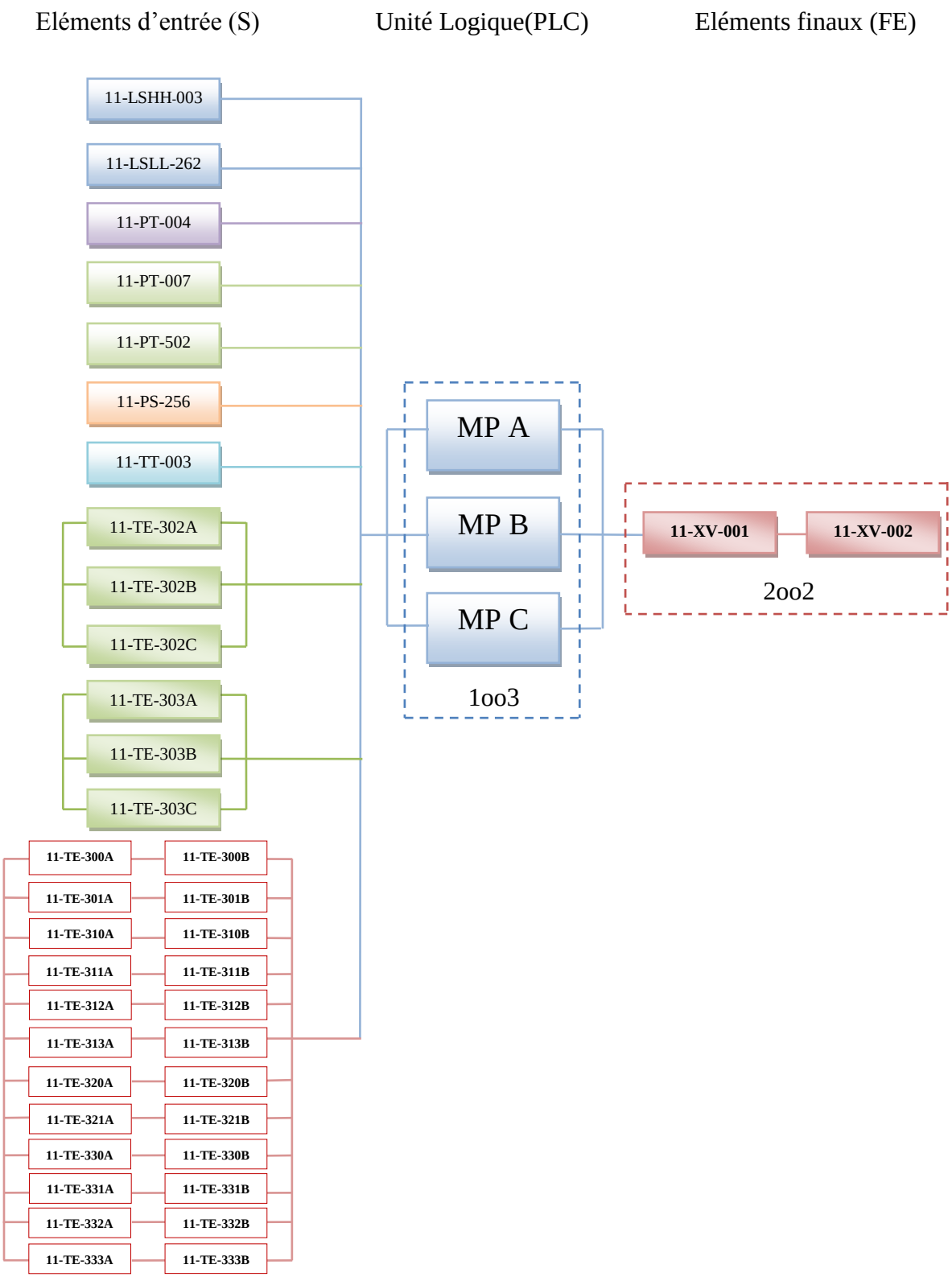


Figure 3.3 : Architecture du système ESD

3.3.3 Activation du système ESD

D'une manière générale, les cas qui nécessitent l'activation d'un système ESD installé dans un processus industriel sont :

- Les pannes des équipements.
- Les erreurs des opérations.
- Manque ou coupure des utilités.
- Incendie et fuite de gaz.

Pour la section soufflante, L'ESD sera activé dans les cas suivants :

- Déclanchement du compresseur 20-K-001 (élément de la section de compression) ;
- Niveau du liquide dans le ballon de séparation pour soufflante (11-B-001) HH ;
- Température de refoulement soufflante HH ;
- Pression de refoulement soufflante HH ;
- Pression d'aspiration soufflante LL ;
- Causes mécaniques de la soufflante :
    - Pression du collecteur d'huile de lubrification LL ;
    - Niveau d'huile dans le réservoir d'huile d'étanchéité LL ;
    - Température palier de la soufflante HH ;
    - Température enroulement moteur de la soufflante HH ;
    - Vibration de la soufflante HH;
    - Position axiale de la soufflante HH ;
- Manque d'air instrument ;
- Détecteur d'incendie.

L'indice HH représente une valeur très haute (HIGH HIGH) et l'indice BB représente une valeur très basse (LOW LOW). On donne comme des exemples **:** La valeur HH du ballon 11-B-001 est de 35% du volume de ballon ($12.3m^3$) et la valeur de Pression BB d'aspiration 11-K-001est 0.01 barG. [**34**]

En plus des cas mentionnés, la coupure de courant (L'alimentation électrique principale ou de secoure) active le système ESD de la section soufflante qui est alimenté par des batteries assurant la continuité de son fonctionnement pendant une courte durée.

Les anomalies concernent les vibrations et les Positions axiales de la soufflante sont traitées par une autre unité logique qui émet, en cas de déviation, un signal d'information à l'unité logique du système ESD. Cette dernière effectue l'arrêt de la section soufflante.

L'unité logique du système ESD reçoit aussi une information pour effectue l'arrêt de la section d'un autre système instrumenté de sécurité qui est le système d'extinction automatique.

Le système ESD de la section soufflante peut être activé en absence des déviations d'une manière intempestive par des faux signaux de ses capteurs, d'une décision erronée de l'unité logique ou d'une action intempestive. Cette activation est caractérisée par un taux de déclenchement intempestif qui sera modélisé et évalué dans ce qui suit.

3.4. Taux de déclenchement intempestif (STR) du Système ESD de la section soufflante

3.4.1 Modélisations du STR par Arbres de défaillances (AdD)

3.4.1.1 Description de la méthode AdD

L'Arbre de Défaillances (Fault Tree ou « FT » en anglais) est un outil graphique très utilisé en Sureté de fonctionnement. Il permet de représenter graphiquement les combinaisons possibles des causes qui permettent la réalisation d'un événement indésirable prédéfini. L'AdD est ainsi formé de niveaux successifs d'événements qui s'articulent par l'intermédiaire de portes logiques.

L'AdD est, donc, une méthode déductive **[32]** qui peut être utilisé comme un outil d'évaluation de la conception. L'AdD permet aussi être utilisé comme un outil de diagnostic prévoyant la ou les défaillances des composants la ou les plus probables lors de la défaillance d'un système.

La construction de l'AdD est la phase la plus cruciale de la méthode **[11].** Selon les références **[42]** et **[54]**, Cette construction est effectuée comme suit :

Un arbre de défaillance est généralement présenté de haut en bas. La ligne la plus haute, ou sommet de l'arbre, comporte uniquement la défaillance (ou événement redouté ou encore événement non souhaité) que l'on cherche à analyser. Chaque ligne détaille la ligne supérieure en présentant la combinaison ou les combinaisons susceptibles de produire

l'événement de la ligne supérieure auquel elles sont rattachées. Ces relations sont présentées par des liens logiques 'OU' ou 'ET'.

La première étape consiste à définir l'événement sommet, c'est-à-dire la défaillance, de façon explicite et précise afin que l'arbre construit réponde bien aux attentes de l'étude (par exemple les événements suivants ne sont pas équivalents : défaillance de la stabilité d'un bâtiment, ruine d'un bâtiment sous l'action d'un séisme, rupture d'un bâtiment sous l'action de la neige, etc.).

La deuxième étape consiste à décrire l'ensemble des événements, par des combinaisons logiques (conjonction ou disjonction), pouvant engendrer l'événement sommet. Il apparaîtra donc des événements moins globaux que l'événement sommet, que l'on nommera événements intermédiaires, et un connecteur logique qui les relie à l'événement sommet.

Les étapes suivantes consistent à décrire successivement l'ensemble des lignes permettant d'expliquer les lignes supérieures (par des événements et des connecteurs logiques) jusqu'à avoir écrit l'ensemble des causes connues. Il s'agit de répéter la deuxième étape jusqu'à l'obtention des événements de base qui sont des événements qui ne se décompose plus en événements plus fins.

Il existe un ensemble de symboles normalisés permettant de représenter l'événement sommet, les événements intermédiaires, les événements de base et les connecteurs. Les principaux symboles utilisés sont regroupés dans le tableau suivant :

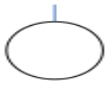
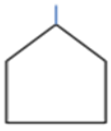
Symbole	Nom	Description
	Événement de Base	Événement du plus bas niveau pour lequel la probabilité d'apparition ou d'information de fiabilité est disponible.
	Événement maison	Événement qui doit se produire avec certitude lors de la production ou de la maintenance. On peut aussi le définir comme un événement non-probabilisé, que l'on doit choisir de mettre à 1 ou à 0 avant tout traitement de l'arbre. Ce type d'événement permet d'avoir plusieurs variantes d'un arbre sur un seul dessin, en modifiant la logique de l'arbre selon la valeur choisie par l'utilisateur
	Événement non développé	Le développement de cet événement n'est pas terminé, soit parce que ses conséquences sont négligeables, soit par manque d'information.

