RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DU 20 AOÛT 1955 SKIKDA
FACULTÉ DE TECHNOLOGIE
DÉPARTEMENT DE GÉNIE DES PROCÉDÉS ET PÉTROCHIMIE

Ref : D012121006D

Thèse

En vue de l'obtention du diplôme de :

Doctorat LMD

Filière : Hygiène et sécurité Industrielle

Spécialité : Sécurité industrielle, environnement et maîtrise des risques

Thème

Système contrôle-commande intelligent et maîtrise des risques : Application à la commande d'un système complexe

Présentée par :

BENSACI Chaima

Soutenue publiquement le 15-07-2021, devant le jury composé de :

Président :	Mohamed Salah MEDJRAM	Professeur	Université de Skikda
Encadrant :	Youcef ZENNIR	Professeur	Université de Skikda
Co-encadrant :	Denis POMORSKI	Professeur	Université de Lille
Examinateur :	Hamid BENTARZI	Professeur	IGEE- Boumerdes
Examinateur :	Azzedine BOUZAOUIT	Professeur	Université de Skikda
Examinateur :	Mounira ROUAINIA	Professeure	Université de Skikda
Examinateur :	Lilia ZIGHED	Professeure	Université de Skikda
Invité :	Fares INNAL	Professeur	Université de Skikda

Année 2020-2021

Remerciements

Avant d'aborder ce travail, je remercie tout d'abord Allah qui m'a donné la volonté, la patience et le courage au cours de ces longues années d'étude.

Je voudrais exprimer également ma très sincère gratitude et reconnaissance à toutes les personnes qui ont contribuées à l'aboutissement de ce travail.

Mes remerciements vont particulièrement à mes directeurs de thèse : Messieurs Youcef Zennir, Professeur à l'université 20 aout 1955 de SKIKDA, et Denis Pomorski, Professeur à l'université de Lille, pour l'aide, la collaboration, l'encouragement, les précieux conseils, la confiance et la compréhension qu'ils ont montrés à mon égard pendant toute la période consacrée à la réalisation de cette thèse.

Je tiens à remercier tous les membres du jury :

- Monsieur Mohamed Salah Medjram, Professeur à l'université de Skikda, pour avoir accepté la présidence du jury de ma soutenance.
- Messieurs Azzedine Bouzaouit et Fares Innal, Professeurs à l'université de Skikda.
- Monsieur Hamid Bentarzi, Professeur à l'université de Boumerdes.
- Madame Rouainia Mounira, Professeure à l'université de Skikda et responsable de la formation doctorale en hygiène et sécurité industrielle.
- Madame Lilia Zighed, Professeure à l'université de Skikda, pour avoir accepté d'examiner et rapporter ce travail.

Ma reconnaissance va aussi à tous mes enseignants. En particulier, le Professeur Fares Innal pour son aide et ses encouragements lors de mes recherches doctorales.

Je remercie encore vivement le directeur du laboratoire LGCES (Laboratoire de génie chimique et environnement de Skikda), le Professeur Mohamed Salah Medjram, qui m'a accueillie au sein de son laboratoire depuis mon premier jour en qualité de doctorante.

J'adresse également un grand merci au directeur du laboratoire de recherche CRIStAL ainsi qu'à toute l'équipe DiCOT (Diagnostic, Commande et Observations pour

des systèmes Tolérants aux fautes) pour leur accueil durant ma période de stage. Je suis particulièrement reconnaissante à Boussad Abci et Bilal Daass pour leur gentillesse, leurs encouragements et toute l'aide qu'ils m'ont apportée tout au long du stage.

Je tiens à remercier aussi toute l'équipe RAMS (Reliability, Availability, Maintenance and Safety). En particulier, Madame Mary Ann Lundteigen, Professeure à l'université NTNU, pour sa supervision pendant trois mois de stage.

Enfin, je saisis l'occasion pour exprimer toute ma gratitude à mes proches. Je suis très reconnaissante à mes parents ; à tous les membres de ma famille, en particulier, Sohaib, Soundous, Razane et Aya ; ainsi qu'à toutes mes amies et collègues pour leur soutien, leur confiance et leur amour. Je ne pourrai jamais assez les en remercier !

ملخص

مع ظهور التقنيات الحديثة ، شهدنا تطور العديد من الأنظمة المعقدة القادرة على التصرف والتفاعل وحتى اتخاذ القرار بشكل مستقل ، نذكر منها على سبيل المثال الأنظمة الروبوتية. تحتل هذه الأنظمة مكانة مهمة في العديد من التطبيقات، بما في ذلك التطبيقات الصناعية. في الوقت الحالي ، تتعرض المناطق الصناعية إلى غزو بشكل متزايد من قبل عدد كبير من الروبوتات المتنقلة، القادرة على أداء المهام المعقدة من خلال التعاون فيما بينها. ومع ذلك ، فإن إدماج هذه الأنظمة في بيئات العمل مع تفاعلات قوية بين الروبوتات كذلك بين الروبوتات و العاملين يشكل نوعا من التعقيد في التحكم والتنسيق، مما يجعل إدارته أكثر صعوبة في بيئة ديناميكية وعالية المخاطر. لذلك أصبحت الحاجة إلى تطوير منهجيات جديدة لتحليل المخاطر والرقابة أمرا مطلوبا.

تركز هذه الأطروحة على دراسة هذا النوع من التعقيد في إطار تطبيقي لمختبر تحاليل، من بين أهم خصوصياته، أن يتم تجهيزه بعدد كبير من الروبوتات المتنقلة ذات العجلات المستقلة، المكلفة بنقل العديد من الأشياء بما فيها المنتجات الخطيرة (المتفجرة، المسببة للتآكل ....)، و المتفاعلة بقوة مع البشر. على وجه الخصوص ، يتم معالجة موضوع السلامة والأمن من خلال تحليل المخاطر باستخدام بنى تنسيق متنوعة (مركزية ،هرمية و هرمية معدّلة) للروبوتات ، مما يسمح بتنقلها ، مع الحرص على تحسين تحكمها.

أولاً ، نقترح منهجية لتحديد وتقييم سيناريوهات المخاطر المحتملة للمختبر ، بهدف تقليلها والسيطرة عليها. تعتمد المنهجية المقترحة على أربع تركيبات من خمس طرق أساسية لتحليل المخاطر تهدف إلى توفير تحليل مفصل لنظام صناعي معقد: تحليل أنماط الفشل وتأثيراتها و درجة خطورتها FMECA ، تحليل أشجار الأعطال FTA ، طريقة تحليل المخاطر STPA ، طريقة ربطة العنق Bowtie ، وكذلك طريقة شبكات بيتري.

أدى تطبيق هذه النُّهُج على مختبرنا الآلي إلى الحصول على مجموعة من متطلبات السلامة والتوصيات الخاصة بالتنقل والتحكم في الروبوتات المتنقلة ، مما يسمح بالحفاظ على سلامة وأمن المؤسسة بأكملها.

أخيرًا ، شرعنا في تطوير بنية التحكم في الروبوتات ، بناءً على خوارزميات تحسين عالية المستوى PSO ، المشتقة من الذكاء الاصطناعي. باحترام متطلبات السلامة والأمن لنظامنا ، من جهة ، حافظنا على استقراره ، ومن جهة أخرى ، قمنا بضمان تنقل أكثر دقة للروبوتات المتنقلة.

الكلمات المفتاحية : تحليل المخاطر ، مراقبة السلامة، نظام معقد، معمل التحليل الكيميائي ، نظام الروبوتات المتعددة ، نظام التحكم / القيادة ، بنيات التحكم ، تحسين أسراب الجسيمات.

Résumé

Avec l'essor des technologies modernes, nous assistons au développement de nombreux systèmes complexes capables d'agir, de réagir, voire de décider de manière autonome, tels les systèmes robotiques. Ces systèmes prennent une place importante dans beaucoup d'applications, y compris les applications industrielles. Actuellement, des zones industrielles sont de plus en plus envahies par des flottes de robots mobiles, capables d'effectuer des tâches complexes en collaborant et en coopérant ensemble. Néanmoins, l'intégration de tels systèmes dans des environnements d'interventions avec une forte interaction robot-robot et robot-humain présente une certaine complexité de contrôle et de coordination, qui devient plus difficile à gérer dans un environnement dynamique et à haut risque. C'est pourquoi le besoin de développer de nouvelles méthodologies d'analyse et de maitrise de risques est devenu plus exigent.

Cette thèse est consacrée à l'étude de cette complexité dans le cadre applicatif d'un laboratoire d'analyses dont l'une des particularités est d'être équipé d'une flotte de robots mobiles à roues autonomes, transportant entre autres des produits à risques (explosifs, corrosifs…), et en interaction forte avec l'humain. En particulier, la sûreté et la sécurité sont traitées à travers une analyse des risques en considérant diverses architectures de coordination (centralisée, hiérarchique et hiérarchique modifiée) des robots, permettant leur navigation, tout en gardant un œil sur l'amélioration de leur contrôle.

Dans un premier temps, nous proposons une méthodologie permettant d'identifier et d'évaluer les scénarios de risques potentiels du laboratoire, dans l'objectif de les minimiser et de les maîtriser. La méthodologie proposée est basée sur quatre combinaisons de cinq méthodes principales d'analyse des risques visant à fournir une analyse détaillée d'un système industriel complexe : l'analyse des modes de défaillance, de leurs effets et de leur criticité AMDEC, l'analyse des arbres de défaillances ADD, la méthode d'analyse des dangers STPA, la méthode du nœud papillon, ainsi que la méthode utilisant les réseaux de Petri.

L'application de ces approches à notre laboratoire robotisé a fait émerger des exigences de sécurité et des recommandations concernant la navigation et le contrôle des robots mobiles, permettant de préserver la sûreté et la sécurité de l'ensemble de l'établissement.

Enfin, nous nous sommes attachés à développer une architecture de contrôle des robots, basée sur des algorithmes méta-heuristiques d'optimisation PSO, issus de l'intelligence artificielle. Les exigences de sûreté et de sécurité de notre système étant respectées, nous en avons d'une part préservé la stabilité, et avons d'autre part assuré une navigation plus précise des robots mobiles.

Mots-clés : *Analyse des risques, Maitrise de la sécurité, Système complexe, Laboratoire d'analyses chimique, Système multi-robots mobiles, Système de contrôle / commande, Architectures de contrôle, Optimisation de l'essaim de particules.*

Abstract

With the advent of new technologies, we are witnessing the development of many complex systems capable of acting, reacting and even deciding autonomously such as robotic systems. These systems occupy a prominent place in many applications, including industrial applications. Today, industrial areas are increasingly invaded by fleets of mobile robots, capable of performing complex tasks by collaborating and cooperating together. However, the integration of such systems in intervention environments with strong robot-robot and robot-human interaction presents a certain complexity of control and coordination, which becomes more difficult to manage in a dynamic and high-risk environment. Thus the need to develop new risk analysis and control methodologies has become more demanding.

This thesis is devoted to the study of this complexity within the application framework of an analysis laboratory which one of its particularities is being equipped with a fleet of autonomous wheeled mobile robots, transporting, among other things, risk products (explosives, corrosives, etc.), and in strong interaction with humans. In particular, safety and security are addressed through a risk analysis by considering various coordination architectures (centralized, hierarchical and modified hierarchical) for robots, allowing their navigation, while keeping an eye towards improving their control.

We initially propose a methodology to identify and assess the laboratory's potential risk scenarios, with the aim of minimizing and controlling them. The proposed methodology is based on four combinations of five main risk analysis methods aimed at providing a detailed analysis of a complex industrial system: Failure modes, Effects and Criticality Analysis FMECA, Fault Tree Analysis FTA, STPA Hazard Analysis Method, the Bow Tie method, as well as the Petri nets method.

The application of these approaches to our robotic laboratory has given rise to safety requirements and recommendations regarding the navigation and control of mobile robots, to maintain the safety and security of the entire establishment.

Finally, we have focused to develop a control architecture for robots, based on meta-heuristic optimization algorithms PSO, derived from artificial intelligence. While respecting the safety and security requirements of our system; we have on the one hand preserved its stability, and on the other hand we have ensured a more precise navigation of the mobile robots.

Keywords: *Risk analysis, Safety control, Complex system, Chemical analysis laboratory, Mobile multi-robot system, Control/Command system, Control architectures, Optimization of particle swarms.*

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ADD	Arbre de Défaillances
ADE	Arbre d'événements
AFNOR	Association française de normalisation
AGV	Automatic Guided Vehicle
AMDE	Analyse des Modes de Défaillance et de leurs Effets
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
ANSI	American National Standards Institute
C	Criticité
CAST	Causal Analysis based on System Theory
CEI	Commission Electrotechnique Internationale
CEN	European committee for standardization
Cobot	Collaborative Robot
EN	European Norm
ESHA	Environmental Survey Hazard Analysis
ETBA	Energy Trace and Barrier Analysis
FAA	Federal Aviation Administration
FFA	Functional Failure Analysis
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
FTA	Fault Tree Analysis
GRIF	GRaphiques Interactifs pour la Fiabilité
HAZOP	HAZard and Operability analysis
HCR	Human-Cooperative Robot

HMI	Human Machine Interface
IANOR	Institut Algérien de Normalisation
ISO	International Organization for Standardization
L	Loss / Perte
OHSAS	Occupational Health and Safety Assessment Series
OSHA	Occupational Safety and Health Administration
RdP	Réseau de Petri
RIA	Robotic Industries Association
RPN	Risk Priority Number
SC	Structure Centralisée
SCH	Structure de contrôle hiérarchique
SH	Structure Hiérarchique
SHARD	Software Hazard Analysis and Resolution in Design
SHM	Structure Hiérarchique Modifiée
SlA	System level accident
S-lH	System level hazard
SMRM	Système Multi-Robots Mobile
STAMP	System-Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
TS	Technical Specification
UCA	Unsafe Control Action
UML	Unified Modeling Language
US	Unsafe scenario
V-Rep	Virtual Robot Experimentation Platform

Introduction générale

Introduction générale

- Problématique et contexte de l'étude

De nos jours, l'utilisation de robots se généralise dans tout type d'environnements : au sein de la maison, dans les champs, en mer, dans l'espace, etc. Ils occupent une place de plus en plus grande, notamment dans les applications de crises, dans les zones d'interventions à risques pour l'homme : déminage, démantèlement de centrales nucléaires, gestion de catastrophes naturelles, incendie, transport de charges lourdes, etc. En particulier, les robots manipulateurs sont légion dans de nombreux secteurs industriels. Leur rôle est de faciliter les tâches complexes, insoutenables ou répétitives des travailleurs, d'augmenter la productivité tout en préservant la sécurité humaine et matérielle dans ces environnements à risques. A l'heure actuelle, l'utilisation de robots mobiles semble incontournable dans le cadre de l'industrie 4.0. En particulier, l'intégration de robots mobiles autonomes est un véritable enjeu pour l'industrie de demain. Ceux-ci permettront de déplacer des produits (parfois toxiques, corrosifs, explosifs…) tout en préservant la sûreté et la sécurité de l'homme et de son environnement.

Contrairement aux robots manipulateurs spécifiquement conçus pour travailler de manière répétitive dans des espaces limités, les robots mobiles autonomes sont prévus pour fonctionner de manière autonome dans des environnements dynamiques peu ou pas structurés. L'utilisation de cette robotique mobile en milieu difficile passe par la résolution de nombreux verrous technologiques et scientifiques. Plusieurs études récentes ont cherché à les définir et les résoudre, notamment dans le contexte de la robotique collaborative et coopérative sécurisée. Citons, à titre d'exemples, les projets CARLoS [1], RoboSafe [2] et SIMERO [3].

Ce travail de thèse trouve tout son sens dans le contexte de la robotique mobile collaborative, permettant de cibler des problématiques autour de la coordination des robots mobiles, ayant pour objectif de réaliser conjointement une tâche dans une zone industrielle difficile. Ce travail fait appel à 5 domaines : l'industrie, la robotique mobile, la sécurité et la maitrise des risques, le contrôle en temps réel et l'intelligence artificielle (figure 1). De l'utilisation de la robotique mobile au domaine de l'industrie, nous avons extrait notre

étude de cas, qui concerne la gestion d'un ensemble de robots mobiles coopératifs déplaçant des produits chimiques potentiellement dangereux au sein d'un laboratoire industriel d'analyses. Nous abordons cette application sous l'angle de la sécurité et de la maîtrise des risques. Plus exactement, nous proposons une combinaison des méthodes d'analyse des risques afin de prévenir les accidents. Les domaines du contrôle en temps réel et de l'intelligence artificielle nous permettent de proposer une approche de contrôle intelligent, implémentée en simulation et sur robots réels.

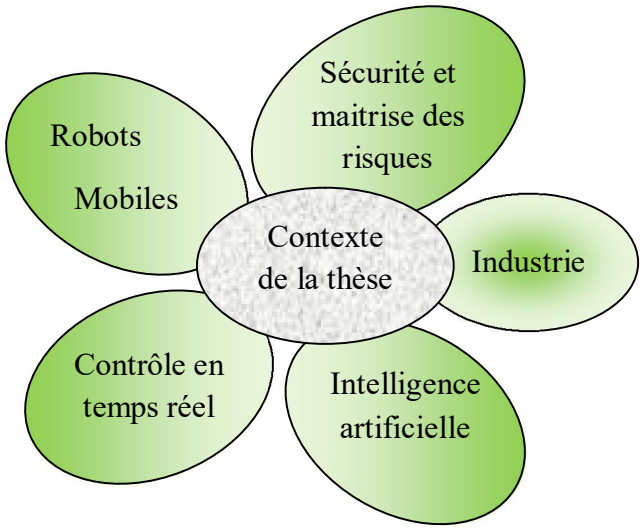


Figure 1 Contexte de la thèse

Plus précisément, la problématique étudiée dans cette thèse concerne le contrôle de la navigation et l'étude de la complexité de coordination d'un système multi-robots mobiles autonomes dans un laboratoire d'analyses robotisé (figure 2), constitué de plusieurs salles, et en présence d'humains et de machines plus ou moins complexes. Cet ensemble de robots mobiles est principalement utilisé pour déplacer des produits chimiques, pouvant entraîner des risques industriels importants avec effets majeurs (toxiques, inflammables, explosifs, etc.). Cette complexité est traitée d'un point de vue « sureté et sécurité » à travers diverses architectures de coordination, permettant la navigation des robots, et tout en gardant un œil sur l'amélioration de leur contrôle.

Dans un premier temps, nous proposons une méthodologie afin d'identifier et d'évaluer les scénarios de risques potentiels des systèmes industriels complexes. Nous développons dès lors des approches permettant de les maitriser. Dans un second temps, nous mettons en place une architecture de contrôle tout en respectant les exigences nécessaires. Cette architecture permettra de préserver le fonctionnement optimal des robots

pour éviter l'exposition aux dangers des humains, du matériel et de l'installation. Il nous faudra par conséquent maitriser la complexité des tâches à exécuter afin d'assurer la commande des robots en temps réel.

Figure 2 Modèle de l'environnement de travail des robots

- Contributions de la thèse

Les principales contributions de cette thèse sont les suivantes :

- Une méthodologie globale et détaillée est proposée pour l'analyse des risques des systèmes complexes. Celle-ci est basée sur un ensemble d'approches, permettant d'analyser le système sous différents angles.
- L'analyse STPA étant une méthode entièrement qualitative, nous avons proposé de la combiner avec d'autres méthodes conventionnelles, comme l'arbre de défaillances, le nœud papillon et les réseaux de Petri. Ces combinaisons permettent d'en améliorer les résultats qualitatifs d'une part, et d'évaluer semi-quantitativement et quantitativement les scénarios de dangers éventuels, d'autre part.
- Un grand nombre de scénarios de risques avec leurs facteurs causaux sont identifiés. Nous nous appuyons sur l'étude d'un système multi-robots mobiles pour le transport de produits dangereux au sein d'un environnement à risques, en utilisant différentes approches de coordination : centralisée, hiérarchique et hiérarchique modifiée.

- Une comparaison des différents types d'architectures de contrôle de systèmes multi-robots mobiles est réalisée et analysée.
- Un ensemble de recommandations et d'exigences de sécurité est fourni pour préserver un fonctionnement sûr et sécurisé du système.
- Une stratégie de contrôle pour optimiser le suivi de la trajectoire des robots mobiles est proposée et implémentée.

- Organisation du manuscrit

Ce manuscrit est organisé en quatre chapitres.

Après une introduction générale, le **premier chapitre** présente les notions de base de la sécurité et du risque industriel, de la gestion de risque et de ses étapes. Il enchaine sur un état de l'art des normes de sécurité dans le domaine de la robotique et introduit les techniques de prévision et d'analyse des risques des systèmes robotisés.

Le **deuxième chapitre** réalise un état de l'art des méthodes d'identification et d'analyse des risques, développées dans la littérature : méthode d'analyse des modes de défaillance AMDE/AMDEC, analyse basée sur le modèle de causalité des accidents STPA, analyse par arbre de défaillances ADD, méthode du nœud papillon et méthode basée sur l'utilisation de réseaux de Petri RdP.

Le **troisième chapitre** est dédié à la mise en œuvre de plusieurs combinaisons de méthodes d'analyse des risques : AMDEC-ADD, STPA-ADD, STPA-nœud papillon, STPA-RdP. Les résultats obtenus sont analysés en termes de sureté et de sécurité à travers une application robotique en environnement de laboratoire à risques.

Le **quatrième chapitre** est consacré au développement de lois de contrôle d'un robot mobile à roues différentielles. Une simulation 3D sous Gazebo et une application temps réel sur robot mobile de type « Turtlebot2^{TM} » permettent de valider cette approche.

Nous terminons ce manuscrit par une conclusion générale et quelques perspectives de ce travail.

Chapitre I

Maitrise des risques et sécurité des systèmes industriels complexes

I.1 Introduction

En raison du développement continu de l'industrialisation et de l'incapacité des travailleurs à accomplir certaines missions difficiles, les sites industriels sont plus en plus équipés de systèmes complexes hautement automatisés, tels les systèmes robotiques. Cette complexité représente un facteur d'efficacité grâce à la capacité de ces systèmes d'exécuter des fonctions hautement intégrées, optimisant les exigences de temps, de prix et d'énergie. Toutefois, cette complexité est un facteur de risque. De ce fait, la gestion des risques et de la sécurité est une exigence incontournable au sein de ces milieux. La gestion de la sécurité dans l'industrie des procédés consiste en un ensemble de procédures et de stratégies permettant d'évaluer les procédés susceptibles de provoquer des incidents catastrophiques tels des incendies, des explosions ou des rejets toxiques (OSHA, 2000) [4]. Par conséquent, le principal objectif d'un processus d'analyse et de gestion des risques consiste à appuyer la prise de décision concernant la mise en place des actions et des barrières de réduction et de contrôle des risques nécessaires en évaluant les risques associés à l'exploitation et à la conception des systèmes techniques [5]. L'automatisation industrielle étendue et le contrôle informatique ont créé de nombreux problèmes de sécurité émergeant, qui ont été largement discutés dans la littérature [6–7]. La préservation de la sécurité des systèmes et des applications industrielles est un des enjeux primordiaux actuels.

Dans ce chapitre, nous présentons d'abord quelques définitions et concepts essentiels à la compréhension de la notion de risque et de sécurité. Dans un deuxième temps, nous décrivons les différentes étapes du processus de gestion des risques. Nous présentons alors l'ensemble des normes et techniques de prévision utilisées pour traiter les problèmes de la sécurité et de la gestion du risque dans les applications robotiques. Enfin, une présentation de différentes classifications des méthodes d'analyse des risques clôt ce chapitre.

I.2 Notions de risques et de sécurité industrielle

Il existe de nombreuses normes liées à la sécurité industrielle qui visent à définir les exigences de base que les installations doivent respecter. Des organisations de normalisation locales et internationales se consacrent à la fourniture de ces normes, telles que : IANOR, AFNOR, CEN, ISO, CEI, etc. A titre d'exemples, nous citons ci-dessous quelques normes de sécurité de référence :

- Les normes canadiennes telles que : la norme CSA Z432 pour la sécurité des machines et la norme CSA Z434 pour la sécurité des robots industriels.
- Les normes américaines : la norme ANSI B11 Série, particulière à certaines machines ; la norme OSHA 1910 pour les machines et leur surveillance ; la norme RIA 15.06 pour les robots industriels.
- Les normes internationales, européennes et de la commission électrotechnique internationale, telle la norme ISO 12100, définissent les concepts de base et les principes généraux de conception pour l'appréciation du risque et sa réduction.
- La norme générique CEI 61508 pour la sécurité fonctionnelle des systèmes électriques/électroniques et électroniques programmables relatifs à la sécurité, et sa norme sectorielle CEI 61511, qui concerne les systèmes instrumentés de sécurité pour le secteur des processus industriels.
- Les normes concernant un aspect particulier de la sécurité des machines EN 547, EN 614.

Afin d'analyser le concept de sécurité inhérente aux systèmes industriels complexes, il nous a semblé primordial de consacrer cette section aux notions de base liées aux risques et à la sécurité industrielle suivant les normes de sécurité.

I.2.1 Notion de danger

Selon les normes CEI 60300-3-9 [8], CEI 61508 [9] et ISO/CEI Guide 51 [10], établies respectivement en 1995, en 2010 et en 2014, le danger désigne « une source potentielle de dommage ou une nuisance pouvant causer des dommages ». Le référentiel OHSAS 18001 [11], établi en 1999, définit également le danger comme étant une source ou une situation pouvant entraîner des blessures ou atteinte à la santé, des dommages matériels et environnementaux ou une combinaison de ces éléments.

Dans ce cadre, la notion de « source » est ambiguë et peut être interprétée de différentes manières. Elle peut représenter une défaillance, une faute ou une erreur dans la terminologie de Laprie et al. [12–13]. Dans le domaine industriel, elle peut également désigner une propriété intrinsèque d'une substance dangereuse ou d'une situation physique inappropriée [14].

Selon Guiochet [13], dans le cadre d'un système automatisé, il est important de prendre en compte l'état dans lequel se trouve le système et les conditions d'environnement pour définir un danger. Ces considérations se rapprochent de la définition

donnée pour les systèmes informatiques par Leveson [15], où le danger (en anglais, hazard) est défini comme « un état ou un ensemble de conditions d'un système (ou d'un objet), qui, couplé à d'autres conditions de son environnement mèneront inévitablement à un accident ».

Dans l'industrie chimique et ses procédés, le danger est « la combinaison d'une matière dangereuse, d'un environnement d'exploitation et de certains événements imprévus qui pourraient entraîner un accident » [16].

I.2.2 Notion de risque

La norme ISO/CEI Guide 51 [10] définit le risque comme étant« la combinaison de la probabilité de la survenue d'un dommage et de sa gravité ». Un dommage inclut dès lors tout type de blessures physiques ou atteinte à la santé des personnes, atteinte aux biens ou à l'environnement.

La probabilité d'occurrence est assimilée à la fréquence à laquelle un événement se produit. Cette fréquence peut s'exprimer comme le nombre d'événements par unité de temps. En d'autres termes, la probabilité qu'un événement se produise correspond aux chances raisonnables que l'événement se produise. La gravité peut, quant à elle, se définir comme le dommage maximum correspondant à un accident ou à un danger [17].

Cependant, la notion de risque dans le domaine industriel est définie comme étant : « un événement accidentel se produisant sur un site industriel lors des différentes activités industrielles et entraînant des conséquences immédiates graves pour le personnel, les populations avoisinantes, les biens et/ou l'environnement ». Généralement, les risques industriels sont répartis en deux catégories selon la gravité qu'ils peuvent entraîner [14] :

- **Risques professionnels :** ils sont à l'origine des accidents du travail et des maladies professionnelles ou à caractère professionnel. Les principales familles de risques professionnels sont : les risques mécaniques, électriques, physiques, chimiques, biologiques, les risques dus aux manutentions manuelles et les risques de transport.
- **Risques environnementaux :** On peut distinguer deux grandes catégories, qui peuvent être des risques de dommages externes, en provenance de la nature ou de l'environnement et ayant un impact sur le site industriel (e.g. inondation, glissement de terrain, feux de forêt …). Ils peuvent également être des risques

technologiques industriels internes engendrés par l'entreprise et ayant un effet sur son environnement. Ces risques industriels sont appelés majeurs, lorsqu'ils sont caractérisés par une probabilité faible et une gravité importante. Ils sont notamment liés à la possibilité qu'un accident catastrophique se produise.

- **Risques industriels majeurs :** par leur nature, ils sont classés en trois principaux types [18] :
  - **Le risque thermique** : souvent appelé « risque d'incendie ». Un incendie se produit lorsque trois facteurs sont combinés : le combustible, le comburant et la source de chaleur. De plus, si le feu atteint des réserves chimiques, des nuages toxiques pour la santé humaine et l'environnement apparaîtront.
  - **Le risque de surpression** : connu également sous le nom de risque d'explosion, correspondant à une évolution rapide d'un système, avec libération soudaine d'énergie et la formation d'ondes de choc. La taille de l'onde de choc peut détruire la stabilité de la structure matérielle et causer des dommages au corps humain. De plus, des produits toxiques peuvent être rejetés dans l'atmosphère.
  - **Le risque de toxicité** : dû à la diffusion de produits dangereux dans l'air, l'eau ou le sol telles les substances ou préparations chimiques. Celles-ci peuvent être corrosives, cancérigènes, mutagènes, toxiques pour la reproduction, explosives, inflammables, etc. Elles peuvent causer, d'une part, des accidents graves (brûlures, intoxications, explosions…), voire des maladies professionnelles (allergies, cancers…). D'autre part, elles peuvent polluer l'environnement lors de déversements accidentels ou d'émissions diffuses.

I.2.3 Notion d'acceptabilité du risque

La notion de risque acceptable est essentielle pour caractériser le degré de confiance attribué au système [13]. Un risque acceptable (ou tolérable) doit prendre en compte un contexte donné. Il est fondé sur les valeurs admises par la société [10]. L'évaluation de l'acceptabilité du risque peut se faire à l'aide d'un ensemble de critères définis en termes qualitatifs ou quantitatifs, selon l'expression du risque [19].

Les critères d'acceptation des risques sont des critères utilisés comme base pour des décisions de niveau global de risque acceptable. Ces critères sont considérés également

comme une référence pour évaluer le besoin de mesures de réduction des risques et doivent donc être définis avant d'exécuter une analyse des risques. De plus, les critères d'acceptation des risques doivent refléter les objectifs de sécurité et les caractéristiques distinctives de l'activité.

