الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole Nationale Supérieure de Technologie

Département : Génie électrique Et Informatique Industrielle

Mémoire de Master en **Automatique**

Spécialité

Automatique et informatique industrielle

Contribution à l'évaluation de la sûreté de fonctionnement de la vanne de Sécurité de la station de forage de l'usine HAMMOD BOUALEM

Réalisé par

HAMDI Hamza
OUAGUINI Abdelhadi

Présenté et soutenu publiquement le (06/07/2023)

Composition du Jury :

Président	Mme BELHACHAT Faiza,	M.C.A	ENST
Promoteur	M. DERMOUCHE Redha,	M.A.A	ENST
Examinateur	Mme BENDOUDA Djamila,	M.C.B	ENST
Examinateur	Mme DROUICHE Imane,	M.C.B	USTHB

Année universitaire 2022 –2023

Remerciements

Louanges à Allah le Tout Puissant.

Qu'Il nous pardonne et nous guide vers le droit chemin.

Nous tenons tout d'abord à exprimer notre gratitude à notre encadrant Mr DERMOUCHE Reda, et Mr ARAFA mustapha (hamoud boualem) pour son précieux soutien, ses conseils avisés et sa disponibilité tout au long de ce projet. Sa grande expertise dans le domaine de l'automatisme a été une source d'inspiration et d'enrichissement pour nous deux.

Nous souhaitons exprimer notre reconnaissance à nos parents, nos familles et nos amis, pour leur soutien indéfectible, leur encouragement et leur confiance en nous. Leur amour et leur soutien inconditionnel ont été une source de motivation tout au long de ce projet.

Nous remercions les membres du jury d'avoir donné de leur temps afin d'examiner cet humble travail.

Nous tenons aussi à remercier l'ensemble du corps professoral et administratif de l'École Nationale Supérieure de Technologie pour la richesse et la qualité de leur enseignement et les grands efforts qu'ils ont déployés pour assurer à leurs étudiants une formation actualisée.

Enfin, merci à toutes celles et ceux qui nous ont aidés dans l'accomplissement de ce mémoire.

Table des matières

Liste des figures I
Liste des tableaux II

Introduction générale **1**

I Introduction aux Systèmes Instrumentés de Sécurité (SIS) **3**
I.1 Introduction 3
I.2 Problématique et objectif 3
I.3 L'instrumentation intelligente 4
I.3.1 Concept d'instrument intelligent 4
I.3.2 Constituants de l'architecture matérielle pour un instrument intelligent 5
I.3.3 Systèmes d'automatisation à intelligence distribuée 5
I.3.4 Evolution des SAP vers les SAID 6
I.4 Systèmes Instrumentés de Sécurité (SIS) 7
I.4.1 Introduction 7
I.4.2 Architecture 1oo1 d'un SIS 7
I.4.3 Normes relatives aux systèmes instrumentés de sécurité 8
I.4.4 Norme CEI 61511 8
I.5 Vers une sécurité intelligente 8
I.6 Systèmes Instrumentés de Sécurité à Intelligence Distribuée 9
I.7 Conclusion 9

II L'évaluation de la sûreté de fonctionnement des SISID **10**
II.1 Introduction 10
II.2 Probabilité de défaillance dangeurese (PFD) 10
II.3 Probabilité de défaillances en sécurité(PFS) 11
II.4 Diagramme de Venn 11
II.5 Evaluation des performances du SIS classique et SISID 12
II.6 Niveaux d'intégrité de sécurité 14
II.7 Conclusion 15

III Simulation et résultats **16**
III.1 Introduction 16
III.2 Le logiciel GRIFF 16
III.3 Intégration de la carte STM32 pour transformer la vanne de production en un instrument intelligent (SISID) 19
III.4 Conclusion 20

Liste des figures

Fig. I.1 La vanne de production de l'unité de forage 4
Fig. I.2 Architecture matérielle d'instruments intelligents 6
Fig. I.3 Evolution des systèmes d'automatisation 6
Fig. I.4 Système instrumenté de sécurité(Architecture 1oo1) 7
Fig. I.5 Norme CEI 61508 et normes dérivées 8
Fig. I.6 Systèmes Instrumentés de Sécurité à Intelligence Distribuée (Architecture 1oo1s 9

Fig. II.1 Système avec modes de défaillance 11
Fig. II.2 Effet d'autodiagnostic sur le système instrumenté de sécurité 11
Fig. II.3 Conception hiérarchique du SISID 12
Fig. II.4 Proportion de défaillance 13

Fig. III.1 Simulation de SIS architecture 1oo1 16
Fig. III.2 Courbe PFD pour les SIS 17
Fig. III.3 Courbe PFD pour les SISID 18
Fig. III.4 Courbe PFD pour les SISID améliorés 19
Fig. III.5 La carte STM32 20

Liste des tableaux

Tab II.1 Données relatives aux constituants du SIS 12
Tab II.2 Taux de défaillances dangereuses et en sécurité 12
Tab II.3 Probabilité de défaillance dangereuse pour l'architecture 1oo1 SIS . . . 13
Tab II.4 Probabilité de défaillances en sécurité pour l'architecture 1oo1 SIS . . 14
Tab II.5 Probabilité de défaillance dangereuse pour l'architecture 1oo1 SISID . 14
Tab II.6 Probabilité de défaillance en sécurité pour l'architecture 1oo1 SISID . . 14
Tab II.7 Niveau d'intégrité de sécurité : Probabilité moyenne de défaillance . . 15

Acronymes

API *Automate Programmable industriel*

CPU *Central Processing Unit*

PFD *Probability of Failure on Demand*

ASIC *Application Specific Integrated Circuit*

PFS *Probability of Failure to Safe*

SIF *Safety Instrumented Function*

SIL *Safety Integrity Level*

Introduction générale

Dans ces derniers temps l'informatique industrielle a connu une croissance remarquable grâce aux développements de la microélectronique, cela a entraîné une véritable révolution technologique caractérisée par une réduction des coûts, des améliorations significatives des performances, une augmentation de la vitesse, une consolidation des composants et une augmentation de la capacité de stockage. Les entreprises modernes ont rapidement compris les avantages de l'échange électronique de données, qui est devenu un aspect indispensable des environnements industriels. Ainsi, les techniques numériques ont migré vers les composants les plus proches des processus industriels, à savoir les capteurs et les actionneurs. Ces derniers intègrent désormais des microcontrôleurs et des interfaces de communication, permettant ainsi un traitement local de l'information réparti sur différentes entités. Cette approche favorise une distribution de l'exécution des tâches et donne naissance à une commande distribuée.

Le développement des réseaux de terrain a joué un rôle clé dans la réalisation du traitement local. Ces réseaux facilitent le partage des ressources en interconnectant les éléments de traitement, réduisant ainsi le besoin de câblage complexe. Cependant, l'interconnexion d'instruments intelligents dans un réseau présente des défis uniques pour l'informatique distribuée. Parmi ces défis, on peut citer la synchronisation, le partage des ressources, la communication, ainsi que les problématiques propres au domaine de l'automatisation, telles que le respect des contraintes temporelles, la définition des scénarios de contrôle, la supervision, la fusion des données, le fonctionnement en mode dégradé et la planification des actions. Un instrument intelligent fait donc partie intégrante d'un système automatisé à intelligence distribuée. Il est doté de fonctionnalités de communication, de configuration, d'autodiagnostic et de validation, en plus de ses capacités de mesure ou d'action. Typiquement, il comprend un processeur ou un microcontrôleur ainsi qu'une interface de communication vers un réseau (généralement un réseau de terrain). Son logiciel peut implémenter des fonctionnalités allant du simple traitement du signal aux méthodes de l'intelligence artificielle. Les instruments intelligents sont connectés en réseau à un système central, tel qu'un ordinateur ou un automate programmable. Il est également possible de créer des applications complètes constituées uniquement d'instruments intelligents interconnecté.

Notre travail se divise en trois chapitres :

Chapitre I : Le premier chapitre sert d'introduction aux Systèmes Instrumentés de Sécurité (SIS). Nous y avons présenté les concepts fondamentaux et la problématique liée à la sécurité industrielle, ainsi que les définitions clés relatives aux SIS.

Chapitre II : Le deuxième chapitre est consacré à l'évaluation des SIS et aux différentes

méthodes utilisées pour cette évaluation. Nous avons exploré les mesures de performance telles que la Probabilité de Défaillance sur Demande (PFD) et le niveau d'Intégrité de Sécurité (SIL). Nous avons également étudié les méthodes d'analyse de fiabilité et les approches utilisées pour calculer les performances des SIS.