Tableau 3.3 : Symboles des événements dans les arbres de défaillances

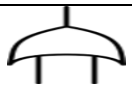
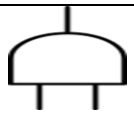
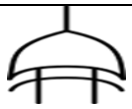
Symbole	Nom	Description	Nombre d'entrées
	OU (OR)	L'événement de sortie apparaît si au moins un des événements d'entrées apparaît.	>1
	ET (AND)	L'événement de sortie apparaît si tous les événements d'entrées apparaissent.	>1
	NON (NOT)	L'événement de sortie apparaît si l'événement d'entrée n'apparaît pas. L'état logique de la sortie est l'inverse de celui d'entrée.	=1
	OU Exclusif (XOR)	L'événement de sortie apparaît si un seul événement d'entrée apparaît.	>1
	VOTE MAJORITAIRE	L'événement de sortie apparaît si au moins k événements d'entrées apparaissent (k<n).	>1

Tableau 3.4 : Symboles des portes dans les arbres de défaillances

Quantification des probabilités d'occurrence : Il s'agit ici d'évaluer la probabilité d'occurrence de l'événement sommet à partir des probabilités d'occurrence des événements de base.

Plusieurs auteurs, donne de plus amples informations sur la construction et l'évaluation qualitative et quantitative des arbres de défaillances**.** Cependant, le calcul du risque qu'un événement indésirable se produise est basé sur les liens de causalité, qui peuvent être :

- Inclusifs (*A* ET *B*) : Pr $(A \cap B)$ = Pr(A).Pr(B) avec *A* et *B* indépendants ;
- Exclusifs (*A* OU *B*) : Pr $(A \cup B)$ = Pr(A) + Pr(B) − Pr $(A \cap B)$;
- Avec le cas particulier où les événements déclencheurs sont parfaitement exclusifs

Pr $(A \cap B)$ = 0.

Recherche des coupes minimales : On nomme coupe minimale un ensemble d'événements de base ou conditions nécessaires ou suffisantes à produire l'événement sommet. Si on retire à une coupe minimale un seul de ses éléments, la défaillance (événement sommet) n'est plus générée.

On trouve les coupes minimales en descendant l'arbre ligne par ligne. Lorsque l'on a identifié l'ensemble des coupes minimales on peut :

- Eliminer les redondances d'événements dans une même coupe (il est inutile de citer plusieurs fois le même événement dans une coupe) ;
- Eliminer les redondances de coupes (quand le même ensemble d'événements a été produit par plusieurs voies, il est inutile de le conserver en plusieurs exemplaires) ;
- Eliminer les « super-coupes » qui en contiennent d'autres (quand un ensemble est strictement contenu dans un autre, il n'est utile de garder que le plus petit).

Sensibilités, Facteurs d'importance : Les composants constitutifs d'un système peuvent avoir une importance plus ou moins grande pour ce système. Un composant correspondant à un point unique de défaillance sera bien entendu plus important qu'un composant de caractéristiques équivalentes mais mis en parallèle avec d'autres composants. Sur un système de très petite taille, l'identification de ces composants importants peut se faire par une simple lecture des coupes. Mais pour un système complexe et sûr dont les coupes sont d'ordre élevé, cette lecture est impossible. C'est pourquoi des facteurs d'importance ont été introduits afin d'établir une hiérarchie des composants.

L'importance d'un composant pouvant varier suivant les objectifs recherchés, plusieurs facteurs d'importance ont été créés. Ci-après, voici cinq facteurs d'importance parmi les plus utilisés ; leurs définitions et signification exacte seront disponibles sur un article dédié à ce sujet :

- Birnbaum (aussi appelé facteur d'importance marginal) ;
- Critique ;
- Diagnostic ;
- Facteur d'augmentation de risque ;
- Facteur de diminution de risque.

Attention, ces différents facteurs d'importance ne vont pas toujours dans le même "sens", il peut être difficile d'identifier formellement les composants à améliorer (en les rendant plus fiables, mieux maintenus…). C'est pourquoi il est conseillé de ne pas se fier à un seul facteur d'importance

Intérêts et limites : Le principal avantage de cette méthode est de pouvoir visualiser l'ensemble des combinaisons d'événements élémentaires conduisant à une défaillance,

c'est-à-dire qu'elle permet d'avoir une vision globale et logique du fonctionnement et des dysfonctionnements d'un système.

La connaissance des coupes minimales permet d'identifier, en phase de conception, les composants d'un système à améliorer pour qu'un événement ne se produise pas ; fiabiliser ces systèmes revient donc à essayer de supprimer les coupes minimales.

Les principales limites de cette méthode sont les suivantes :

- Les événements intermédiaires doivent être indépendants les uns des autres pour que le calcul des probabilités d'occurrence soit correct,
- L'arbre des défaillances ne rend pas compte de l'aspect temporel des scénarios d'événements conduisant à la défaillance,
- Cette méthode est binaire, un événement peut soit se produire, soit ne pas se produire.

3.4.1.2 Construction de l'AdD

Les figures 3.4, 3.5, et 3.6 représente une modélisation par la méthode AdD du taux de déclenchement intempestif de système ESD de la section soufflante qui sera considéré comme un événement sommet. Cette construction est établie à l'aide d'un logiciel nommé GRIF (Graphiques Interactifs pour la Fiabilité) développé par la société française TOTAL. Notons que les défaillances de causes communes sont prises en considérations lors de la construction.