Les critères d'acceptation des risques peuvent être basés sur les exigences des autorités, l'expérience, les connaissances théoriques et les normes [19–20].

I.2.4 Notion de sécurité

Le concept de sécurité est devenu l'un des enjeux les plus importants pour de nombreux domaines technologiques. Il a de nombreuses significations. Il est parfois utilisé pour exprimer « l'absence de conditions pouvant entraîner des dégâts ou des pertes » [20].

De la même manière que la fiabilité et la disponibilité dans diverses normes, la sécurité d'un système est également définie en matière d'aptitude comme suit : « 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 » [21].

A titre d'exemple, dans le domaine de la robotique industrielle, la sécurité est définie comme la prévention de dégâts sur l'humain, le robot et les éléments avec lesquels le robot interagit [22].

Dans notre étude, nous allons adopter la définition du terme « sécurité » en suivant le guide ISO/CEI 51[10]. Elle introduit l'absence du risque inacceptable [13]. Contrairement aux autres définitions (valeurs absolues) mentionnées ci-dessus, cette définition fournit une valeur pratique pour le terme « sécurité ».

La sécurité peut donner un niveau de confiance aux systèmes et installations vis-à-vis des risques encourus. Elle doit inclure tout type de populations potentiellement affectées (humaine, matérielle et fonctionnelle). De ce fait, la sécurité industrielle concerne également différents aspects comprenant :

- La sécurité individuelle (des humains et travailleurs)
- La sécurité des installations industrielles (mécaniques, électriques, chimiques, informatiques…)
- La sécurité des équipements et matériels (appareils et machines industriels)

- La sécurité des réseaux de communication
- La sécurité des produits…

L'objectif est la réduction de ces risques liés aux activités de l'entreprise, sur les plans environnemental, social et économique [23].

I.2.5 Notion de sureté de fonctionnement et sa relation avec la sécurité

La norme CEI 60050 définit le terme « sureté de fonctionnement » comme étant : « L'aptitude à fonctionner quand et tel que requis ; la sûreté de fonctionnement comprend la disponibilité, la fiabilité, la maintenabilité, l'efficacité de la logistique de maintenance et, dans certains cas, d'autres caractéristiques telles que la durabilité, la sûreté et la sécurité ».

La sureté de fonctionnement englobe une riche palette de méthodes et d'outils qui permettent la maitrise des risques et, par conséquent, d'atteindre la sécurité. Autrement dit, la sécurité exige un certain niveau de confiance dans le comportement des systèmes industriels, et l'objectif de la sureté de fonctionnement est de le justifier [24–25].

I.3 Gestion du risque et son processus

La norme générique IEC 60300-3-9 définie en 1995 [8] et la norme ISO 31000 (2018) [26] caractérisent la gestion du risque (en anglais : Risk Management) comme un processus de gestion continue dont l'objectif est d'identifier, d'analyser et d'évaluer les dangers potentiels dans un système ou liés une activité. Ce processus permet d'identifier et d'introduire des mesures de contrôle et de traitement vis-à-vis des risques pour éliminer ou réduire les dommages potentiels aux personnes, à l'environnement ou à d'autres biens [20]. Cette approche a été recommandée dans de nombreux domaines technologiques, y compris la robotique. De ce fait, plusieurs normes ont été élaborées afin de mettre en œuvre le processus de gestion pour les systèmes critiques dans l'industrie [6] :

- La norme centrale ISO 26262 pour l'industrie automobile
- La norme de référence EN 62061 pour les machines industrielles
- La norme ISO 10218 pour la robotique.

Le processus de gestion du risque comporte trois étapes principales : son analyse, son évaluation et sa réduction. La figure I.1 illustre schématiquement les différentes étapes de ce processus.

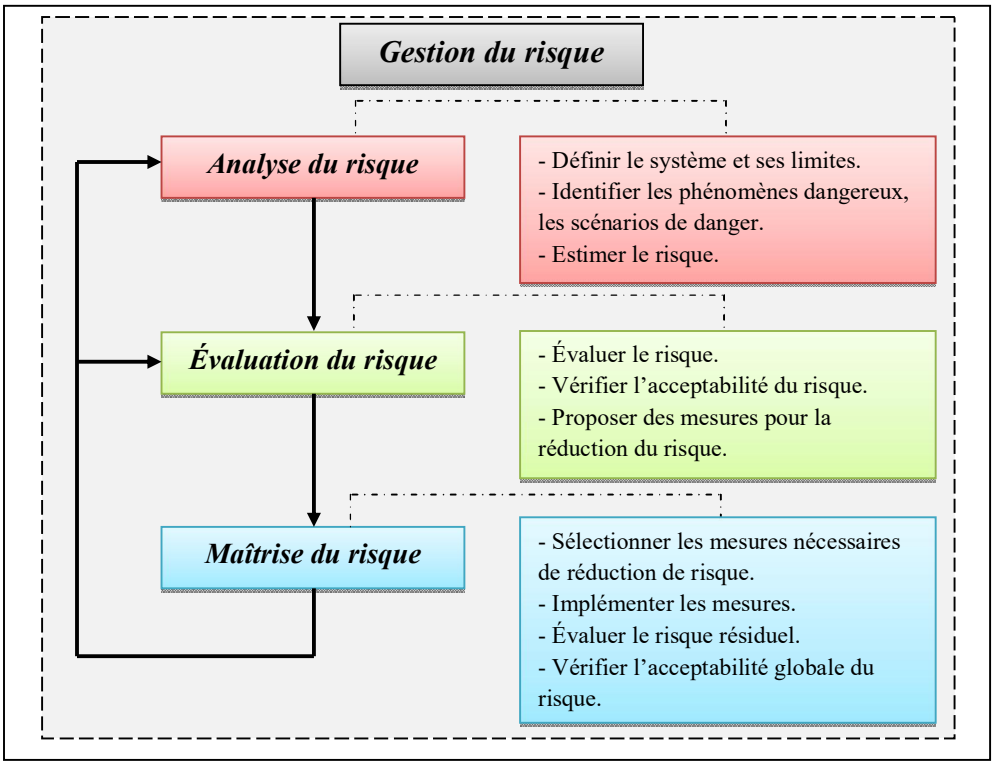


Figure I.1 Les trois étapes de la gestion du risque, selon la norme IEC 60300-3-9 définie en 1995 [20]

I.3.1 Analyse du risque

Une analyse des risques est une approche proactive, en ce sens qu'elle traite exclusivement des accidents potentiels. Elle s'oppose à l'enquête sur les accidents, qui est une approche réactive, cherchant à déterminer les causes et les circonstances des accidents qui se sont déjà produits. Elle peut également être définie selon la norme IEC 60300-3-9, 1995 [8] et le Guide ISO/CEI 51 [10], comme une utilisation systématique des informations disponibles pour identifier les dangers et estimer les risques pour les individus, les biens et l'environnement [20], dont le but est de comprendre la nature et les caractéristiques des risques [26].

L'analyse du risque peut être effectuée selon différents niveaux de détails et de complexité suivant l'objectif de l'analyse, la fiabilité des informations et des ressources disponibles. Les techniques d'analyse peuvent être qualitatives, quantitatives, ou être une combinaison de celles-ci (ISO 31000, 2018) [26].

La démarche générale de l'analyse de risque comprend trois étapes principales :

1. **Identification des dangers :** dans cette étape, les dangers liés au système, ainsi que les événements dangereux potentiels, sont identifiés.

2. **Analyse de fréquence :** cette étape adopte généralement une analyse déductive dont le but est d'identifier les causes de chaque événement dangereux. Elle estime sa fréquence en se basant sur des données expérimentales et/ou des jugements d'experts.
3. **Analyse des conséquences :** une analyse inductive est effectuée afin d'identifier toutes les séquences potentielles d'événements pouvant résulter de l'événement dangereux. L'objectif consiste donc à identifier toutes les conséquences finales potentielles ainsi que leur probabilité d'occurrence [20].

I.3.2 Estimation du risque

Cette étape nous permet de calculer ou mesurer le risque. L'estimation comprend la détermination de la gravité des dommages et la probabilité d'occurrence des phénomènes dangereux conduisant à ce dommage.

Toute étude commence par une estimation qualitative ; et lorsque les données nécessaires sont disponibles, elle se poursuit par une étude quantitative [13].

I.3.3 Evaluation du risque

L'évaluation du risque est un processus dans lequel des jugements sont réalisés sur la tolérabilité (ou l'acceptabilité) du risque sur la base d'une analyse des risques et en tenant compte de facteurs tels les aspects socioéconomiques et environnementaux (lEC 60300-3-9, 1995) [20].

L'activité d'évaluation se réalise par une comparaison des résultats de l'analyse avec un ensemble de critères d'acceptation des risques. Cette étape aide à la prise de décision par rapport à l'acceptabilité du risque probable [13 ; 20].

En fonction de l'objectif visé, l'évaluation du risque peut être divisée en trois types principaux.

I.3.3.1 Evaluation qualitative : Matrice de risques

Ce type d'évaluation est basé sur des méthodes qualitatives. Ces méthodes ne fournissent pas une représentation et une description numériques ; cependant, elles offrent de puissantes capacités de perception du risque qui peuvent être utilisées pour sa mitigation [27]. Les probabilités et les conséquences sont déterminées d'une manière purement

qualitative [20]. Parmi ces méthodes, la matrice de risques est généralement adoptée par le milieu industriel du fait de sa simplicité et de son efficacité.

La matrice de risques est la technique d'évaluation qualitative la plus utilisée depuis sa création. Elle a été initialement développée par Garvey & Lansdowne en 1998 [28]. L'évaluation des risques repose sur différents paramètres dont les principaux sont la probabilité d'occurrence du danger et la gravité de ses conséquences [17]. Plusieurs chercheurs (Ni, Chen et Chen, 2010 [29] ; Ruge, 2004 [30]) ont classé la matrice de risques comme une approche semi-quantitative. Cependant, si les deux paramètres du risque sont exprimés de manière qualitative, la matrice des risques devient une approche purement qualitative. Dans cette approche, les paramètres sont placés dans un plan défini par deux axes gradués, créant ainsi ce qu'on appelle « la grille de criticité ». Une limitation en acceptabilité doit être identifiée sur cette grille. Le principal avantage de la matrice des risques est qu'elle permet de représenter des données de risques complexes sous une forme compressée. Elle permet également de visualiser les différents résultats d'évaluation [27]. Un modèle simple de matrice de risques est représenté sur la figure I.2.

Probabilité d'occurrence \ *Gravité des conséquences*	Négligeable	Significative	Grave	Très grave
Très fréquent	Moyen	Important	Critique	Critique
Fréquent	Faible	Moyen	Important	Critique
Peu fréquent	Faible	Moyen	Moyen	Important
Rare	Faible	Faible	Faible	Moyen

Figure I.2 Matrice simple de risques [28]

I.3.3.2 Evaluation semi quantitative :

Les termes « évaluation semi-quantitative des risques » sont parfois utilisés pour quantifier les probabilités et les conséquences approximativement dans des intervalles. Les approches semi-quantitatives sont utilisées, en particulier, lorsque la mesure directe du risque n'est pas possible [20 ; 27].

I.3.3.3 Evaluation quantitative :

Contrairement aux techniques semi-quantitatives, les méthodes quantitatives évaluent les risques avec précision. Du point de vue de la prise de décision et de l'analyse de la sécurité, la nature inhérente de ces méthodes les rend supérieures aux méthodes qualitatives et semi-quantitatives [27].

L'objectif de cette phase est de déboucher sur des décisions plus judicieuses. Elle revient à comparer les résultats de l'analyse du risque aux critères de risque établis afin d'estimer le niveau de risque et de déterminer si une action de traitement supplémentaire est exigée [26].

I.3.4 Maitrise du risque

La maîtrise du risque aborde l'ensemble des étapes au cours desquelles les mesures de réduction des risques doivent être sélectionnées.

Selon la définition du risque, il existe deux principaux types de moyens de réduction du risque : les mécanismes de protection, qui sont conçus pour réduire la gravité du dommage, et les actions de prévention, qui visent à réduire la probabilité d'occurrence du dommage [13]. Il s'agit d'identifier les barrières nécessaires pour ramener le niveau de risque des différents scénarios d'accidents à un niveau jugé satisfaisant ou acceptable. La figure I.3 montre l'influence des mesures de prévention et de protection sur la réduction du risque.

Citons quelques exemples de barrières de protection : le 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 peut être assurée par une conception sûre de l'installation ou par l'ajout de systèmes assurant la sécurité de l'installation en cas de dérive. Afin de protéger une installation contre les surpressions, les barrières de prévention peuvent consister en une soupape de sécurité ou un disque de rupture.

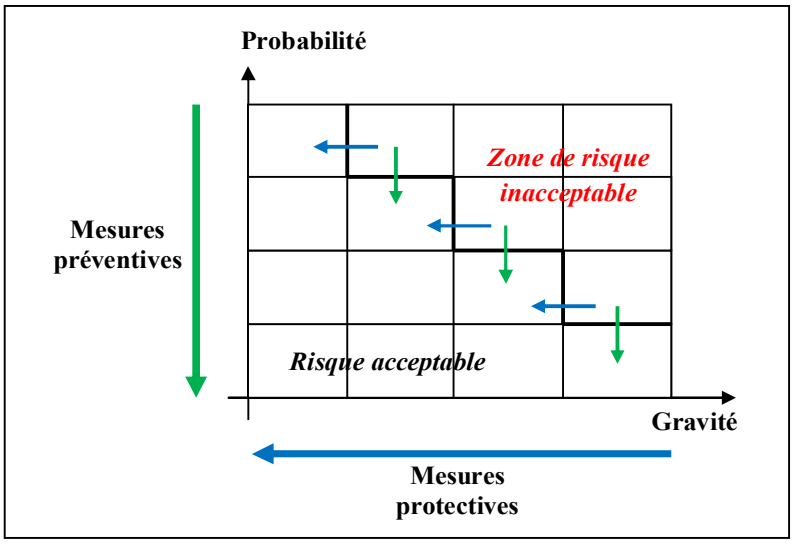


Figure I.3 Influence des mesures de prévention et de protection sur la réduction du risque

I.4 Sécurité des systèmes robotisés – Etat de l'art

La technologie des robots a été largement utilisée dans divers domaines. Les deux premiers apports de ces machines étaient de répondre aux besoins de l'industrie manufacturière et aux besoins de l'industrie dans un contexte dangereux pour l'homme. Leur objectif a toujours été d'améliorer les performances et d'offrir une plus grande flexibilité.

Le premier robot industriel était un robot à bras. Sa fonction essentielle était le déplacement de produits d'un endroit à un autre. A l'heure actuelle, il est complété dans le domaine manufacturier par des robots mobiles de transport (en anglais, Automated Guided Vehicle ou AGV), des robots de picking, ou des robots d'assistance ayant beaucoup de points communs avec les robots de service. A titre d'exemple, citons les robots d'assistance prenant la forme d'un bras mécatronique, dédiés à des tâches industrielles pénibles tels le brossage, le burinage ou encore la manipulation. De plus, le déplacement d'objets ou d'équipements par les robots aux côtés des humains dans des environnements contraints font l'objet de nombreux développements. À titre d'exemple, citons le robot Kiva d'Amazon, dont le rôle est de déplacer les étagères sur lesquelles sont stockés les produits à livrer jusqu'aux personnes chargées de leur mise sous plis. Citons également le robot mobile collaboratif conçu par Air-Cobot pour effectuer l'inspection de l'extérieur d'un avion. La figure I.4 présente différents types de robots industriels.

Figure I.4 Différents types de robots industriels

Une conséquence directe du déploiement de robots dans l'industrie est le risque accru de nouveaux accidents pour les travailleurs et leur environnement immédiat. Par conséquent, de nouveaux enjeux liés à la sécurité et à la prévention des accidents sont apparus dans ce domaine. Les risques dus à l'utilisation de ces robots doivent être identifiés et réduits [31 ; 32]. Dans la section suivante, nous présentons l'ensemble des normes utilisées visant à préserver la sécurité des systèmes robotisés dans le cadre d'un environnement industriel.

I.4.1 Normes relatives à la sécurité des systèmes robotisés

Plusieurs normes de certification ont été recommandées afin de commercialiser les machines, y compris les robots industriels. Il s'agit notamment de la norme ISO 12100, qui spécifie une méthodologie pour assurer la sécurité dans la conception des machines et de la norme ISO 13849, qui fournit des exigences sur la conception et les principes d'intégration des parties des systèmes de commande relatives à la sécurité. En outre, la norme IEC 61508, dédiée à la sécurité fonctionnelle, permet de lier le matériel au logiciel. L'idée centrale de ces normes est de fournir des fonctions de sécurité spécifiques au domaine et

des niveaux de confiance associés qui doivent être garantis. Cependant, ces directives sont élaborées pour des machines fixes. Pourtant, en raison du contact physique requis entre les utilisateurs et les pièces mobiles du robot, ces directives ou normes ne sont pas entièrement applicables [6]. De ce fait, l'élaboration de normes spécifiques aux systèmes robotisés devenait une exigence incontournable.

La première norme de sécurité spécifique pour les robots, ISO 10218 : 1992, est tout à fait adaptée aux robots industriels classiques de type « manipulateur ». Ses recommandations sont principalement basées sur l'isolement entre le robot et l'humain afin d'éviter le risque de collision. Ce principe utilise une barrière physique telle qu'une clôture ou une barrière immatérielle (i.e. un capteur optoélectronique), de sorte que le robot s'arrête immédiatement lorsqu'une personne ou un objet passe à travers celle-ci [33]. La norme ISO 10218 a été révisée deux fois depuis sa création : en 2006, puis en 2011.

La première révision ISO 10218-1 : 2006 concerne les fabricants de robots. Elle est basée sur la conception et la construction du robot lui-même. Elle introduit le nouveau concept de « modes de fonctionnement collaboratifs » pour lequel des robots spécialement conçus travaillent en coopération directe avec les humains tout en respectant constamment les limites strictes de vitesse maximale et de force statique. La deuxième révision de l'ISO 10218 : 2011 est composée de deux parties. La première, l'ISO 10218-1 : 2011, est une mise à jour de la version précédente. La deuxième partie de la norme, l'ISO 10218-2 : 2011 [34], détaille les exigences de sécurité pour l'installation de cellules robotisées [35].

Il existe également d'autres réglementations industrielles intégrant les risques pour les travailleurs dans le cadre de l'utilisation de robots. Citons la spécification technique ISO / TS 15066 : 2016 [36] pour les robots collaboratifs, la norme américaine ANSI / RIA R15.06 [37] et la norme européenne EN 775, adaptations de l'ISO 10218. Contrairement à l'idée d'isolement mentionnée dans les normes conventionnelles, les mises-à-jour qui sont apparues depuis 2006 fournissent d'autres types de systèmes de sécurité afin de détecter les obstacles lors de leurs mouvements. Elles appliquent des stratégies d'évitement appropriées. En cas d'impact inattendu ou inévitable, les dommages seront minimisés [35].

La dernière spécification technique ISO / TS 15066 : 2016 [36] tente de préciser davantage la collaboration homme-robot en complétant les exigences et les lignes directrices établies par la norme ISO 10218.

Enfin, signalons que la norme internationale ISO 8373 (2012) spécifie le vocabulaire relatif aux robots et aux dispositifs robotiques. Outre la définition de termes bien établis tels que « robots » et « systèmes de contrôle », elle définit de nouveaux termes liés au développement de nouvelles tâches collaboratives dans des environnements industriels et non industriels, tels « l'interaction homme-machine » et « les robots de service » [35].

I.4.2 Techniques utilisées pour la prévision des risques des systèmes robotisés

Dans le cadre de toute application relevant d'une institution donnée, la sécurité est primordiale. Un processus d'analyse et de gestion des risques doit y être appliqué afin de garantir un certain niveau de sécurité. L'objectif est de savoir dans quelle mesure nous pouvons faire confiance à ces systèmes. D'autant plus que ceux-ci pourront être développés afin de couvrir un éventail plus large d'applications.

De nombreux chercheurs ont ciblé le domaine de la gestion des risques et de la conception de la sécurité. Dès lors, un ensemble de méthodes d'analyse, telles l'analyse des modes de défaillance et de leurs effets (AMDE) et l'analyse des arbres de défaillances[1] (ADD), ont été largement utilisées pour traiter le problème de l'évaluation de la sécurité, notamment dans le cadre du développement d'applications robotiques industrielles conventionnelles [38–40]. Certains chercheurs ont également abordé les problèmes de sécurité d'applications utilisant des robots autonomes et collaboratifs. Dès lors, ils se sont penchés sur l'élaboration de combinaisons de différentes méthodes d'analyse des risques ou sur l'amélioration des méthodes conventionnelles. Toutes ces propositions visent une adaptation de ces méthodes dans le cadre de systèmes complexes de plus en plus interconnectés.

En 2009, Kazanzides [41] a combiné les deux méthodes conventionnelles AMDE et ADD. Son objectif était d'analyser les dangers et de mettre en place une boucle de contrôle de sécurité pour un robot chirurgical.

Une autre approche a été proposée par S. Lee et Yam [42] en 2012, similaire à la précédente, mais inversement combinée. Les analyses ADD et AMDE sont combinées afin d'examiner les défaillances potentielles des robots coopératifs HCR (en anglais, Human-Cooperative Robot) qui conduisent à un mouvement dangereux du robot. Cette approche fournit les fonctions de sécurité appropriées à ces défaillances avec un niveau de sécurité requis.

[1]Encore appelés « arbres de fautes » ou « arbres de pannes »

En 2010, une nouvelle approche, dénommée HAZOP (acronyme de « Hazard and Operability studies »), a été proposée par Böhm & Gruber [43]. Elle a été appliquée à un robot mobile thérapeutique. Par leur approche, les auteurs ont tenté de couvrir tous les dangers associés aux composants et liés aux opérations.

En 2009**,** Alexander et al. [44] ont combiné un ensemble de techniques pour identifier les dangers et dériver les exigences de sécurité pour les systèmes autonomes. Dans un premier temps, l'analyse ETBA (acronyme de « Energy Trace and Barrier Analysis ») et les Checklists sont utilisées pour fournir une identification des dangers. Dans un second temps, une analyse détaillée est réalisée à l'aide des méthodes FFA (acronyme de « Functional Failure Analysis ») et HAZOP.

En 2012, Woodman et al. [45] proposent une approche basée sur l'analyse SHARD (acronyme de « Software Hazard Analysis and Resolution in Design ») ainsi qu'une Checklist des risques dans le cadre de la mise en œuvre d'un robot mobile autonome personnel.

En 2014, Dogramadzi et al. [46] ont développé une approche environnementale appelée ESHA (acronyme de « Environmental Survey Hazard Analysis ») pour l'identification des dangers dans le contexte d'applications utilisant des robots mobiles autonomes.

Martin-Guillerez et al. [47] en 2010, Machin [48] en 2015 et Guiochet [49] en 2016 ont discuté le problème de l'interaction entre l'homme et le robot en développant la technique HAZOP basée sur une modélisation UML (acronyme de « Unified Modeling Language »). Cette étude visait à traiter l'interaction homme-robot dans le cadre d'un robot manipulateur mobile.

Toutefois, la composition des systèmes robotisés actuels conduit à l'apparition d'un type de danger émergeant, non plus causé par la défaillance des composants, mais par l'utilisation intensive des logiciels, le niveau d'autonomie caractérisant leurs systèmes de contrôle et le nombre important d'interactions entre les composants. Les techniques conventionnelles d'analyse des risques telles l'AMDEC, l'ADD et HAZOP, basées sur la théorie de la fiabilité et la décomposition fonctionnelle, et qui décrivent le système comme un certain nombre de sous-systèmes presque indépendants [50] , ne sont plus adéquates. En particulier, elles ne peuvent représenter les interactions indirectes entre les composants du

système et ne prennent pas en compte les conditions qui conduisent à des comportements inappropriés.

Au cours des dernières décennies, Leveson a développé une analyse appelée STPA (acronyme de « System Theoretic Process Analysis ») [51–52] basée sur la théorie du système qui considère la sécurité comme un problème de contrôle plutôt qu'un problème de défaillance des composants. STPA est une technique d'analyse des dangers. Elle est dédiée à l'identification des dangers des systèmes automatisés de haute complexité. La complexité est illustrée par les architectures de contrôle/commande et les interactions entre ces dernières. Ces techniques manipulent du matériel, des logiciels, des opérateurs humains, afin de les intégrer dans un processus unifié [50].

Récemment, l'analyse STPA a été très utilisée grâce à sa capacité à analyser de nombreux types de systèmes automatisés. Citons les systèmes de conduite [53], les systèmes aéronautiques [50 ; 54], le transport aérien [55], les systèmes d'exploration aérospatiale [56], les systèmes chirurgicaux robotisés [57]. Elle est également utilisée dans le cadre des systèmes autonomes tels les véhicules autonomes [58], et les navires autonomes [59–60]. Citons enfin son utilisation dans plusieurs industries tels le secteur énergétique [61], le secteur sous-marin [62–64], l'industrie des procédés [65–66] et l'industrie nucléaire [67–70].

De plus, un certain nombre d'études comparatives de l'analyse des dangers STPA avec différentes méthodes conventionnelles d'analyse des risques ont rapporté une évaluation positive de l'application de l'analyse STPA, et ceci sur divers systèmes complexes. Donnons quelques exemples : En 2010, Ishimatsu et al. [71] ont comparé les résultats de l'analyse STPA avec les résultats de l'ADD, montrant que l'approche STPA identifie des facteurs de causalité supplémentaires à ceux identifiés par l'analyse ADD. En 2011, Nakao et al. [72] concluent que l'approche STPA rend la génération d'exigences et de contraintes de sécurité plus facile et plus flexible. En 2013, Fleming et al. [55] soutiennent que l'analyse STPA permet l'identification des défauts liés au logiciel et au comportement dynamique du système, contrairement aux méthodes plus anciennes telles que l'AMDE, l'ADD, etc.

La figure I.5 résume l'ensemble des techniques d'analyse des systèmes robotisés utilisées par les chercheurs dans le domaine de la sécurité et de la prévision des risques.

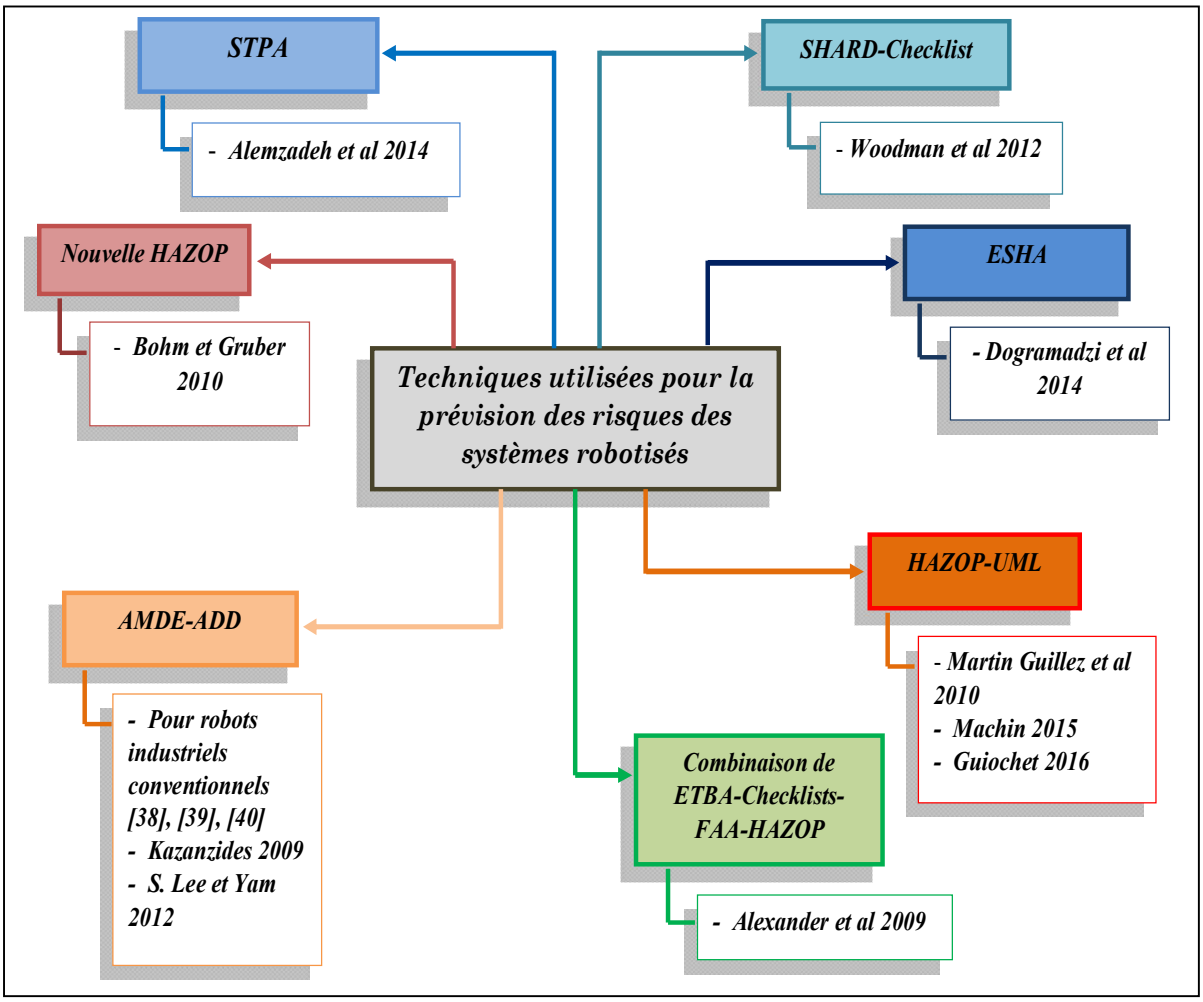


Figure I.5 Techniques de prévision des risques pour les systèmes robotisés

I.5 Méthodes d'analyse des risques

La gestion des risques est l'un des enjeux importants que doivent affronter les industriels. Afin d'y faire face, plusieurs méthodes et outils d'analyse des risques ont été élaborés dans le but de fournir une investigation systématique et bien structurée des installations industrielles et de leurs différentes applications. Texier [73] a rassemblé 62 méthodes d'analyse des risques susceptibles d'être appliquées en milieu industriel.

L'objectif d'une analyse des risques consiste à estimer les causes, les conséquences, puis à construire les scénarios d'apparition du danger.