Chapitre III : Le dernier chapitre , nous avons réalisé une simulation pour confirmer nos études antérieures. Cette simulation a permis de démontrer de manière concrète les avantages d'un dispositif autodiagnostique dans l'amélioration de la sécurité d'un système, en augmentant son niveau SIL conformément aux normes de sécurité. Cette étape a renforcé notre compréhension des effets positifs de l'ajout de dispositifs autodiagnostiques sur la fiabilité et la performance des SIS.

Chapitre I

Introduction aux Systèmes Instrumentés de Sécurité (SIS)

I.1 Introduction

Dans ce premier chapitre, nous amorçons notre exploration des Systèmes Instrumentés de Sécurité (SIS), un domaine essentiel dans de nombreux secteurs industriels. Les SIS jouent un rôle crucial en garantissant la sécurité des processus industriels et en minimisant les risques liés aux accidents majeurs

I.2 Problématique et objectif

Pendant notre stage dans le cadre de notre projet de fin d'études à Hamoud Boualam, nous avons remarqué une problématique récurrente liée à une vanne de production. Malgré la présence de capteurs d'ouverture et de fermeture qui sont censés indiquer l'état de la vanne, nous avons constaté à plusieurs reprises un dysfonctionnement lors de son ouverture ou de sa fermeture.

Ce problème représente une préoccupation majeure pour la sécurité et le bon fonctionnement du système dans lequel la vanne est intégrée. En effet, une mauvaise ouverture ou fermeture de la vanne peut entraîner des conséquences graves telles que des fuites, des perturbations dans les processus en cours ou même des accidents potentiels.

Face à cette problématique, nous avons proposé une solution visant à étudier et contribuer à l'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité intégrant de l'intelligence. Notre objectif est de concevoir un Systèmes Instrumentés de Sécurité qui permettra de prévenir ce genre de problème lié à la vanne et sera capable d'analyser les données fournies par les capteurs d'ouverture et de fermeture de la vanne, ainsi que d'autres variables pertinentes, afin de détecter les anomalies et les comportements déviants.

Pour cela nous allons développer des stratégies de sécurité adaptatives qui permettront d'agir de manière préventive pour éviter ces dysfonctionnements. Cela pourrait inclure des actions telles que des alertes en temps réel, des ajustements automatiques des paramètres de la vanne ou même des procédures de maintenance préventive L'objectif ultime de notre étude et contribution sera d'améliorer la fiabilité et la sécurité des systèmes instrumentés de

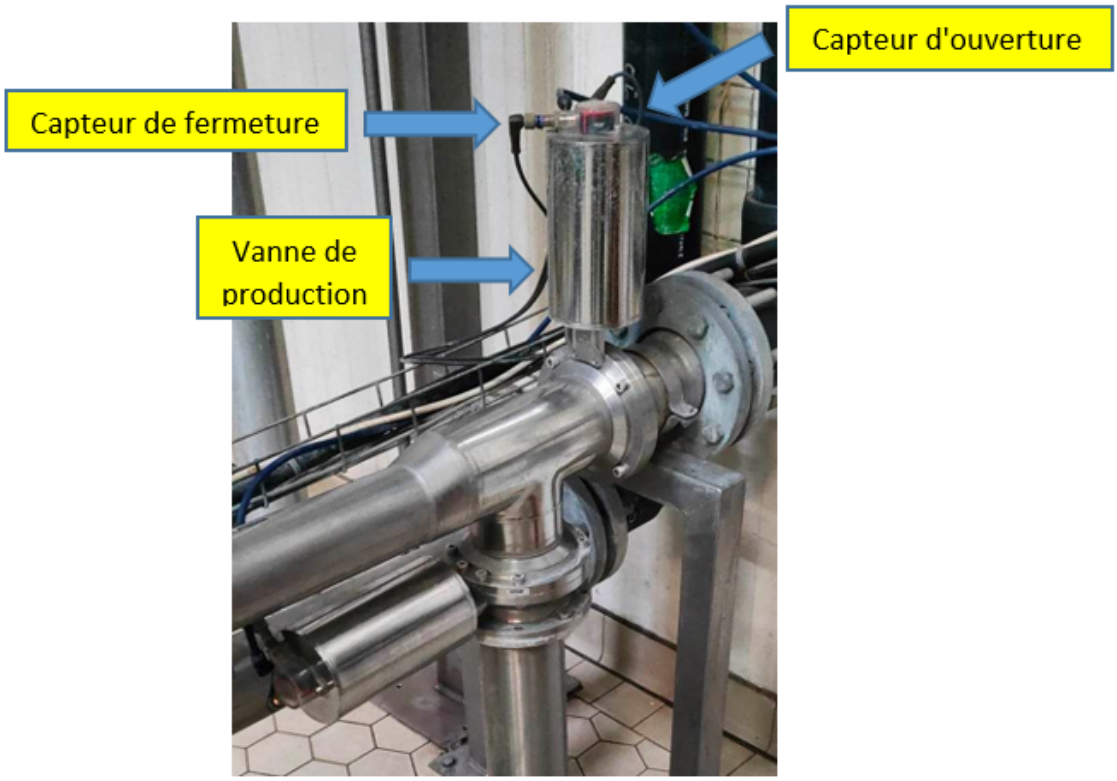


Fig. I.1 – La vanne de production de l'unité de forage

sécurité, en intégrant de l'intelligence pour prévenir les problèmes liés à l'ouverture et à la fermeture de cette vanne. Nous espérons ainsi minimiser les risques potentiels, assurer le bon fonctionnement des processus industriels et garantir la protection des personnes et de l'environnement.

I.3 L'instrumentation intelligente

I.3.1 Concept d'instrument intelligent

Un instrument intelligent est un dispositif résultant de l'association de l'instrumentation, de l'électronique et de l'informatique, qu'il s'agisse d'un capteur ou d'un actionneur. Il intègre des fonctionnalités supplémentaires telles que la validation, l'autodiagnostic, la communication, la compensation, etc. Ces instruments sont capables de s'adapter aux changements survenant dans leur environnement. Leur ensemble de fonctionnalités leur confère une crédibilité dans leur fonction au sein d'un système distribué. La validation de la mesure pour les capteurs et le compte-rendu de l'action réalisée par les actionneurs reflètent cette crédibilité, tandis que la participation dans un système distribué se manifeste par leur contribution à la commande, à la sécurité (alarmes), et à l'exploitation du système.Un instrument intelligent est défini comme un instrument dont le principal objectif est la mesure ou la commande d'une variable de processus, et qui inclut de la flexibilité dans son utilisation avec des paramètres réglés par le fabricant ou l'opérateur.Le cycle de vie d'un instrument intelligent comprend la production de progiciels spécifiques générés par le fabricant et utilisés pour la configuration par l'opérateur.

En résumé, un instrument intelligent, utilisé dans les systèmes d'automatisation industrielle, est un dispositif doté de fonctionnalités avancées, telles que la communication, la configuration, l'autodiagnostic et la validation, en plus de ses capacités de mesure ou d'action de base. Il intègre des technologies provenant de l'instrumentation, de l'électronique et de l'informatique, lui permettant de traiter localement les informations et de prendre des décisions en fonction des données reçues. Ces instruments sont connectés à un système central via un réseau de communication, facilitant ainsi la supervision, la commande et la gestion des processus industriels de manière plus efficace et précise[1].

I.3.2 Constituants de l'architecture matérielle pour un instrument intelligent

L'architecture matérielle d'un instrument intelligent, qu'il s'agisse de capteurs ou d'actionneurs, est basée sur un système à microprocesseur qui assure une communication constante avec les différents composants via un bus interne. Cette architecture dépend de l'application et de l'environnement de communication, et peut être associée à des robots ou à des automates programmables. L'instrument intelligent comprend les éléments suivants :

1- Un élément de sensation : Il relie le monde extérieur au système de capteur en générant un signal électrique en réponse aux propriétés physiques de l'environnement telles que la température, la pression, la lumière, le son, la vibration, etc.
2- Un élément d'interface : Il conditionne le signal et le convertit en données numériques avant de le transférer à l'élément de traitement.
3- Un élément de traitement : Il comprend un microcontrôleur avec une mémoire associée et un logiciel. C'est la composante principale de l'architecture où le signal entrant est traité.
4- Un élément de communication : Il permet une communication bidirectionnelle entre l'élément de traitement et les utilisateurs.
5- Une source d'alimentation : Elle fournit l'énergie nécessaire au fonctionnement de l'instrument intelligent.

Cette architecture matérielle d'un instrument intelligent présente des similarités avec celle d'une machine informatique classique. L'instrument peut être considéré comme une entité offrant des services, manipulant des variables et faisant appel à un ensemble de ressources pour les utilisateurs externes[2].