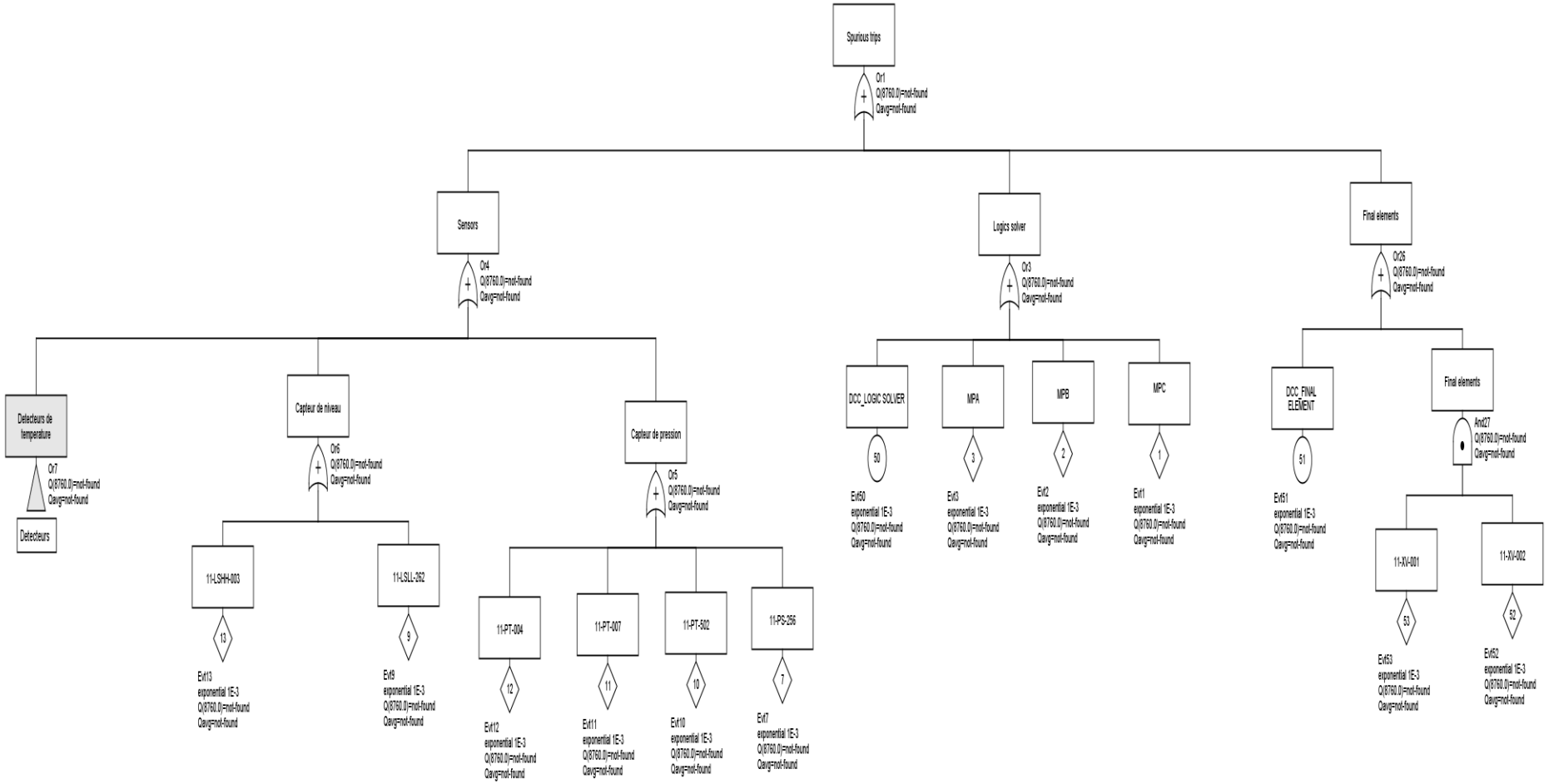


Figure 3.4 : Modélisation de déclenchement intempestif du système ESD par AdD

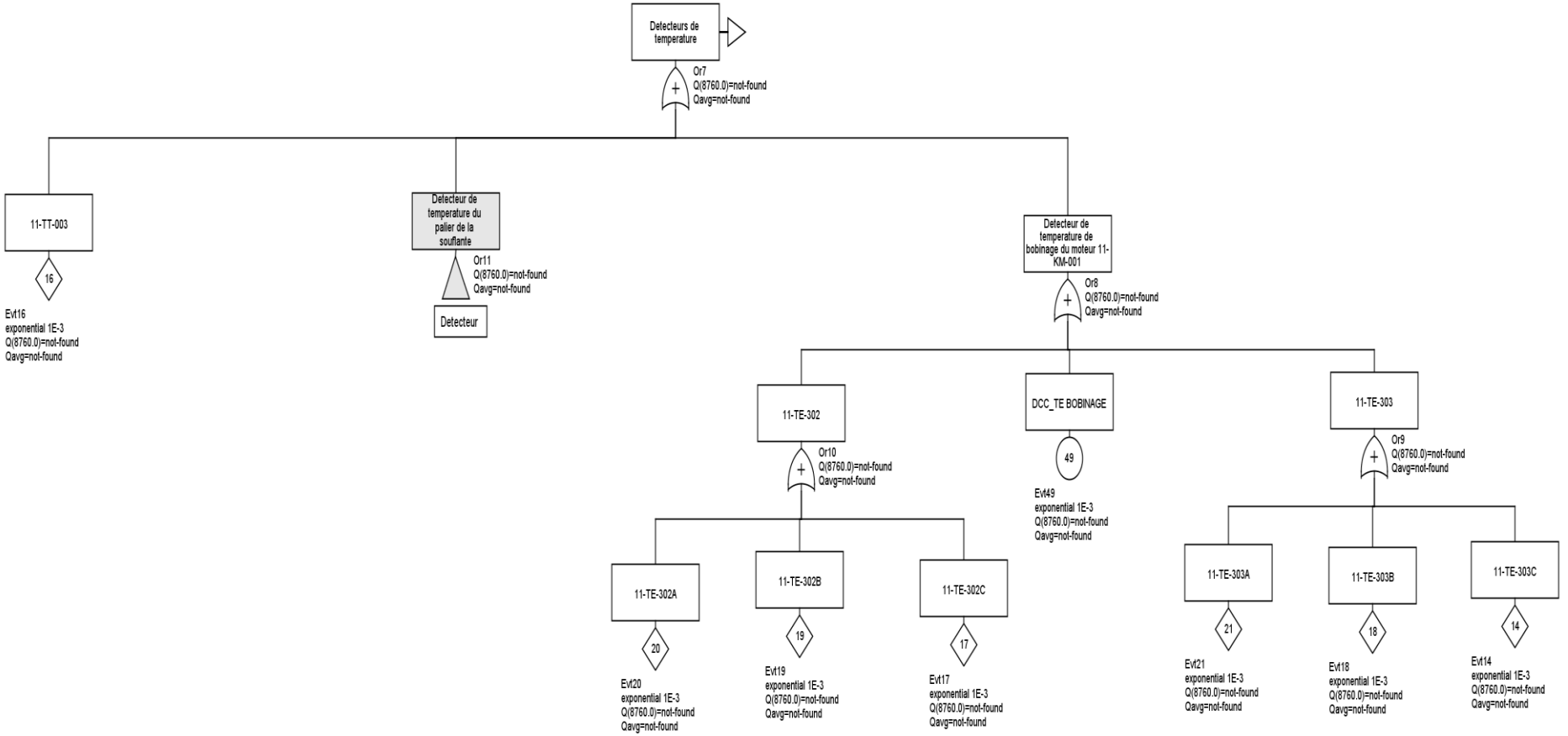


Figure 3.5 : Modélisation de déclenchement intempestif du système ESD par AdD (Suite 1)

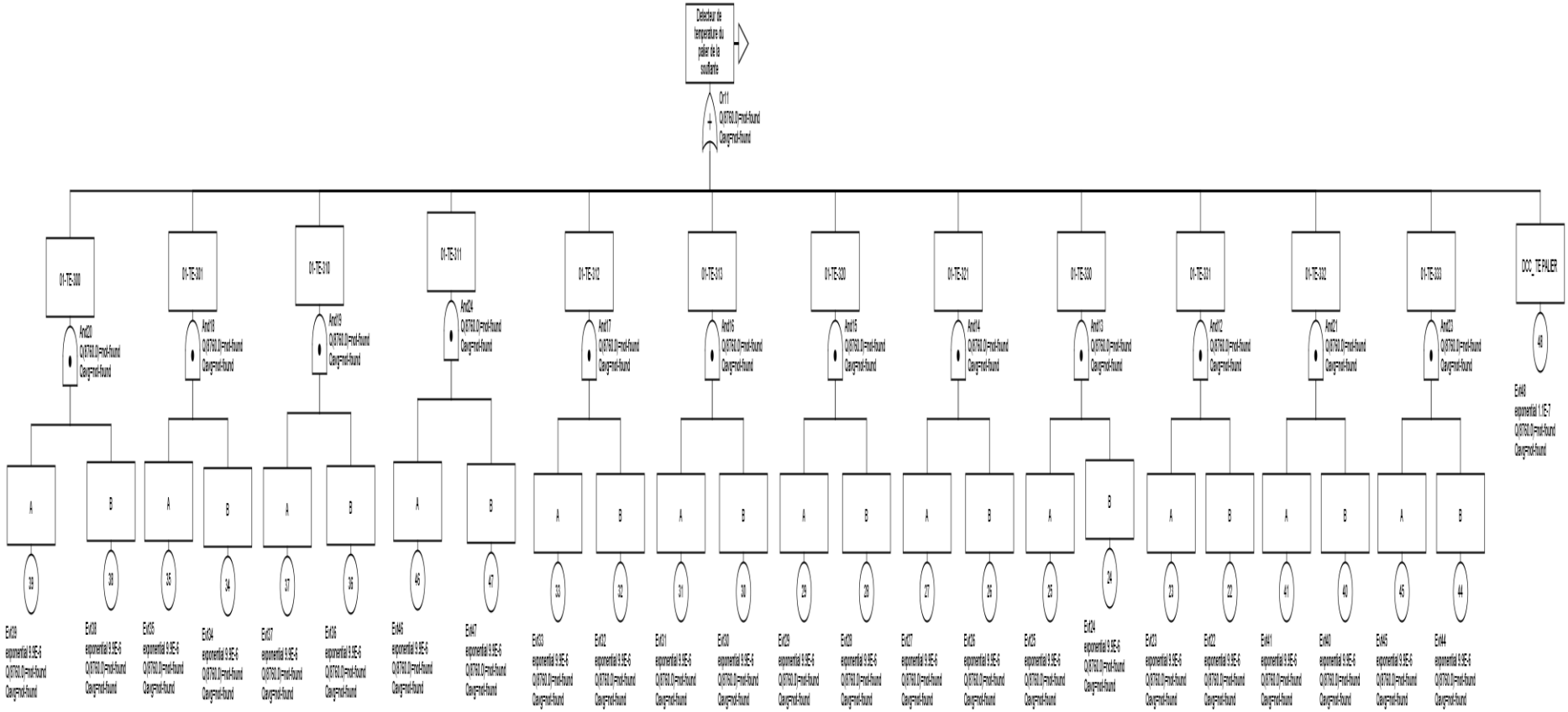


Figure 3.6 : Modélisation de déclenchement intempestif du système ESD par AdD (Suite 2)

3.4.2 Estimation du STR modélisé par l'AdD

Méthode de calcul

Selon la 3ème partie du rapport technique ISA-TR 84.00.02 **[18]**, l'estimation du taux de déclenchement intempestif STR (en tant que événement sommet suite à une modélisation par la méthode AdD) est différente de celle de la probabilité de défaillance à la demande PFD puisque le STR est un taux et n'est pas une probabilité. Pour la porte 'ou' le STR de deux événements de base est la somme des STR relatifs à chaque composant, et pour la porte 'et', le STR est calculé mathématiquement pour deux événements de base comme suit :

STR=Probabilité de défaillance du composant 1x Fréquence de défaillance du composant 2

+Probabilité de défaillance du composant 2 x Fréquence de défaillance du composant 1

Source de données

Les données utilisées pour évaluer le STR du système d'arrêt d'urgence ESD de la section soufflante sont regroupées dans le tableau 3.5 .Ces données sont tirées de la référence *PDS Data Handbook, 2006 Edition* [**49**]. Des exemples de dossiers de données de cette référence sont annexés à la fin de ce mémoire.

Elément	λ_{SO} (h^{-1})	λ_{DD} (h^{-1})	Commentaires
Transmetteur de niveau	**1.60E-6**	**0.80E-6**	• La référence [**49**] donne les valeurs de λ_D et λ_{DU} ; on déduire donc la valeur de λ_{DD} / $\lambda_{DD} = \lambda_D - \lambda_{DU}$. • $\lambda_{SO} = \lambda_{ST}$ présenté dans la référence [**49**], puisque la définition du λ_{SO} est incluse dans la définition de λ_{ST} donnée dans la même référence.
Transmetteur de pression	**0.50E-6**	**0.50E-6**	
Manocontact (pressure Switch)	**1.10E-6**	**0.70E-6**	
Transmetteur (détecteur) de température	**1.10E-6**	**0.40E-6**	
Module de traitement (une seule carte)	**15.0E-6**	**10.0E-6**	
Vanne d'isolement	**2.70E-6**	**0.70E-6**	

Tableau 3.5 : Données des éléments du système ESD.

Pour la caractérisation des défaillances de causes commune (DCC) on utilise ces données :

- $\beta^{DD} \approx \beta^{SO}$
- $\beta^{DD} \approx \beta^{SO} \approx 10\%$ pour les parties : éléments d'entrée(S) et éléments finaux (FE).
- $\beta^{DD} \approx \beta^{SO} \approx 1\%$ pour la partie : unité logique(PLC).