Selon la norme IEC 31010:2009 [74], une méthodologie particulière d'analyse des risques peut être choisie en fonction de plusieurs facteurs :

- Le type et l'étendue du risque analysé.
- Le contexte de l'étude et les objectifs recherchés.

- Le degré d'expertise, les ressources humaines et autres ressources requises : une méthode bien structurée peut produire de meilleurs résultats qu'une procédure sophistiquée, pour autant qu'elle réponde aux objectifs de l'analyse.
- Les besoins des facteurs de décision selon le niveau de détail requis pour l'analyse. Dans certains cas, un niveau élevé de détails est requis pour prendre une bonne décision, tandis que dans d'autres cas, une compréhension plus générale est suffisante.
- L'ampleur des conséquences potentielles. La décision sur la profondeur de l'évaluation des risques devra être effectuée selon la perception préliminaire des conséquences.
- La disponibilité des informations et des données.

I.5.1 Classification des différentes méthodes d'analyse

Les méthodes d'analyse des risques peuvent être classées selon plusieurs critères. Cette classification est présentée à la figure I.6 :

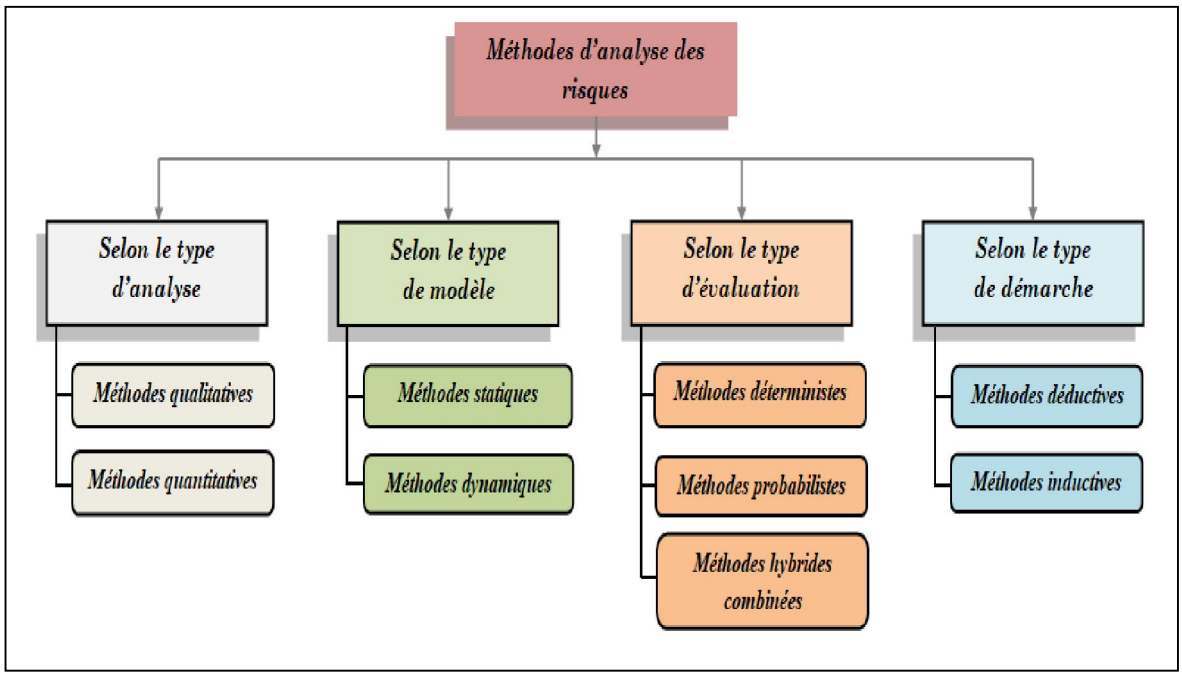


Figure I.6 Classification des méthodes d'analyse des risques

- **Selon le type d'analyse –** Il existe deux principaux types d'analyse, à savoir, qualitative et quantitative [73].
- **Selon le type de modèle –** L'analyse des risques peut être effectuée de deux manières, soit on suit une approche statique, qui permet l'analyse du système d'un point de vue structurel sans avoir à considérer les changements du système

au cours du temps, soit une approche dynamique qui tient compte des aspects comportemental et temporel du système [75].

- **Selon le type d'évaluation –** La phase d'évaluation des risques peut être réalisée selon trois approches différentes : évaluation des conséquences des dommages (approche déterministe), évaluation de la probabilité d'accident (approche probabiliste), évaluation combinée des deux approches précédentes (approche hybride combinée) [73].
- **Selon le type de démarche adoptée par la méthode –** Généralement, deux catégories de démarches sont considérées : la première, déductive ou descendante ; et la seconde, inductive ou ascendante.

  La première est basée sur la déduction logique : l'analyse va du général au particulier, la détermination des défaillances et leurs combinaisons induisant un effet indésirable donné (cette approche considère un événement redouté dont elle cherche à expliquer les causes). Nous partons alors des conséquences pour remonter aux causes. A titre d'exemple, citons l'analyse par arbre de défaillances (ADD), qui est utilisée pour déduire et représenter, avec un arbre logique, des combinaisons d'événements (comme des défaillances) conduisant à un événement majeur.

  A l'inverse, la seconde catégorie, inductive ou ascendante, est basée sur l'induction logique. Il s'agit d'une démarche cause-effet, c'est-à-dire que cette approche va du particulier au général, de l'observation à la modélisation, des causes pour identifier les conséquences selon un enchaînement d'événements. A titre d'exemples, citons l'analyse des modes de défaillance, de leurs effets et de leur criticité AMDEC et l'analyse de risques et de sécurité de fonctionnement HAZOP. Ces méthodes sont basées sur l'utilisation d'un tableau listant les écarts (ou modes de défaillance), leurs causes, leurs conséquences et les éventuelles actions correctives [75–76].

I.5.2 Types d'entrées

Dans les travaux de Tixier [73], sept catégories de données d'entré ont été proposées. Ces données ont été adoptées par différentes méthodes d'analyse des risques. Ces données peuvent être techniques telles les caractéristiques du processus ; qualitatives, telles les politiques de sécurité ; ou être constituées de bases de données quantitatives.

- **Les plans ou schémas** sont utilisés pour la description du site, de l'installation, des unités.
- **Les processus et les réactions** sont utilisés pour la description des opérations et des tâches, physiques et caractéristiques chimiques du processus, paramètres, conditions de fonctionnement normal.
- **Les fiches et les étiquettes des substances** sont utilisées pour comprendre le type, les propriétés physiques et chimiques, les données toxicologiques de la substance.
- **La probabilité et la fréquence** sont liées au type de défaillance, à la probabilité et fréquence de défaillance, défaillance humaine, taux de défaillance et probabilité d'exposition.
- **La politique et les gestions** tels les politiques de maintenance, les systèmes de gestion de la sécurité.
- **L'environnement** est lié à l'environnement du site, aux données topographiques et densité de population.
- **Le texte et les connaissances historiques** telles les normes, les réglementations et connaissances historiques.

I.5.3 Types de sorties

Les résultats d'une analyse des risques peuvent être qualitatifs (e.g. recommandations) ou quantitatifs (e.g. indice de niveau de risque). Tixier [73] synthétise quatre types de sortie :

- **Processus de gestion**, lié aux actions, recommandations, procédures de formation ou d'exploitation.
- **Listes** telles les listes d'erreurs, de dangers, d'effets, de causes/conséquences, de défaillances et de dommages.
- **Probabiliste**, lié au taux de défaillance, à la fiabilité, à la probabilité de scénarios ou de dommages, à la fréquence des accidents.
- **Hiérarchisation**, lié à l'indice de niveau de risque, la gravité et la criticité, l'incendie, l'explosion, la classification selon le type de risque.

I.5.4 Tableau récapitulatif

Sur la base de la littérature, nous dressons un tableau récapitulatif (tableau I.1). Il illustre les différentes classifications des méthodes d'analyse des risques considérées dans ce chapitre et fournit quelques exemples pour chaque classification.

Tableau I.1 Classifications des méthodes d'analyse de risques appliquées aux systèmes industriels complexes

Type de méthodes d'analyse		Type de données utilisées	Type de sorties obtenues	Exemple de méthodes
Méthodes qualitatives	**Méthodes déterministes**	- Plans ou schémas - Processus et réactions - Fiches et étiquettes des substances - Politique et gestions - Environnement - Texte et connaissances historiques	-Processus de gestion - Listes -Hiérarchisation	- Analyse des modes de défaillance et de leurs effets, AMDE - Checklist -Analyse préliminaire des risques, PRA -Hazard and operability analysis, HAZOP
	Méthodes probabilistes	-Probabilité et fréquence	- Listes - Probabiliste	-Structural reliability analysis, SRA -Technique delphi
	Méthodes combinées	- Plans ou schémas - Probabilité et fréquence	- Processus de gestion - Listes - Probabiliste - Hiérarchisation	-Reliability block diagram, RBD - Analyse de fiabilité structurelle
Méthodes quantitatives	**Méthodes déterministes**	- Plans ou schémas - Processus et réactions - Fiches et étiquettes des substances - Politique et gestions - Environnement - Texte et connaissances historiques	- Processus de gestion - Listes - Hiérarchisation	- Analyse des risques d'accident, AHI - Méthodologie SAATY - Identification et classement des risques, HIRA
	Méthodes probabilistes	- Plans ou schémas -Probabilité et fréquence	- Listes - Probabiliste	-Arbre de défaillances, ADD -Arbre d'événements, ETA

	Méthodes combinées	- Plans ou schémas - Processus et réactions - Fiches et étiquettes des substances - Politique et gestions - Environnement -Texte et connaissances historiques	- Processus de gestion - Listes - Probabiliste - Hiérarchisation	- Analyse des modes de défaillance, de leurs effets et de leur criticité, AMDEC (en anglais : FMECA) - Évaluation quantitative des risques, QRA - Indicateurs de niveau de risque, RLI

I.6 Conclusion

Au sein des milieux industriels, l'importance de la sécurité n'est plus à démontrer. Par conséquent, une démarche de gestion des risques est tout à fait adaptée, et cela, pour plusieurs raisons :

- Pour fournir une analyse rigoureuse du système étudié, permettant la prévision des risques susceptibles.
- Pour évaluer le niveau de sécurité des différents types de systèmes complexes.
- Pour proposer des barrières de sécurité pour la maîtrise des risques d'accident associés aux différents types de systèmes complexes.

Le début de ce chapitre a été consacré à une étude bibliographique ayant pour objet la réalisation d'un aperçu général du processus de gestion des risques. Celui-ci permet d'optimiser et de préserver la sécurité industrielle. Nous avons mis en évidence l'ensemble des normes de sécurité adoptées dans le domaine de la robotique industrielle. Les différentes techniques appliquées dans le cadre de la prévision et de l'évaluation des risques ont été présentées. Ces méthodes d'analyse des risques ont dès lors été classifiées. Enfin, ce chapitre se termine par une classification des différentes méthodes d'analyse des risques.

Chapitre II
Les méthodes d'analyse des risques

II.1 Introduction

Ce chapitre présente la base théorique adoptée dans ce travail de thèse. Il propose un aperçu des principales méthodes d'identification et d'analyse des risques, développées dans la littérature : méthode d'analyse des modes de défaillance AMDE/AMDEC, analyse basée sur le modèle de causalité des accidents STPA, analyse par arbre de défaillances ADD méthode du nœud papillon et l'analyse avec réseaux de Petri RdP. Ce chapitre tente d'en apporter une compréhension générale en mettant en évidence la mise en œuvre de chaque méthode, leurs principes, avantages et limites. Au chapitre III, ces méthodes sont reprises et combinées dans le cadre de l'analyse des risques de notre laboratoire robotisé.

II.2 Méthode AMDE/ AMDEC

L'AMDE (i.e. l'analyse des modes de défaillance et de leurs effets) ou AMDEC (i.e. l'analyse des modes de défaillance, de leurs effets et de leur criticité) est la traduction française du sigle américain FMECA (pour « Failure Modes Effects and Criticality Analysis ») ou FMEA. Cette analyse a été développée et appliquée aux États-Unis en septembre 1949 dans le domaine du spatial et de l'aéronautique. Depuis, elle a été largement utilisée dans de nombreux autres domaines de l'industrie.

L'AMDE est une méthode d'analyse ascendante de démarche inductive. Une étude de l'échec de chaque composant du système est réalisée. L'objectif principal de l'analyse AMDE est, à l'origine, de révéler les pannes possibles dans le processus de conception précoce d'un système ou d'un produit pouvant affecter sa sécurité et ses performances. Elle permet également l'introduction de contre-mesures pour atténuer ou minimiser les effets des problèmes potentiellement identifiés. La procédure pour une analyse AMDE/AMDEC est clairement définie dans la norme CEI 60812 [77].

La méthode représente une analyse systématique des composants du système afin d'identifier tous les modes de défaillance significatifs et leur importance pour les performances du système. Un seul composant est considéré à la fois, les autres composants sont alors supposés fonctionner parfaitement. Pour l'AMDEC, l'équipe d'étude mesure également la gravité, la probabilité d'occurrence et de détection utilisées pour calculer la criticité de risque pour les modes de défaillance identifiés. L'objectif est de classer les modes de défaillance identifiés en fonction de leur gravité, permettant alors de hiérarchiser les contre-mesures [78].

II.2.1 Principe de la méthode

Le principe de l'analyse AMDEC comprend les points décrits ci-dessous [79] :

- Définir le système à étudier, ses fonctions et son schéma de composants physiques.
- Décomposer le système en éléments connus. Le niveau de détails de la décomposition se détermine à partir de la connaissance des modes de défaillance et des fréquences.
- Associer à chaque élément ses modes de défaillance. Chaque mode de défaillance correspond à un comportement différent de son comportement prescrit.
- Identifier les causes de chaque mode de défaillance et ses effets sur le système.
- Pour chaque mode de défaillance et pour chaque élément, associer sa criticité en fonction des effets qu'il produit. Cette étape permet de distinguer l'AMDEC de l'AMDE.

La criticité permet la hiérarchisation des défaillances selon leur impact global sur le système. Elle peut être exprimée par un ensemble de paramètres telles que :

- **La gravité** : ampleur de l'effet de la défaillance.
- **La probabilité d'occurrence** : taux de défaillance, fréquence d'apparition.
- **La détectabilité** : probabilité ou niveau de détection du mode de défaillance.

Afin d'évaluer la criticité, plusieurs méthodes existent. Les méthodes courantes incluent le niveau de risque ; ainsi que l'ordre de priorité du risque, dénommé RPN (acronyme de « Risk Priority Number »).

Le niveau de risque est obtenu en combinant la gravité des conséquences d'un mode de défaillance à sa probabilité. Le niveau de risque peut être exprimé qualitativement, semi-quantitativement ou quantitativement. D'autre part, **l'ordre de priorité du risque** est une mesure semi-quantitative de la criticité obtenue en multipliant l'échelle de notation de la gravité (généralement comprise entre 1 et 10), la probabilité de défaillance et la détectabilité.

Lorsque la valeur de la criticité est jugée inacceptable, il est impératif de proposer des actions correctives tels l'installation des moyens de prévention et de protection, la reconception du système, le développement des procédures de maintenance préventive.

La procédure de mise en œuvre de cette méthode est illustrée sur la figure II.1.

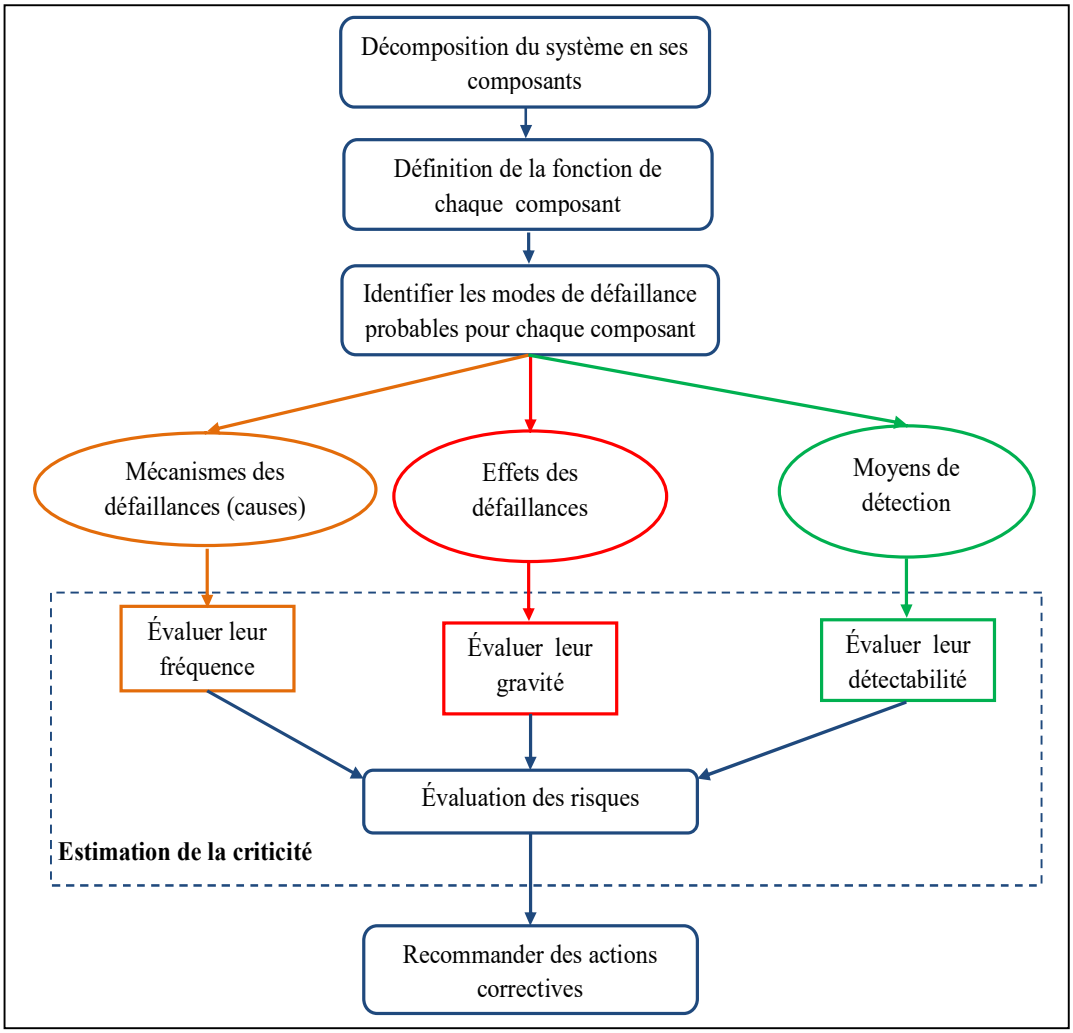


Figure II.1 Procédure de mise en œuvre de l'AMDE et de l'AMDEC

Le résultat principal de l'analyse AMDE est une liste de modes de défaillance, de mécanismes de défaillance et d'effets pour chaque composant ou étape d'un système ou d'un processus. En supplément, la méthode AMDEC comprend une note d'importance basée sur la probabilité de défaillance du système, le niveau de risque résultant du mode de défaillance ou combinaison du niveau de risque et de la « détectabilité » du mode de défaillance. Le tableau II.1 montre un exemple obtenu par l'analyse AMDEC [76 ; 80].

Tableau II.1 Exemple de tableau AMDEC

Composant	Fonction	Mode de défaillance	Cause	Effet	Moyens de détection	Actions correctives	Gravité	Fréquence	Détectabilité	Evaluation des risques

II.2.2 Avantages et limites de la méthode

Les principaux avantages des analyses AMDE/AMDEC sont les suivants [78] :

- Elles sont largement applicables aux modes de défaillance des différents types de systèmes : équipements, matériels, produits et procédés. Elles sont également utilisables concernant les services aux humains, les logiciels et les procédures.
- Elles identifient de manière systématique les modes de défaillance des composants, leurs causes et leurs effets sur le système. Elles les affichent avec un format facile à lire.
- Elles identifient la criticité des modes de défaillance de chaque composant. En conséquence, les composants les plus critiques du système sont extraits.
- Elles évitent les remplacements coûteux des équipements en service en identifiant les problèmes dès le début du processus de conception, facilitant ainsi la phase de maintenance.
- Elles proposent les exigences pour les systèmes de redondance et de sécurité.

Concernant leurs limites :

- Ces méthodes ne peuvent être utilisées que pour identifier des modes de défaillance indépendants. Elles seront inefficaces dans le cadre d'une combinaison de modes de défaillance entrainant la défaillance du système global. Dans ce cas, une analyse complémentaire via d'autres outils tels les arbres de défaillances ou les diagrammes de fiabilité peut répondre aux exigences.
- L'AMDE se limite à analyser une cause unique d'un effet.
- Si l'étude n'est pas correctement ciblée, elle peut être longue et coûteuse.
- L'analyse peut être difficile pour les systèmes multicouches complexes.

L'AMDE et l'AMDEC peuvent fournir des données pour d'autres techniques d'analyse, telles l'analyse par arbres de défaillances ou la méthode nœud papillon au niveau qualitatif ou quantitatif – L'objectif étant d'améliorer les résultats et de dépasser les limites de l'analyse.

II.3 Méthode de l'arbre de défaillances ADD

La méthode d'analyse par arbre de défaillances (ADD), connue en anglais sous le nom « Fault Tree Analysis (FTA) », a été développée par Bell Telephone Labs en 1962 pour l'évaluation de la sécurité de leur système de contrôle de lancement du missile balistique intercontinental Minuteman.

Par la suite, la société Boeing a continué à développer la technique et a utilisé des logiciels pour faciliter l'application de la méthode. Ces outils sont très utiles pour représenter les résultats de l'analyse qualitative sous forme d'arbre graphique d'une part, et rechercher des coupes minimales, fournir une analyse quantitative et déterminer les probabilités requises [76] d'autre part.

Depuis les années 1970, l'analyse par arbres de défaillances est devenue très répandue. Elle a été largement utilisée pour divers systèmes. Ses applications incluent la plupart des industries, notamment l'aérospatiale et l'industrie nucléaire. Elle est également adoptée par les industries de la robotique et des logiciels [81].

Un arbre de défaillances est un diagramme logique illustrant la relation entre l'événement indésirable spécifique pour le système, et les défaillances de ses composants. L'événement indésirable constitue l'événement au sommet de l'arbre et les différentes défaillances des composants constituent l'événement de base de l'arbre. Les événements de base n'indiquent pas nécessairement une défaillance pure d'un composant. Ils peuvent également indiquer une erreur humaine ou un dysfonctionnement dû à des conditions environnementales extrêmes. Une description détaillée de l'analyse ADD a été présentée dans [81–82].

II.3.1 Principe de la méthode

L'arbre de défaillances est une approche d'analyse des risques descendante qui suit une démarche déductive où l'analyste part d'un événement redouté final (dysfonctionnement ou accident) et remonte jusqu'aux causes de base et conditions. Il vise à représenter toutes les combinaisons pouvant induire l'événement étudié, d'où sa représentation schématique sous forme d'arbre logique. L'analyse peut être réalisée à travers la question récurrente suivante : comment cet événement s'est-il produit et quelles en sont ses causes ? Dès lors, cette représentation peut être utilisée pour calculer la probabilité de l'événement redouté en fonction des probabilités des événements de base.

II.3.2 Objectifs

L'objectif de l'analyse qualitative est de synthétiser tout ce qui peut conduire à l'événement redouté, afin de déterminer tous les scénarios produisant cet événement et extraire les ensembles de coupes minimales.

A contrario, l'objectif de l'analyse quantitative est d'évaluer la vraisemblance de la survenue de l'événement étudié à partir des combinaisons d'événements élémentaires. En cas de manque de données probabilistes, l'arbre peut évaluer le nombre de scénarios conduisant à l'événement étudié, ainsi que le nombre minimum d'événements suffisants pour qu'il se produise.

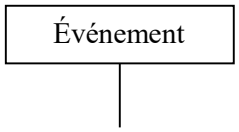
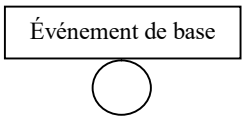
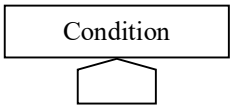
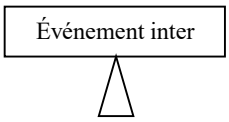
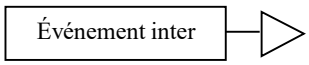
II.3.3 Mise en œuvre de la méthode

L'analyse par arbres de défaillances comprend généralement plusieurs étapes :

1. Sélection de l'événement principal redouté et de l'ensemble des événements intermédiaires et de base associés.
2. Construction de l'arbre de défaillances en combinant les événements à l'aide d'opérateurs logiques, telles les portes ET et OU, jusqu'à ce que l'événement de base soit atteint.
3. Analyse qualitative de l'arbre de défaillances obtenu et identification des ensembles de coupes minimales. Cette étape conduit à extraire l'ensemble des événements de base ou l'ensemble des conditions nécessaires et suffisantes pour provoquer l'événement-sommet. La suppression d'un seul élément suffit à ne plus provoquer la défaillance.
4. Analyse quantitative de l'arbre de défaillances. Une analyse qualitative est toujours intéressante, même sans quantification. Cependant, l'une des principales qualités de l'analyse quantitative est de pouvoir évaluer la probabilité d'apparition de l'événement-sommet en fonction des probabilités des événements de base.

De nombreuses normes aident à la réalisation des arbres de défaillances. Citons : IEC 61025 [83], NUREG-0492 [84], guides et publications [85]. Pour construire un arbre de défaillances, un ensemble d'éléments de base sont nécessaires. Nous décrivons les principaux éléments utiles pour la construction de l'arbre de défaillances dans le tableau II.2 [81 ; 85].

Tableau II.2 Eléments constitutifs de l'arbre de défaillances

Type de nœuds	Description	Représentation
Événement-sommet ou événement intermédiaire	L'événement intermédiaire est une combinaison d'un ensemble d'événements de base. Alors que l'événement sommet rassemble l'ensemble des combinaisons de tous les événements possibles.	
Événement de base	Défaillance d'un composant de base ou cause basique.	
Événement de condition	Il établit une condition requise pour que l'événement de porte se produise.	
Événement de transfert	Pointeur vers une branche d'arbre. Indique une branche de sous-arbre utilisée ailleurs.	Renvoi vers un sous-arbre  Sommet d'un sous-arbre 
Événement de porte	Opérateur logique combinant des nœuds d'entrée. Représente un état de défaillance qui a d'autres causes à développer. **Connecteur OU :** les entrées sont identiques à la sortie, mais plus spécifiquement définies comme cause. **Connecteur ET :** les défauts d'entrée représentent collectivement la cause du défaut de sortie.	Connecteur OU  P (A ou B) = P(A) + P(B) – P(A) × P(B) Connecteur ET  P (A et B) = P(A) × P(B)

II.3.4 Avantages et limites de la méthode

L'avantage de cette méthode est qu'elle permet de visualiser toutes les combinaisons d'événements de base qui conduisent à l'événement indésirable, c'est-à-dire qu'elle permet

d'avoir une compréhension globale du fonctionnement et des dysfonctionnements du système. Par ailleurs, l'extraction des coupes minimales permet d'identifier les composants critiques du système étudié.

Par rapport à son utilisation quantitative, cette méthode permet de calculer la probabilité d'occurrence de l'événement redouté, à condition de pouvoir disposer des probabilités des événements de base. Elle est particulièrement puissante pour la détermination de la criticité d'un équipement.

L'une des limites de cette méthode est qu'elle ne considère qu'un seul événement redouté. Par conséquent, une analyse complète prenant en compte tous les scénarios probables d'événements redoutés est généralement problématique en termes de ressources et d'aspect calculatoire.

Par ailleurs, cette méthode n'est efficace que lorsque les événements intermédiaires sont indépendants les uns des autres, permettant alors un calcul de la probabilité d'occurrence correct. De plus, l'arbre de défaillances ne peut pas capturer l'aspect temporel du scénario qui a causé la panne [85].

L'analyse ADD augmente la faisabilité des méthodes d'analyse tabulaire telle l'AMDE car elle permet de visualiser les combinaisons des causes possibles, obtenant ainsi plus de scénarios de risques. La combinaison de l'ADD avec la méthode AMDE permet de soutenir une analyse approfondie, celle-ci pouvant fournir une évaluation quantitative prenant en compte, par exemple, tous les risques [82 ; 86]. Cette combinaison a été largement utilisée par plusieurs études dans le secteur de la robotique collaborative [41–42].

II.4 Méthode STAMP/STPA

La méthode STPA est une technique d'analyse et d'identification des dangers basée sur un modèle de causalité des accidents, appelé STAMP. Avant d'introduire cette analyse STPA, nous décrivons le modèle STAMP dans ce qui suit.

II.4.1 Modèle STAMP

La théorie des systèmes a amené un modèle de causalité des accidents connu sous le nom STAMP (acronyme de « System-Theoretic Accident Model and Processes »), qui est considéré comme une base philosophique et intellectuelle de l'ingénierie des systèmes

[56 ; 87]. Le modèle STAMP élargit le modèle traditionnel de causalité au-delà d'une chaîne d'événements de défaillance directement liés ou de défaillances de composants pour inclure des processus plus complexes et des interactions dangereuses entre les composants du système. Le modèle STAMP dépend de trois concepts fondamentaux [51], illustrés sur la figure II.2.

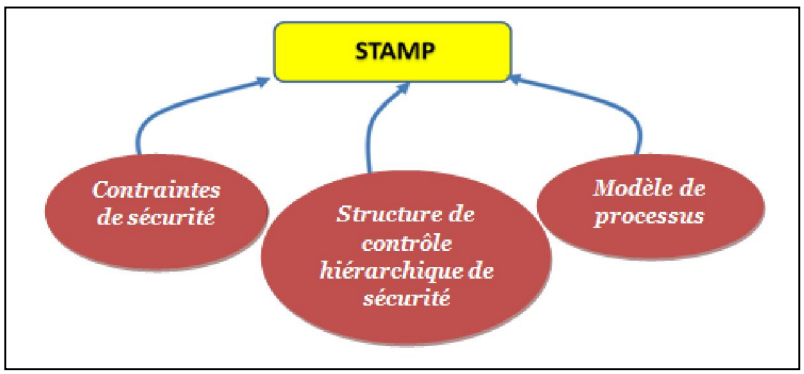


Figure II.2 Concepts fondamentaux de STAMP

Dans le modèle STAMP, les systèmes sont considérés comme des composants liés entre eux dans les deux sens afin de maintenir un état d'équilibre dynamique. Ces interactions entre les éléments du système (de même entre un système et d'autres systèmes ou opérateurs) sont représentées de manière similaire à des boucles fermées de contrôle dans lesquelles les contrôleurs fournissent des actions de contrôle ou transmettent des commandes vers le processus surveillé afin qu'ils reçoivent des réponses ou des rétroactions [57]. De ce fait, la sécurité est considérée comme un problème de contrôle dynamique et non comme un problème de prévention des pannes. En d'autres termes, l'objectif est passé de la prévention des défaillances à l'imposition de contraintes sur le comportement du système.