I.3.3 Systèmes d'automatisation à intelligence distribuée

Les systèmes d'automatisation à intelligence distribuée sont composés de capteurs et d'actionneurs intelligents, également appelés instruments intelligents. Ces instruments jouent un rôle essentiel aux côtés des systèmes de communication, formant ainsi les éléments fondamentaux des systèmes d'automatisation à intelligence distribuée (SAID). Ils se distinguent par leur capacité à traiter localement les données, offrant ainsi des fonctionnalités étendues au-delà de leurs fonctions de base, à savoir la mesure pour les capteurs et l'action pour les actionneurs. L'intelligence des instruments se manifeste par leur capacité de traitement local, qui leur permet d'effectuer des opérations avancées telles que la validation, l'autodiagnostic, la compensation et bien d'autres. Ces fonctions supplémentaires ajoutent de la valeur aux mesures effectuées par les capteurs et aux actions réalisées par les actionneurs. Les ins-

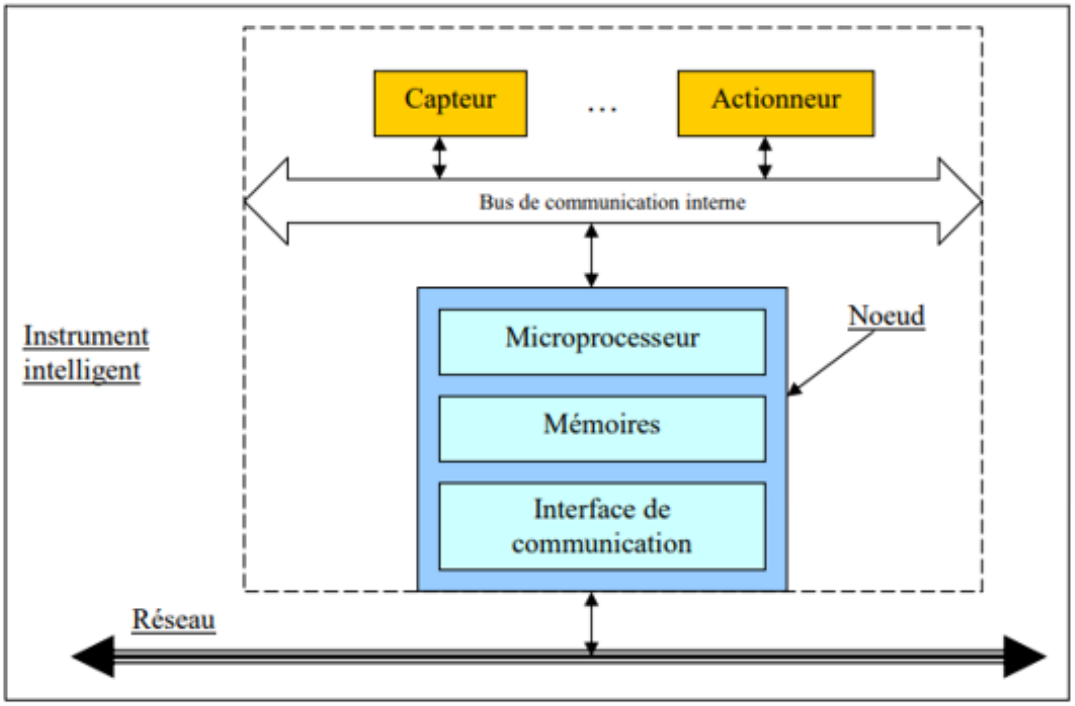


Fig. I.2 – Architecture matérielle d'instruments intelligents

truments intelligents ne se limitent donc pas à la simple collecte de données ou à l'exécution d'actions, mais ils contribuent également à la prise de décisions, à la sécurité et à l'efficacité globale des systèmes d'automatisation.

I.3.4 Evolution des SAP vers les SAID

Au fil des années, les systèmes d'automatisation programmables (SAP) ont connu une évolution remarquable pour devenir des systèmes d'automatisation à intelligence distribuée (SAID). Cette transition s'est appuyée sur les progrès technologiques dans les domaines de l'informatique, de l'électronique et des communications[3].

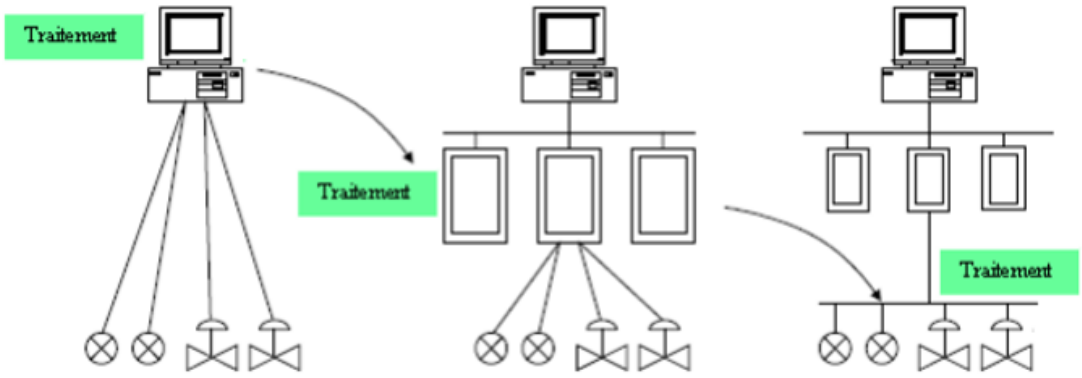


Fig. I.3 – Evolution des systèmes d'automatisation

En résumé, les systèmes d'automatisation à intelligence distribuée sont des systèmes dans

lesquels les décisions sont prises de manière distribuée entre plusieurs unités autonomes, tandis que les systèmes automatisés de production sont des systèmes qui utilisent des machines et des équipements automatisés pour produire des biens.

I.4 Systèmes Instrumentés de Sécurité (SIS)

I.4.1 Introduction

Les Systèmes Instrumentés de Sécurité (SIS) sont mis en place dans les systèmes automatisés afin de prévenir les risques pour les individus, l'environnement et les biens. Ils jouent un rôle essentiel en contribuant à la prévention et à la protection contre les dysfonctionnements pouvant entraîner des conséquences graves. Les SIS sont des moyens de sécurité qui surveillent les procédés industriels et veillent à ce qu'ils ne dépassent pas certaines limites critiques. Lorsqu'un danger potentiel est détecté, les SIS activent les dispositifs de sécurité correspondants pour éviter tout accident ou dommage. Ces systèmes sont conçus pour exécuter des fonctions de sécurité dans les industries de production par processus. Ils garantissent que les procédés industriels fonctionnent dans des conditions sûres en empêchant tout dépassement des seuils de sécurité prédéfinis. L'objectif des SIS est de réduire les risques liés aux systèmes automatisés, en minimisant les conséquences des défaillances ou des situations dangereuses. Ils assurent une protection supplémentaire en complément des mesures préventives déjà en place. La conception et la mise en œuvre des SIS nécessitent une évaluation des risques associés aux procédés industriels, ainsi que la détermination des fonctions de sécurité requises. Il est essentiel de s'assurer que les SIS sont capables de répondre aux objectifs de sécurité préalablement définis et de maintenir les procédés dans un état sûr.

I.4.2 Architecture 1oo1 d'un SIS

Cette architecture comprend un seul canal et donc un seul chemin matériel que peut parcourir un signal dans la chaîne de traitement d'une demande. Généralement, pour une architecture MooN, le premier chiffre désigne le nombre d'éléments que l'on doit avoir en état de marche pour que le système assure la fonction de sécurité et le second chiffre indique le niveau de redondance.

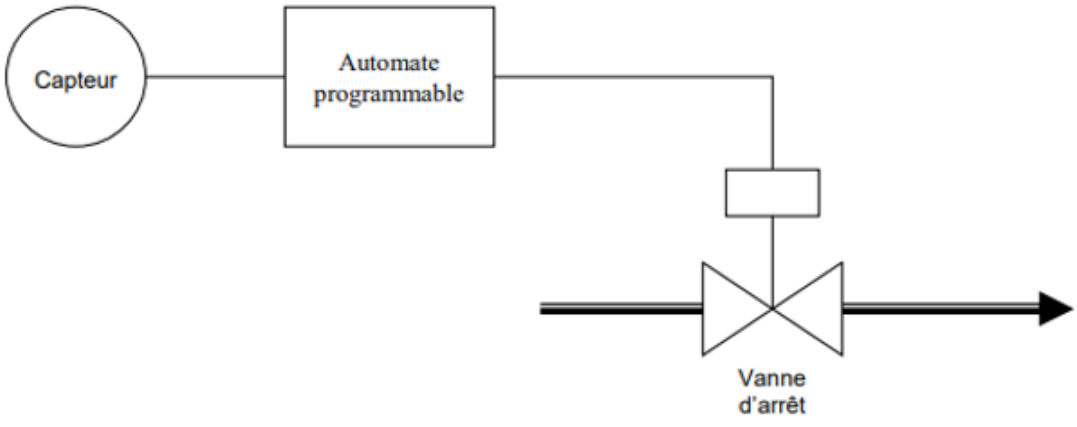


Fig. I.4 – Système instrumenté de sécurité(Architecture 1oo1)

Dans le cas de l'architecture 1oo1, toute défaillance dangereuse entraîne la défaillance du système. Une défaillance sûre se traduit par la mise dans une position de repli prédéfinie ou par une exécution intempestive de la fonction de sécurité [4].