Pour les architectures élémentaires du système d'arrêts d'urgence de la section soufflante, le tableau suivant (3.6) englobe l'ensemble des formules simplifiées qui seront utilisées pour l'estimation du STR en question pour des raisons de comparaison entre les différentes approches :

Architecture	*Lundteigen*/ Rausand)	ISA	SINTEF	Markov
1001	$\lambda_{SO} + \lambda_{DD}$	$\lambda_S + \lambda_{DD}$	λ_{SU}	$\lambda_{SU} + \lambda_{SD}$
1003	$(3 - 2\beta_{SO})\,\lambda_{SO} + \beta_{DD}\,\lambda_{DD}$	$3.\,[\lambda_S + \lambda_{DD}] + \beta\,(\lambda_S + \lambda_{DD})$	$3\,\lambda_{SU}$	$3\cdot((1-\beta_{SD})\,\lambda_{SD} + (1-\beta_{SU})\,\lambda_{SU}) + \beta_{SD}\,\lambda_{SD} + \beta_{SU}\,\lambda_{SU}$
2002	$\beta_{SO}\,\lambda_{SO} + \beta_{DD}\,\lambda_{DD}$	$2.\lambda_S\,[\lambda_S + \lambda_{DD}].\mathrm{MTTR} + \beta\,(\lambda_S + \lambda_{DD})$	$\beta\,\lambda_{SU}$	$2\cdot(\lambda_{SD} + \lambda_{SU})\,[(1-\beta_{SD})\,.\,\lambda_{SD}.\mathrm{MTTR}_{SD} + (1-\beta_{SU})\lambda_{SU}(T_1/2+\mathrm{MTTR}_{SD})] + \lambda_S D_{CC}$

Tableau 3.6 : Formules du STR selon différentes approches.

Les résultats de calcul se présentent dans le tableau suivant :

Désignation	$\mathbf{STR}_{\mathbf{LUND/RAUSA}}$ (h^{-1})	$\mathbf{STR}_{\mathbf{ISA}}$ (h^{-1})	$\mathbf{STR}_{\mathbf{SINTEF}}$ (h^{-1})	$\mathbf{STR}_{\mathbf{Markov}}$ (h^{-1})	$\mathbf{STR}_{\mathbf{ADD}}$ (h^{-1})
Eléments d'entrée (S)	1.91 E-05	2.22 E-05	8.42 E-06	1.48 E-05	**1.45 E-05**
Unité Logique (PLC)	4.48 E-05	7.53 E-05	3.60 E-05	4.47 E-05	**4.47 E-05**
Eléments finaux (FE)	3.40 E-07	3.40 E-07	2.70 E-07	3.28 E-07	**5.40 E-07**
STR_{ESD}	6.43 E-05	9.78 E-05	4.47 E-05	5.99 E-05	**5.97 E-05**

Tableau 3.7 : Résultats du STR selon différentes approches.

Discussions

- Suite à une comparaison entre les résultats trouvés, on peut constater que les valeurs du taux de déclenchement intempestif estimées par la méthode AdD sont similaires aux valeurs estimées par application des formules proposées par la méthode de Markov.
- La valeur du STR pour le sous-système « éléments finaux (FE) » est relativement faible par à port aux valeurs correspond aux deux autres sous-systèmes d'où la formule du STR_{ESD} qui sera utilisée dans la suite de ce mémoire est la suivante :

$$STR_{ESD} \approx STR_{Si} + STR_{LS} \qquad (3.1)$$

3.5. Conclusion

Au cours de ce chapitre qui représente une application sur un SIS opérationnel, nous avons tout d'abord présenté le champ d'application qui est des installations appeler RGTE ***(R***écupération des ***G***az ***T***orchés du champ d'***E***djelet). Ces installations comprennent principalement deux (02) parties essentielles : une section soufflante et une autre de compression. Puis nous avons modélisé et évalué le taux de déclenchement intempestif (STR) d'un système d'arrêt d'urgence ESD installé dans la section soufflante par l'application de la méthode AdD et pour des raisons comparatives nous avons évalué le même STR par les différentes formules de la littérature. Après l'analyse des résultats trouvés, on a constaté que le STR relatif au système instrumenté de sécurité, objet d'étude est assez élevé et pour les industriels, il est donc incontestable de réduire aux maximum possible (Optimiser) ce type de déclenchements en tenant compte des contraintes qui impliquent implicitement des stratégies de maintenance qui permet de minimiser le STR à des valeurs adéquates aux seuils prédéfinis par les concepteurs des SIS. Ce problème sera l'objet principal du quatrième et dernier chapitre.

Chapitre 4

Optimisation du taux de déclenchement intempestif d'un système d'arrêt d'urgence ESD

4.1. Introduction

La gestion de la maintenance des équipements est devenue un enjeu de taille et représente aujourd'hui une préoccupation industrielle majeure. En effet, les systèmes industriels sont de plus en plus complexes, hautement automatisés et robotisés. Ces équipements sont soumis à des mécanismes de dégradation dus aux conditions de fonctionnement et/ou d'environnement : usure, fatigue, vieillissement et altérations physico-chimiques diverses. En conséquence, ces divers dysfonctionnements exigent une maintenance accrue, afin de garantir un niveau de service optimal en termes de fiabilité et de disponibilité. Pour remédier aux défaillances de ces systèmes, il est possible de se contenter de pratiquer une maintenance corrective, mais cela n'empêcherait pas de subir les conséquences des pannes.

Une attitude plus "défensive" consiste à mettre en œuvre une maintenance préventive systématique destinée à limiter, voire à empêcher, ces défaillances. On court alors le risque de dépenses excessives et d'indisponibilités inutiles si les périodes d'intervention ne sont pas correctement calibrées. Devant cette situation, l'équipe de maintenance ne doit plus se contenter de surveiller et de réparer les pannes, mais elle doit aussi envisager des stratégies de maintenance préventives. Ces dernières doivent réaliser un compromis acceptable entre la disponibilité du système et les coûts associés à son entretien et à son fonctionnement. C'est dans ce contexte que se situe l'optimisation de la maintenance.

Dans ce dernier chapitre, nous allons d'abord donner quelques concepts et définitions précises liés à la maintenance puis nous présentons les différents types de maintenance, précisons la signification d'un problème d'optimisation et mettons le point sur les principales méthodes d'optimisation des stratégies de maintenance. Ensuite, nous essayons de posé le problème de la minimisation du STR relatif au système d'arrêt d'urgence STR_{ESD} évalué au niveau du chapitre précédent après la définition de la fonction objective et les contraintes relatives et pour conclure, les résultats trouvés serons discutés.

4.2. Concepts et définitions

Le terme maintenance est forgé sur les racines latines *manus* et *tenere*. Selon Larousse: le mot maintenance est l'ensemble de tout ce qui permet de maintenir ou de rétablir un système en état de fonctionnement. D'après l'Afnor (NF X60-010) « la maintenance est l'ensemble des actions permettant de maintenir ou de rétablir un bien dans un état spécifié ou en mesure d'assurer un service déterminé.»

Dans une entreprise, maintenir, c'est donc effectuer des opérations (dépannage, réparation, graissage, contrôle, etc.) qui permettre de conserver le potentiel du matériel pour assurer la production avec efficacité et qualité.

4.2.1 Actions de maintenance

Depuis que l'homme a exercé sa capacité de création pour concevoir et utiliser des outils, puis des dispositifs divers et variés jusqu'aux machines et installations techniques, il a découvert, et subi les phénomènes de dégradation et d'usure qui peu à peu rendait l'objet en question inutilisable. Très vite donc, il a été conduit à envisager des actions pour :

- Soit éviter, ou au moins ralentir, ces phénomènes de dégradation et leur évolution ;
- Soit remettre cet objet dans un état tel qu'il puisse accomplir de nouveau la fonction ou rendre le service pour lequel il avait été conçu lorsque le développement trop important d'une dégradation avait entraîné sa mise hors d'usage.

4.2.2 Types de maintenance

Dans le cadre d'une politique de maintenance relative à un système technique donné, les responsables sont conduits à envisager plusieurs stratégies de maintenance adaptées aux enjeux techniques et économiques de ce système [**52**] :

➢ **Maintenance préventive :** maintenance exécutée à des intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'un bien. On a le choix entre plusieurs politiques de maintenance préventive. Les plus fréquentes sont les suivantes :

- **Maintenance systématique :** maintenance *préventive exécutée à des intervalles de temps préétablis ou selon un nombre défini d'unités d'usage mais sans contrôle préalable de l'état du bien*. On fixe des règles strictes pour déterminer les dates de maintenance selon l'importance d'un équipement dans un système :
    - Un âge fixé de l'équipement ; il faut alors disposer d'un moyen pour connaître l'âge de l'équipement durant la vie du système ;
    - Un âge fixé du système ; c'est le cas des révisions des automobiles préconisées par les constructeurs ;
    - Des dates fixes : elle est plus coûteuse en temps et en pièces de rechange.
- **Maintenance conditionnelle :** consiste à *vérifier périodiquement l'état des pièces qui se dégradent* et à n'intervenir que si l'*état de dégradation est suffisamment avancé* pour compromettre la fiabilité du bien. Elle nécessite des moyens de mesure ou de test

permettant d'apprécier l'état de dégradation. L'évolution des capteurs de mesure (par exemple, les capteurs de vibrations) et des dispositifs d'analyse automatique (par exemple, l'analyse des huiles de graissage) associés aux télémesures et aux ordinateurs rendent cette politique plus accessible. Elle est très efficace, mais la gestion des ressources de maintenance est plus difficile et nécessite souvent le recours à l'ordinateur [**52**].

- **Maintenance prévisionnelle :** *maintenance conditionnelle* exécutée en suivant les *prévisions extrapolées de l'analyse et de l'évaluation de paramètres significatifs de la dégradation du bien*. Elle permet *d'anticiper et de prévoir au mieux le moment où l'intervention devra être réalisée*. Lorsqu'elle est techniquement réalisable et économiquement rentable, cette forme de maintenance est sûrement la plus élaborée et conduit à la meilleure optimisation de la maintenance [**52**].