Les avantages de l'utilisation du modèle STAMP sont les suivants :

- Il fonctionne sur des systèmes très complexes car il agit de haut en bas plutôt que de bas en haut.
- Le modèle STAMP traite les logiciels, les humains, les organisations, la culture de la sécurité, etc. sans avoir à les traiter différemment ou séparément.
- Il permet de créer des outils plus puissants, tels STPA (analyse des risques), CAST (analyse des accidents), identification et gestion des principaux indicateurs de risque croissant, analyse des risques organisationnels, etc.

Comme le modèle STAMP s'applique à toute propriété émergente, l'analyse STPA peut être utilisée pour n'importe quelle propriété système, y compris la cyber-sécurité.

Le modèle STAMP n'est pas, à proprement parler, une méthode d'analyse. Il s'agit plutôt d'un modèle ou d'un ensemble d'hypothèses sur la façon dont les accidents se produisent. Le modèle STAMP est une alternative aux événements en chaîne de défaillances (effet « dominos ») qui sous-tendent les techniques conventionnelles d'analyse de la sécurité (telles l'analyse par arbre des défaillances, l'analyse par arbre des événements, la méthode HAZOP et l'AMDEC). Tout comme ces méthodes d'analyse conventionnelles basées sur l'hypothèse que les accidents se produisent à travers un modèle d'événements en chaîne de défaillances, STAMP peut être utilisé comme modèle de base pour construire de nouvelles méthodes d'analyse. Notons que, comme le modèle d'événements en chaîne de défaillances est un sous-ensemble du modèle STAMP, les résultats obtenus par les outils basés sur STAMP sont plus généraux que ceux obtenus par les techniques conventionnelles d'analyse de sécurité.

Basés sur le modèle STAMP, les deux outils les plus largement utilisés aujourd'hui sont STPA (acronyme de « System-Theoretic Process Analysis ») et CAST (analyse causale basée sur la théorie des systèmes). L'analyse STPA est une méthode d'analyse proactive qui analyse la cause potentielle des accidents pendant le développement afin que les dangers puissent être éliminés ou maîtrisés [52].

II.4.2 Méthode STPA

La méthode STPA (acronyme de « System-Theoretic Process Analysis ») fait partie des approches systématiques d'identification des dangers qui dépendent du modèle de causalité STAMP. Son objectif est d'élaborer une nouvelle stratégie d'analyse qui surmonte les limites de l'analyse classique des dangers en identifiant un ensemble plus large de scénarios de dangers et de facteurs de causalité [53].

Récemment, l'analyse STPA a été très utilisée grâce à sa capacité à analyser de nombreux types de systèmes automatisés. Citons les systèmes de conduite [53], les systèmes de transport aérien [55], y compris les systèmes robotisés [57]. Elle est également utilisée dans le cadre des systèmes autonomes tels que les véhicules autonomes [58] et les navires autonomes [59–60].

II.4.3 Principe de la méthode

L'analyse STPA est réalisée selon quatre étapes principales. La méthodologie de cette analyse est illustrée sur la figure II.3.

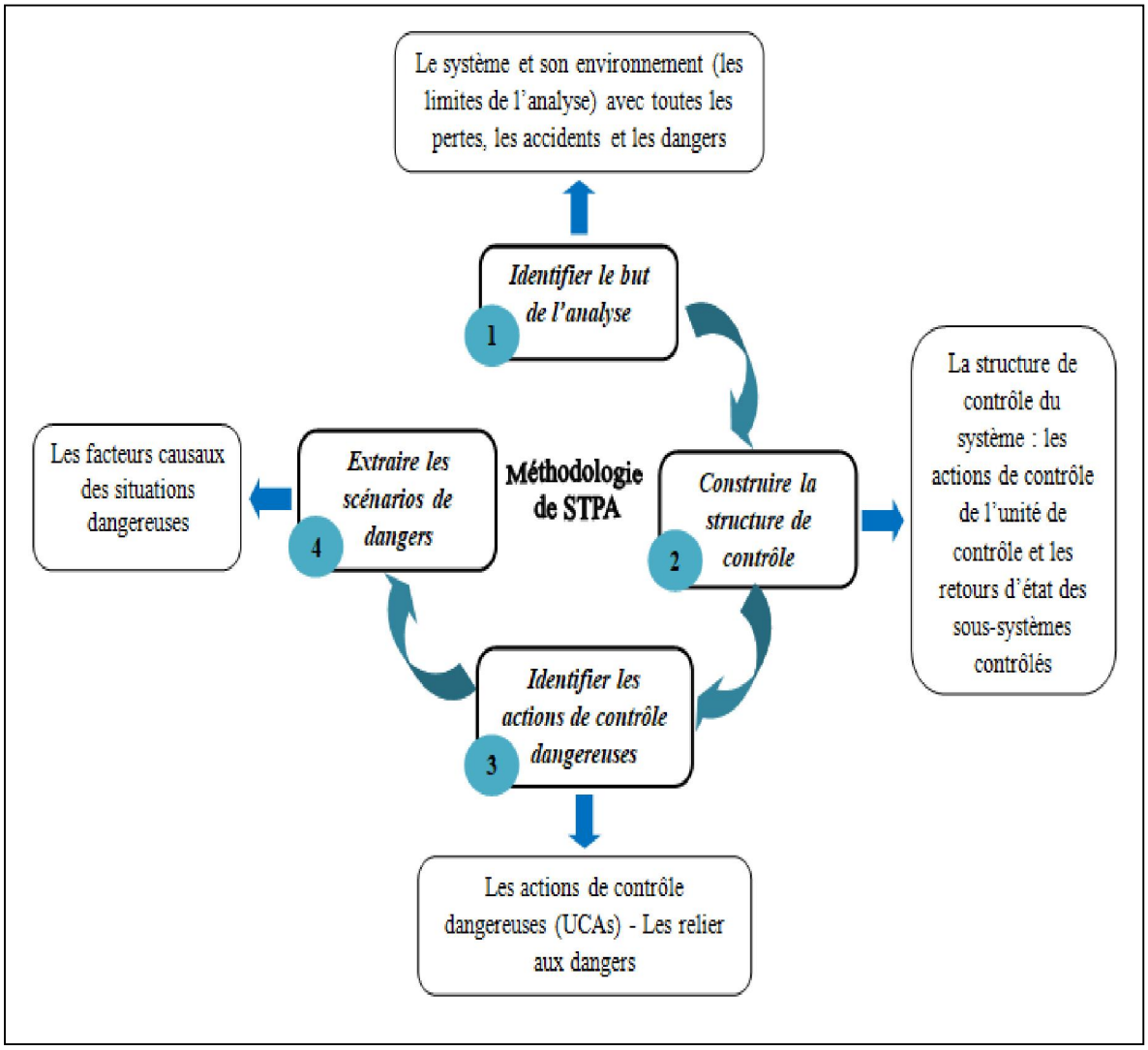


Figure II.3 Méthodologie STPA basique

La première étape de toute méthode d'analyse est la définition de l'objectif de celle-ci, principalement en identifiant les types de pertes, les accidents et les dangers de haut niveau du système étudié. En particulier, les questions posées sont : Quel type de pertes l'analyse visera-t-elle à éviter ? L'analyse STPA sera-t-elle appliquée uniquement aux objectifs de sécurité traditionnels comme la prévention des pertes de la vie humaine ou sera-t-elle appliquée plus largement à la sécurité, à la confidentialité, aux performances et à d'autres propriétés du système ? Quel est le système à analyser et quelle est la limite de celui-ci ?

La deuxième étape consiste à construire un modèle du système, appelé « structure de contrôle ». Une structure de contrôle capture les relations fonctionnelles et les interactions en modélisant le système comme un ensemble de boucles de contrôle de rétroaction. La structure de contrôle commence généralement à un niveau très abstrait et est affinée de manière itérative pour capturer plus de détails sur le système.

La troisième étape consiste à analyser les actions de contrôle dans la structure de contrôle afin d'examiner comment elles pourraient conduire aux pertes définies dans la première étape. Les actions de contrôle font l'objet d'une analyse à l'aide de mots-guides prédéfinis en vérifiant [51 ; 88] :

- Si une action de contrôle « est fournie », celle-ci peut occasionner un danger.
- Si une action de contrôle ou une mesure nécessaire pour prévenir un danger n'est « pas fournie ».
- Si une action de contrôle « est envoyée avec une synchronisation imprécise », trop tôt ou trop tard, celle-ci peut entraîner un danger.
- Si « appliquer une action de contrôle pendant une longue période ou la perdre trop tôt », alors celle-ci peut produire un danger.

Ces actions de contrôle non sécurisées sont utilisées pour créer des exigences et contraintes du système.

La quatrième étape extrait les facteurs causaux pour lesquels un contrôle dangereux pourrait se produire au niveau du système. Des scénarios sont créés pour expliquer :

1. Comment une rétroaction incorrecte, des exigences inadéquates, des erreurs de conception, des défaillances de composants et d'autres facteurs peuvent entraîner des actions de contrôle dangereuses, et finalement entraîner des pertes.
2. Comment des actions de contrôle sûres peuvent être fournies mais non suivies ou exécutées correctement, entraînant une perte.

II.4.4 Avantages et limites de la méthode

L'analyse STPA est utilisée actuellement dans le cadre des systèmes complexes, y compris les systèmes robotiques. En outre, plusieurs évaluations et comparaisons avec les techniques conventionnelles d'analyse des risques ont été réalisées [52] Celles-ci ont révélé que l'analyse STPA présente un nombre d'avantages. Nous les résumons dans les points suivants :

- L'analyse STPA trouve les scénarios dangereux mis en évidence par les approches conventionnelles, telles l'analyse par arbres de défaillances et l'analyse des modes de défaillance et ses effets. Elle permet également de trouver de nombreux autres scénarios qui n'impliquent pas de défaillances de composants, souvent liés au logiciel.
- Elle semble également nécessiter moins de ressources, et est plus rapide.

Un autre avantage de l'utilisation d'un outil basé sur un modèle est qu'il peut être appliqué plus tôt dans le processus de conception et dans des situations où des données de composants spécifiques ne sont pas disponibles. L'analyse peut commencer dès que les objectifs de base de haut niveau du système sont identifiés et que les décisions de conception sont évaluées pour leur impact sur la sûreté et la sécurité avant que des révisions coûteuses ne soient nécessaires [52].

Toutefois, notons les limites suivantes :

- Cette méthode exige que les personnes impliquées dans l'analyse soient plus ouvertes qu'avec les autres méthodes conventionnelles. Puisque les méthodes STAMP identifient plus de scénarios causaux, il est essentiel que les informations/résultats et les modèles de structure de contrôle soient soigneusement contrôlés et mis à jour avec la conception réelle du système (contrôle de configuration / contrôle des données). De plus, selon le système analysé, une équipe d'experts spécialisés sera nécessaire pour s'assurer que tous les scénarios sont analysés [46 ; 53 ; 87 ; 89–90].
- Une autre limitation est que l'analyse STPA est encore une méthode purement qualitative en raison de la difficulté d'évaluer certains scénarios. Son utilisation n'est donc pas suffisante pour une analyse plus rigoureuse.

II.4.5 Comparaison de l'analyse STPA à d'autres méthodes

L'intérêt de l'analyse STPA contrairement aux autres méthodes apparaît évidemment dans sa capacité à identifier un grand nombre de scénarios de dangers possibles, qu'ils soient causés par une défaillance ou par d'autres raisons comme les conditions d'environnement ou les effets organisationnels.

En outre, cette approche est basée sur la théorie des systèmes et de leurs propriétés au lieu de la théorie de la fiabilité. Il nous est permis de nous concentrer sur les interactions

survenues entre les composants du système et d'envisager le système sous différents angles. L'analyse STPA fait apparaître le danger à travers des interactions dangereuses et inopinées entre les composants du système d'une part, et à travers une application inadéquate des contraintes de sécurité d'autre part. Les autres méthodes telles l'ADD, l'AMDE… analysent la conception du système physique au lieu des fonctions de contrôle du système [51]. En particulier, la méthode HAZOP focalise sur l'analyse de la partie physique des boucles de contrôle uniquement, contrairement à l'analyse STPA qui se concentre plutôt sur les actions de contrôle. Les méthodes classiques se concentrent sur la défaillance des composants du système et n'examinent pas le comportement dangereux / non sécurisé lui-même, ni les autres facteurs comme les facteurs sociaux et organisationnels. L'intérêt de l'analyse STPA consiste donc à « prévenir les défaillances » et à « prévenir les actions et opérations dangereuses en appliquant des contraintes de sécurité au comportement du système ».

Bien que la défaillance soit un problème qui nécessite beaucoup d'attention, d'autres causes involontaires doivent également être mises en évidence afin d'être maîtrisées [91–92].

II.5 Méthode du nœud papillon

L'analyse du nœud papillon (ou BowTie en anglais) est une méthode schématique simple qui combine les avantages des deux analyses appelées « arbre de défaillances » (ADD) et « arbre d'événements » (ADE). Elle décrit et analyse les scénarios de risque tout en identifiant l'événement redouté central, ses causes et ses conséquences. Elle peut être considérée comme la combinaison d'un arbre de défaillances analysant la cause d'un événement et d'un arbre d'événements analysant les conséquences. Cependant, le nœud papillon se concentre sur les barrières de sécurité entre les causes et le risque (i.e. barrières de prévention), et entre le risque et les conséquences (i.e. barrières de protection). Ces barrières de sécurité sont mises en place afin de réduire la probabilité de l'événement dangereux et d'en atténuer les conséquences. Cette analyse est tout à fait adaptée pour fournir une vue globale et large des scénarios de danger pouvant survenir sur le système [92–96]. Le diagramme de nœud papillon peut être représenté sous la forme indiquée sur la figure II.4.

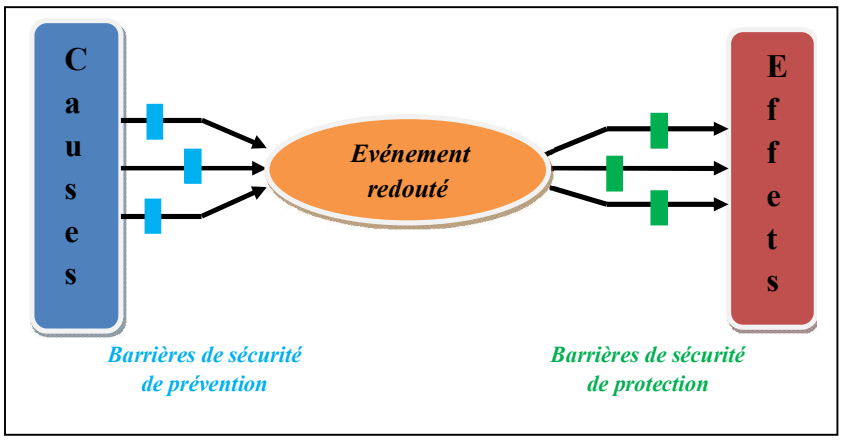


Figure II.4 Schéma global du diagramme« nœud papillon »

Cette méthode est notamment utilisée afin de s'assurer de l'existence de barrières ou de contrôles pour chaque voie de défaillance [78].

L'origine de la méthode n'est pas tout à fait claire, mais depuis le début des années 1990, la compagnie pétrolière Shell a apporté une contribution significative à l'amélioration de l'utilisation de la méthode. Les diagrammes nœud papillon ont été utilisés activement dans les rapports de sécurité pour l'industrie pétrochimique au Royaume-Uni et ont ensuite été adoptés, par exemple, par la FAA (i.e. la « Federal Aviation Administration ») des États-Unis.

Le diagramme nœud papillon relie les causes et les conséquences à travers une série de lignes d'événements et illustre les « itinéraires » qui ont conduit aux accidents. Les barrières qui ont été ou devraient être définies sont associées à leurs lignes d'événements.

Le diagramme nœud papillon n'est pas conçu pour identifier les événements dangereux, mais plutôt pour illustrer les contrôles physiques et procéduraux mis en place pour la gestion de ces événements [20] .

II.5.1 Principe de la méthode

La méthode du nœud papillon consiste en une analyse d'une structure arborescente comprenant ses deux directions (causes, conséquences). Cette méthode est largement utilisée pour la gestion des risques des installations dangereuses pour des raisons quantitatives et probabilistes [97].

Pour comprendre le principe de fonctionnement du diagramme en nœud papillon, une liste de terminologies est décrite dans le tableau II.3.

Tableau II.3 Liste des terminologies utilisées pour un nœud papillon

Terminologie	Description
EIn	Evénement indésirable qui correspond à une dérive ou à une défaillance par rapport aux spécifications nominales.
EI	Evénement initiateur, cause directe d'une perte de contrôle ou d'intégrité physique.
ERC	Evénement redouté central, perte de contrôle sur un équipement dangereux ou perte d'intégrité physique d'une substance dangereuse.
ERS	Evénement redouté secondaire, conséquence directe de l'événement redouté central. L'ERS caractérise le terme source de l'accident.
PhD	Phénomène dangereux, phénomène pouvant engendrer des dommages majeurs.
EM	Effets majeurs, dommages occasionnés au niveau des cibles (personnels, environnement, installations) par des effets dangereux.
Barrière de prévention	Barrière visant à prévenir la perte de contrôle ou d'intégrité physique.
Barrière de protection	Barrière ou mesure visant à limiter les conséquences de la perte de contrôle ou d'intégrité physique.

La structure détaillée du nœud papillon, associée aux terminologies décrites dans le tableau II.3,est illustrée sur la figure II.5 [97].

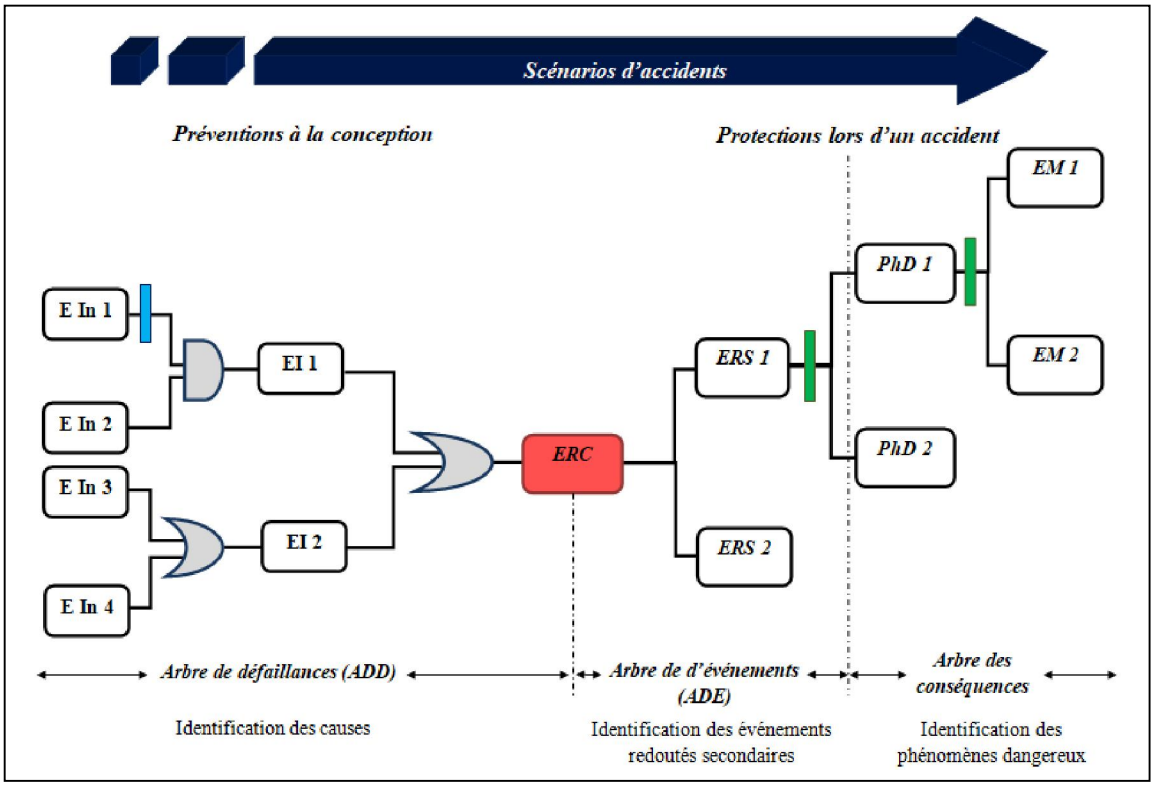


Figure II.5 Structure détaillée du nœud papillon

L'élément central du nœud papillon est appelé « événement redouté central (i.e. ERC) ». Il fait généralement référence à une perte de contrôle ou à une perte d'intégrité physique.

Le côté gauche du nœud papillon ressemble à un arbre de défaillances, essayant de trouver la raison de cette perte de contrôle. Alors que, son côté droit est l'ensemble des deux arbres, à savoir l'arbre d'événements et l'arbre des conséquences, se concentrant sur la détermination des conséquences de cet événement redouté et leurs effets majeurs.

Les barrières de sécurité sont représentées sur le schéma de la figure II.5 sous la forme de barres verticales pour indiquer qu'elles s'opposent à l'élaboration de scénarios d'accident.

En fait, dans ce schéma, chaque chemin qui mène de la défaillance d'origine (événements indésirables ou courants) jusqu'à l'apparition de dommages (effets majeurs) spécifie un scénario d'accident particulier pour un même événement redouté central. Cet outil démontre mieux une bonne maîtrise des risques en introduisant clairement le rôle des barrières de sécurité dans le processus d'accident. L'utilisation d'un logiciel dédié peut faciliter sa mise en œuvre.

II.5.2 Avantages et limites de la méthode

Les principaux avantages de l'utilisation du nœud papillon sont les suivants :

- Elle fournit une visualisation concrète, facile à comprendre, des scénarios d'accidents résultants, tout en donnant une représentation graphique claire non seulement du problème mais également des barrières de prévention et de mitigation mises en place.
- Elle met en évidence les mesures de contrôle et les barrières à prendre en compte pour la prévention et la réduction du niveau de risque et leur efficacité.
- Elle peut être utilisée dans le cadre de conséquences souhaitables.
- Son utilisation ne nécessite pas un niveau élevé de connaissances professionnelles.

Ses principales limitations sont :

- Cette méthode n'est pas valable pour tous les problèmes. En particulier, lorsque l'ERC (i.e. l'événement redouté central) décrit dans l'arbre de défaillances ne correspond pas à celui considéré au sommet de l'arbre d'événements [97].
- Elle ne peut pas décrire le cas où plusieurs causes se produisent en même temps.
- Elle peut simplifier à l'extrême les situations complexes, en particulier lors de la tentative de quantification, ce qui peut conduire à des résultats non précis [78].

II.6 Méthode par réseaux de Petri

Les réseaux de Petri (RdP) ont été introduits pour la première fois par Carl Adam Pétri dans son PhD de 1962. Son objectif initial était une représentation graphique du comportement des automates. Au début des années 1980, Ces Rdp ont été utilisés en sureté de fonctionnement afin de générer des processus de Markov à grande échelle. Puis ils ont été considérés comme un modèle adapté à la simulation de Monte-Carlo [98].

Le RdP est un formalisme de modélisation puissant adapté à l'étude des systèmes dynamiques à événements discrets, combinant une théorie mathématique bien définie avec une représentation graphique du comportement des systèmes. Son aspect théorique fournit une modélisation et une analyse comportementale de la dynamique du système, tandis que sa représentation graphique permet de visualiser les changements d'état modélisés du système [99]. Par conséquent, les RdP ont été largement usités pour modéliser divers types de systèmes complexes tels les systèmes de contrôle-commande [100], les systèmes

robotiques [101], les systèmes de communication [102]. Ainsi, Ceux-ci ont montré d'excellentes capacités de modélisation et de calculs dans le domaine de la sureté de fonctionnement et de la sécurité [103–105]. Ils sont très utiles pour la modélisation du comportement fonctionnel et dysfonctionnel des systèmes et l'évaluation de leurs performances [98]. À titre d'exemple, de nombreux travaux existants ont utilisé les RdP pour évaluer la fiabilité [106–107] et la disponibilité [64 ; 108 ; 109].

II.6.1 Représentation graphique et principe du RdP

Comme Pétri l'a décrit, le RdP de base est un type particulier de graphes bipartis dirigés, composé principalement de trois parties complémentaires :

- *Un graphe statique*, qui ne change pas au cours du temps. Il est constitué de trois éléments de base :
    - Les places, représentées sous forme de cercles. Chaque place représente un état ou une condition.
    - Les transitions, représentées par des barres. Chaque transition représente un événement, une transformation ou un changement d'état.
    - Les arcs dirigés, représentées par des flèches, relient les places aux transitions ou les transitions aux places. Chaque arc peut être affecté d'un nombre naturel, nommé « poids » (normalement supposé être à 1).
- *Des éléments dynamiques*, appelés « jetons » et représentés par des points qui indiquent l'état du système à un instant donné. Cela permet de décrire le comportement du système modélisé. Les jetons peuvent représenter des objets, des machines, des humains, des informations, des conditions…. La distribution de jetons dans les places est appelée « marquage du réseau ». La présence ou l'absence d'un jeton dans une place peut indiquer si une condition associée à cette place est vraie ou fausse. Si chaque place d'entrée p de la transition t contient au moins le nombre de jetons égal au poids de l'arc dirigé reliant p à t, alors cette transition t est activée.
- *Des prédicats et des assertions* au moyen de variables peuvent être introduits dans le RdP. Le prédicat (souvent précédé de deux points d'interrogations « ??») est une condition pour valider ou désactiver les transitions lorsque les variables sont vérifiées ou non vérifiées. L'assertion (souvent précédée de deux points d'exclamations « !! ») est une formule permettant de mettre à jour les variables après le franchissement de la transition associée [98–99]. L'utilisation de ces deux

éléments peut enrichir la lisibilité des modèles RdP complexes, améliorant ainsi leur compréhensibilité [110].

Un exemple simple de RdP est représenté en figure II.6.

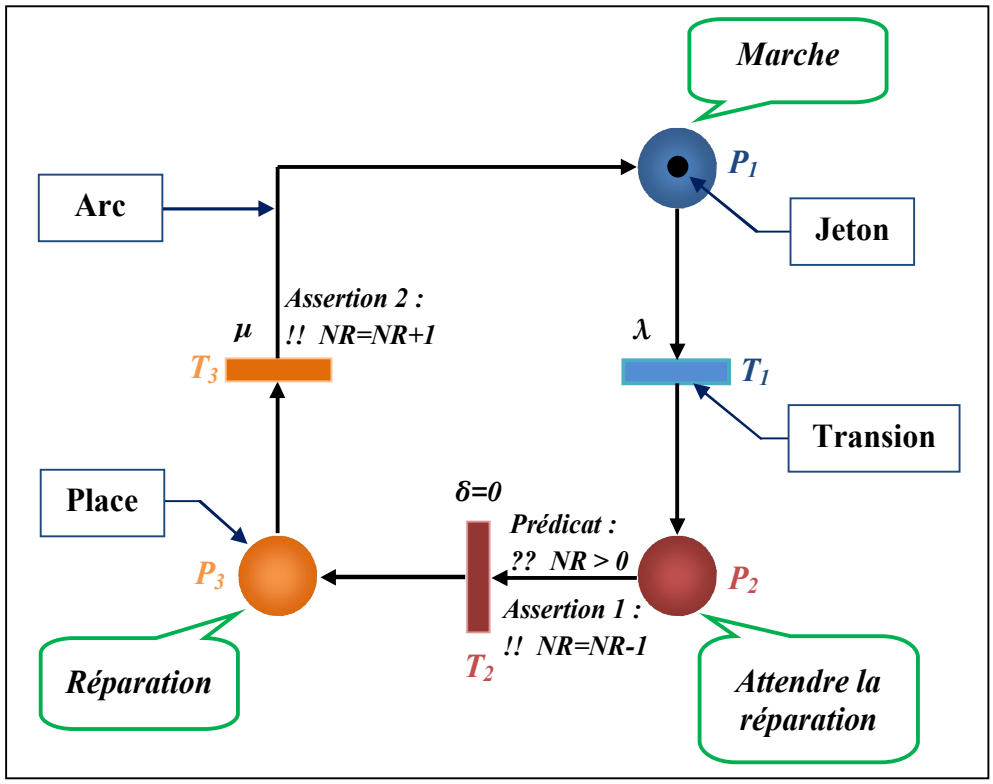


Figure II.6 Exemple de RdP

Dans le monde réel, presque tous les événements sont liés au temps. Pour cela, la nécessité d'inclure des variables temporelles dans les modèles de systèmes dynamiques semble évidente. Lorsqu'un RdP intègre la variable « temps » dans le modèle du système, il devient un RdP temporisé. Les RdP temporisés sont une extension des PdP de base pour lesquels chaque transition est associée à une variable de temps appelée « délai » avec sa fonction de densité de probabilités. Les jetons peuvent se déplacer entre les places lorsque la transition activée est tirée. La transition est tirée lorsque le délai associé s'écoule (étant donné que la transition reste activée pendant les délais). Le délai entre la transition activée et le franchissement peut être fixe (déterministe) ou aléatoire (stochastique). Une fois les transitions caractérisées par des délais déterministes et stochastiques dans un modèle, les RdP deviennent difficiles à résoudre analytiquement. Dans ce cas, une simulation Monte Carlo est généralement couplée avec le modèle RdPS (RdP stochastique) afin de faciliter l'évaluation des performances des systèmes [98].

Des informations supplémentaires sur la construction du modèle RdP sont présentées dans la norme CEI 62551 : 2012 [111], ainsi que dans de nombreux travaux et ouvrages, citons parmi eux : (Signoret, 2008 [98] ; Blume, 2007 [112] ; Guirault, 2013 [113]; Reisig, 2013 [114]).