I.4.3 Normes relatives aux systèmes instrumentés de sécurité

La norme CEI 61508 joue un rôle central dans le développement de normes sectorielles et de produits liés à la sécurité dans divers domaines tels que les machines, les procédés continus, le ferroviaire, le nucléaire, et bien d'autres. Elle constitue une référence majeure qui guide la conception et l'évaluation des systèmes électriques/électroniques/programmables et des produits associés en termes de sécurité [5] .

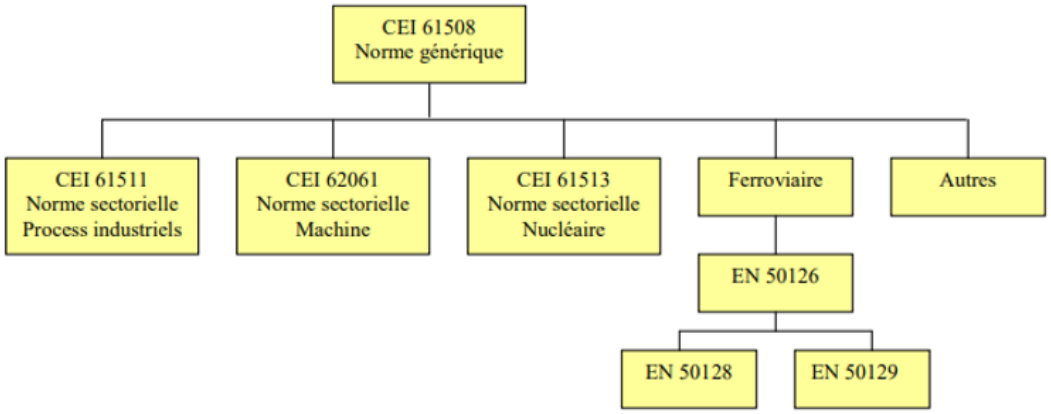


Fig. I.5 – Norme CEI 61508 et normes dérivées

En influençant ces différentes normes sectorielles, la norme CEI 61508 définit les exigences et les critères de sécurité à respecter pour assurer la fiabilité et la protection des personnes, de l'environnement et des installations dans tous les secteurs d'activité. Elle fournit des lignes directrices essentielles pour le développement, la mise en œuvre et l'évaluation des systèmes et des produits impliqués dans la sécurité[4].

I.4.4 Norme CEI 61511

La norme CEI 61511 est une norme sectorielle qui concerne les systèmes instrumentés de sécurité dans les processus industriels. Elle comprend trois parties :

1- Cadre et exigences.
2- Lignes directrices d'application.
3- Conseils pour la détermination des niveaux d'intégrité de sécurité.

Cette norme vise à établir des pratiques standardisées pour spécifier, concevoir, installer, maintenir et démanteler les systèmes instrumentés de sécurité, afin de garantir la sécurité des processus industriels tout au long de leur cycle de vie [4] .

I.5 Vers une sécurité intelligente

Les instruments intelligents sont intégrés dans des applications sécuritaires plus "intelligentes" afin d'établir une communication avec les équipements de production et éventuel-

lement avec les humains. Cette intégration vise à optimiser leur comportement et/ou leur intégration aux équipements intelligents en leur fournissant des fonctionnalités sécuritaires qui leur permettent de comprendre leur environnement et de réagir localement en fonction du rôle de l'équipement auquel ils sont associés. À l'heure actuelle, il existe une tendance croissante à utiliser des instruments intelligents dans les applications sécuritaires, car ils sont capables de diagnostiquer les défaillances et de mesurer certains paramètres complexes avec une confiance accrue [6].

I.6 Systèmes Instrumentés de Sécurité à Intelligence Distribuée

Les Systèmes Instrumentés de Sécurité à Intelligence Distribuée (SISID) sont une évolution des systèmes instrumentés de sécurité (SIS) utilisés dans les industries à haut risque. Au lieu des architectures traditionnelles basées sur une logique centralisée, le SISID vise à mettre en place une intelligence distribuée, où les décisions de sécurité sont prises de manière autonome au niveau local par des unités interconnectées.

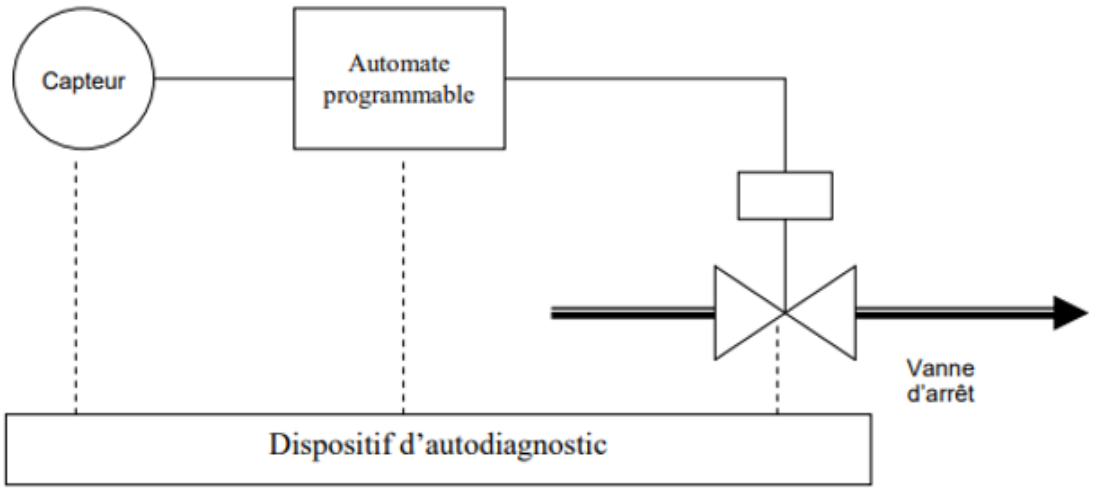


Fig. I.6 – Systèmes Instrumentés de Sécurité à Intelligence Distribuée (Architecture 1oo1s

L'autodiagnostic des dispositifs vise à détecter les défaillances afin de garantir la fiabilité des équipements conformément au niveau d'intégrité requis pour les fonctions de sécurité [6] .

I.7 Conclusion

En conclusion, ce premier chapitre a établi un contexte solide pour la suite du mémoire en présentant les concepts fondamentaux des Systèmes Instrumentés de Sécurité (SIS) et en mettant en évidence leur rôle essentiel dans la sécurité industrielle. Il a fourni les bases nécessaires pour comprendre les enjeux et les défis liés aux SIS, ouvrant ainsi la voie à une analyse plus approfondie de leur évaluation dans le chapitre suivant.

Chapitre II

L'évaluation de la sûreté de fonctionnement des SISID

II.1 Introduction

L'évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité à intelligence distribuée par rapport aux systèmes traditionnels constitue une étape cruciale dans les industries à risques élevés. Les systèmes instrumentés de sécurité (SIS) ont pour rôle de prévenir les accidents et de protéger les installations industrielles contre les dangers potentiels. Avec l'émergence de l'intelligence distribuée, où les décisions de sécurité sont prises localement par des nœuds autonomes interconnectés, il est essentiel de mesurer et de comparer les performances de ces systèmes par rapport aux approches traditionnelles.Dans ce chapitre, nous présenterons les résultats obtenus à partir de tests comparatifs entre les systèmes instrumentés de sécurité à intelligence distribuée et les systèmes traditionnels. Ces tests ont été réalisés dans le but d'évaluer la sûreté de fonctionnement, la fiabilité et la réactivité des deux approches dans des conditions réelles. Dans le cadre de notre évaluation de la sûreté de fonctionnement des systèmes instrumentés de sécurité (SIS) et des systèmes instrumentés de sécurité à intelligence distribuée (SISID), nous avons réalisé le calcul du "Probability of Failure on Demand" (Probabilité de défaillance sur demande en français) (PFD) et du "Probability of Failure to Safe" (probabilité de défaillances en sécurité) (PFS). Ces paramètres sont essentiels pour évaluer la fiabilité et la performance des systèmes [7].