➢ **Maintenance corrective :** maintenance exécutée après la détection d'une panne et destinée à remettre un bien dans un état dans lequel il peut accomplir la fonction requise. Cette maintenance corrective peut être décomposée encore en :

- **Maintenance palliative :** consiste à *pallier provisoirement l'effet d'une défaillance* afin de permettre la *continuité de l'exploitation du bien* sans pour autant traiter les causes. L'action exécutée est presque toujours *une action de dépannage*. Si cette maintenance n'est pas complétée par une action de fond destinée à traiter la cause première, on est conduit à constater la *répétition de la défaillance* en question et on parle alors de *défaillance répétitive* [**52**].
- **Maintenance curative :** Il s'agit là d'une maintenance qui *s'attaque réellement au fond du problème* en essayant de *« soigner » le mal et traitant la cause première*, si le diagnostic permet de remonter jusqu'à cette cause première.

➢ **Auto-maintenance :** exécutée par un utilisateur ou un personnel d'exploitation du bien (entretien de routine : graissage ou les réglages simples...). Ce type ne demandant pas le déploiement de moyens logistiques importants (pièces de rechange, outillage, documentation, compétences, …).

Dans la pratique, on est amené, *pour réduire les coûts de maintenance et assurer la disponibilité des systèmes*, à *combiner ces différentes politiques dans le plan de maintenance*, par exemple à prévoir une partie des actions de maintenance à dates fixes et à en profiter pour effectuer les vérifications sur les pièces soumises à la maintenance

conditionnelle. ***En conclusion,*** quelle que soit la stratégie de maintenance préconisée, il est nécessaire de la mettre en œuvre dans le cadre d'une méthodologie rigoureuse, fondée sur :

- La connaissance technologique des biens concernés ;
- Leurs conditions d'exploitation dans le système productif ;
- Leur criticité dans le processus de production ;
- Les coûts directs et indirects engendrés.

4.2.3 Problème d'optimisation

Les problèmes d'optimisation occupent actuellement une place grandissante dans la communauté scientifique. Ces problèmes peuvent être combinatoires (discrets) ou à variables continues, avec un seul ou plusieurs objectifs (optimisation mono ou multi-objectif), statiques ou dynamiques, avec ou sans contraintes. Cette liste n'est pas exhaustive et un problème peut être, par exemple, à la fois continu et dynamique. [**25**]

Un problème d'optimisation est défini par un ensemble de variables, une fonction objectif (ou fonction de coût) et un ensemble de contraintes. L'espace de recherche est l'ensemble des solutions possibles du problème. Il possède une dimension pour chaque variable. Pour des raisons pratiques et de temps de calcul, l'espace de recherche des méthodes de résolution est en général fini. Cette dernière limitation n'est pas gênante, puisqu'en général le décideur précise exactement le domaine de définition de chaque variable. La fonction objective définit le but à atteindre, on cherche à minimiser ou à maximiser celle-ci. L'ensemble des contraintes est en général un ensemble d'égalités et d'inégalités que les variables doivent satisfaire. Ces contraintes limitent l'espace de recherche. [**25**]

4.2.4 Méthode d'optimisation des stratégies de maintenance

Les méthodes d'optimisation recherchent une solution, ou un ensemble de solutions, dans l'espace de recherche, qui satisfont l'ensemble des contraintes et qui minimisent, ou maximisent, la fonction objective. Parmi ces méthodes, les *métaheuristiques* sont des algorithmes génériques d'optimisation : leur but est de permettre la résolution d'une large gamme de problèmes différents, sans nécessiter de changements profonds dans l'algorithme. Elles forment une famille d'algorithmes visant à résoudre des problèmes d'optimisation difficile, pour lesquels on ne connaît pas de méthode classique plus efficace. Les *métaheuristiques* s'inspirent généralement d'analogies avec la physique

(recuit simulé), avec la biologie (algorithmes évolutionnaires) ou encore l'éthologie (colonies de fourmis, essaims particulaires). Toutes sortes d'extensions ont été proposées pour ces algorithmes, notamment en optimisation dynamique.

L'optimisation dynamique s'efforce de minimiser ou maximiser une fonction objective qui varie en fonction du temps. En pratique, l'optimisation dynamique peut être appliquée, par exemple, pour déterminer de bonnes manœuvres dans le domaine aéronautique ; pour le contrôle de robots, de réactions chimiques ; pour le routage dans les réseaux, etc. [**25**]

Par rapport à l'optimisation statique, des difficultés supplémentaires apparaissent. Par exemple, les informations que l'algorithme a pu accumuler sur le problème, au cours de son exécution, peuvent être « périmées » à l'issue d'un changement dans la fonction objectif. Un moyen simple pour résoudre un problème dynamique consiste à redémarrer un algorithme d'optimisation statique, à chaque fois qu'un changement se produit dans la fonction objective (sous réserve, entre autres, de pouvoir déterminer l'instant du changement). En pratique, procéder ainsi n'est pas toujours possible et peut s'avérer inefficace. Des algorithmes dédiés à l'optimisation dynamique ont alors été proposés dans la littérature. [**25**]

La plupart des *métaheuristiques* d'optimisation dynamique proposées dans la littérature sont *bio-inspirées*. Elles appartiennent principalement à la classe des algorithmes évolutionnaires et à celle des essaims particulaires. Néanmoins, ce type d'algorithmes, conçus initialement pour l'optimisation statique, ne peut pas être employé directement en optimisation dynamique. En effet, dans le cadre de l'optimisation dynamique, ces algorithmes présentent plusieurs défauts intrinsèques. Il est alors nécessaire d'utiliser des techniques particulières, afin de les adapter aux problèmes dynamiques.

Parmi les principales techniques proposées dans la littérature, certaines consistent à introduire ou à maintenir la diversité des solutions testées à chaque itération de l'algorithme (pour les algorithmes faisant évoluer une population de solutions). Il ne s'agit toutefois pas de maintenir l'algorithme dans une phase de diversification continuelle (i.e. l'algorithme doit rester capable de converger avec précision). Dans le même ordre d'idées, des techniques visant à diviser la population de solutions en plusieurs sous-populations, réparties dans l'espace de recherche, permettent de suivre plusieurs optima à la fois et d'augmenter la probabilité d'en trouver de nouveaux. D'autres techniques sont basées sur l'utilisation d'informations sur les états passés de la fonction objective, dans le but

d'accélérer la convergence de l'algorithme au fil des changements du problème. Cependant, ces techniques ne sont utiles que si les changements ne sont pas drastiques (i.e. la fonction objectif ne doit pas être complètement transformée après un changement). Enfin, des techniques cherchant à prédire les futurs changements dans la fonction objective ont vu le jour récemment. Elles nécessitent toutefois que les changements suivent un certain schéma, pouvant être appris. [**25**]

4.3. Définition de la fonction objective et les contraintes relatives

4.3.1 Expression générale de la fonction objective

Résoudre un problème d'optimisation consiste à rechercher, parmi un ensemble de solutions qui vérifient des contraintes données, la ou les solutions qui rendent minimale (ou maximale) une fonction mesurant la qualité de cette solution. Cette fonction est appelée *fonction objective*. Pour modéliser un problème d'optimisation, on commence en générale par définir les éléments qui composent les contraintes et la fonction objective. Parmi ces éléments, certains sont connus et sont appelés *paramètres du problème* et d'autres éléments sont inconnus et appelés *inconnus* ou *variables*. Les contraintes et la fonction objective s'expriment à l'aide de formules mathématiques qui combinent les paramètres connus et les variables du problème. Les variables correspondent souvent à des décisions à prendre de manière à obtenir l'optimum souhaité [**10**].

La fonction objective qui sera utilisée pour l'optimisation du taux de déclenchement intempestif du système d'arrêt d'urgence ESD modélisé et évalué au niveau du chapitre précédent est issue de l'approche binomiale, elle peut en effet être utilisée d'une manière effective au niveau de la procédure d'optimisation présentée dans la suite de ce chapitre :

$$\text{STR (KooN)} \approx A_N^K \cdot \lambda_{Sind}^K \cdot \left[\prod_{i=1}^{K-1} \text{MDTS}_i\right] + \left[\beta\,\lambda_{SU} + \beta_D\,\lambda_{SD}\right] \quad (4.1)$$

Avec:

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

$\lambda_S = \lambda_{SU} + \lambda_{SD}$

$\lambda_{Sind} = (1-\beta_{SU})\,\lambda_{SU} + (1-\beta_{SD})\,\lambda_{SD}$

$MDTS_{1ooi} = \frac{\lambda_{SU}}{\lambda_S} \cdot \left(\frac{T_1}{i+1} + MTTR_{SD}\right) + \frac{\lambda_{SD}}{\lambda_S} \cdot MTTR_{SD}$

T_1 : durée entre deux tests périodiques.