II.6.2 Avantages et limites de la méthode

Les principaux avantages de l'utilisation du RdP sont les suivants [115] :

- Les RdP fournissent une représentation graphique et précise du système. Cela facilite la visualisation de systèmes complexes.
- Les RdP peuvent être utilisés pour représenter un système à différents niveaux de détails, en fonction les informations requises.
- Le comportement du système peut être analysé à travers le mouvement des jetons.
- Les RdP ont la capacité de modéliser les concepts logiciels tels le parallélisme ou la concurrence, les conflits et la synchronisation des événements.
- Les techniques d'analyse de RdP bien développées fournissent une analyse qualitative systématique et complète du système.
- Les RdP temporisés peuvent évaluer quantitativement les performances du système.

Les RdP présentent les limitations suivantes [115] :

- La modélisation des comportements dynamiques complexes est difficile et leur présentation graphique non explicite (incapacité d'intégrer l'évidence).
- Problème de lisibilité, traçabilité et compréhensibilité des modèles complexes.
- L'analyse des RdP n'est pas une tâche facile et dépend de la taille du système.
- Les RdP stochastiques RdPS sont des outils de modélisation très efficaces pour l'analyse et l'évaluation des performances des systèmes. Malheureusement, ils ne conviennent qu'aux petits systèmes et la représentation devient plus difficile et ingérable avec l'augmentation de la taille et de la complexité de ceux-ci. En outre, l'espace d'état d'accessibilité devient également très grand.

II.7 Tableau récapitulatif des méthodes

Ce paragraphe a pour objectif de dresser un tableau comparatif (tableau II.4) des méthodes d'analyse des risques présentées dans ce chapitre.

Tableau II.4 Tableau récapitulatif des méthodes d'analyse des risques

Méthodes	Type de démarche	Type d'analyse	Avantages	Limites
AMDE / AMDEC	Inductive (Analyse ascendante)	Qualitative, Semi-Quantitative, Quantitative / Statique	- Ces méthodes sont largement applicables aux modes de défaillance, quel que soit le type de système étudié. - Elles identifient de manière systématique les modes de défaillance des composants, leurs causes et leurs effets sur le système. - Elles identifient les composants les plus critiques du système. - Elles évitent les remplacements coûteux des équipements en service. - Elles proposent les exigences pour les systèmes de redondance et de sécurité.	- Ces méthodes ne peuvent être utilisées que pour identifier des modes de défaillances indépendantes. Elles ne peuvent pas être utilisées pour déterminer une combinaison des modes de défaillances entrainant la défaillance du système global. - L'AMDE est limitée à analyser une cause unique d'un effet. - Si l'étude n'est pas correctement ciblée, elle peut être longue et coûteuse. - L'analyse peut être difficile pour les systèmes multicouches complexes.
Arbre de défaillances	Déductive (Analyse descendante)	Qualitative, Quantitative / Statique	- Cette méthode permet de visualiser toutes les combinaisons d'événements de base qui conduisent à l'événement indésirable, c'est-à-dire qu'elle peut avoir une compréhension globale de fonctionnement et des dysfonctionnements du système. - L'extraction des coupes minimales permet d'identifier les composants critiques du système étudié. - Elle permet de calculer la probabilité d'occurrence de l'événement redouté. - Elle est particulièrement puissante pour la détermination de la criticité d'un équipement.	- Cette méthode ne considère qu'un seul événement redouté. Par conséquent, une analyse complète prend généralement beaucoup de temps et de ressources. - Cette méthode n'est efficace que lorsque les événements intermédiaires sont indépendants les uns des autres afin que le calcul de la probabilité d'occurrence soit correct. - Cette méthode ne peut pas capturer l'aspect temporel du scénario d'événements qui a causé la panne.

STPA	Déductive (Analyse descendante)	Qualitative / Statique	- L'analyse STPA détecte un grand nombre de scénarios dangereux, y compris ceux trouvés par d'autres méthodes conventionnelles, telles que l'analyse par arbre de défaillances, l'analyse des modes de défaillance et ses effets, ainsi que de nombreux autres scénarios qui n'impliquent pas de défaillances de composants, souvent liés au logiciel. - L'analyse STPA requiert moins de ressources, y compris temporelles. - C'est un outil basé sur un modèle. Elle peut donc être appliquée plus tôt dans le processus de conception. - L'analyse STPA peut commencer dès que les objectifs de base de haut niveau du système sont identifiés et que les décisions de conception sont évaluées pour leur impact sur la sûreté et la sécurité avant que des révisions coûteuses ne soient nécessaires.	- Cette méthode exige que les personnes impliquées dans l'analyse soient spécialisées et ouvertes d'esprit, plus qu'avec les autres méthodes conventionnelles. - Il est essentiel que les informations / résultats et les modèles de structure de contrôle soient soigneusement contrôlés. - L'analyse STPA est encore une méthode purement qualitative en raison de la difficulté d'évaluer certains scénarios. Son utilisation n'est donc pas suffisante pour une analyse plus rigoureuse.
Nœud papillon	Inductive / Déductive (Analyse dans les deux sens)	Qualitative, Semi-Quantitative, Quantitative / Statique	- Cette méthode fournit une visualisation concrète, facile à comprendre, des scénarios d'accidents résultants, tout en donnant une représentation graphique claire non seulement du problème mais également des barrières de prévention et de mitigation mises en place. - Elle met en évidence les mesures de contrôle et les barrières à prendre pour la prévention et la réduction du niveau de risque et leur efficacité. - Elle peut être utilisée pour des conséquences souhaitables. - Son utilisation ne nécessite pas un niveau élevé de connaissances professionnelles.	- Cette méthode n'est pas valable pour tous les problèmes. En particulier, lorsque l'ERC (i.e. événement redouté central) décrit dans l'arbre de défaillances ne correspond pas à celui considéré au sommet de l'arbre d'événements. - Elle ne peut pas décrire le cas où plusieurs causes se produisent en même temps. - Elle peut simplifier à l'extrême les situations complexes, en particulier lors de la tentative de quantification, ce qui peut conduire à des résultats non précis.

Réseaux de Petri	Déductive (Analyse descendante)	Qualitative, Quantitative / Dynamique	- Les RdP fournissent une représentation graphique et précise du système. - Les RdP peuvent être utilisés pour représenter un système à différents niveaux de détails. - Le comportement du système peut être analysé à travers le mouvement des jetons. - Les RdP ont la capacité de modéliser les concepts logiciels tels le parallélisme ou la concurrence, les conflits et la synchronisation des événements. - Les techniques d'analyse de RdP bien développées fournissent une analyse qualitative systématique et complète du système. - Les RdP temporisés peuvent évaluer quantitativement les performances du système.	- La modélisation des comportements dynamiques complexes est difficile et leur présentation graphique non explicite. - Problème de lisibilité, traçabilité et compréhensibilité des modèles complexes. - L'analyse des RdP n'est pas une tâche facile et dépend de la taille du système. - Les RdP stochastiques RdPS ne conviennent qu'aux petits systèmes et la représentation devient plus difficile et ingérable avec l'augmentation de la taille et de la complexité de ceux-ci. En outre, l'espace d'état d'accessibilité devient également très grand.

II.8 Conclusion

Dans ce chapitre, et sur la base d'une littérature abondante, nous avons présenté un aperçu général des différentes méthodes d'analyse des risques utilisées dans notre étude aux chapitres suivants : la méthode d'analyse des modes de défaillance AMDE/AMDEC, l'analyse basée sur le modèle de causalité des accidents STPA, l'analyse par arbre de défaillances ADD, la méthode du nœud papillon et l'analyse par réseaux de Petri RdP. Nous avons dès lors explicité la méthodologie de mise en œuvre de chacune d'entre elles. Pour conclure, un tableau comparatif de ces méthodes a été dressé. Il décrit leurs avantages et leurs limites.

A titre d'exemple, tout en apportant de nombreuses contributions, les méthodes basées sur une représentation graphique sont généralement très complémentaires des méthodes tabulaires. Par conséquent, dans le cadre de l'analyse des risques de notre laboratoire robotisé, nous concluons qu'il est souhaitable de proposer une approche basée sur une combinaison de ces méthodes. En effet, leur complémentarité permet de dépasser les limites et de profiter des avantages de chacune d'entre elles. Cette démarche est présentée au chapitre suivant.

Chapitre III

Analyse des risques d'un laboratoire d'analyses utilisant un système de robots mobiles

III.1 Introduction

Ce chapitre présente la mise en œuvre de plusieurs combinaisons de méthodes d'analyse des risques : AMDEC-ADD, STPA-ADD, STPA-nœud papillon, STPA-RdP stochastiques. Deux objectifs sont principalement visés. Tout d'abord, l'enjeu de la sureté et de la sécurité est abordé dans des applications robotiques, en environnements industriels. En particulier, nous souhaitons proposer une méthodologie d'analyse complète et détaillée des scénarios de risques, dans le cas de notre laboratoire d'analyses robotisé. Dans un deuxième temps, nous proposons une comparaison des résultats obtenus à travers les différentes approches.

Le contenu principal de ce chapitre est basé sur les articles publiés en revues [116–117] et en conférences internationales [118–120].

III.2 Etude d'un laboratoire d'analyses robotisé

Cette section consiste à construire une analyse détaillée des risques d'un laboratoire d'analyses robotisé en utilisant les approches détaillées au chapitre II. En particulier, cette étude de cas vise à étudier les scénarios de risques produits lors de la phase d'exploitation des systèmes robotiques.

Au préalable, avant d'entamer tout processus d'analyse des risques, nous proposons de décrire le système étudié et son utilisation.

III.2.1 Présentation générale du système, des scénarios de fonctionnement et des architectures de contrôle

Le système global étudié consiste à un système industriel complexe. Cette complexité peut être liée à ses fonctionnalités et tâches à réaliser, comme elle peut être liée à ses dimensions. Il est principalement composé de robots mobiles à roues coopérant ensemble afin de transporter des produits chimiques dangereux pour la santé humaine et l'environnement (toxiques, inflammables, explosifs...) au sein d'un laboratoire d'analyses chimiques, en présence de machines d'analyses et de travailleurs humains. Le laboratoire dispose de plusieurs salles, une grande salle d'analyses, des salles de stockage de produits chimiques une salle de chargement de la batterie et une salle de présentation des résultats d'analyses. Un modèle du laboratoire a été développé sous le simulateur V-Rep.

Ces robots peuvent être situés dans la même salle d'analyses, comme le montre la figure III.1.

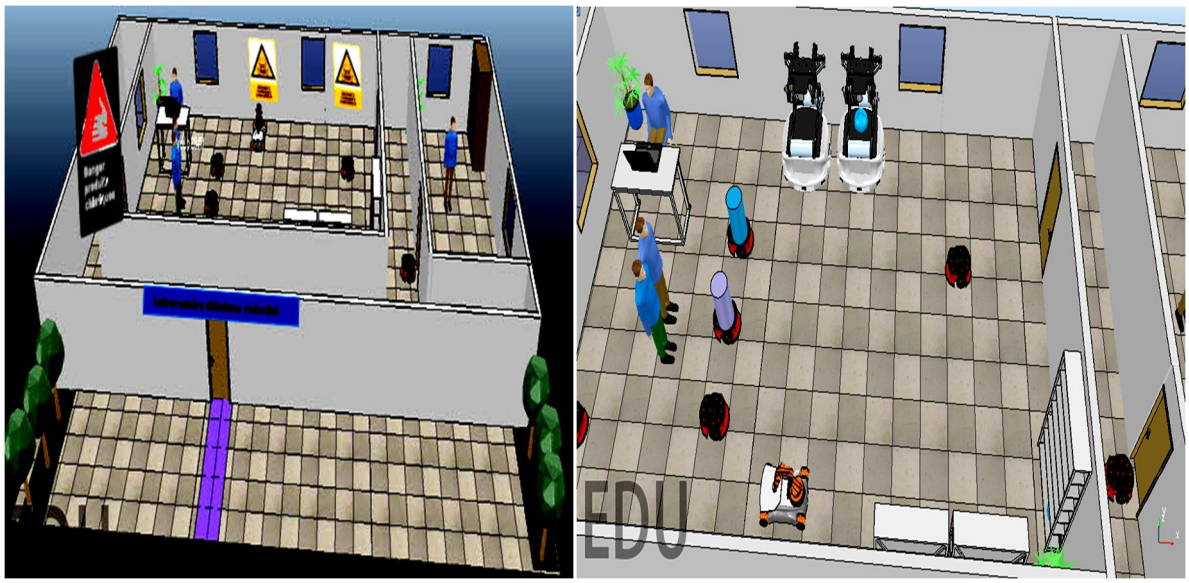


Figure III.1 Robots en fonctionnement normal se déplaçant dans un laboratoire composé d'une salle exposée à divers risques

Ils peuvent également se déplacer entre différentes salles du laboratoire. La figure III.2 montre un robot se déplaçant d'une salle à l'autre.

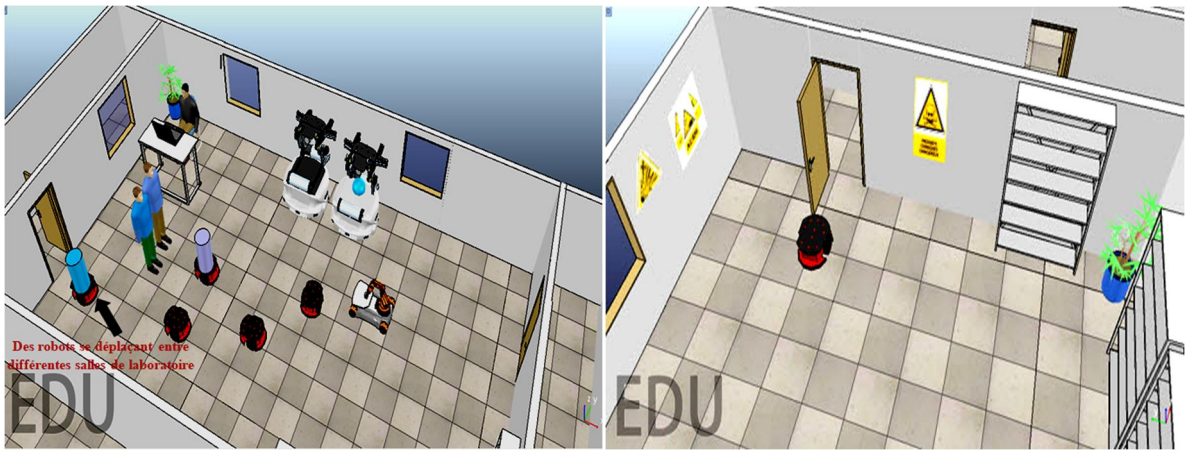


Figure III.2 Robots se déplaçant entre plusieurs salles d'un laboratoire à risques

Dans le cas d'un système multi-robots opérant ensemble au sein d'un environnement commun, différents types d'approches de contrôle et de coordination peuvent être utilisés. Ces approches sont étroitement liées à la complexité de ce système et au mode de fonctionnement de celui-ci, notamment en ce qui concerne sa taille et le type de coordination et de communication. En outre, la fonctionnalité de collaboration entre les

différentes entités autonomes est essentielle pour assurer la stabilité et la cohérence de l'ensemble du système [121]. Ces différents types d'approches sont illustrés à travers la figure III.3.

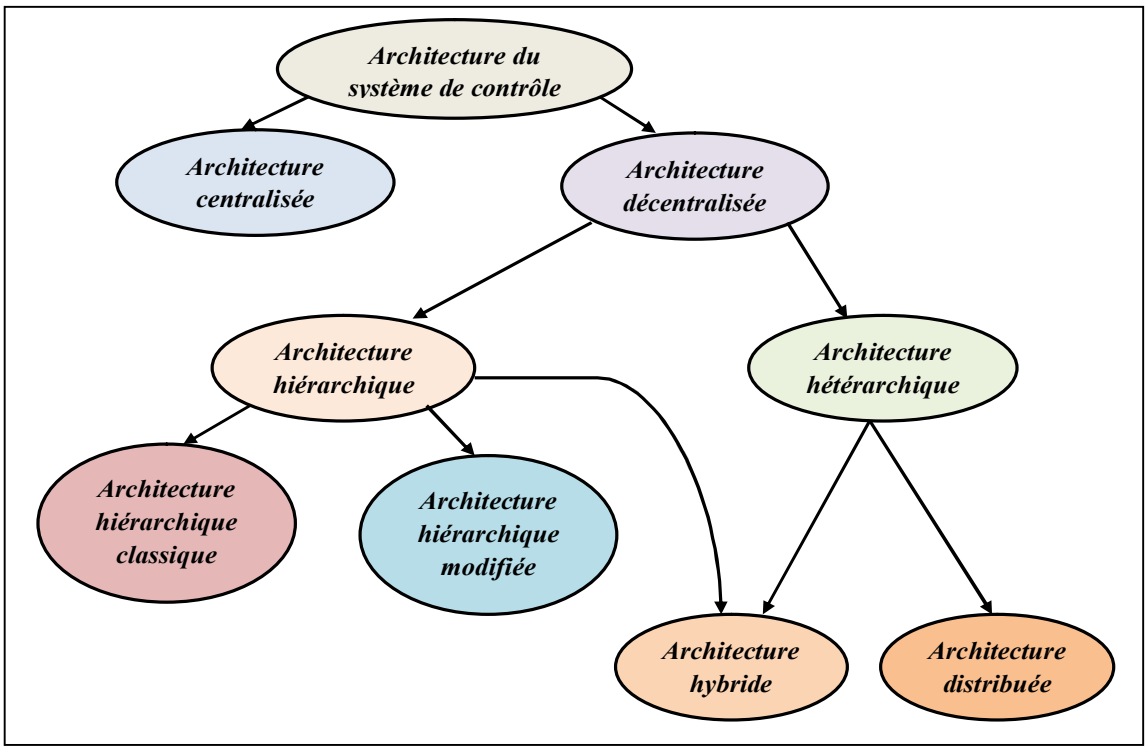


Figure III.3 Différentes approches de contrôle des systèmes industriels

Notre travail de thèse s'intéresse aux différentes approches de contrôle hiérarchiques à un ou plusieurs niveaux. Nous considérons dès lors les architectures centralisée, hiérarchique et hiérarchique modifiée.

III.2.2 Accidents liés à l'utilisation des robots

Lors d'une collaboration de robots pour effectuer une tâche demandée, des accidents sont susceptibles de se produire entre des robots, mais également entre un robot défaillant et un être humain résultant d'un problème de communication, d'interaction ou d'organisation. La figure III.4 présente quelques scénarios d'accidents possibles.

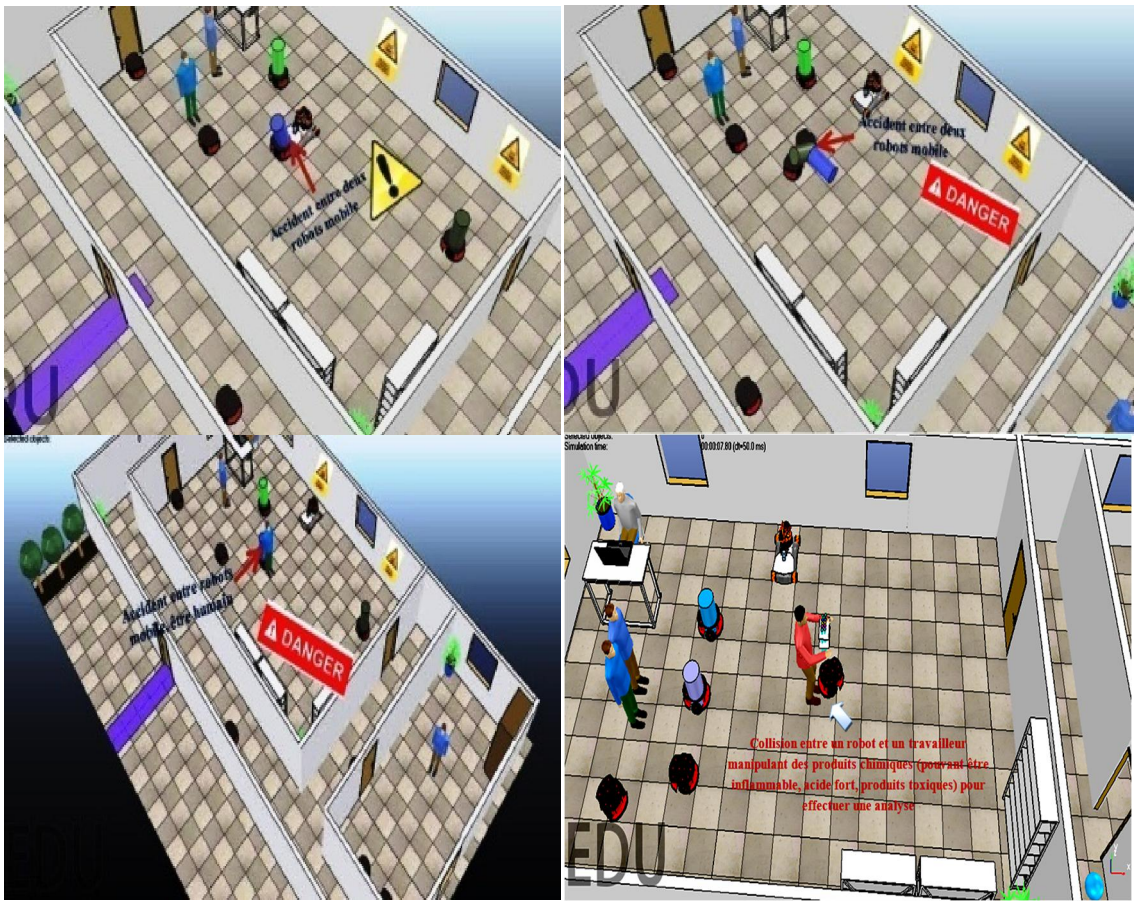


Figure III.4 Quelques scénarios d'accidents possibles : collision robot-robot, collision robot-travailleur humain

Les accidents potentiels peuvent être répartis comme suit :

1. **Premier cas :** collision de robots vides à grande vitesse.
2. **Deuxième cas :** collision entre un robot chargé de produits chimiques et des robots vides.
3. **Troisième cas :** collision de robots chargés de produits chimiques.
4. **Quatrième cas :** collision entre robot et être humain.
5. **Cinquième cas :** un robot tombe en panne lorsqu'il déplace des produits dangereux, sa tâche principale est le transport de ces produits en un temps imparti.

Le tableau III.1 classe les différents accidents possibles selon la gravité de ses conséquences.

Tableau III.1 Classification des accidents possibles et de leurs conséquences

Accidents possibles		**Conséquences des accidents**	**Criticité**
1er cas		- Dégradation des robots	C_1
2ème cas	Le robot chargé de produits explosifs	- Risque d'explosion - Effets toxiques du déversement de produits chimiques	C_4
	Le robot chargé de produits extrêmement ou facilement inflammable	- Risque d'incendie - Effets toxiques de la fumée d'incendie - Effets toxiques du déversement de produits chimiques	C_3
	Le robot chargé de gaz toxique	- Risque de toxicité et d'asphyxie	C_2
3ème cas	Les robots chargés d'explosifs, de produits inflammables, de gaz toxique ou de produits incompatibles	- Risque d'explosion, incendie, vapeurs ou gaz inflammables, toxicité et asphyxie, poussière	C_4
4ème cas	Le robot chargé de produits explosifs	- Risque d'explosion, risque de décès	C_4
	Le robot chargé de produits extrêmement ou facilement inflammables	- Risque d'incendie, de brûlure humaine	C_3
	Le robot chargé de gaz toxique	- Risque de toxicité humaine et d'asphyxie	C_2
	Le robot chargé de produits corrosifs et irritants	- Destruction de la peau humaine ou des tissus oculaires	C_2
5ème cas		- Perte de mission, Possibilité de modification des propriétés du produit chimique	C_1

La criticité des différents accidents possibles a été évaluée qualitativement selon deux critères principaux : la gravité des dommages et la probabilité d'occurrence de l'accident. Dans ce type de laboratoire, nous considérons les risques de criticité de C1 comme des risques acceptables, et les risques de criticité supérieure à C2 comme des risques intolérables.

III.3 Aperçu de la méthodologie d'analyse

Le schéma présenté sur la figure III.5 illustre clairement la démarche à suivre pour une analyse détaillée des scénarios de risques d'un système industriel robotisé (i.e. laboratoire d'analyses).

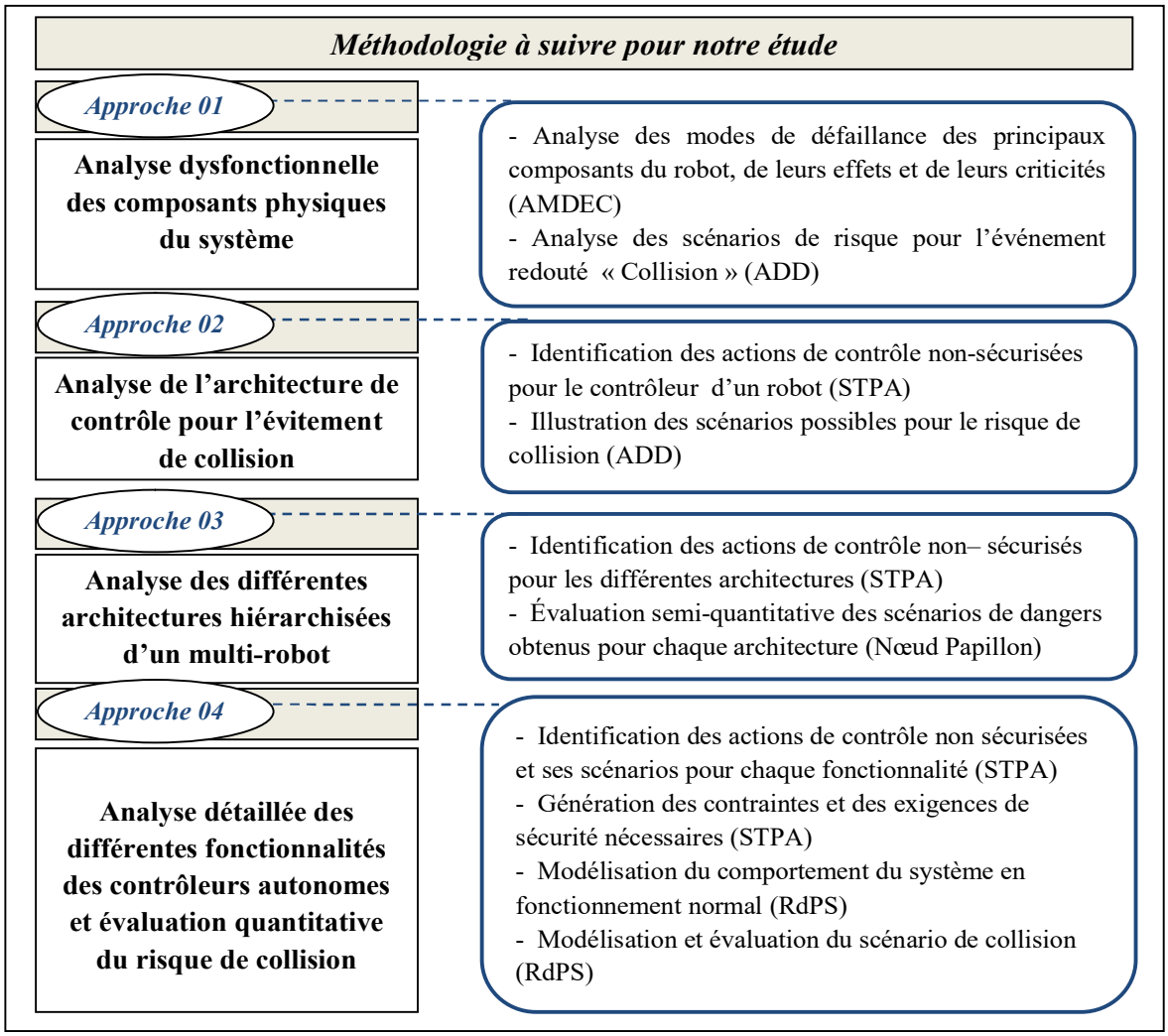


Figure III.5 Aperçu global de la méthodologie suivie dans notre étude

L'objectif de cette étude est d'assurer la sureté de fonctionnement dans un environnement de travail, afin d'optimiser la sécurité des êtres humains, des établissements et de préserver le bon fonctionnement des agents (i.e. des robots). Pour atteindre cet objectif, nous devons d'abord assurer la sécurité microscopique, résoudre les problèmes de navigation et de contrôle de chaque robot mobile, afin d'assurer la sécurité macroscopique au niveau du laboratoire. Il nous faudra alors prendre en compte les interactions entre les différents agents pour préserver l'environnement tout entier de la survenue d'accidents potentiels. La figure III.6 présente la théorie de la sécurité implémentée dans ce travail. La sécurité microscopique sous-entend la sureté de fonctionnement de chaque entité robotique

tandis que la sécurité macroscopique fait référence à la sureté et la sécurité de tout le laboratoire, y compris du système multi-robots.

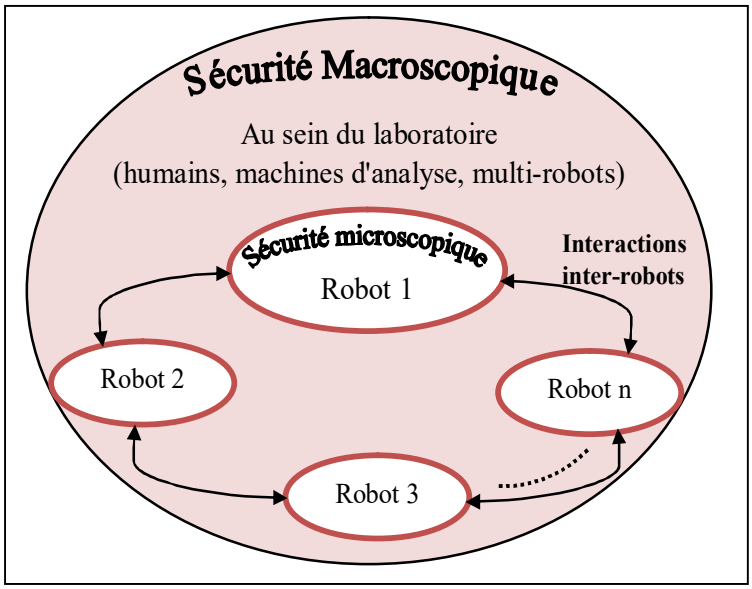


Figure III.6 Sécurités macroscopique / microscopique

III.4 Approche 1 : Analyse préliminaire des modes de défaillance du système à l'aide de la combinaison AMDEC/ADD

La partie « sureté de fonctionnement » est basée sur la combinaison de deux démarches différentes, l'une inductive, l'autre déductive. Dans un premier temps, nous appliquons l'analyse AMDEC (Analyse des modes de défaillance, de leurs effets et de leur criticité) sur un seul robot. Dans un second temps, nous complétons cette partie en utilisant l'analyse ADD (Analyse par arbre de défaillances) afin d'analyser le risque de collision entre robots.