II.2 Probabilité de défaillance dangeurese (PFD)

La probabilité de défaillance dangereuse est une mesure de la fiabilité d'un équipement ou d'un composant. Il représente la probabilité qu'une défaillance se produise dans un intervalle de temps donné. Le taux de défaillance peut varier en fonction du temps et peut être constant, décroissant ou croissant[7].
Si on calcule ce paramètre mathématiquement voici les formules utilisées :
PFD(t) = 1-R(t)-PFS(t) [8]
PFD(t) = 1-A(t) [5]
A(t) : Disponibilité du système
PFDavg : Probabilité moyenne de défaillance dangereuse

II.3 Probabilité de défaillances en sécurité(PFS)

La PFS, quant à lui, représente la probabilité qu'un SIS ou un SISID échoue par unité de temps. Il prend en compte la fiabilité globale du système sur une période donnée, en prenant en compte les taux de défaillance des composants et les temps de réparation. Le PFS permet d'évaluer la disponibilité du système dans son ensemble et de quantifier le niveau de risque résiduel [7].

II.4 Diagramme de Venn

La figure (Fig. II.1) montre le diagramme de Venn d'un système incluant le bon fonctionnement et les deux modes primaires de défaillances, le mode de défaillances sûres et le mode de défaillances dangereuses[2].



Fig. II.1 – Système avec modes de défaillance

Pour les deux modes de défaillances, les défaillances dangereuses sont beaucoup plus graves puisque les systèmes de protection ne peuvent assurer la mise en sécurité du processus et les défaillances ne peuvent être révélées [9].
L'effet global des autodiagnostics sur le système avec ses modes de défaillances peut être décrit par la figure (Fig. II.2) suivante :

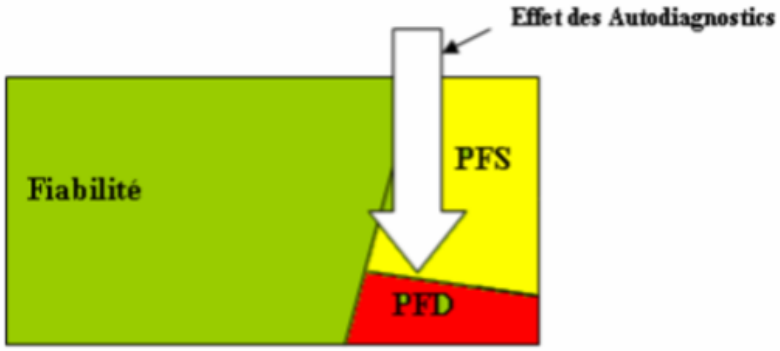


Fig. II.2 – Effet d'autodiagnostic sur le système instrumenté de sécurité

Note : Dans notre étude, nous avons utilisé les paramètres d'un modèle simulé à l'aide du logiciel Möbius, qui utilise des réseaux de petri mentionné dans l'article [2] pour évaluer la sûreté de fonctionnement des systèmes instrumentés de sécurité à intelligence distribuée.La figure (Fig. II.3) illustre le modèle utilisé :

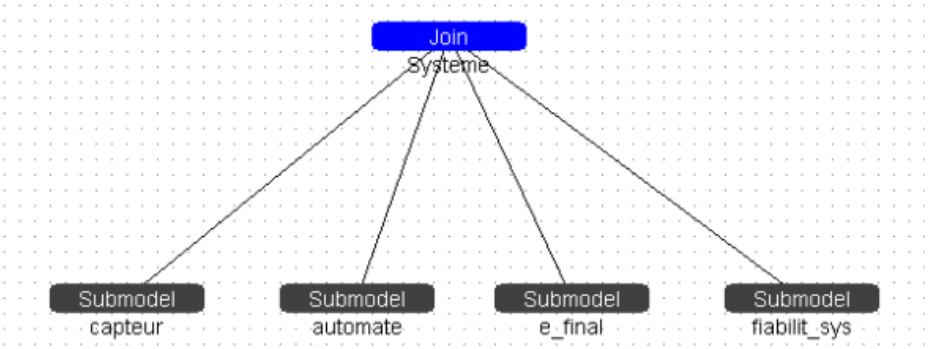


Fig. II.3 – Conception hiérarchique du SISID

Ce modèle présente une approche bien établie et largement acceptée pour l'évaluation de la fiabilité de ces systèmes. En utilisant ces paramètres, nous avons pu estimer le (PFD) et le (PFS).

II.5 Evaluation des performances du SIS classique et SISID

Le tableau (Tab. II.1) extraite de [6] est utilisée pour déterminer les taux de défaillance des composants du SIS montrée dans la figure (Fig. I.5) modélisé sous le logiciel GRIFF.

Tab. II.1 – Données relatives aux constituants du SIS

Composant	Taux de défaillances(par heure)	Pourcentage des défaillance sûr
Capteur	$6.10^{-}6$	40
Unité de Traitement	$2.10^{-}5$	70
Elément final	$9.10^{-}6$	58.3

Le tableau (Tab. II.2) montre les différents paramètres utilisés pour le traitement de notre modèle :

Tab. II.2 – Taux de défaillances dangereuses et en sécurité

Composant	Taux de défaillances dangereuses	Taux de défaillances sûres
Capteur	$3{,}6.10^{-}6$	$2{,}4.10^{-}6$
Unité de Traitement	$6.10^{-}5$	$1{,}4.10^{-}5$
Elément final	$3{,}75.10^{-}6$	$5{,}25.10^{-}6$

Avec

$\lambda D = \lambda DD + \lambda DU$

$\lambda S = \lambda SD + \lambda SU$

Ou :

λD : Taux de défaillances dangereuses

λDD : Taux de défaillances dangereuses détectées,
λDU : Taux de défaillances dangereuses non détectées,
λS : Taux de défaillances en sécurités
λSD : Taux de défaillances en sécurités détectées,
λSU : Taux de défaillances en sécurité non détectées.
La figure suivante illustre la répartition des défaillances selon [6] :

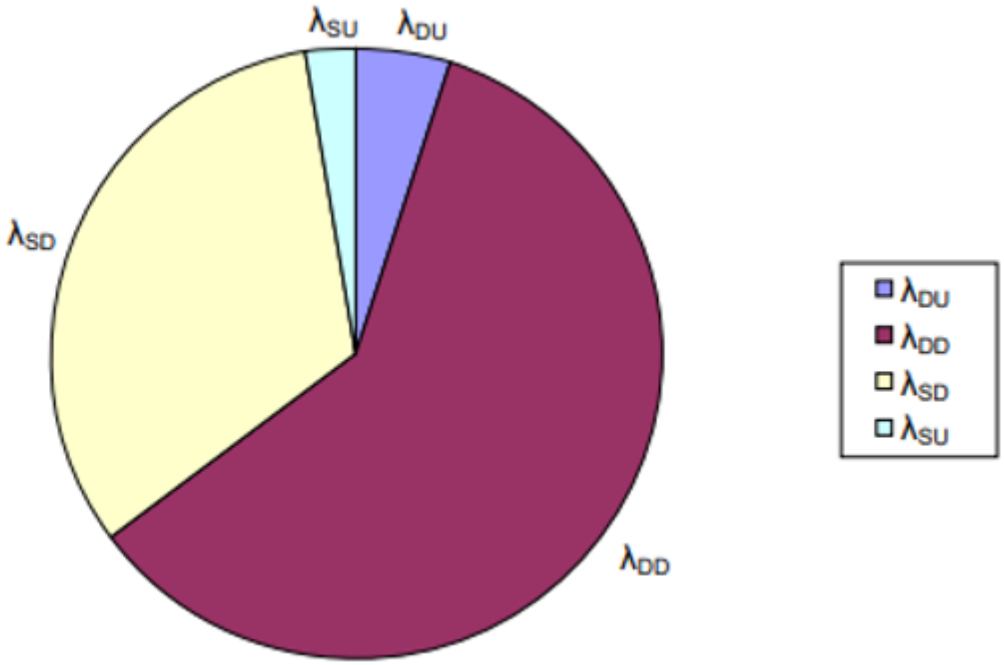


Fig. II.4 – Proportion de défaillance

Les systèmes nouvellement conçus disposent d'autodiagnostic et d'autotests internes qui permettent de déceler un certain nombre de défaillances par la désactivation des sorties lorsque des défauts internes sont détectés. Cette fonctionnalité peut être exploitée par les systèmes instrumentés de sécurité pour permettre de convertir les défaillances sûres en défaillances dangereuses.

La modélisation et ainsi la simulation nous ont permis de déterminer les probabilités relatives au système 1oo1 pour différentes durées. On prend pour durée T la valeur de 10000 heures. Cette durée correspond à la période entre deux tests notée Ti par la norme.