$MTTR_{SD}$: durée moyenne de réparation d'une défaillance sûre (détectée).
Pour déterminer l'expression du STR relatif au système d'arrêt d'urgence ESD (STR_{ESD}), on va appliquer l'approche présentée dans la formule (4.1) sur l'expression suivante :

$$STR_{ESD} \approx STR_{Si} + STR_{LS} + STR_{FE} \quad (4.2)$$

Avec :

STR_{Si} Taux de déclenchement intempestif du sous-système *capteurs*,

STR_{LS} Taux de déclenchement intempestif du sous-système *unité logique*,

STR_{FE} Taux de déclenchement intempestif du sous-système *éléments finaux.*

Selon les résultats trouver dans le chapitre précédent (Section 3.4.2), l'expression précédente sera simplifiée comme suit :

$$STR_{ESD} \approx STR_{Si} + STR_{LS} \quad (4.3)$$

Le STR_{Si} est déterminé comme suit :

$$STR_{Si} = 7\ STRsi_{(1001)} + 12\ STRsi_{(2002)} + 2\ STRsi_{(1003)} \quad (4.4)$$

Après l'application de l'approche binomiale l'expression (4.4) sera détaillée comme suit :

$$STR_{Si} = \frac{8\,\lambda_{SU_{Si}}}{\lambda_{S_{Si}}} A^2\ T_1 + 24A^2 MTTR_{SD} + 6A + 14(\beta_{Si}\,\lambda_{SU_{Si}} + \beta_{D_{Si}}\lambda_{SD_{Si}}) + 7\lambda_{S_{Si}} \quad (4.5)$$

Avec:

$$A = \left[(1 - \beta_{SU_{Si}})\,\lambda_{SU_{Si}} + (1 - \beta_{SD_{Si}})\,\lambda_{SD_{Si}}\right]$$

Le STR_{LS} est déterminé comme suit :

$$STR_{LS} = 3B' + \left(\beta_{LS}\,\lambda_{SU_{Ls}} + \beta_{D_{Ls}}\lambda_{SD_{Ls}}\right) \quad (4.6)$$

$$B' = \left[(1 - \beta_{SU_{Ls}})\,\lambda_{SU_{Ls}} + (1 - \beta_{SD_{Ls}})\,\lambda_{SD_{Ls}}\right]$$

Après la combinaison des expressions (4.5) et (4.6), on obtient l'expression globale du STR_{ESD} sous une fonction linéaire de forme « a T_1 + b » avec :

$$a = \frac{8\lambda_{SU_{Si}}}{\lambda_{S_{Si}}} A^2 \quad (4.7)$$

$$b = 24A^2 MTTR_{SD} + 6A + 14\left(\beta_{Si}\,\lambda_{SU_{Si}} + \beta_{D_{Si}}\lambda_{SD_{Si}}\right) + 7\lambda_{S_{Si}} + 3B' + \left(\beta_{LS}\,\lambda_{SU_{LS}} + \beta_{D_{LS}}\lambda_{SD_{LS}}\right) \quad (4.8)$$

Les paramètres A et B' sont respectivement définie précédemment.

L'application numérique par utilisation des mêmes données de calcul utilisées précédemment, on aura la valeur approximative du STR_{ESD}, tel que : $STR_{ESD} \approx 7.03E\text{-}11\ T_1 + 5.91E\text{-}5$. Selon le planning de maintenance préventive de la

section soufflante, la durée entre deux tests périodiques est fixée de 02 ans, alors T_1= 17520 h et le STR_{ESD} = 6.03 E-5 h^{-1}.

Dans ce qui suit, on va minimiser cette valeur du STR_{ESD} sous un ensemble des contraintes qui seront définies dans la prochaine section.

4.3.2 Définition des contraintes relatives

La valeur du STR estimée a une signification en termes de coûts liés aux pertes de production imputables aux déclenchements intempestifs. Pour ce, les contraintes de l'optimisation du STR sont définie en termes des coûts inspirer d'un modèle appeler "*Coûts du Cycle de vie d'un système (y compris les SIS)*." [**01**].

Le coût opérationnel " *The operating cost* " d'un SIS (C^{OP}) pour une année de fonctionnement inclus le coût des tests périodiques (C^T), les coûts de maintenance préventive (C^{MP}), et les coûts de maintenance corrective (C^{MC}) :

$$C^{OP} = C^{T} + C^{MP} + C^{MC} \quad (4.9)$$

Avec :

$$C_j^T = \sum_i \sum_j \frac{1}{T1} C_{ij}^T N_r B_{ijr} \quad (4.10)$$

$$C_j^{MP} = \sum_i \sum_j \frac{1}{M_{ij}} C_{ij}^{MP} N_r B_{ijr} \quad (4.11)$$

$$C_j^{MC} = 8760 \sum_i \sum_j f_{ij} C_{ij}^{MC} N_r B_{ijr} \quad (4.12)$$

T_1 est la durée entre deux tests périodiques,

M est la fréquence de maintenance qu'on peut la déterminer par le nombre des opérations de maintenance préventive N^{MP} sur la durée T_1,

f_{ij} est la fréquence de réparation donnée par $f_{ij} = \lambda_{ij}^T$ et λ_{ij}^T est le taux de défaillance total.

C_{ij}^T , C_{ij}^{MP}, C_{ij}^{MC} sont des coûts relatifs au chaque sous-système j de type i,

N_r est le nombre de redondances et B_{ijr} est la variable binaire correspondante au nombre r de redondances sélectionnées.

Suite à la mise en œuvre des expressions (4.10), (4.11) et (4.12), on définit les éléments qui composent les contraintes de l'optimisation du STR_{ESD} et on obtient :

$$C_{ESD}^{T} = \frac{1}{TI}(37\ C_{Si}^{T} + 3\ C_{Ls}^{T}) \ \leq \ C_{ESDMAX}^{T} \quad (4.13)$$

$$C_{ESD}^{MP} = \frac{1}{M}(37C_{Si}^{MP} + 3C_{Ls}^{MP}) \leq \ C_{ESDMAX}^{MP} \quad (4.14)$$

$$C_{ESD}^{MC} = 8760\ (37\lambda_{Si}C_{Si}^{MC} + 3\lambda_{Ls}C_{Ls}^{MC} \leq C_{ESDMAX}^{MC} \quad (4.15)$$

C_{ESDMAX}^{T} , C_{ESDMAX}^{MP} et C_{ESDMAX}^{MC} sont des valeurs maximales autorisée pour les coûts des tests périodiques, les coûts de maintenance préventive, et les coûts de maintenance corrective du système d'arrêt d'urgence ESD, elles sont estimées par un expert de terrain suite à une analyse économique en tenant compte plusieurs facteurs à savoir la situation économique de l'entreprise en question tel que:

$$\begin{cases} C_{ESDMAX}^{T} = 8288.712\ €/an \\ C_{ESDMAX}^{MP} = 82887.12\ €/an \\ C_{ESDMAX}^{MC} = 33154.848\ €/an \end{cases}$$

On cherche maintenant l'optimum souhaité $STR_{ESD*} \leq STR_{ESD}$ sous les contraintes : $C_{ESD}^{T} \leq C_{ESDMAX}^{T}$, $C_{ESD}^{MP} \leq C_{ESDMAX}^{MP}$ et $C_{ESD}^{MC} \leq C_{ESDMAX}^{MC}$:

Puisque la fonction globale du STR_{ESD} ainsi que toutes les contraintes précédemment définies sont exprimées en fonction de la durée entre deux tests périodiques T_1, ce variable sera considéré comme une variable de décision et après la résolution d'un ensemble des inégalités on trouve la valeur optimal du T_1 tel que : T_1 = 4940.8 h et la valeur du $STR_{ESD*} \approx 5.94E\text{-}5\ h^{-1}$.

4.4. Conclusion

La satisfaction des objectives de sécurité et de disponibilité d'une installation industrielle moderne pourrait être assuré par des systèmes instrumentés, dans cette optique, le quatrième et dernier chapitre de ce document était consacré à l'optimisation de l'STR d'un SIS choisis comme exemple d'application. Pour ce faire, nous avons d'abord situé d'une manière précise le problème à optimiser : présentation des différents paramètres et variables entrant en jeu. Ensuite, l'équation linéaire basée sur le développement booléenne, choisie pour résoudre ce problème, a été présentée. Nous avons finalement étudié la stratégie d'optimisation de STR basée sur trois types de maintenance : curvative, préventive et de test périodique sur un intervalle de temps donné pour retrouver des solutions qui répondent aux différentes contraintes imposées. Ceci confirme que le choix d'une meilleure stratégie de maintenance préventive planifiée durant des intervalles de test optimal permet de réduire le taux de déclenchement intempestif des SIS à des niveaux qui assure l'amélioration de ses performances.

Conclusion générale

Nous présentons dans cette conclusion générale l'essentiel des travaux réalisés, les difficultés rencontrées ainsi que les perspectives à envisager.

L'objectif de ce travail, rappelons-le, s'agissait d'évaluer quantitativement le taux de déclenchement intempestif (STR : Spurious Trip Rate) d'un système instrumenté de sécurité (SIS) installé dans un processus industriel opérationnel (en phase d'exploitation), par application de la méthode de l'arbre de défaillance. Etant donné que le STR évalué est assez élevé, nous nous somme proposés de le réduire en tenant compte des coûts de maintenance. Ainsi, nous avons posé un problème de minimisation du STR sous un ensemble de contraintes en termes de coûts de maintenance. Ces contraintes impliquent implicitement des stratégies de maintenance qui permet de minimiser le STR à des valeurs adéquates aux seuils prédéfinis par les concepteurs des SIS.

Notons, comme résultat, qu'il est impératif de réduire au maximum possible ce type de déclenchements qui provoquent des pertes préjudiciables pour les industriels. La minimisation de ces déclenchements nécessite l'application de stratégies de maintenance adéquates pour les systèmes instrumentés de sécurité afin d'arriver á un compromis dans la balance ***sécurité - disponibilité.*** Le développement de ces stratégies peut faire l'objet de travaux futurs

Enfin, à noter que les difficultés majeures rencontrées peuvent être résumées d'une part, dans la terminologie liée aux activations intempestives des systèmes instrumentés de sécurité et dans la disponibilité des données pour les calculs, d'autre part.

ANNEXE 1

Exemple d'un dossier de données *"Input Devices"* de la référence *PDS Data Handbook, 2006 Edition*.

Module : Input devices	**PDS Reliability Data Dossier**
Component : Pressure Transmitter, Conventional	
Description The pressure transmitter includes the sensing element, local electronics and the process isolation valves.	***Date of Revision*** 2006-01-27
	Remarks

Recommended Values for Calculation

Total rate	*Coverage*	*Undetected rate*
λ_D = 0.8 per 10^6 hrs	C_D = 0.60	λ_{DU} = 0.3 per 10^6 hrs
λ_{ST} = 0.5 per 10^6 hrs	C_{ST} = 0.50	λ_{STU} = 0.3 per 10^6 hrs
λ_{Crit} = 1.3 per 10^6 hrs	$P_{TIF} = 5 \cdot 10^{-4}$	
	r = 0.3	

Assessment

The failure rate estimate is mainly based on data from OREDA phase III. An insufficient amount of data has been found in OREDA phase IV in order to update this estimate (no data from phase V). The rate of DU failures is estimated assuming a coverage of 60 % (as compared to 90 % in the 2003 handbook). If a higher coverage is claimed, special documentation/verification should be required. The rate of ST failures is estimated assuming a coverage of 50 % (expert judgment).