III.4.1 Analyse des modes de défaillance, de leurs effets et de leurs criticités

Dans ce travail, nous ne présentons que les résultats de l'analyse AMDEC concernant les principaux composants du robot mobile. Lors de notre étude, nous avons considéré un robot de type Turtlebot2. Sa description est présentée dans l'annexe 1. Les éléments de la criticité de chaque mode de défaillance sont estimés selon les échelles présentées dans l'annexe 2. Le tableau III.2 montre le résultat de l'analyse AMDEC sur un seul robot.

Tableau III.2 Résultats de l'analyse AMDEC pour un robot de type TurtleBot2

Composant	Fonction	Mode de défaillance	Cause	Effet	Moyens de détection	Gravité	Occurrence	Détectabilité	RPN	Actions a- Préventive b- Protective
Capteur visuel **(Caméra RGB)**	Détection visuelle d'obstacles (balayage d'objets et détection de couleurs)	- Mauvaise qualité d'image	- Faible ou forte luminosité	- Pas de détection des obstacles statiques et dynamiques	- L'opérateur peut détecter la qualité de luminosité - Le capteur IR peut également détecter les obstacles	3	3	3	27	a- Il est nécessaire d'effectuer des tests périodiques pour vérifier le bon fonctionnement des capteurs
		- Image incomplète	- Défaillance du moteur responsable de la rotation du capteur			3	2	2	12	
Capteur de profondeur infrarouge **(Capteur IR)**	Mesure la distance entre l'obstacle ou l'objet et le capteur (détecte la profondeur)	- Aucune indication n'a été donnée par le capteur (valeur nulle)	- Panne interne du capteur - Perte de connexion - Défaillance de l'émetteur IR - Niveau de batterie faible	- Envoi de commandes incorrectes - Action indésirable du robot	- La camera RGB peut également détecter les obstacles - Le capteur de contact peut détecter une collision - Le tableau de bord de la Kobuki montre le niveau de batterie (un capteur indique l'état de la batterie)	4	4	2	32	a- Test des capteurs et émetteurs pendant chaque période de temps prédéterminée a- Déclencher une alarme au niveau du logiciel de supervision si la batterie atteint un niveau jugé insuffisant b- Arrêter le robot s'il y a contact avec un obstacle

		- Indication erronée du capteur (valeurs aléatoires ou constantes)	- Calibrage inadéquat - Défaillance du capteur	- Erreur lors du calcul des coordonnées des objets sur des points particuliers - Risque de collision avec les êtres humains ou avec les autres robots (dommages humains et matériels)	- La camera RGB peut également détecter les obstacles - Le capteur de contact peut détecter une collision	4	3	2	24	a- Vérifier l'étalonnage du capteur lors de l'initialisation b- Arrêter le robot s'il y a contact avec un obstacle
		- Valeurs aberrantes ou déviation du nuage de points résultant	- Éclairage puissant - Propriétés de la surface de l'objet (surfaces brillantes)	- Apparition de taches laser avec un faible contraste dans l'image infrarouge	- Le capteur de contact peut détecter une collision	4	3	3	36	a- Penser à régler l'éclairage du laboratoire b- Arrêter le robot s'il y a contact avec un obstacle

Contrôleur de robot	Contrôle du robot – Commande de chaque roue	- Bloqué ou gelé (commande constante)	- Blocage du programme ou du système d'exploitation - Problème de communication	- Envoi de commandes constantes - Mouvement non contrôlé ou bloqué à un moment donné (robot gelé)	- Surveillance de l'opérateur - Le capteur de contact peut détecter une collision	3	4	3	36	a- Utiliser un matériel de contrôle performant b- Installer des techniques de protection pour le logiciel b- Alerte à l'utilisateur et arrêt d'urgence du robot
		- Contrôle aléatoire (pic)	- Panne logicielle interne ou panne matérielle	- Mouvements indésirables	- Surveillance de l'opérateur	3	2	3	18	a- Techniques de prévention des pannes pour le développement de logiciels a- La solution dépend de la technique de redondance choisie b- Arrêt d'urgence par l'opérateur
		- Sortie nulle	- Problème d'alimentation, panne matérielle ou logicielle	- Mouvement bloqué	- Tableau de bord Kobuki (vérifier l'état de la charge de la batterie)	2	3	2	12	a- Déclencher une alarme au niveau du logiciel de supervision si la batterie atteint un niveau jugé insuffisant

		- Commande incorrecte	- Instructions non correctes - Indications erronées des capteurs	- Un mouvement incorrect peut provoquer des accidents		3	1	5	15	
Moteur	Rotation des roues afin de déplacer le robot	- Problème de démarrage (ne fonctionne pas)	- Problème d'alimentation - Batterie défaillante - Câble déconnecté ou endommagé - Tension d'alimentation trop basse - Chute de tension trop élevée - Panne interne du moteur	- Mouvement bloqué - Perte de mission	- Tableau de bord Kobuki (état des moteurs, de la batterie)	2	3	3	18	a- Test périodique des moteurs, câbles et batterie
Roues	Déplacement du robot	- Problème de mouvement	- Panne moteurs ou blocage des roues - Commande incorrecte	- Mouvement bloqué	- Surveillance de l'opérateur	2	3	3	18	a- Essais périodiques des roues et des moteurs

III.4.2 Analyse de l'arbre de défaillances

La figure III.8 présente l'analyse ADD appliquée à l'environnement complet du laboratoire. Nous avons retenu, comme événement redouté, la collision de robots. Il correspond au risque dominant. Nous traitons ainsi les causes possibles pouvant entraîner le risque de collision du robot avec d'autres obstacles statiques ou dynamiques. Cette collision peut conduire à des risques industriels graves : risque d'explosion, risque d'incendie, déversements chimiques, déchets dangereux (gaz toxiques, poussière, fumée, etc.). A titre d'exemple, le risque d'explosion peut apparaître si l'un de ces trois cas se produit (figure III.7) :

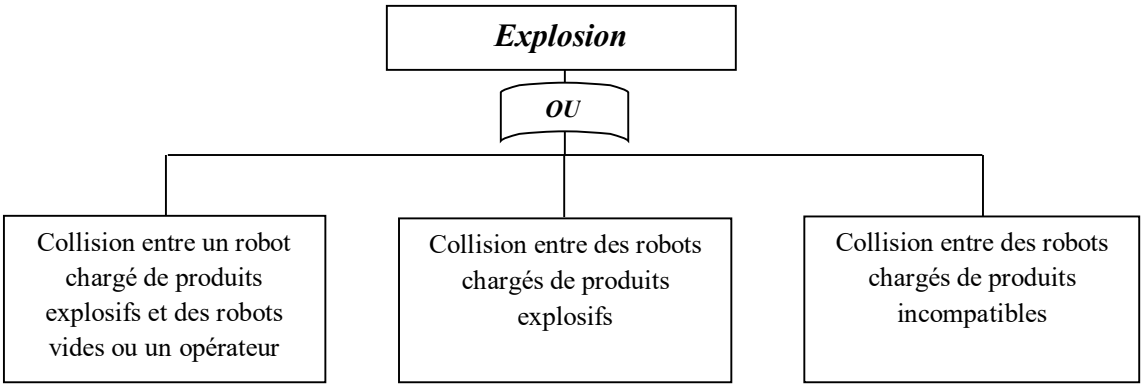


Figure III.7 Causes pouvant conduire à une explosion

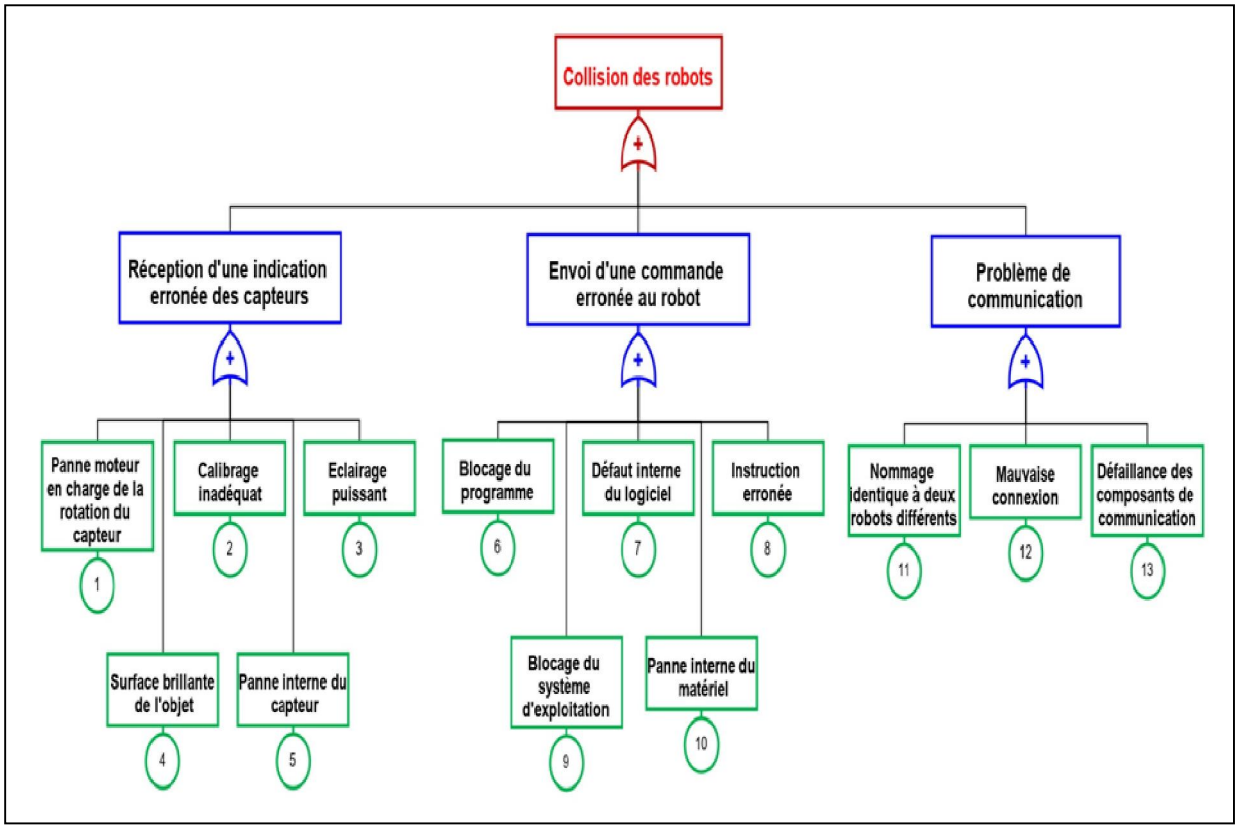


Figure III.8 Application de l'analyse ADD pour le risque de collision

III.4.3 Discussion

Après l'application de l'analyse AMDEC sur un robot ; les recommandations obtenues pour assurer son bon fonctionnement et minimiser ses risques sont les suivantes :

- Il est nécessaire d'effectuer des tests périodiques pour vérifier le bon fonctionnement des différents composants (capteurs, actionneurs...).
- La mise en place de moyens de prévention et de protection contre les risques tels que des panneaux d'interdiction et des extincteurs au sein du laboratoire.
- Installer une alarme au niveau du logiciel de supervision si le niveau de batterie atteint un niveau jugé insuffisant.
- L'arrêt automatique du robot si le capteur de contact détecte une collision avec un obstacle.
- L'utilisation de techniques de protection des logiciels utilisés.
- L'arrêt d'urgence par l'opérateur en cas de dysfonctionnement grave.
- Une alerte qui indique l'existence d'un défaut interne du robot.

Selon l'analyse ADD, la défaillance pouvant conduire à une collision de robots dépend de trois problèmes majeurs :

- indication erronée des capteurs ;
- envoi d'une commande incorrecte au robot ;
- des problèmes de communication.

III.5 Approche 2 : Analyse de l'architecture de contrôle à l'aide de la combinaison STPA/ADD

Cette section présente une identification des dangers potentiels applicable à un système industriel robotisé (i.e. laboratoire d'analyses). Nous considérons toujours le problème de collision d'un robot avec des obstacles statiques ou dynamiques (i.e. autres robots ou opérateur), tout en utilisant une autre combinaison de deux méthodes d'analyse des risques : L'analyse STPA et l'analyse par arbre de défaillance (ADD) afin de clarifier les scénarios de danger attendus. Dans cette partie, nous nous concentrons sur l'architecture de contrôle, et en particulier sur le contrôleur d'évitement d'obstacles.

Afin d'appliquer l'analyse STPA sur un système, la structure de contrôle hiérarchique (SCH) du système doit être développée au préalable.

III.5.1 Structure de contrôle hiérarchique

Le système à analyser doit d'abord être décrit comme une SCH utilisant un simple ensemble de règles de modélisation, ce qui permet de rendre le système plus lisible. Toutes les SCH sont composées de 4 concepts principaux : unités de contrôle, actions de contrôle, retour d'état et processus contrôlé. La figure III.9 montre la SCH de haut niveau pour un seul robot. Le plus important, à ce stade, est de fournir un contrôle autonome et en toute sécurité du mouvement des roues et de leurs vitesses afin d'avoir un mouvement du système multi-robots fluide et sans collision. Ceci est parfaitement réalisé à travers la collaboration des robots au sein du laboratoire. Par conséquent, la première étape de la STPA consiste à analyser la structure de contrôle d'un robot et à identifier les comportements à risques pouvant être causés par des actions de contrôle dangereuses. Puis, dans une seconde étape de l'analyse STPA, nous déterminons les scénarios de danger et les facteurs causaux de chaque action dangereuse de contrôle ou de chaque réaction indésirable du processus. Enfin, nous organisons les scénarios identifiés dans des arbres avec le même principe que l'ADD.

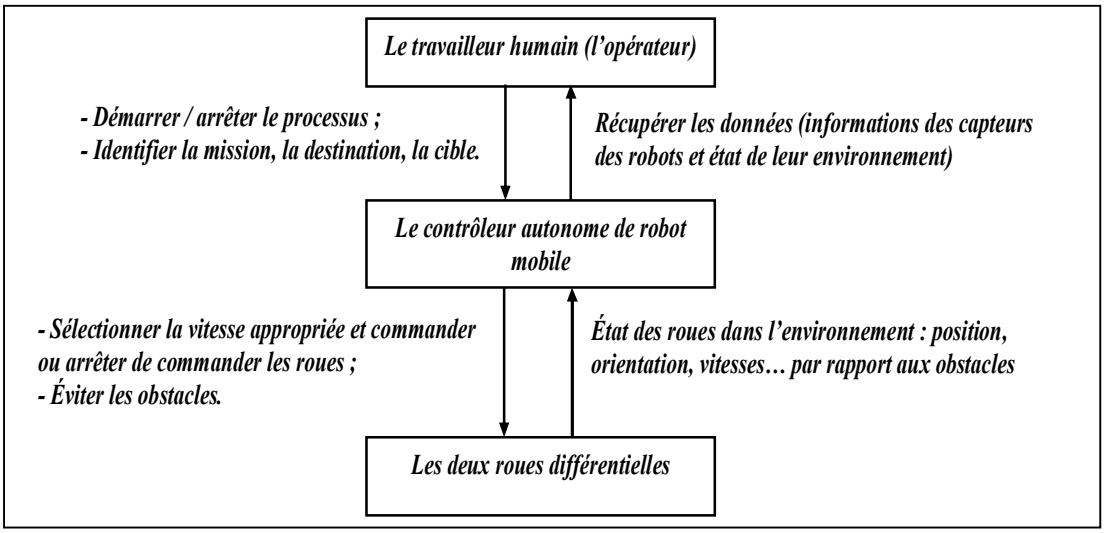


Figure III.9 Architecture de contrôle hiérarchique de haut niveau du système robotique

III.5.2 Résultats de l'analyse

Les résultats de l'analyse STPA sont regroupés dans les tableaux III.3 et III.4.

Le tableau III.3 montre l'ensemble des actions dangereuses de contrôle (UCAs) et leurs facteurs de causalité, tandis que l'identification des dangers de chaque UCA, leurs accidents et pertes probables sont rassemblés dans le tableau III.4.

Tableau III.3 Analyse STPA des dangers

Nombre d'UCA	Actions dangereuses de contrôle (UCAs)	Facteurs de causalité (scénarios)
UCA1	Le robot n'évite pas un obstacle dynamique ou statique (e.g. autres robots chargés de produits chimiques, travailleurs, machines d'analyses, murs...).	- Mauvaise / aucune détection des distances entre les obstacles et le robot ou problème concernant la position des obstacles (petits obstacles, surfaces brillantes, imprécisions de mesure). - Défaillance des capteurs / étalonnage inapproprié. - Défaillance des composants de communication (i.e. du récepteur robot). - Algorithme de contrôle inadéquat du robot. - Paramètres inadéquats de contrôle. - Saturation de la carte mémoire du robot.
UCA2	Le contrôleur émet une commande incorrecte pour l'évitement de collision.	
UCA3	La commande est arrêtée trop tôt ou appliquée trop longtemps.	

UCA4	Le contrôleur ne choisit pas la vitesse appropriée des robots (trop élevée).	- Défaillance des moteurs. - Blocage des roues. - Action de contrôle conflictuelle de l'actionneur.
UCA5	Le contrôleur fournit une commande après un délai (retard).	- Réception en même temps d'une large gamme d'informations de retour d'état de robots. - Saturation de la carte mémoire du robot. - Blocage du programme. - Retards de retour d'état.
UCA6	Le contrôleur modifie la valeur de vitesse en un temps incorrect.	

Tableau III.4 Identification des dangers, accidents et pertes pour chaque UCA

UCAs	Dangers	Accidents probables	Pertes
UCA1	- Le robot viole la distance de sécurité avec les autres robots ou les objets. - Les robots pénètrent dans la zone dangereuse. - Déversement de produits chimiques.	- Collision de robots chargés de produits chimiques. - Collision entre robot et le travailleur humain. - Le robot chargé de produits chimiques percute le mur ou tombe. - Déversement de produits chimiques sur le travailleur. - Mélange de produits chimiques incompatibles. - Un incendie s'est déclaré dans le laboratoire. - Une explosion pourrait se produire dans le laboratoire.	- Dommages humains, blessures ou décès. - Installation, machines et robots endommagés. - Perte de produits chimiques. - Production réduite. - Environnement contaminé. - Effets toxiques des déversements de produits chimiques, des fumées d'incendie, des gaz toxiques, des vapeurs et des poussières.
UCA2	Le robot entre dans un état incontrôlé ou adopte une attitude non-sécurisée.		
UCA3	Le robot entre dans un état incontrôlé ou adopte une attitude non-sécurisée.		
UCA4	Le robot entre dans un état dangereux.		
UCA5	Le robot ne peut pas réagir rapidement dans des situations dangereuses (i.e. lorsqu'il y a des obstacles).		
UCA6	Le robot adopte une attitude non-sécurisée.		

Grâce aux résultats de l'analyse STPA présentés dans le tableau III. 4, un ensemble d'événements indésirables est clairement identifié. Nous avons sélectionné les plus dangereux d'entre eux (explosion ; incendie ; dommages sur les travailleurs humains, décès ou blessures) pour réfléchir plus profondément aux causes possibles de ces dangers en utilisant une analyse par arbre de défaillances ADD.

L'analyse de l'arbre de défaillances que nous avons utilisée est différente de l'analyse conventionnelle par arbre de défaillances : elle ne représente pas seulement les défaillances ; elle inclut également d'autres causes. Nous regroupons dans cet arbre les causes de toute la hiérarchie de contrôle et les comportements inappropriés des travailleurs et des robots en plus des défauts. Un ensemble de scénarios de dangers est illustré dans les arbres présentés aux figures III.10, III.11 et III.12.

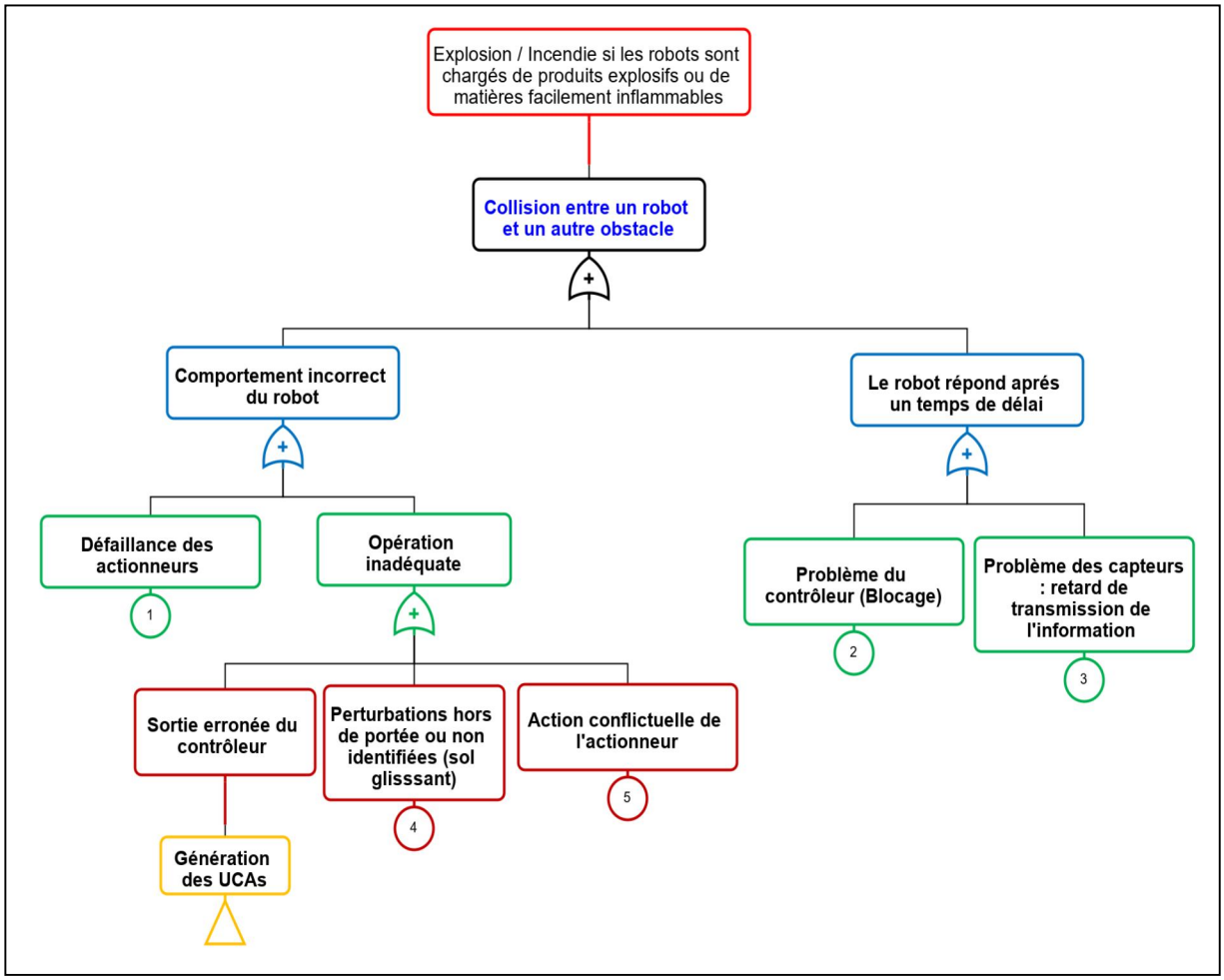


Figure III.10 Arbre représentant les scénarios de risques d'explosion/incendie partie 1

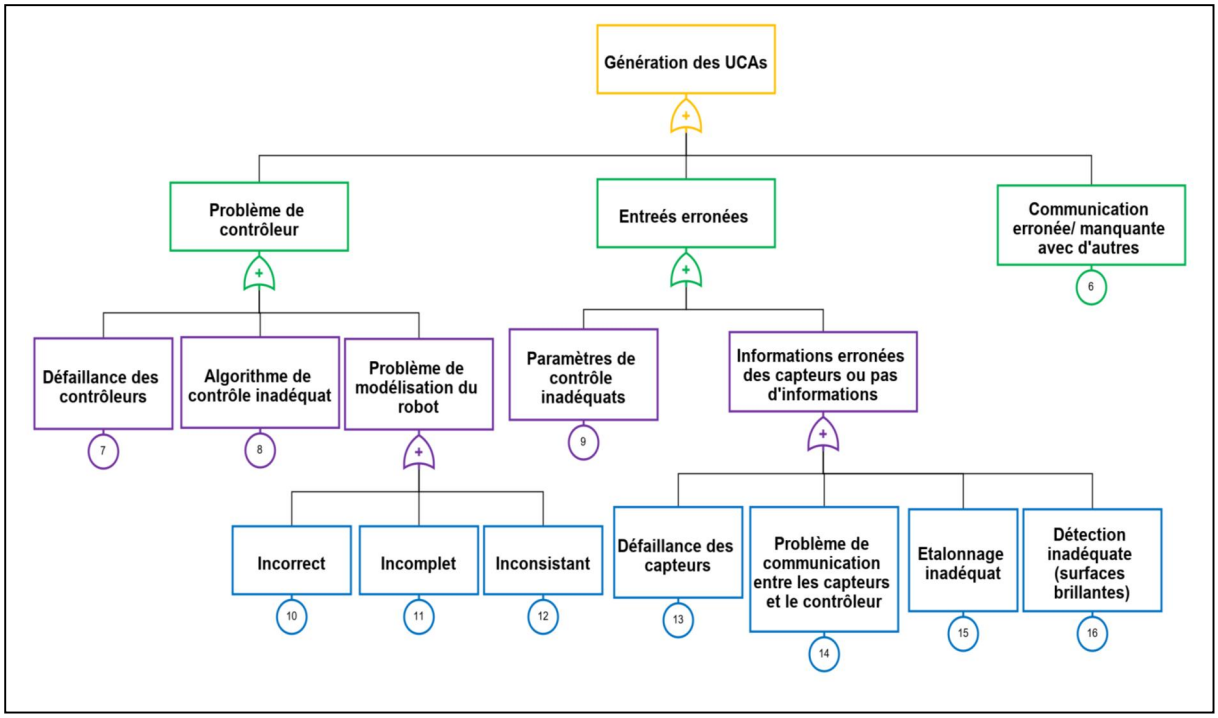


Figure III.11 Arbre représentant les scénarios de risques d'explosion/incendie partie 2

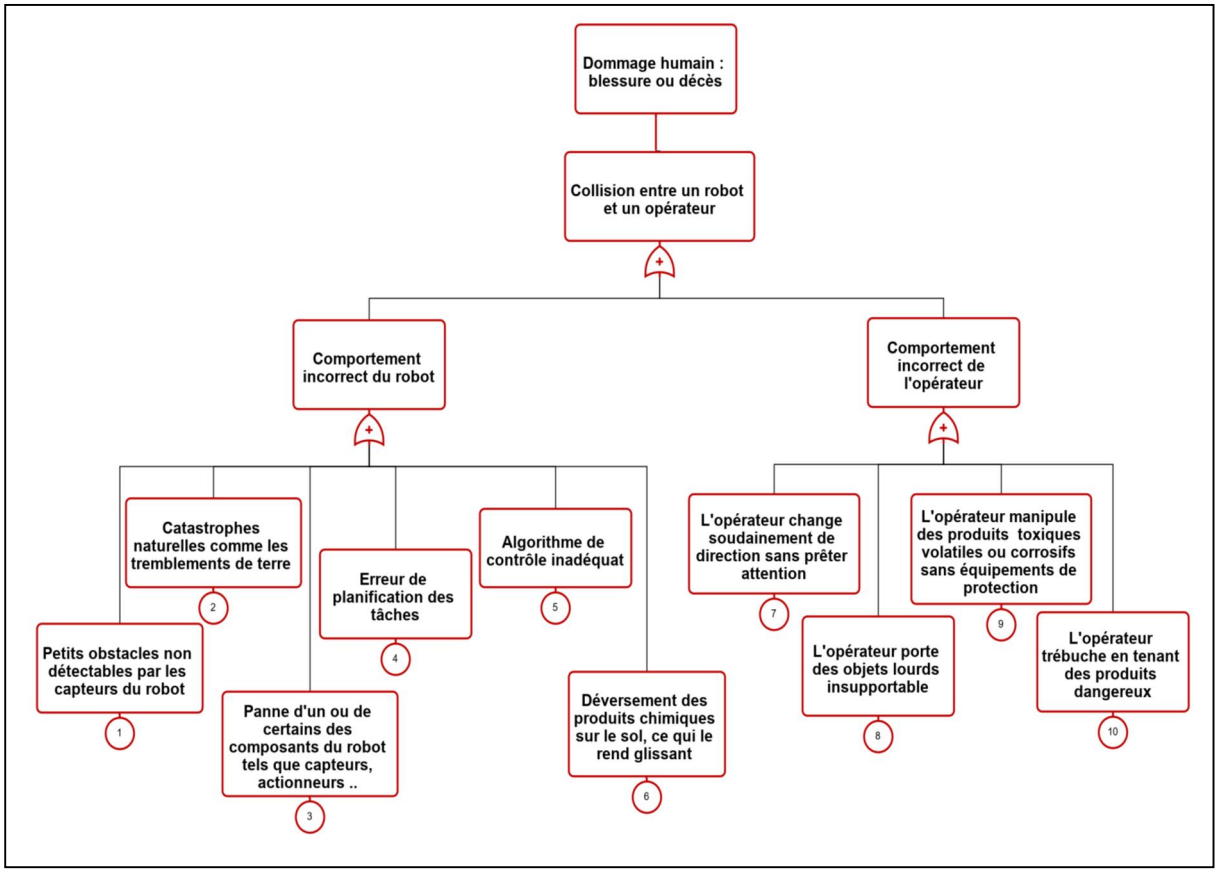


Figure III.12 Arbre représentant les scénarios de travailleurs tués ou blessés

III.5.3 Discussion

Sur la base des résultats obtenus par l'application des méthodes d'analyses STPA/ADD, nous pouvons conclure que les sources de danger dans ce type de laboratoire robotisé peuvent être d'origine humaine, robotisée ou environnementale (perturbations environnementales). Les deux systèmes mobiles (i.e. travailleurs et robots) peuvent être dommageables s'ils réalisent des comportements inappropriés. Ces sources sont résumées sur la figure III.13.