Voici les résultats obtenu pour la Probabilité de défaillance dangereuse de l'architecture 1oo1 dans le tableau (Tab. II.3) suivant :

Tab. II.3 – Probabilité de défaillance dangereuse pour l'architecture 1oo1 SIS

Durée	PFD
4380	$5{,}6796.10^{-2}$
5000	$6{,}4571.10^{-2}$
8760	$1{,}1037.10^{-1}$
10000	$1{,}2497.10^{-1}$

et pour la Probabilité de défaillances en sécurité les résultats sont illustré dans le tableau (Tab. II.4) suivant :

Tab. II.4 – Probabilité de défaillances en sécurité pour l'architecture 1oo1 SIS

Durée	PFS
4380	$9{,}047.10^{-}2$
5000	$6{,}1.026.10^{-}1$
8760	$1{,}7275.10^{-}1$
10000	$1{,}9467.10^{-}1$

Et pour le système SISID les résultats sont regroupés dans les tableaux suivants :
pour la Probabilité de défaillance dangereuse voici les résultats obtenus dans le tableau (Tab. II.5) :

Tab. II.5 – Probabilité de défaillance dangereuse pour l'architecture 1oo1 SISID

Durée	PFD
1000	$0{,}73.10^{-}2$
5000	$3{,}85.10^{-}2$
8760	$0{,}689.10^{-}1$
10000	$0{,}781.10^{-}1$

et pour la Probabilité de défaillances en sécurité les résultats sont illustré dans le tableau (Tab. II.6) suivant :

Tab. II.6 – Probabilité de défaillance en sécurité pour l'architecture 1oo1 SISID

Durée	PFS
1000	$2{,}66.10^{-}2$
5000	$1{,}18.10^{-}2$
8760	$1{,}95.10^{-}1$
10000	$2{,}20.10^{-}1$

Interprétation

En effet, lorsque le taux de détection par les moyens d'autotests intégrés est élevé, le taux de défaillances dangereuses diminue et le taux de défaillances sûres augmente. Cela s'explique par la transformation des défaillances dangereuses en défaillances sûres. Par conséquent, nous observons une réduction de la Probabilité de Fausses Détections (PFD) et une augmentation de la Probabilité de Fausses Absences (PFS) par rapport aux valeurs du système SIS classique.

II.6 Niveaux d'intégrité de sécurité

Les normes CEI 61508 et CEI 61511 définissent le niveau d'intégrité de sécurité (Safety Integrity Level : SIL) pour définir le niveau de réduction du risque, c'est-à-dire le niveau d'intégrité de sécurité que doit avoir le système de protection. Plus le SIL à une valeur élevée,

plus la réduction du risque est importante. A partir de l'architecture du système instrumenté de sécurité réalisant la fonction instrumentée de sécurité, la moyenne de la probabilité de défaillance à la demande PFDavg (Average Probability of Failure on Demand) est évaluée sur un intervalle [0, t] [4].
Pour l'évaluation de la PFDavg , le niveau d'intégrité de sécurité peut être déterminé à partir du tableau (Tab.II.7) suivant :

Tab. II.7 – Niveau d'intégrité de sécurité : Probabilité moyenne de défaillance

Niveau d'intégrité de sécurité (SIL)	Probabilité moyenne de défaillance
4	$10^-5 <= PFDavg < 10^-4$
3	$10^-4 <= PFDavg < 10^-3$
2	$10^-3 <= PFDavg < 10^-2$
1	$10^-2 <= PFDavg < 10^-1$

II.7 Conclusion

En conclusion, dans le deuxième chapitre de ce mémoire nous avons concentré sur l'évaluation des Systèmes Instrumentés de Sécurité (SIS) et a présenté les différentes méthodes utilisées pour évaluer leur performance. Nous avons examiné en détail les mesures telles que la Probabilité de Défaillance sur Demande (PFD) et le niveau d'Intégrité de Sécurité (SIL), qui sont des critères clés pour évaluer la fiabilité des SIS. La simulation prévue dans le chapitre suivant viendra consolider nos résultats et renforcer la pertinence de l'intégration de ces dispositifs pour améliorer la sécurité des SIS.

Chapitre III

Simulation et résultats

III.1 Introduction

Cette partie se concentre sur l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité (SIS) et des Systèmes Instrumentés de Sécurité d'Intelligence Distribuée (SISID) à l'aide du logiciel GRIFF avec le module SIL. Dans les industries à risques, ces systèmes jouent un rôle crucial dans la prévention des accidents majeurs et la protection des personnes, de l'environnement et des installations.

III.2 Le logiciel GRIFF

Pour simuler et évaluer les système instrumentés de sécurité on a utilisé le logiciel griff qui est largement reconnu pour son utilisation dans l'analyse de sûreté de fonctionnement. Il permet de modéliser et de simuler différents scénarios, en prenant en compte les défaillances potentielles des composants, les réactions du système et les mesures de sécurité mises en place. Et pour le module SIL (safety integrity level) est spécialement conçu pour évaluer le niveau d'intégrité de sécurité des systèmes. Il utilise une approche basée sur les normes internationales telles que l'IEC 61508 et l'IEC 61511 pour déterminer le niveau de performance requis pour atteindre une certaine sûreté de fonctionnement.

La figure suivante montre l'architecture de SIS d'architecture 1oo1 dans le logiciel griff :

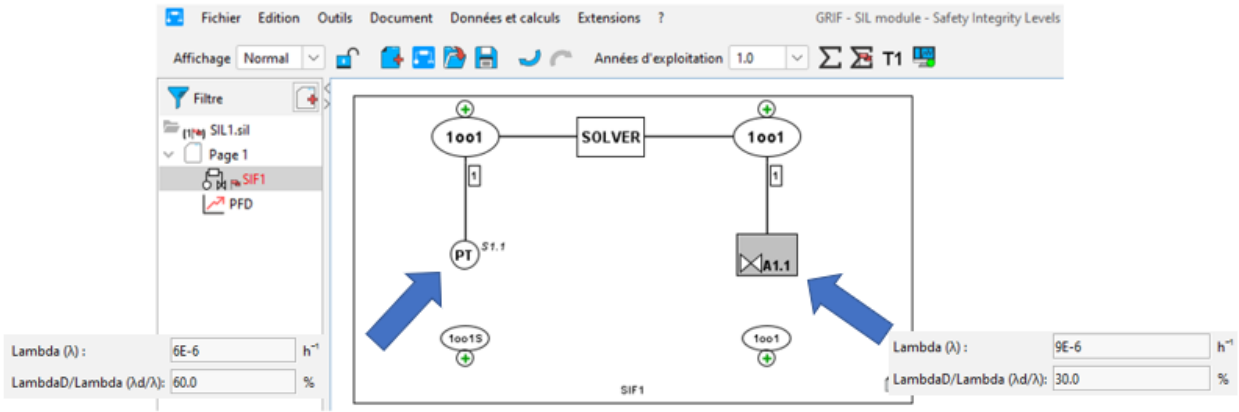


Fig. III.1 – Simulation de SIS architecture 1oo1

Après qu'on introduit les paramètres du capteur et l'actionneur on lance la compilation pour commencer l'évaluation.
La répartition en pourcentage du niveau de SIL pour SIS est illustrée dans la figure (Fig. III.2) suivante :

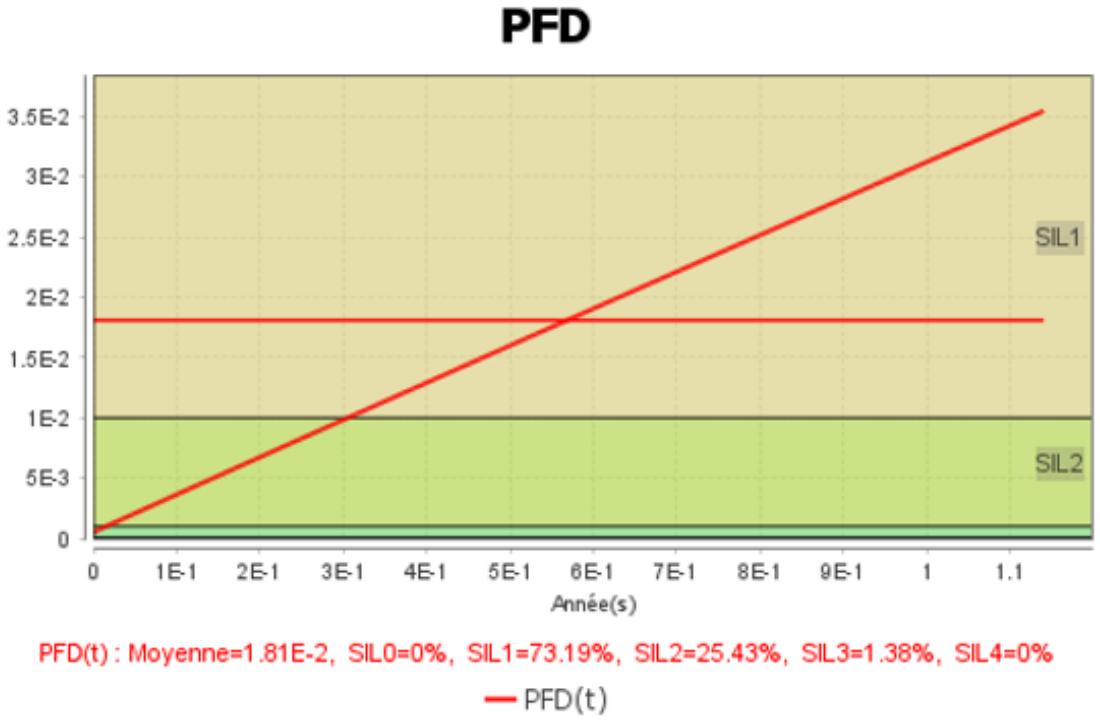


Fig. III.2 – Courbe PFD pour les SIS

Interprétations et remarques :