The P_{TIF} is entirely based on expert judgments. The estimated r is based on reported failure causes in OREDA as well as expert judgments. A summary of some of the main arguments is provided in section 2.4.

Failure Rate References

Overall failure rate (per 10^6 hrs)	*Failure mode distribution*	*Data source/comment*
λ_{Crit} = 1.3	λ_D = 0.8 per 10^6 hrs λ_{DU} = 0.3 per 10^6 hrs λ_{STU} = 0.4 per 10^6 hrs $P_{TIF} = 3 \cdot 10^{-4}$ - $5 \cdot 10^{-4}$ 1)	Recommended values for calculation in 2004-edition. Assumed C_D = 60% 1) For smart/conventional respectively
λ_{Crit} = 1.3	λ_{DU} = 0.1 per 10^6 hrs λ_{STU} = 0.4 per 10^6 hrs $P_{TIF} = 3 \cdot 10^{-4}$ - $5 \cdot 10^{-4}$ 1)	Recommended values for calculation in 2003-edition. Assumed C_D = 90% 1) For smart/conventional respectively

Module : Input devices **Component : Pressure Transmitter, Conventional**		**PDS Reliability Data Dossier**
N/A	**D: N/A** **ST: N/A** ***Observed*** C_D = ***N/A*** C_{ST} = ***N/A***	OREDA phase IV database Data relevant for conventional pressure transmitters. *Filter:* Inv. Equipment class = pressure Sensors AND Inv. Design class = pressure AND Inv. Att. Type process sensor = transmitter AND Inv. Phase = 4 AND (Inv. System = Gas processing OR Oil processing OR Condensate processing) AND Inv. Phase = 4 No. of inventories =21 No. of critical (D or STT) failure =0 Surveillance Time (hours) = 332 784
λ_{Crit} **= 1.5**	**D: 0.64** **ST: 0.64** ***Observed*** C_D ***= 100%*** **(calculated for transmitters having some kind of self-test arrangement only)**	OREDA phase III database, Data relevant for conventional pressure transmitter. Failure criteria: TAXCOD =’PSPR’. AND. FUNCIN=’OP’ .OR ’GP’ No. of inventories = 186 Total no. of failure = 89 Cal. Time= 4 680 1820 hrs *Note! Only failure classified as "critical" are included in the failure rate estimates*.
	λ_{DU} = 0.6 per 10^6 hrs [1)] λ_{DU} = 26 per 10^6 hrs [2)] SFF = 60 % [1)]	Exida: Generic DP/pressure transmitter [1)] In clean service [2)] Impulse line plugging likely
	Fail to obtain signal: 0.83	T-Book: pressure transmitter
	Fail to obtain signal: 0.91	T-Book: pressure difference transmitter/ pressure difference cell

ANNEXE 2

Exemple d'un dossier de données *"Final Elements"* de la référence *PDS Data Handbook, 2006 Edition*.

Module : Final Elements **Component : ESV/XV**	**PDS Reliability Data Dossier**
Description Main valves including actuator. Valve de-energised to close. *Not* including pilot valve	***Date of Revision*** 2006-01-27 ***Remarks*** ESV/XV incl. actuator (ex.pilot)

Recommended Values for Calculation

Total rate	*Coverage*	*Undetected rate*
λ_D = 2.7 per 10^6 hrs	C_D = 0.25	λ_{DU} = 2.0 per 10^6 hrs
λ_{ST} = 2.7 per 10^6 hrs	C_{ST} = 0	λ_{STU} = 2.7 per 10^6 hrs
λ_{Crit} = 5.4 per 10^6 hrs	$P_{TIF} = 1 \cdot 10^{-5}$ (extended functional testing) $= 1 \cdot 10^{-5}$ (standard functional testing) $= 1 \cdot 10^{-3}$ (incomplete test/partial stroke) $r = 0.5$	

Assessment

The failure estimate is an update of the previous estimate in the 2003 handbook. Data from OREDA 2002 and input from operators indicate that the previous failure rate estimate for valves was too optimistic. Furthermore, part (i.e.approx.50%) of the failure rate reported under the sub-unit "control and monitoring" has now been included as part of the valve itself (as opposed to previously when this was all included under the pilot valve-the failure rate for pilot valve has been reduced correspondingly). This has resulted in a higher proportion of safe failures as compared to the previous estimate. It is assumed that the shutdown valves are de-energised to close.

Data from RNNS for the period 2003-2004 for riser ESVs has been reviewed. Assuming annual testing, a $\lambda_{DU} = 3.5 \cdot 10^{-4}$ results (incl. pilot valve). This is somewhat higher than the data given in this handbook ($\lambda_{DU} = 2.9 \cdot 10^{-6}$ for complete ESV including pilot valve).

The coverage factor for D failures have been set to 25%, due to registered detection methods in OREDA IV (i.e. failures detected by other means than "on demand" and during testing contribute towards the coverage factor).

The P_{TIF} values are estimated based on expert judgments. The size of the P_{TIF} will vary depending on the completeness of the functional testing. Here, three (rough) alternatives are indicated, where for the smallest P_{TIF} (*extended functional test*) it is assumed that the test also includes a complete tightness test.

The estimated r is based on reported failure causes in OREDA as well as expert judgments. A summary of some of the main arguments is provided in Section 2.4.

Module : Final Elements **Component : ESV/XV**		**PDS Reliability Data Dossier**
Failure Rate References		
Overall failure rate (per 10^6 hrs)	***Failure mode distribution***	***Data source/comment***
λ_{Crit} = 5.4	λ_D = 2.7 per 10^6 hrs λ_{DU} = 2.0 per 10^6 hrs λ_{STU} = 2.7 per 10^6 hrs $P_{TIF} = 10^{-6} - 10^{-5}$ 1)	Recommended Values for calculation in 2004-edition. Assumed C_D = 25% 1) For complete and incomplete functional testing respectively.
λ_{Crit} = 1.6 **λ_D/λ_{ST} =4.3**	λ_{DU} = 1.3 per 10^6 hrs λ_{STU} = 0.3 per 10^6 hrs $P_{TIF} = 10^{-6} - 10^{-5}$ 1)	Previously recommended values for calculation in 2003-edition. 1) For complete and incomplete functional testing respectively.
14.4	**D: 14.4** **ST: 0.0** ***Observed*** ***C_D = N/A*** 1) ***C_{ST} = N/A*** 1) *Detection method unknown*	OREDA phase V database Data relevant for process ESD/PSD valves, excluding the pilot and control & monitoring. *Filter:* Inv. Equipment class = VALVES AND (Inv. System = Gas export OR Inv. System = Gas processing OR Inv. System = Oil export OR Inv. System = Oil processing OR Inv. System = Emergency shutdown) AND Inv. OREDA Phase =5 AND Inv. Att. Application =ESD/PSD AND (Fail. Item Failed <> Pilot valve AND Fail. Subunit Failed <> Control & Monitoring) AND Fail. Severity class = critical No. of inventories = 8 No. of critical D failure = 2 No. of critical ST failure = 0 Surveillance Time (hours) = 140 160 …

Bibliographies

[**01**] A.C. Torres-Echeverría, *Modelling and Optimization of Safety Instrumented Systems Based on Dependability and Cost Measures*. PhD - theses; 2009.

[**02**] A.C. Torres-Echeverría, S. Martorell and H.A Thompson. *Design optimization of a safety-instrumented system based on RAMS+C addressing IEC61508 requirements and diverse redundancy*. Reliability Engineering and System Safety, 94, p.162-179; 2009.

[**03**] A. Desroches, *Concepts et méthodes probabilistes de base de la sécurité*. Lavoisier; France; 1995.

[**04**] A.E. Summers, *Viewpoint on ISA TR84.0.02 — simplified methods and fault tree analysis.* ISA Transaction 2000; 39:125–131; 2000.

[**05**] A. MKHIDA, *Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'Intelligence*. Thèse de Doctorat de l'Institut National Polytechnique de Lorraine ; 2008.

[**06**] A. Rauzy, Y.Dutuit, and Signoret, J.-P, *Assessment of safety integrity levels with fault trees*. In *ESREL Estoril*, Portugal; 2006.

[**07**] A. Villemeur, *Evaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : la méthode de l'Espace des Etats*. Eyrolles, Paris, France; 1987.

[**08**] A. Villemeur, *Sûreté de fonctionnement des systèmes industriels*. Eyrolles, Paris, France ; 1988.

[**09**] Center for Chemical Process Safety, CCPS, *Guidelines for safe and reliable instrumented protective systems*. Wiley & Sons, Inc., Hoboken, New Jersey; 2007.

[**10**] Clementina Ramírez-Marengo, Julio de Lira-Flores, Antioco López-Molina, Richart Vázquez-Román, Victor Carreto-Vázquez, M. Sam Mannan A formulation to optimize the risk reduction process based on LOPA. Journal of Loss Prevention in the Process Industries 489 – 494 2013

[**11**] Djebabra M., & Saadi S., 1999b, « *Méthodologie d'étude de sûreté de fonctionnement des systèmes : analyse des défaillances* ». Phoebus la revue de la sûreté de fonctionnement. N°12 (**1999**), pp. 24-32.

[**12**] Dutuit.Y, F. INNAL et G. DECONINCK, *étude complémentaire des systèmes instrumentés de sécurité - Rapport TOTAL 2009_version finale,* l'ADERA (Association pour le Développement de l'Enseignement et des Recherches auprès des universités, des centres de recherche et des entreprises d'Aquitaine), 2009.

[**13**] EN 50126, *Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS)*; 1999.

[**14**] EN 50128, *Railway applications. Communications, signaling and processing systems. Software for railway control and protection systems;* 2001.