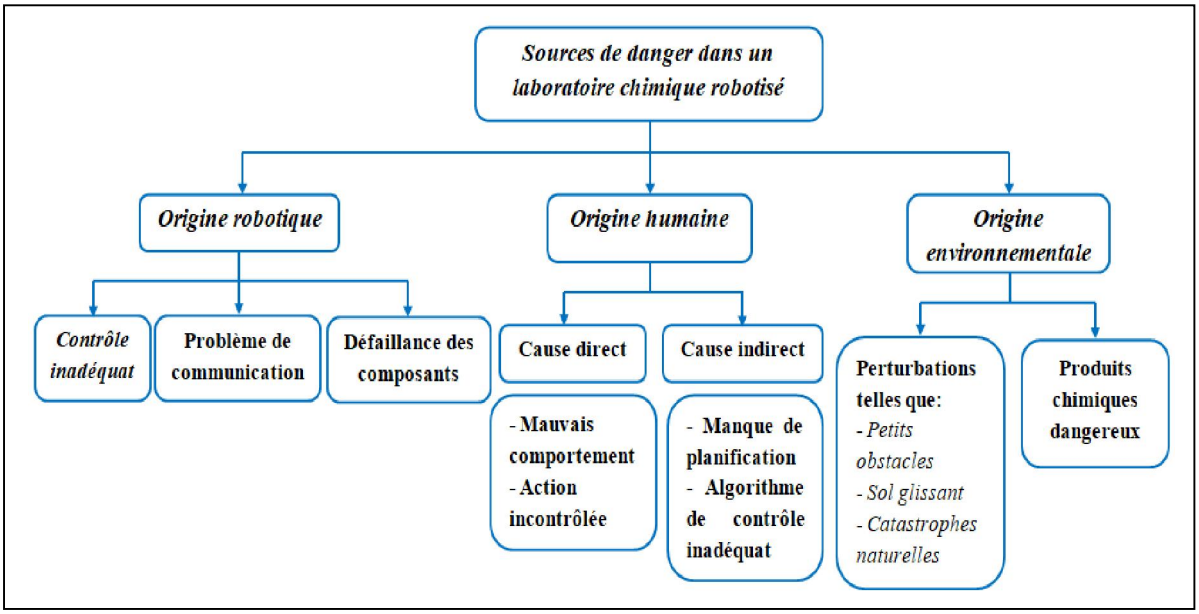


Figure III.13 Diagramme donnant les sources de danger du laboratoire de chimie

A travers l'analyse des dangers ; quelques recommandations ont été obtenues afin de préserver la sureté et la sécurité du laboratoire :

- Assurer un bon contrôle des robots ;
- Assurer un choix correct des paramètres de contrôle ;
- Assurer le fonctionnement normal du robot en améliorant la fiabilité de ses composants ;
- Assurer l'hygiène de l'environnement de travail ;
- Equipements de protection obligatoires pour chaque opérateur ;
- Renforcement des contraintes de sécurité : distances de sécurité, limites de vitesse... ;
- Assurer une bonne coopération, communication et coordination entre les robots par un choix correct de l'architecture de contrôle du système multi-robots.

III.6 Approche 3 : Comparaison des différentes architectures hiérarchisées de contrôle (de haut niveau) d'un système multi-robots à l'aide des méthodes STPA et nœud papillon

Il existe plusieurs approches de pilotage. Nous pouvons les utiliser pour coordonner le contrôle des différentes entités robotiques, gérer leurs mouvements et organiser leurs tâches [91; 122]. Ce travail de recherche a permis d'analyser les trois types d'approches hiérarchiques. L'objectif principal est de choisir la meilleure architecture pour le fonctionnement d'un système multi-robots dans un environnement complexe.

III.6.1 Structure centralisée SC

Comme le montre la figure III.14, une unité de commande contrôle tous les robots et a un pouvoir de décision. Elle maintient les informations globales de toutes les activités du système multi-robots. Cette unité gère, traite les événements en temps réel, synchronise et coordonne toutes les tâches.

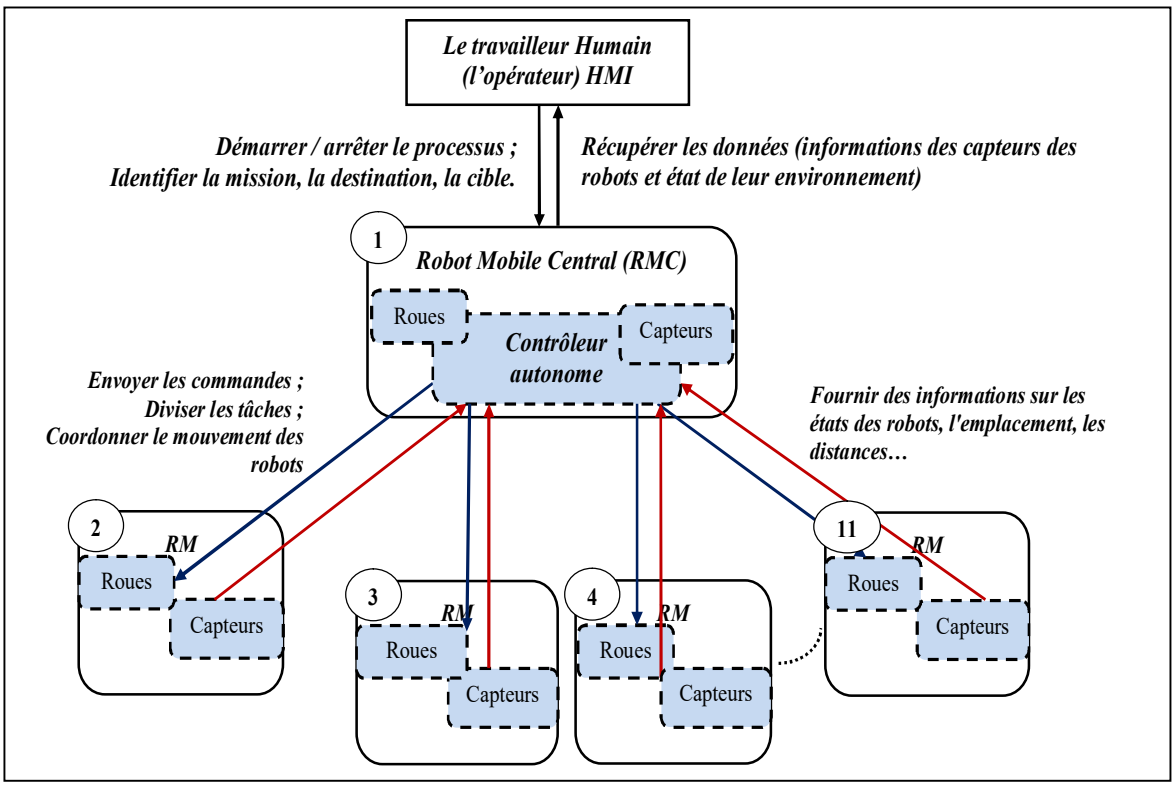


Figure III.14 Structure de contrôle centralisée pour SMRM (flèche bleue pour l'envoi de commandes, flèche rouge pour la réception du feedback)

III.6.2 Structure hiérarchique SH

La figure III.15 représente les résultats de l'approche de contrôle hiérarchique. Les robots sont liés par des relations de type « maître-esclave ». Cette hiérarchie a été largement étudiée et a été largement utilisée et déployée dans l'industrie depuis les années 1970 [91]. Dans ce type d'approche, les décisions de gestion sont prises par le leader de haut niveau, qui doit nécessairement disposer de toutes les informations nécessaires pour prendre des décisions permettant une performance globale correcte.

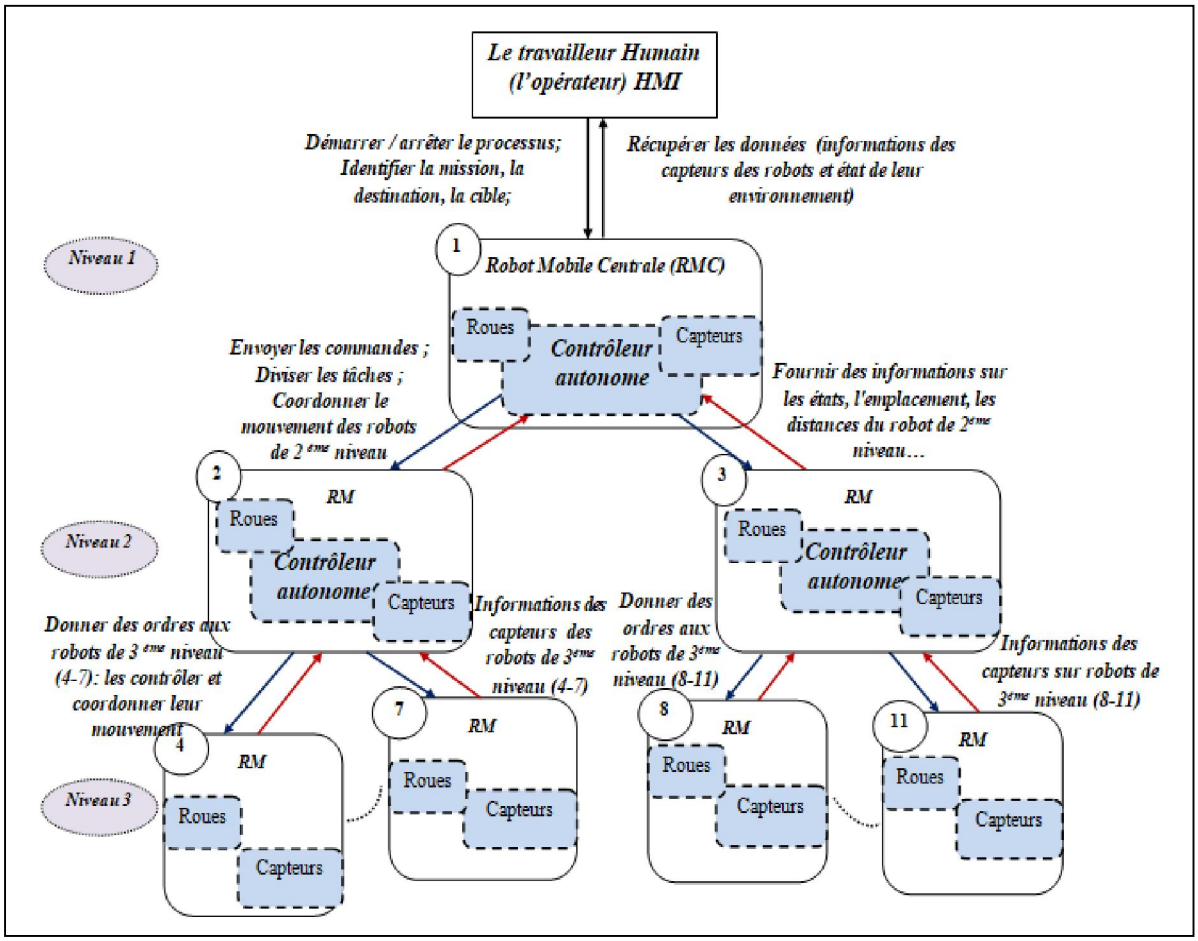


Figure III.15 Structure de contrôle hiérarchique pour SMRM (flèche bleue pour l'envoi des commandes, flèche rouge pour la réception des commentaires)

III.6.3 Structure hiérarchique modifiée SHM

Il existe une autre forme d'approche hiérarchique pour laquelle des robots de même niveau peuvent communiquer et se coordonner. Ce type d'approche est appelé « approche hiérarchique modifiée » (voir figure III.16).

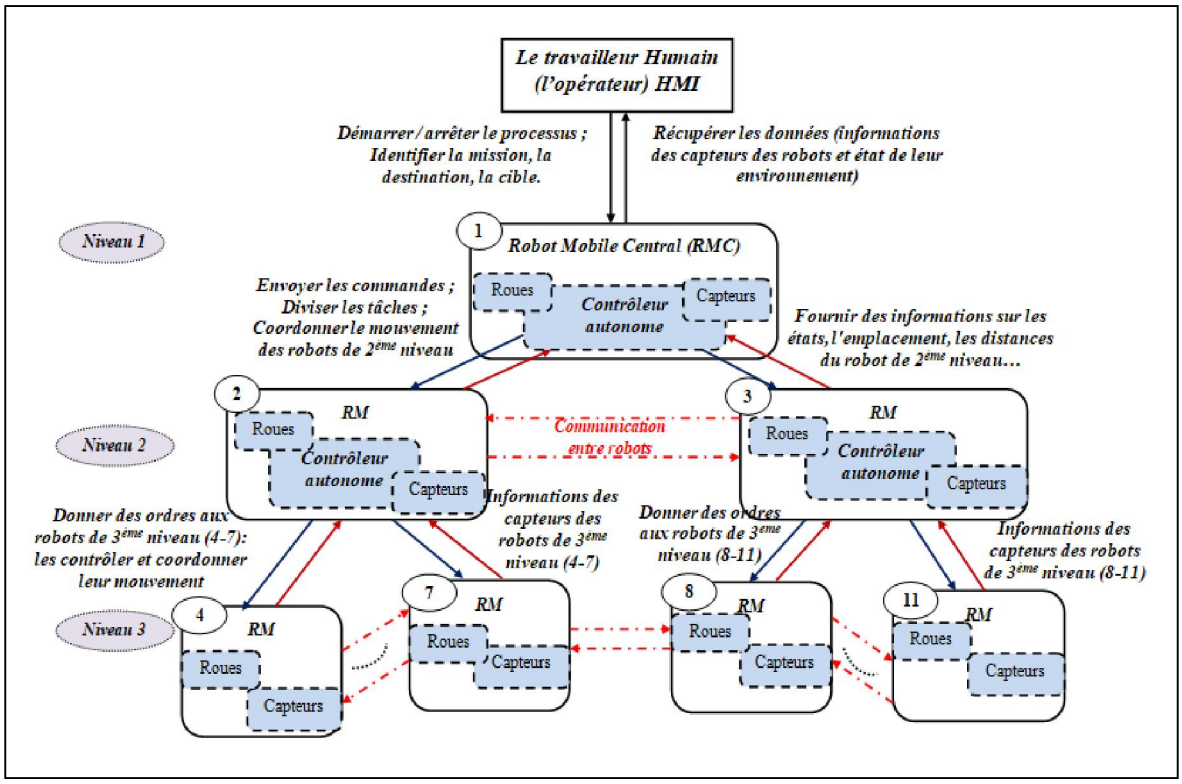


Figure III.16 Structure de contrôle hiérarchique modifiée pour SMRM

III.6.4 Résultats de l'analyse des dangers STPA

Afin de réaliser l'analyse STPA sur le système considéré [53; 87], nous appliquons les deux dernières étapes de l'organigramme de la figure II.3.

- **Étape 3 :** les résultats obtenus en termes de risques possibles sont rassemblés dans le tableau III.6.
- **Étape 4 :** les causes possibles des dangers obtenus sont résumées dans le tableau III.7.

Pour permettre l'analyse STPA, les pertes, les accidents de haut niveau et les dangers du système multi-robots susceptibles de se produire dans ce laboratoire doivent être identifiés. Le tableau III.5 détaille l'ensemble des dangers, les accidents et pertes qui en résultent. En effet, chaque danger peut produire un ensemble d'accidents en termes de pertes humaines ou matérielles (« losses » en anglais). La gravité de ces dangers est évaluée à partir de la gravité de ces pertes.

Tableau III.5 Tableau des pertes, accidents et dangers

Pertes	Accidents au niveau du système	Dangers au niveau du système
L-1 : Blessure des travailleurs humains (dommages aux humains) ***Gravité = 3***	**SlA-1 :** Deux robots ou plus sans produits chimiques entrent en collision ***(L-4, L-5)***	**S-lH1 :** Les robots enfreignent la distance requise pour la sécurité ***(SlA-1, SlA-2, SlA-3, SlA-4, SlA-5)*** [Gravité importante]
L-2 : Blessure mineure à l'homme ***Gravité = 2***	**SlA-2 :** Collision entre deux ou plusieurs robots pendant qu'ils déplacent des produits ***(L-3, L-4, L-5, L-6)***	**S-lH2 :** Excès de vitesse des robots (ceux-ci dépassent la vitesse de sécurité) ***(SlA-1, SlA-2, SlA-3, SlA-4)*** [Gravité importante]
L-3 : Perte de produits chimiques ***Gravité = 2***	**SlA-3 :** Collision entre un / plusieurs robots et un humain ***(L-2, L-3, L-4, L-5)*** **SlA-4 :** Collision entre un / plusieurs robots transportant des produits et un humain ***(L-1, L-3, L-4, L-5, L-6)***	**S-lH3 :** Les robots ont un problème de comportement (fonctionnement anormal des robots) ***(SlA-1, SlA-2, SlA-4)*** [Gravité importante]
L-4 : Perte de mission ***Gravité = 2***	**SlA-5 :** Les robots percutent un mur ou un objet fixe (machines d'analyses), ou tombent au sol ***(L-3, L-4, L-5)***	**S-lH4 :** Arrêt inattendu du fonctionnement des robots ***(SlA-6)*** [Gravité mineure]
L-5 : Dommages aux robots, machines ***Gravité = 2***	**SlA-6 :** Fonctionnement interrompu des robots et des machines d'analyses ***(L-4)***	**S-lH5 :** Déversement de produits chimiques à haut risque (inflammables, toxiques...) ***(SlA-7)*** [Gravité importante]
L-6 : Dommages à l'environnement de travail : poussières toxiques, gaz, brûlures… ***Gravité = 3***	**SlA-7 :** Incendie, empoisonnement (zone, émission de gaz) ***(L-3, L-4, L-5, L-6)***	**S-lH6 :** Fonctionnement anormal des robots sans produits ***(SlA-1, SlA-3, SlA-5)*** [Gravité mineure]

III.6.4.1 Identification des scénarios de dangers par STPA

L'analyse STPA permet d'extraire des scénarios dangereux qui se produiraient dans les différentes situations mentionnées dans la partie II.4.3. Les événements de risque correspondants et leurs facteurs de causalité se trouvent dans les tableaux III. 6 et III.7. Cette étape permet d'extraire un grand nombre de scénarios et leurs causes. Chaque scénario peut être lié aux dangers mentionnés dans la liste obtenue dans le tableau III.5. Pour donner plus d'importance à l'analyse et rendre les scénarios résultant de l'approche STPA plus significatifs, une évaluation semi-quantitative a été réalisée sur la base des résultats de l'analyse du nœud papillon. Cette évaluation nous donne une classification en fonction de la criticité de chaque scénario.

Tableau III.6 Tableau d'identification des dangers STPA

Actions de contrôle	**Scénarios non sécurisés (dangereux) (US)**	**Risque au niveau du système (S-lH)**		
		SC	**SH**	**SHM**
Lancer / arrêter le processus (par l'opérateur)	**US1 :** L'opérateur lance un programme inadéquat ou deux programmes différents en même temps sur le robot maître.	S-lH6	S-lH6	S-lH6
	US2 : L'opérateur n'arrête pas le processus en cas d'urgence, ou celui-ci intervient trop tard.	S-lH3	S-lH3	S-lH3
Unité de contrôle et de coordination				
Envoyer des commandes, coordonner le mouvement des robots (par le maître, 1er niveau)	**US3 :** Le contrôleur fournit la commande de guidage à un robot esclave, de 2ème niveau, sans précision.	S-lH3	S-lH3	S-lH3
	US4 : Le contrôleur fournit la commande d'exécution incorrecte pour éviter les obstacles (direction incorrecte).	S-lH3	S-lH3	S-lH3
	US5 : La commande d'opération est fournie aux robots par intermittence.	S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5
	US6 : La commande d'opération n'est pas fournie aux robots de 2ème niveau, de manière inattendue (opération interrompue).	S-lH1 S-lH4	S-lH1 S-lH4	S-lH1 S-lH4
	US7 : La commande d'arrêt n'est pas fournie quand elle est nécessaire / La commande d'évitement n'est pas fournie par le maître à un robot esclave de 2ème niveau, devant un obstacle dynamique ou statique.	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US8 : Le contrôleur fournit la commande correcte, mais trop tard.	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US9 : La même valeur de commande fournie pendant une longue période.	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US 10 : Le maître ne coordonne pas le mouvement entre les deux robots du 2ème niveau, ou la coordination est fournie trop tard.	S-lH3	S-lH3	S-lH3

Envoyer des ordres, des commandes et coordonner le mouvement des robots (par contrôleurs, 2e niveau)	**US11 :** Les contrôleurs de 2ème niveau fournissent la commande de guidage à un robot esclave de 3ème niveau, sans précision.	N/A	S-lH3	S-lH3
	US12 : La commande d'opération est fournie aux robots par intermittence.		S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5
	US13 : La commande d'opération n'est pas fournie aux robots du 3ème niveau, de manière inattendue (opération interrompue).		S-lH1 S-lH4	S-lH1 S-lH4
	US14 : La commande d'évitement n'est pas fournie par le maître à un robot esclave de 3ème niveau, devant un obstacle dynamique ou statique.		S-lH1 S-lH5	S-lH1 S-lH5
	US15 : Le contrôleur fournit la commande correcte, mais trop tard.		S-lH1	S-lH1
	US16 : Le contrôleur maître émet un ordre incorrect.		S-lH1 S-lH3	S-lH1 S-lH3
	US17 : Un signal de commande émis par le contrôleur trop tard.		S-lH1 S-lH5	S-lH1 S-lH5
	US18 : Un signal de commande interrompu ou fourni pendant une longue période.		S-lH1 S-lH5	S-lH1 S-lH5
	US 19 : Le maître ne coordonne pas le mouvement entre les robots du 3ème niveau, ou la coordination est fournie trop tard.		S-lH3	S-lH3
Sélectionner la vitesse appropriée (accélérer, réduire la vitesse)	**US 20 :** Le contrôleur fournit une valeur de vitesse élevée aux robots sur un sol glissant (déversement de produits chimiques sur le sol).	S-lH1 S-lH2 S-lH3	S-lH1 S-lH2 S-lH3	S-lH1 S-lH2 S-lH3
	US 21 : Les robots se déplacent sans respect des contraintes de vitesse.	S-lH1 S-lH2 S-lH5	S-lH1 S-lH2 S-lH5	S-lH1 S-lH2 S-lH5
	US 22 : Accélération pour éviter un obstacle tandis qu'un autre robot apparaît soudainement sur la face arrière.	S-lH1	S-lH1	S-lH1
	US 23 : Fournit une commande de vitesse inattendue pour changer de direction tandis que d'autres robots sont derrière.	S-lH1	S-lH1	S-lH1
	US 24 : Le contrôleur maître ne fournit pas de commandes (pour réduire la vitesse lorsque cela est nécessaire) devant un obstacle statique ou dynamique.	S-lH1 S-lH2	S-lH1 S-lH2	S-lH1 S-lH2
	US 25 : Un choix incorrect de la valeur de vitesse fournie par le contrôleur pour les robots.	S-lH1 S-lH2	S-lH1 S-lH2	S-lH1 S-lH2
	US 26 : Un changement de valeur de vitesse fournie dans un timing incorrect (trop tard ou trop tôt) - augmentation ou diminution pendant le fonctionnement du robot.	S-lH1 S-lH2	S-lH1 S-lH2	S-lH1 S-lH2
Unité de traitement				
Traiter les informations du capteur	**US 27 :** L'unité de traitement fournit des informations erronées.	S-lH1 S-lH3	S-lH1 S-lH3	S-lH1 S-lH3
	US 28 : L'unité de traitement fournit des informations traitées trop tard.	S-lH1 S-lH3	S-lH1 S-lH3	S-lH1 S-lH3
Unité d'exécution				
Contrôler les roues (contrôleur d'actionneurs)	**US 29 :** Ne fournit pas la rotation aux roues (à une roue ou aux deux).	S-lH3 S-lH4	S-lH3 S-lH4	S-lH3 S-lH4

Unité de communication				
Fournir une communication	**US 30 :** Au sein du robot, la communication entre les sous-contrôleurs est absente (contrôleur de guidage et contrôleur d'évitement de collision), ou fournie trop tard.	S-lH3	S-lH3	S-lH3
	US 31 : La communication externe n'est pas assurée entre le maître et ses esclaves (communication interrompue).	S-lH4	S-lH4	S-lH4
	US 32 : Mauvaise communication externe entre le maître et ses esclaves.	S-lH3 S-lH4	S-lH3 S-lH4	S-lH3 S-lH4
	US 33 : Communication entre robots : si elle n'est pas fournie entre des groupes de robots de même niveau (pour détecter la position des autres robots).	N/A	N/A	S-lH1 S-lH3
	US 34 : Communication entre robots : si elle est fournie entre des groupes de robots de même niveau trop tard.			S-lH3

Tableau III.7 Tableau des facteurs causaux pour les scénarios de risque identifiés

Nombre de scénarios dangereux (US)	Facteurs causaux de danger		
	SC	**SH**	**SHM**
US1 **US2**	- Perte de concentration humaine, fatigue extrême…	- Identique au SC.	- Identique au SC.
US3 **US11** **US16**	- Données erronées des capteurs détectant la position (défaillance des capteurs de position, défaillance du capteur d'angle de braquage, réception des informations des capteurs avec retard, étalonnage des capteurs inadéquat, fusion des données inadéquate). - Défaillance des roues.	- Données erronées des capteurs détectant la position (défaillance des capteurs de position, défaillance du capteur d'angle de braquage, étalonnage des capteurs inadéquat, fusion des données inadéquate). - Défaillance des roues.	- Identique au SH.
US4 **US12**	- Aucune indication d'obstacles par les capteurs de distance (petits obstacles non observables par les capteurs, surfaces brillantes d'obstacles, imprécisions dans les mesures). - Défaillance du capteur de détection d'obstacles. - Calibrage inapproprié ou insuffisant des capteurs. - Défaillance des roues.	- Identique au SC.	- Identique au SC.

US5/ US8 **US13** **US17**	- Connexion défaillante. - Niveau de batterie faible. - Exécution lente des commandes en raison d'un grand nombre d'informations reçues en même temps. - Blocage du programme ou du logiciel. - Les retours d'information sont arrivés après un délai au contrôleur.	- Connexion défaillante. - Niveau de batterie faible. - Blocage du programme ou du logiciel.	- Identique au SH.
US6 **US14**	- Blocage du logiciel. - Défaillance des actionneurs (moteurs, roues). - Défaillance des contrôleurs d'actionneurs. - Défaillance du contrôleur maître. - Défaillance des composants de communication des robots esclaves (récepteur robot esclave). - Connexion défaillante. - Capacité limitée de la carte mémoire.	- Blocage du logiciel. - Défaillance des actionneurs (moteurs, roues). - Défaillance des contrôleurs d'actionneurs. - Défaillance des contrôleurs principaux. - Défaillance des composants de communication. - Connexion interrompue.	- Identique au SH.
US7 **US15**	- Défaillance du capteur de détection d'obstacles. - Indication erronée / inexistante des obstacles par les capteurs de distance (petits obstacles non observables par les capteurs, surfaces brillantes d'obstacles, imprécisions dans les mesures). - Programme ou algorithme de contrôle inadéquat ou incorrect (les exigences ne sont pas correctement définies dans le fichier programme). - Blocage du logiciel.	- Identique au SC.	- Identique au SC.
US9 **US18**	- Exécution lente des commandes en raison d'un grand nombre d'informations reçues en même temps. - Défaillance du capteur de détection d'obstacles. - Indication erronée / inexistante des obstacles par les capteurs de distance (petits obstacles non observables par les capteurs, surfaces brillantes	- Défaillance du capteur de détection d'obstacles. - Indication erronée / inexistante des obstacles par les capteurs de distance (petits obstacles non observables par les capteurs, surfaces brillantes d'obstacles, imprécisions dans les	- Identique au SH.

	d'obstacles, imprécisions dans les mesures). - Programme ou algorithme de contrôle inadéquat ou erroné (l'exigence n'est pas correctement définie dans le fichier programme). - Connexion erronée. - Blocage du logiciel.	mesures). - Programme ou algorithme de contrôle inadéquat ou incorrect (l'exigence n'est pas correctement définie dans le fichier programme). - Blocage du logiciel. - Connexion erronée.	
US10 **US19**	- Données erronées de capteurs (étalonnage inadéquat, défaillance des capteurs). - Blocage du logiciel.	- Identique au SC. - Pas de communication entre les groupes.	- Identique au SC. - Connexion erronée / Communication incorrecte entre les groupes de robots.
US20	- Déversement de produits chimiques ou d'eau sur le sol / problème d'hygiène.	- Identique au SC.	- Identique au SC.
US21	- Défaillance du capteur de vitesse.	- Identique au SC.	- Identique au SC.
US22 **US23**	- Algorithme de contrôle inadéquat ou incomplet (distance de sécurité entre robots insuffisante pour les urgences, problème de coordination). - Exécution lente des commandes en raison d'un grand nombre d'informations reçues en même temps.	- Algorithme de contrôle inadéquat ou incomplet (distance de sécurité entre robots insuffisante pour les urgences, problème de coordination). - Connexion lente.	- Identique au SH.
US24 **US25** **US26**	- Défaillance du capteur de vitesse. - Exécution lente des commandes en raison d'un grand nombre d'informations reçues en même temps. - Blocage du logiciel.	- Défaillance du capteur de vitesse. - Blocage du logiciel.	- Défaillance du capteur de vitesse. - Blocage du logiciel.
US27	- Données erronées des capteurs (défaillance des capteurs ou étalonnage inadéquat). - Données mal fusionnées.	- Identique au SC.	- Identique au SC.
US28	- Nombre important d'informations des capteurs fournies au robot maître. - Connexion erronée, exécution lente du logiciel.	- Connexion erronée. - Exécution lente du logiciel.	- Identique au SH.
US29	- Défaillance de moteurs, panne de contrôleur d'actionneurs, commande incorrecte, tension de batterie faible.	- Identique au SC.	- Identique au SC.
US30	- Algorithme de contrôle et de coordination inadéquat.	- Identique au SC.	- Identique au SC.

	- Défaillance de logiciel, capteurs.		
US31 **US32**	- Connexion interrompue / échouée. - Défaillance des composants de communication. - Blocage du logiciel.	- Identique au SC.	- Identique au SC.
US33 **US34**	Aucune communication fournie.	Aucune communication fournie.	- Perte de la connexion entre les robots ou connexion lente. - Défaillance des composants de connexion.