- Cette figure montre que le SIS qui dispose d'un niveau de SIL égal à 1 avec 0 pourcent dans la zone correspondante à SIL 0 où la norme ne peut plus être appliquée.
- Le SIS demeure dans la zone SIL 1 pendant 73.19 pourcent et le reste du temps est réparti entre les zones correspondantes aux SIL 2 et au SIL 3 et au SIL 4.

D'ailleurs, lorsqu'un SIS est conçu pour un niveau de SIL, il peut disposer d'un niveau de SIL supérieur mais pas le contraire. Pour la zone qui correspond au niveau de SIL 4, le SIS passe 0 pourcent ce qui est très négligeable.

et maintenant pour les Systèmes Instrumentés de Sécurité à Intelligence Distribuée on fait la configuration des paramètres corespondante pour que l'architecture aura comme dispositif autodiagnostique et poura détecter les défaillance dangereuse en augmentant le taux de Diagnostic en ligne des pannes dangereuses a 80 pourcent on aura les résultats suivantes illustrés dans cette figure (Fig. III.3) :

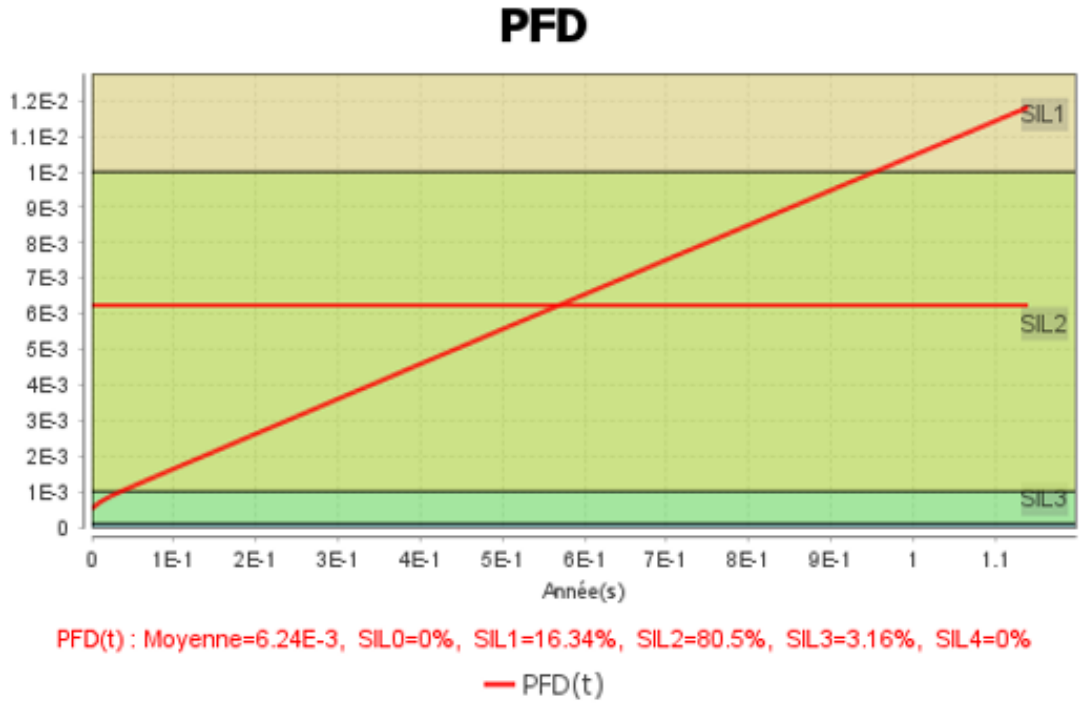


Fig. III.3 – Courbe PFD pour les SISID

Interprétations et remarques

- Cette figure illustre une variation de près de 10 pourcent à la baisse du pourcentage du niveau SIL du SISID lorsque aucun dispositif autodiagnostique n'est présent, tandis qu'il augmente de 55 pourcent au niveau 2
- Pour la zone qui correspond au niveau de SIL 4, le SIL passe 0 pourcent ce qui est très négligeable.
- Malgré que on est toujours dans le niveau SIL 1 mais il est préférable que notre système passe au niveau 2 et 3 mais on reste limité avec les taux défaillances des composant.

Pour cela, dans l'étape qui a suivi, nous avons augmenté le taux de diagnostic en ligne des pannes dangereuses à 98,5 pourcent et obtenu les résultats suivants :

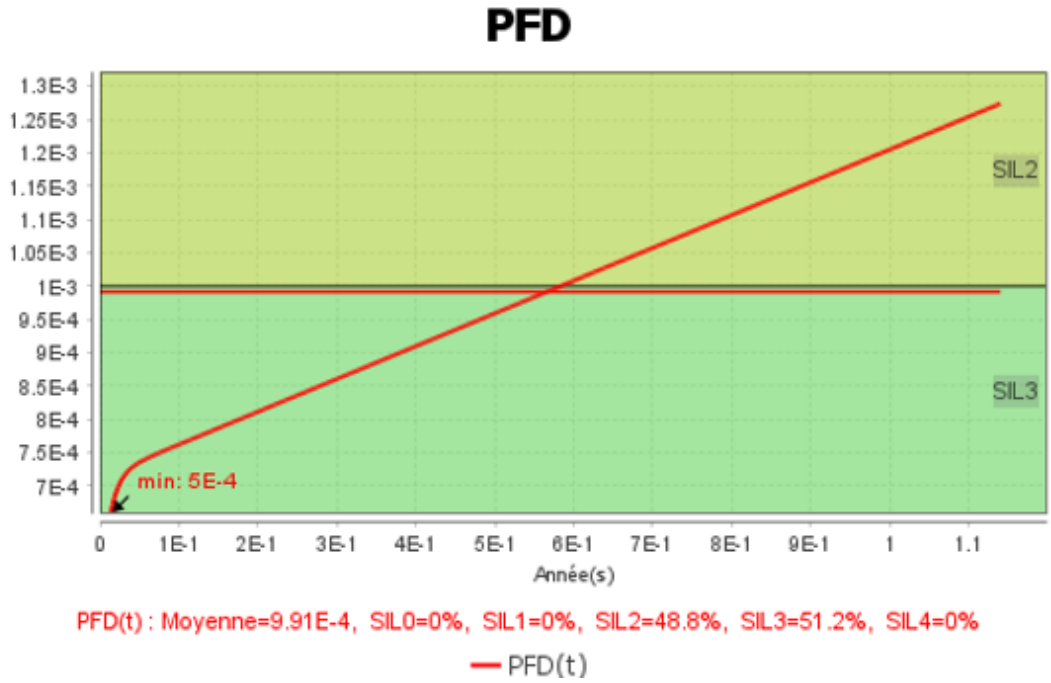


Fig. III.4 – Courbe PFD pour les SISID améliorés

Interprétations et remarques :

- Cette figure illustre une amélioration du niveau SIL, car notre système a commencé à atteindre le niveau SIL 3
- Notre système atteint un niveau SIL (Safety Integrity Level) 3 avec un pourcentage de 51 pourcent.
- Le niveau SIL 3 est généralement associé à des systèmes nécessitant une fiabilité et une sécurité accrues pour traiter des situations potentiellement dangereuses.

III.3 Intégration de la carte STM32 pour transformer la vanne de production en un instrument intelligent (SISID)

Après une évaluation approfondie de notre système industriel, il est devenu évident que l'incorporation d'un dispositif autodiagnostique est essentielle pour améliorer la fiabilité, la sécurité et les performances de notre vanne. Dans cette optique, nous avons proposé une solution novatrice consistant à ajouter la carte STM32 à notre vanne existante. Cette solution permettra de transformer notre vanne en un instrument intelligent, offrant une meilleure gestion des pannes et une réduction des temps d'arrêt imprévus.