[**15**] EN 50129, *Safety related electronic systems for signaling;* 1998.

[**16**] F. INNAL, *Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508,* Thèse de Docteur de L'Université BORDEAUX 1 ; 2008.

[**17**] F.R Farmer, *Sitting criteria: a new approach.* Atom,1967.

[**18**] ISA-TR84.00.02. *Safety instrumented functions (SIF)-safety integrity level (SIL) Evaluation techniques part3: Determining the SIL of a SIF via Fault tree Analysis* Technical Report, Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society; 2002.

[**19**] ISA-TR84.00.02. *Safety instrumented functions (SIF)-safety integrity level (SIL) Evaluation techniques part 4: Determining the SIL of a SIF via Markov analysis.* Technical Report, Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society; 2002.

[**20**] ISA-TR84.00.02. *Safety instrumented functions (SIF)-safety integrity level (SIL) Evaluation techniques part2: Determining the SIL of a SIF via Simplified Equations*. Technical Report, Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society; 2002.

[**21**] ISO/CEI Guide 51, *Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes.* Organisation internationale de normalisation (ISO); 1999.

[**22**] ISO/CEI Guide 73. *Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes.* Organisation internationale de normalisation (ISO) ; 2002.

[**23**] J.D. Andrews, L.M. Bartlett, *A branching search approach to safety system design optimisation.* Reliability Engineering and System Safety 2005; 87: 23–30.

[**24**] Jean Héng, DUNOD 2002, *« Pratique de la maintenance préventive »*

[**25**] J.LEPAGNOT, Conception de *métaheuristiques* pour l'optimisation dynamique. Application à l'analyse de séquences d'images IRM. Thèse de doctorat en informatique de l'université Paris-Est, 2011.

[**26**] J. L. Le Moigne, *La théorie du système général – Théorie de la modélisation. PUF*, Paris, France.7 ; 1984.

[**27**] KENEXIS. *Safety Instrumented Systems Engineering Handbook*; Kenexis Consulting Corporation – Columbus, OH; 2010.

[**28**] *Layer of protection analysis; simplified process assessment;* center for chemical process safety of the American institute for chemical Engineers; New York; 2001.

[**29**] L. Lu, J Jiang. *Analysis of on-line maintenance strategies for k-out of-n standby safety systems.* Reliability Engineering and System Safety 2007; 92: 144–55.

[**30**] M.A. Lundteigen, et M. Rausand, *Spurious activation of safety instrumented systems in the oil and gas industry: basic concepts and formulas*. Reliability Engineering and System Safety, 93:1208–1217; 2008.

[**31**] M.A Lundteigen, *Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation*. PHD-theses at NTNU; 2008.

[**32**] Mihalache A.G., 2007, « Modélisation et évaluation de la fiabilité des systèmes mécatroniques : application sur système embarque », Thèse de doctorat à l'école doctorale d'ANGERS.

[**33**] M.J.M Houtermans, Spurious *Trip Levels-How To Design Plants That are Safe and Do Not Trip*, (White Paper). RISKNOWLOGY GmbH, Zug, Switzerland; 2006.

[**34**] Mitsubishi Heavy Industries, LTD. MCEC (REV: 0) *Plant Operation Manual / Volume-1 and 2*; 2004.

[**35**] Mitsubishi Heavy Industries, LTD. MCEC (REV: 3), *DESIGN BASIS;* 16 apr. 2003.

[**36**] M. Rausand, et A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition; 2004.

[**37**] M. Sallak. *Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité*. Thèse de Doctorat de l'Institut National Polytechnique de Lorraine ; 2007.

[**38**] Norme CEI 61508, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité* – Parties 1 à 7, octobre 1998-2000. *Commission Electrotechnique Internationale*, Genève, Suisse.

[**39**] Norme CEI 61511, *Sécurité fonctionnelle - Systèmes instrumentés de sécurité pour le domaine de la production pour processus* – Parties 1 à 3, janvier 2003-juillet 2003. *Commission Electrotechnique Internationale*, Genève, Suisse.

[**40**] Norme CEI 61513, *Centrales nucléaires : Instrumentation et contrôle commande des systèmes importants pour la sureté, Prescriptions générales pour les systèmes. Commission Electrotechnique Internationale*, Genève, Suisse; 2001.

[**41**] OHSAS 18001, *Système de management de la santé et de la sécurité au travail* – Spécification. BSI, AFNOR; 2007.

[**42**] Pagès, A. & Gondran, M. 1980, « *Fiabilité des systèmes* », Eyrolles, Paris.

[**43**] P. Hokstad, and K. Corneliussen, *Reliability Prediction Method for Safety Instrumented Systems; PDS Method Handbook, 2003 Edition*. SINTEF Report STF38 A 02420, SINTEF, Trondheim, Norway; 2003.

[**44**] Rudall Blanchard Associates (REV : 1), *Etude d'Impact Environnemental RGTE* ; 2005.

[**45**] Rudall Blanchard Associates (VER : 1), *Etude de Dangers de Projet RGTE ;* 2005.

[**46**] S. Cho, J. Jiang, *Analysis of surveillance test interval by Markov process for SDS1 in CANDU nuclear power plants*. Reliability Engineering and System Safety, in press, doi: 10.1016/j.ress.2006.10.007; 2006.

[**47**] S.HADDAD, *Evaluation et Optimisation des Performances des Systèmes Instrumentés de Sécurité pour une Meilleure Maîtrise des Risques*. Mémoire de Magister de l'université Hadj Lakhdar de Batna ; 2012.

[**48**] SINTEF. *Reliability prediction methods for safety instrumented systems,PDS method handbook.* 2006 edition; 2006.

[**49**] SINTEF. *Reliability Data for safety instrumented systems, PDS Data handbook*. 2006 edition ; 2006.

[**50**] S. Sklet. *Safety barriers: Definitions, classification and performance. Journal of Loss Prevention in the process industries*, vol 19, pp 494-506; 2005.

[**51**] W. MECHRI. *Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis*, Thèse de Docteur de L'Université de Tunis El Manar ; 2011.

[**52**] Yann Dijoux., 2008, *« Modèles d'âge virtuel et de risques concurrents pour la maintenance imparfaite* », Thèse de doctorat, INSTITUT POLYTECHNIQUE DE GRENOBLE.

[**53**] YOKOGAWA*: Distributed Control System (DCS) graphic display plan*, Mitsubishi Heavy Industries, LTD. MCEC (REV: 2); 2003.

[**54**] Zwingmann X., 2005, *« Modèle d'évaluation de la fiabilité et de la maintenabilité au stade de la conception* », Thèse de doctorat, Université LAVAL, QUÉBEC.

Résumé :

L'objectif principal des systèmes instrumentés de sécurité (SIS) est de maintenir un état de sécurité d'une installation ou d'un équipement si les événements dangereux se produisent, mais dans certains cas, et même en absence de ces derniers, les SIS peuvent être activés d'une manière intempestive. Ces activations sont caractérisées en terme de fréquence par un taux de déclenchement intempestif (STR : *spurious trip rate*). Dans ce mémoire, nous avons présenté les concepts et définitions relatifs aux activations intempestives des SIS, discuté leurs causes et leurs effets puis nous avons présenté une synthèse des formules analytique pour évaluer le taux de déclenchement intempestif selon différentes approches de la littérature. Ce taux est modélisé et évalué pour un SIS installé dans un processus industriel opérationnel (en phase d'exploitation), par application de la méthode de l'arbre de défaillance. Etant donné que le STR évalué est assez élevé, nous avons proposé de le réduire en tenant compte des coûts de maintenance. Ainsi, nous avons posé un problème de minimisation du STR sous un ensemble de contraintes en termes de coûts de maintenance. Ces contraintes impliquent implicitement des stratégies de maintenance qui permet de minimiser le STR à des valeurs adéquates aux seuils prédéfinis par les concepteurs des SIS.

Mots clés : Systèmes Instrumentés de Sécurité, Activation Intempestive, Taux de Déclenchement Intempestif STR, Coûts de Maintenance, Minimisation du STR.

الملخص:

إن الهدف الأساسي من أنظمة السلامة المجهزة (**Système Instrumenté de Sécurité SIS**) هو الحفاظ على الحالة الآمنة للأجهزة أو المعدات في حالة وقوع أحداث خطيرة، لكن في بعض الأحيان، و حتى في حالة عدم وقوع هذه الأخيرة، يمكن تفعيل هذه الأنظمة بطريقة زائفة. ويتميز هذا التفعيل رياضيا بتواتر يعرف بمعدل التنشيط الزائف (**Taux de déclenchement intempestif STR**). في هذه المذكرة، قدمنا المفاهيم والتعاريف المتعلقة بالتفعيلات الزائفة لأنظمة السلامة المجهزة ، وناقشنا أسبابها وآثارها ومن ثم قدمنا ملخصا لصيغ تحليلية لتقييم معدلات التنشيط الزائف حسب المناهج الموجودة في هذا المجال. قمنا بعد ذلك بنمذجة و تقييم معدل التنشيط الزائف لنظام (**SIS**) موجود في وحدة صناعية في مرحلة الاستغلال بواسطة طريقة ' شجرة الأعطاب'. و بما أن المعدل المقيم مرتفع نسبيا، قمنا باقتراح تخفيضه مع أخذ بعين الاعتبار تكاليف الصيانة. وهكذا طرحنا مشكلة تخفيض معدل التنشيط الزائف (**STR**) تحت مجموعة قيود ضمن تكاليف الصيانة. هذه القيود تحتوي ضمنيا على استراتيجيات صيانة تعمل على تخفيض معدل التنشيط الزائف (**STR**) إلى قيم تتناسب و العتبات المحددة مسبقا من قبل مصممي أنظمة السلامة المجهزة (**SIS**).

المصطلحات الأساسية: أنظمة السلامة المجهزة، التفعيلات الزائفة، معدل التنشيط الزائف، تكاليف الصيانة، تخفيض معدل التنشيط الزائف.