Ce choix s'est basé sur plusieurs facteurs clés :

- Coût abordable et documentation disponible : La carte STM32 présente l'avantage d'être une solution économique, ce qui permet de réduire les coûts de mise en œuvre. De plus, la disponibilité de documentations techniques détaillées facilite son intégration et son développement.
- Modules de sortie analogique : La carte STM32 dispose de modules de sortie analogique, ce qui répond parfaitement aux besoins industriels. Ces modules permettent de

générer des signaux analogiques précis et de contrôler avec précision les actions de la vanne, offrant ainsi une réponse adaptée aux exigences du processus industriel.

- Robustesse et fiabilité : La carte STM32 est réputée pour sa robustesse et sa fiabilité. Elle est conçue pour résister aux environnements industriels les plus exigeants, ce qui en fait une solution fiable pour assurer les fonctions de sécurité critiques de la vanne.
- De plus, notre choix d'intégrer la carte STM32 à notre vanne est également soutenu par nos connaissances théoriques et notre expérience pratique avec la plateforme STM32, acquises lors de notre formation à l'école. Cette familiarité avec la carte STM32 nous permettra de mettre en œuvre efficacement l'intégration, d'exploiter pleinement ses fonctionnalités et de résoudre d'éventuels problèmes de manière plus efficiente.

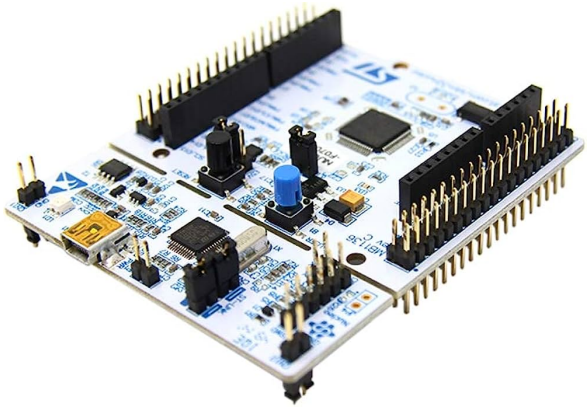


Fig. III.5 – La carte STM32

En intégrant la carte STM32 à notre vanne, nous sommes convaincus de pouvoir améliorer considérablement la fiabilité, la sécurité et les performances globales de notre système. Les avantages liés à cette solution comprennent une réduction des temps d'arrêt imprévus, une détection précoce des pannes, ainsi qu'une meilleure capacité de gestion des pannes. Grâce à la carte STM32, notre vanne deviendra un instrument intelligent, renforçant ainsi la sécurité et l'efficacité de notre processus industriel.

III.4 Conclusion

En conclusion, l'ajout d'un dispositif autodiagnostique à un système présente des avantages significatifs en termes d'amélioration de la sécurité, tels que l'augmentation du niveau SIL (Safety Integrity Level) selon les normes de sécurité. La simulation effectuée dans ce chapitre a démontré de manière convaincante que l'intégration d'un tel dispositif permet une augmentation du niveau de confiance dans le fonctionnement fiable du système

Conclusion générale

Ce mémoire met en évidence l'importance cruciale des Systèmes Instrumentés de Sécurité (SIS) dans les industries à haut risque et souligne l'impact positif d'un dispositif autodiagnostique sur la sécurité globale du système.

L'étude approfondie réalisée a démontré que l'intégration d'un dispositif autodiagnostique offre un avantage significatif en améliorant la fiabilité et la performance des SIS. Ce dispositif permet une détection proactive des défaillances potentielles, une vérification régulière de son propre fonctionnement et des mesures correctives appropriées. En conséquence, les risques d'erreurs et de défaillances du système sont réduits, contribuant ainsi à un niveau de sécurité accru.

De plus, l'ajout d'un dispositif autodiagnostique répond aux exigences réglementaires en matière de sécurité industrielle et renforce la conformité aux normes de sécurité établies. Cela renforce la confiance des parties prenantes et garantit une protection optimale des personnes, de l'environnement et des actifs.

En somme, l'intégration d'un dispositif autodiagnostique dans les SIS présente un avantage indéniable en termes de sécurité. Il offre une solution proactive pour améliorer la fiabilité du système, réduire les risques potentiels et assurer un environnement de travail plus sécurisé dans les industries à haut risque. Cette conclusion souligne l'importance de prendre en compte les avantages des dispositifs autodiagnostiques lors de la conception, de la mise en œuvre et de la gestion des SIS, afin de garantir une protection optimale contre les accidents majeurs

Résumé :

Les Systèmes Instrumentés de Sécurité (SIS) sont évalués à l'aide de mesures telles que la PFD et le SIL. L'ajout de dispositifs autodiagnostiques améliore la sécurité des SIS en détectant les défaillances et en prenant des mesures correctives.

Mots-clés :

Systèmes Instrumentés de Sécurité (SIS), évaluation, dispositif autodiagnostique, fiabilité, sécurité industrielle, Probabilité de Défaillance sur Demande (PFD), Intégrité de Sécurité (SIL), performance, prévention des accidents, surveillance, réactivité.

Abstract :

Safety Instrumented Systems (SIS) are evaluated using measures such as PFD and SIL. The addition of self-diagnostic devices enhances the safety of SIS by detecting failures and taking corrective actions.

Keywords :

Safety Instrumented Systems (SIS), evaluation, self-diagnostic device, reliability, industrial safety, Probability of Failure on Demand (PFD), Safety Integrity Level (SIL), performance, accident prevention, monitoring, responsiveness.

ملخص :

تلعب أنظمة الأمان المعززة بأجهزة الاستشعار والتحكم (SIS) دورًا حاسمًا في منع الحوادث الصناعية. تقييم هذه الأنظمة، استنادًا إلى معايير مثل احتمال فشل الطلب (PFD) ومستوى السلامة الشاملة(SIL) ، أمر ضروري لضمان موثوقيتها. إضافة أجهزة التشخيص الذاتي إلى أنظمة SIS ذات أهمية قصوى، حيث تمكِّن من المراقبة المستمرة والكشف المبكر عن الأعطال واتخاذ التدابير التصحيحية. يتحسن بذلك استجابة وأداء أنظمةSIS مما يعزز سلامة المنشآت الصناعية.

كلمات مفتاحية :

أنظمة الأمان المعززة بأجهزة الاستشعار والتحكم (SIS)، تقييم، جهاز التشخيص الذاتي، موثوقية، السلامة الصناعية، احتمال فشل الطلب (PFD)، مستوى السلامة الشاملة (SIL)، أداء، منع الحوادث، مراقبة، استجابة.

Bibliographie

[1] D. LE JURY, *Contribution à l'étude de la sûreté de fonctionnement des systèmes instrumentés intelligents*. PhD thesis, UNIVERSITE BADJI MOKHTAR–ANNABA, 2021.

[2] A. Mkhida, *Contribution à l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité à Intelligence Distribuée.(Contribution to assessing the dependability of safety instrumented systems integrating intelligence)*. PhD thesis, National Polytechnic Institute of Lorraine, Nancy, France, 2008.

[3] J. Akaichi, *Systèmes automatisés de production à intelligence distribuée des stratégies de répartition basées sur une approche de classification*. PhD thesis, Lille 1, 1996.

[4] C. IEC, "Iec 61508 : Sécurité fonctionnelle des systèmes électriques électroniques programmables relatifs à la sécurité," *International standard*, 1998.

[5] S. S. Grossel, "Functional safety : a straightforward guide to applying iec 61508 and related standards, david j. smith, kenneth gl simpson, elsevier, butterworth-heinemann, oxford, uk and burlington, ma (2004), 263 pages, 59.95,″ 2005.

[6] W. M. Goble and H. Cheddie, *Safety instrumented systems verification : Practical probabilistic calculations*. Isa, 2005.

[7] P. Lamy, *Probabilité de défaillance dangereuse d'un système : explications et exemple de calcul.* PhD thesis, Institut National de Recherche et de Sécurité (INRS), 2002.

[8] W. M. Goble and J. Bujkowski, "Extending iec61508 reliability evaluation techniques to include common circuit designs used in industrial safety systems," in *Annual Reliability and Maintainability Symposium. 2001 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 01CH37179)*, pp. 339–343, IEEE, 2001.

[9] E. Marszal and W. Goble, "High reliability computing for control and safety," in *PACS2001. Proceedings of the 2001 Particle Accelerator Conference (Cat. No. 01CH37268)*, vol. 1, pp. 279–282, IEEE, 2001.