III.6.4.2 Évaluation des dangers à travers la méthode du nœud papillon

Le logiciel GRIF [123] a été utilisé afin de développer les différents modèles de nœuds papillon. Les nœuds papillon représentés sur les figures III.17, III.18 et III.19 incluent respectivement des scénarios prévus de risque dans le cas d'un contrôle incorrect. Nous identifions les causes pouvant entraîner des dangers et leurs effets. Le nœud du milieu de chaque nœud papillon représente le même événement indésirable, qui est la perte de contrôle du maître.

L'utilisation de la méthode du nœud papillon aide à :

- Visualiser les résultats de l'analyse STPA (les causes fréquentes de chaque architecture et les dangers) ;

- Fournir plus de détails sur les facteurs de causalité obtenus par analyse STPA ;

- Définir les barrières de sécurité existantes pour chaque architecture ;

- Enfin, évaluer les dangers à l'aide de la matrice de classification des risques en combinant la fréquence de l'événement indésirable obtenue à partir des fréquences des causes avec la gravité de chaque danger.

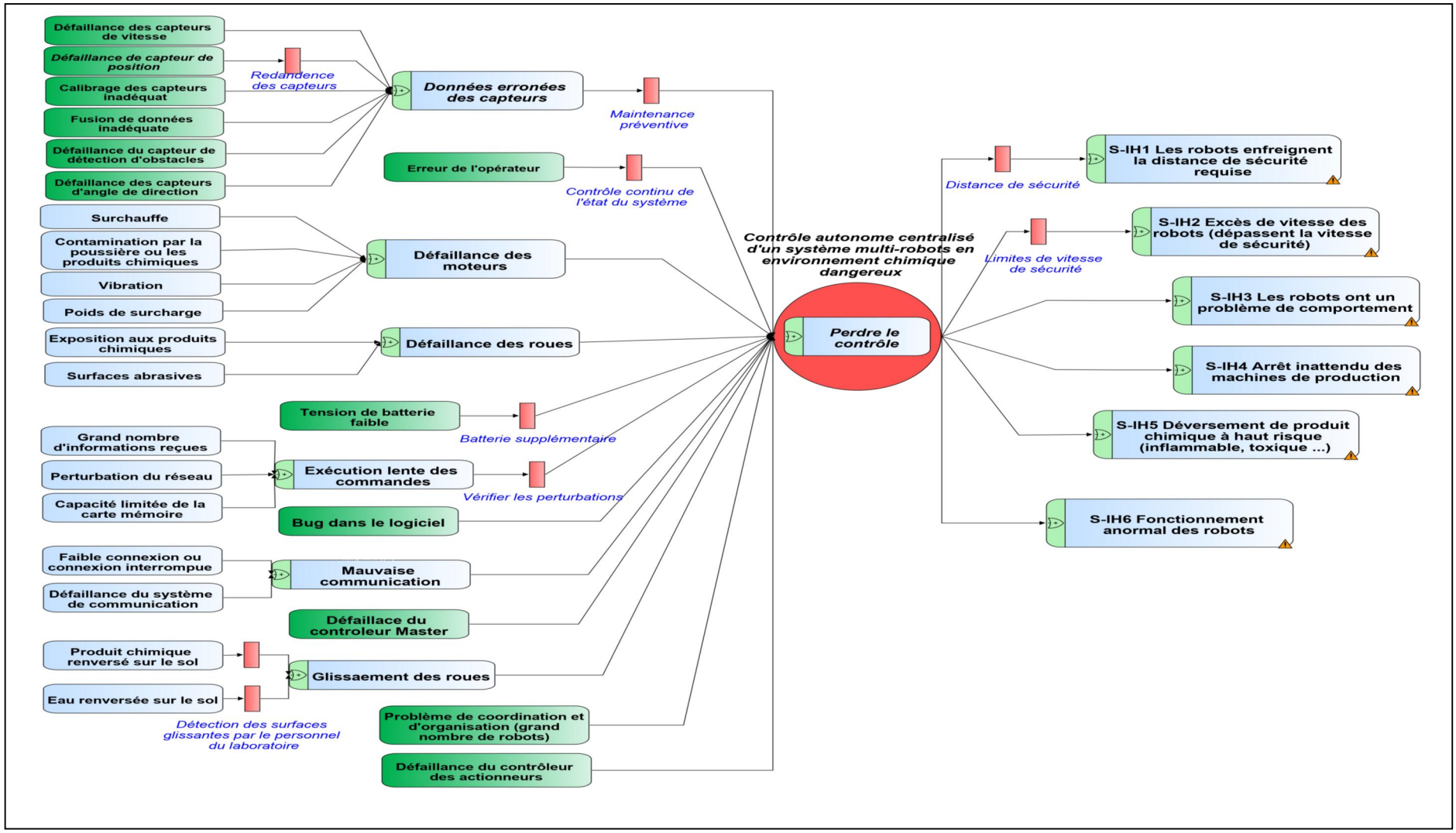


Figure III.17 Modèle nœud papillon pour l'approche de contrôle centralisé

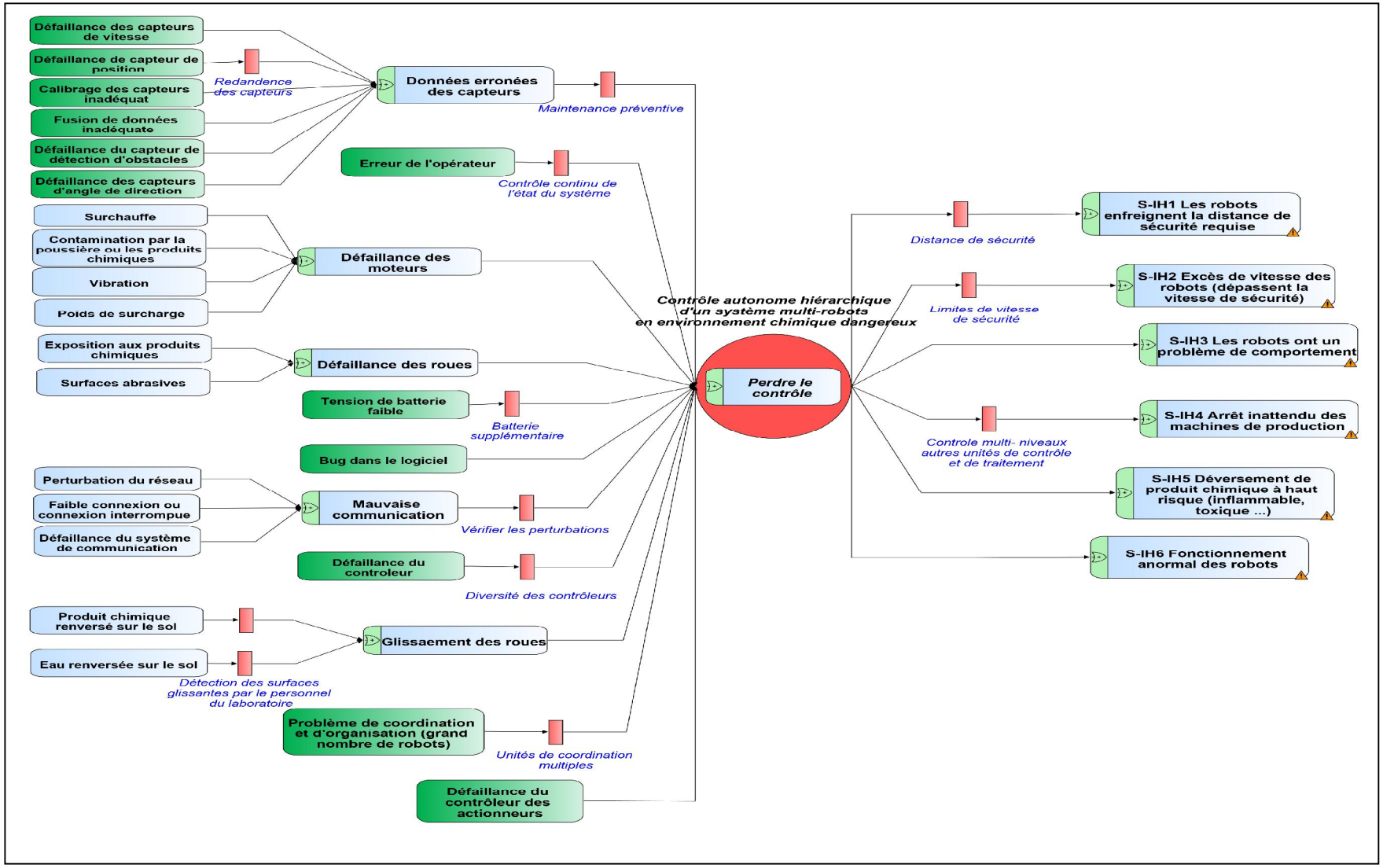


Figure III.18 Modèle nœud papillon pour l'approche de contrôle hiérarchique

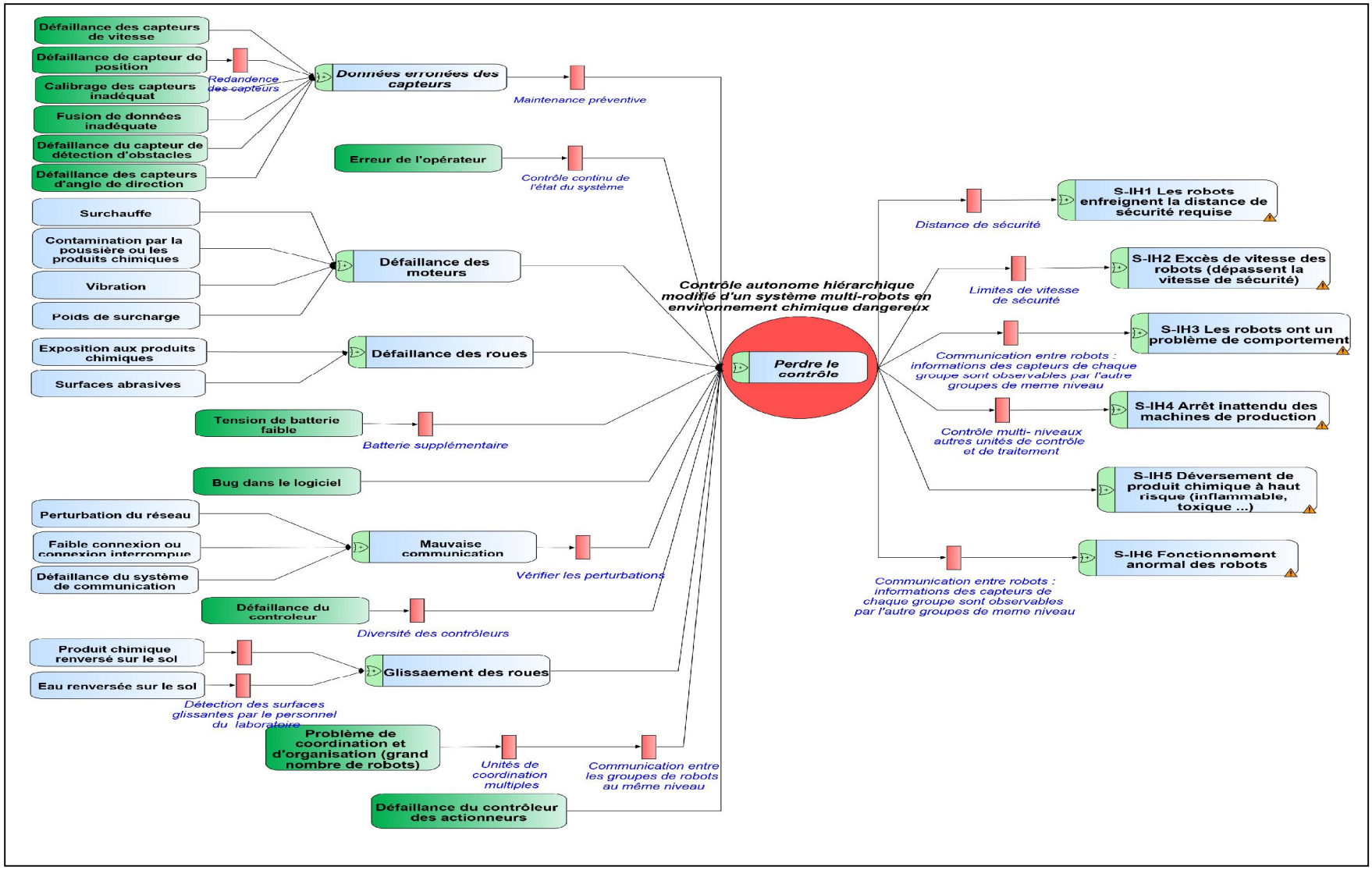


Figure III.19 Modèle nœud papillon pour l'approche de contrôle hiérarchique modifiée

III.6.4.3 Classification des scénarios de dangers

L'évaluation de la criticité est réalisée selon la matrice des risques que nous avons définie dans le logiciel GRIF. Ceci est réalisé par la combinaison de la fréquence des conséquences et de leur gravité. Les figures III.20, III.21 et III.22 montrent les matrices de classification des risques des trois types d'approches.

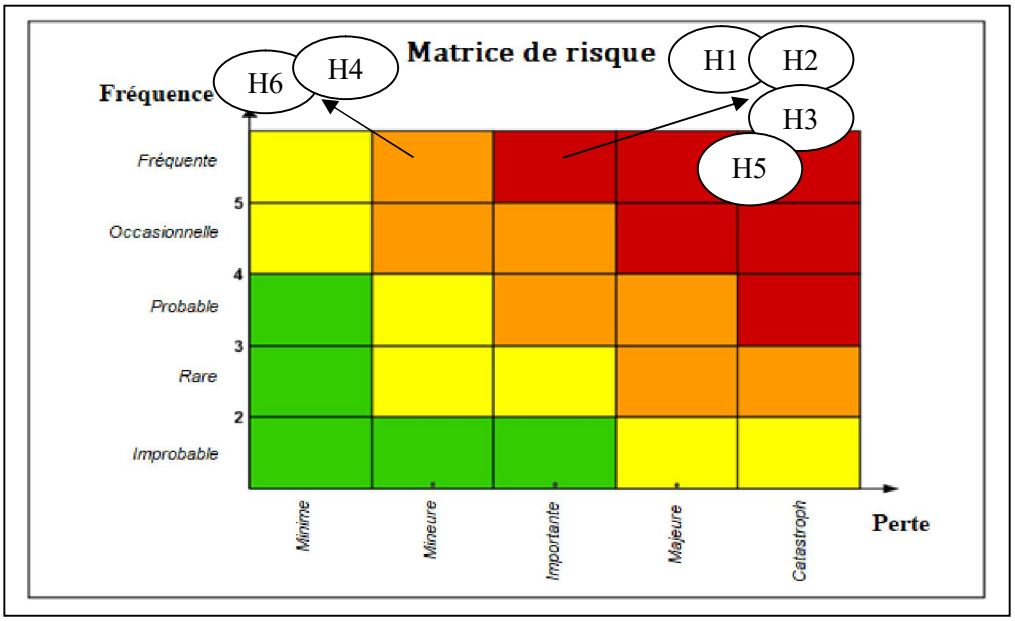


Figure III.20 Classification des risques pour une approche centralisée

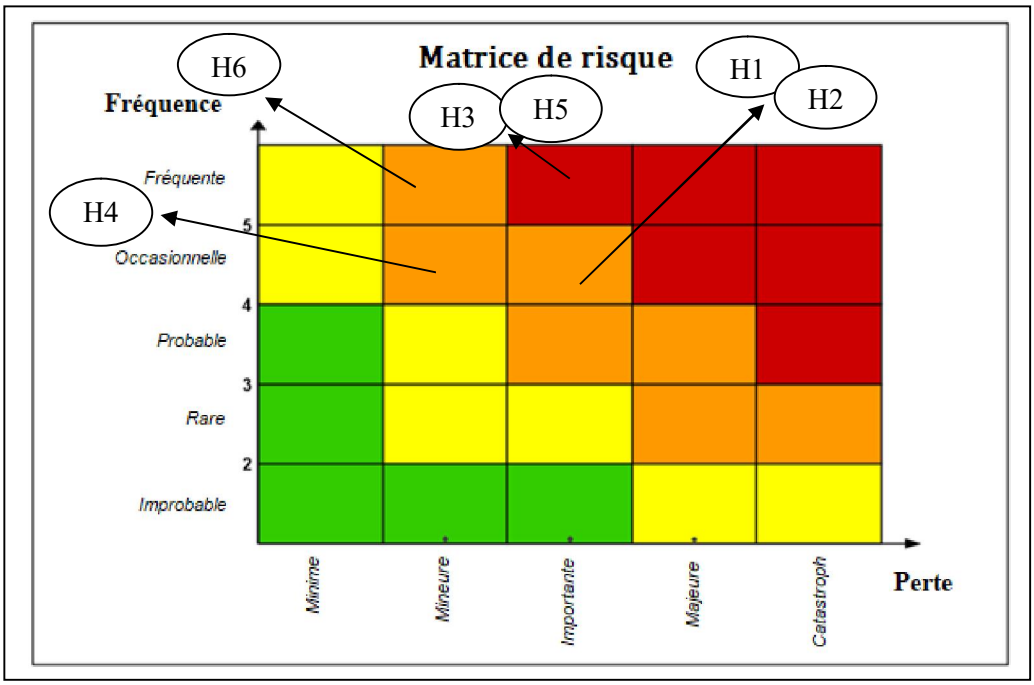


Figure III.21 Classification des risques pour une approche hiérarchique

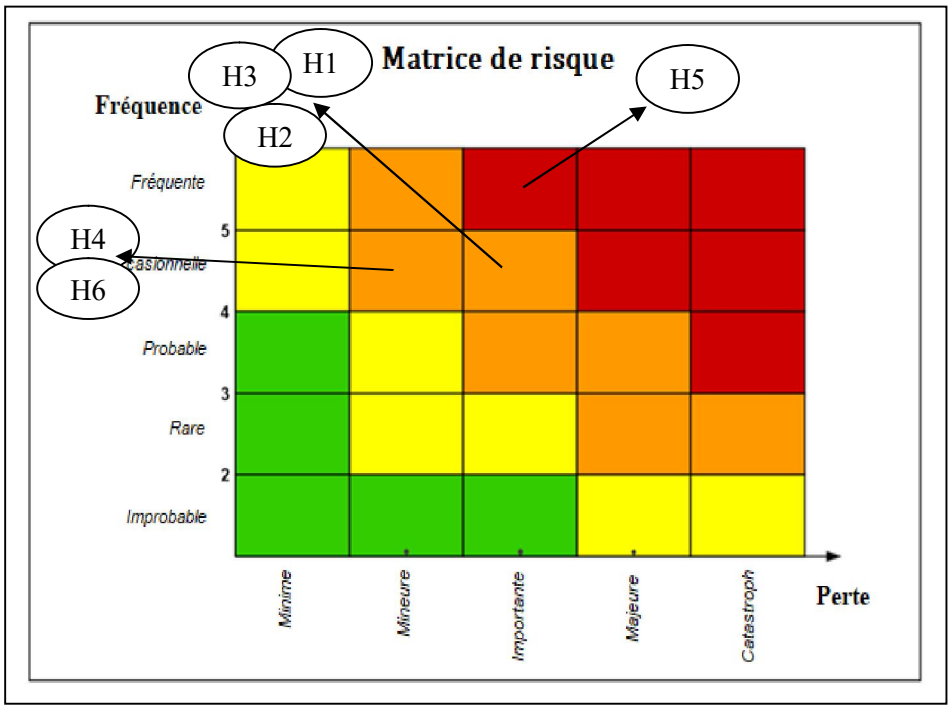


Figure III.22 Classification des risques pour une approche hiérarchique modifiée

Ces matrices de risques contiennent quatre catégories de risques, allant de l'impact le plus bas au plus élevé respectivement :

- Aucun impact là où le risque est acceptable (couleur verte).
- Incorporer des mesures de réduction des risques là où le risque est raisonnable (couleur jaune).
- Gérer pour une amélioration continue là où le risque est important (couleur orange).
- Et risque intolérable (couleur rouge).

Un effet classé dans le niveau de criticité inférieur présente un faible danger. Un effet classé dans un niveau de criticité plus élevé présente un danger élevé. À partir de l'évaluation par nœud papillon réalisée ci-dessus, quatre dangers ont atteint la colonne des risques intolérables pour le système organisé selon l'approche de contrôle centralisé. Pour le système organisé selon une structure hiérarchique modifiée, deux dangers ont atteint la zone rouge. Enfin, le système caractérisé par l'approche hiérarchique a vu un seul danger atteindre la zone intolérable. Le tableau III.8 récapitule les résultats obtenus à partir de la matrice de classification des risques.

Tableau III.8 Tableau récapitulatif des résultats obtenus à partir de la matrice de classification des risques

Type d'architecture	Classification des dangers au niveau du système
SC	(H1, H2, H3, H5) Zone de risque intolérable (gravité : très grave, fréquence : assez normale)
	(H4, H6) Zone de risque important (gravité : grave, fréquence : assez normale)
SH	(H3,H5) Zone de risque intolérable (gravité: très grave, fréquence : assez normale)
	(H1, H2) Zone de risque important (gravité : très grave, fréquence : occasionnelle) H4 Zone de risque important (gravité : grave, fréquence : occasionnelle) H6 Zone de risque important (gravité : grave, fréquence : assez normale)
SHM	H5 Zone de risque intolérable (gravité : très grave, fréquence : assez normale)
	(H1, H2, H3) Zone de risque important (gravité : très grave, fréquence : occasionnelle) (H4, H6) Zone de risque important (gravité : grave, fréquence : occasionnelle)

III.6.5 Discussion des résultats

Une comparaison des trois architectures a été réalisée (voir tableau III.8). Celle-ci se base sur les résultats obtenus à partir de l'évaluation des scénarios de risque résultant de la combinaison STPA / nœud papillon. Quelques remarques sont données ci-dessous :

- D'après le tableau III.9 ci-dessous, nous pouvons conclure que l'approche la plus critique est l'approche centralisée, suivie de l'approche hiérarchique.
- L'approche hiérarchique modifiée a surpassé les deux autres approches, en raison de deux propriétés principales : le contrôle multi-niveaux et la communication inter-robots au même niveau, afin que le maître puisse être libéré de l'énorme flux d'informations entrantes.

Tableau III.9 Comparaison des résultats obtenus par classification des risques

Types d'architecture	**SC**	**SH**	**SHM**
Classification des scénarios de danger obtenus par STPA	- 91 % scénarios atteignent un niveau de risque intolérable. - 9 % scénarios atteignent un niveau de risque important.	- 69 % scénarios atteignent un niveau de risque intolérable. - 31 % scénarios atteignent un niveau de risque important.	- 26 % scénarios atteignent un niveau de risque intolérable. - 74 % scénarios atteignent un niveau de risque important.

Après avoir appliqué les méthodes STPA et nœud papillon, nous pouvons réaliser les remarques suivantes :

Sur la base des résultats des analyses STPA / nœud papillon, l'approche hiérarchique modifiée est limitée à un nombre faible de contraintes, en comparaison aux autres structures étudiées. Par conséquent, elle peut être considérée comme étant l'approche la plus adaptée aux systèmes multi-robots.

La méthode du nœud papillon n'est pas très utile dans le cadre des approches de contrôle. Son principal apport consiste à améliorer l'analyse et à la rendre plus efficace. Elle donne une vue d'ensemble des scénarios de danger de chaque architecture et contribue à les évaluer et à faciliter notre comparaison.

L'avantage de l'analyse STPA repose sur l'évaluation des actions de contrôle entre contrôleurs. L'application de cette analyse fournit un large éventail de scénarios de danger et de facteurs de causalité, y compris les problèmes logiciels, environnementaux, humains et techniques. De plus, les scénarios obtenus à partir de l'analyse STPA sont plus détaillés que pour les autres méthodes conventionnelles. Enfin, elle donne plus d'importance à la partie « contrôle ». Il est ainsi envisageable de proposer des barrières au niveau de l'algorithme de contrôle (i.e. au niveau du logiciel).

Dans ce contexte, nous pouvons mettre en exergue certaines mesures préventives périodiques pour assurer une plus grande efficacité de la démarche de contrôle et réduire le niveau de risques :

- Le niveau de confiance de la partie « contrôle » et « fiabilité des composants » doit être garanti.
- Tous les programmes doivent être validés.

- Les intégrations logicielles et matérielles doivent être vérifiées.
- Aucune modification des programmes n'est autorisée sans accord préalable.
- Des capteurs doivent être ajoutés afin de détecter le glissement et différencier les êtres humains des autres robots (utilisation d'une caméra par exemple).
- Plusieurs contraintes de sécurité doivent être ajoutées au niveau de l'algorithme de contrôle/commande : distances de sécurité par rapport aux humains, par rapport aux robots et autres objets ; précision de suivi ; conditions de fonctionnement.

III.7 Approche 4 : Analyse détaillée de l'architecture de contrôle d'un système multi-robots à l'aide de l'analyse conjointe STPA et RdP

Dans cette section, l'analyse STPA consiste à analyser les différentes fonctionnalités des contrôleurs autonomes durant le déplacement d'un système multi-robots mobiles à l'aide d'une architecture de contrôle détaillée. L'analyse avec réseaux de Petri stochastiques RdPS, quant à elle, offre une modélisation et une évaluation du comportement fonctionnel du système et des scénarios de risques.

III.7.1 Étape 1 : Objectif de l'analyse

Cette étape consiste à définir les limites du système.

III.7.1.1 Identification des pertes

Sept types de pertes ont été identifiés et classés dans le tableau III.10 ci-dessous :

Tableau III.10 Classification des pertes selon leur gravité

L1	**Perte de vies humaines** (opérateurs et travailleurs), blessures, maladies, asphyxie, empoisonnement.
L2	**Environnement toxique ou pollué** (émission de gaz toxiques, poussières, émission de fumées de produits chimiques, fuite de produits chimiques...).
L3	**Perte ou endommagement des machines** d'analyses ou d'autres matériaux de laboratoire.
L4	**Perte de produits** chimiques (déversement de produits chimiques).
L5	**Perte de mission** (pas de transport de produits, pas d'analyse).
L6	**Perte ou endommagement des robots.**

L7	**Perte de réputation :** ce n'est peut-être pas la perte la plus importante, mais elle peut être une perte pertinente à conserver (le fonctionnement sûr de la robotique doit donner moins d'accidents, permettant une réputation accrue de l'entreprise qui se rend au laboratoire).

III.7.1.2 Identification des accidents, dangers et contraintes de sécurité du système

Les tableaux III.11 et III.12 ci-dessous identifient clairement les accidents, les dangers (Hazard en anglais) et les contraintes de haut niveau du système. Pour chaque danger, une contrainte doit être formulée.

Tableau III.11 Identification des accidents et des dangers potentiels

Accidents au niveau du système (S-lA)	Dangers au niveau du système (S-lH)
S-lA1 : Collision entre des robots chargés de produits chimiques (deux ou plus). **S-lA2** : Collision entre un robot (chargé de produits chimiques) et un travailleur humain. **S-lA3** : Collision entre robots (sans produit chimique). **S-lA4** : Collision entre robot et travailleur humain (sans produit chimique). **S-lA5** : Choc du robot contre le mur ou contre d'autres obstacles statiques (machines d'analyses) ou chute de celui-ci. **S-lA6** : Déversement de produits chimiques.	**S-lH1** : Les robots (chargés ou non de produits chimiques dangereux) entrent ensemble dans une zone étroite (les robots ne respectent pas la distance de sécurité entre eux ou avec les humains) (**L1 - L7**). **S-lH2** : Le robot (chargé ou non de produits chimiques dangereux) ne respecte pas la distance de sécurité par rapport aux autres obstacles statiques (**L2 - L7**). **S-lH3** : Le robot (chargé ou non de produits chimiques dangereux) ne respecte pas la vitesse de sécurité lors de sa navigation (**L1 - L7**). **S-lH4** : Le robot (chargé ou non de produits chimiques dangereux) pénètre dans une zone glissante (déversement de produits) (**L1 - L7**). **S-lH5**: Le robot (chargé ou non de produits chimiques dangereux) entre dans un état incontrôlé (**L1 - L7**).

Tableau III.12 Tableau présentant les contraintes de sécurité au niveau du système

S-lC	Contraintes au niveau du système (S-lC)
S-lC1	Les robots ne doivent pas entrer ensemble dans la même zone, surtout si la zone est étroite (le robot doit détecter l'entrée de la zone – cette entrée ne pourra se faire que un par un) **S-lH1.**
S-lC2	Les robots doivent respecter la distance de sécurité et ne violent pas la distance minimale de séparation – s'il y a violation, celle-ci doit être détectée pour éviter toute collision **S-lH2.**
S-lC3	Les robots ne doivent pas dépasser une certaine vitesse limite, notamment en cas de transport des produits et en cas de dépassement du robot, il faut alors l'arrêter **S-lH3.**
S-lC4	Doit maintenir une propreté permanente du sol et ne pas jeter de matériaux glissants sur le sol (contrainte de sécurité à **S-lH4** en dehors des limites de la commande du robot).
S-lC5	Les robots glissants doivent être détectés et si ce n'est pas le cas ils doivent ajuster leur vitesse et ralentir (contrainte de sécurité à **S-lH4** relative à la commande du robot).
S-lC6	Les paramètres de contrôle et les algorithmes des robots doivent être surveillés et s'il y a un problème dans le contrôle (ou indications de mauvais contrôle des robots) le robot doit être arrêté **S-lH5.**

III.7.2 Étape 2 : Développement de la structure de contrôle hiérarchique en utilisant STAMP

L'objectif de l'approche STAMP est d'accroître la compréhension de la structure de contrôle des systèmes et son processus. La structure montre clairement les interrelations et les interactions entre les différents composants du système multi-robots. L'ensemble des actions, des commandes et le retour d'état sont identifiés. Il est également important de décrire les perturbations environnementales qui peuvent affecter le système et son fonctionnement. La figure III.23 montre la structure détaillée de contrôle entièrement autonome d'un robot mobile à roues différentielles, dans laquelle l'opérateur démarre le processus et identifie la tâche du robot ou la cible. Le contrôleur du robot fusionne les données des capteurs, calcule les chemins possibles et choisit le chemin optimal pour sa mission. Il contrôle également le mouvement des roues.

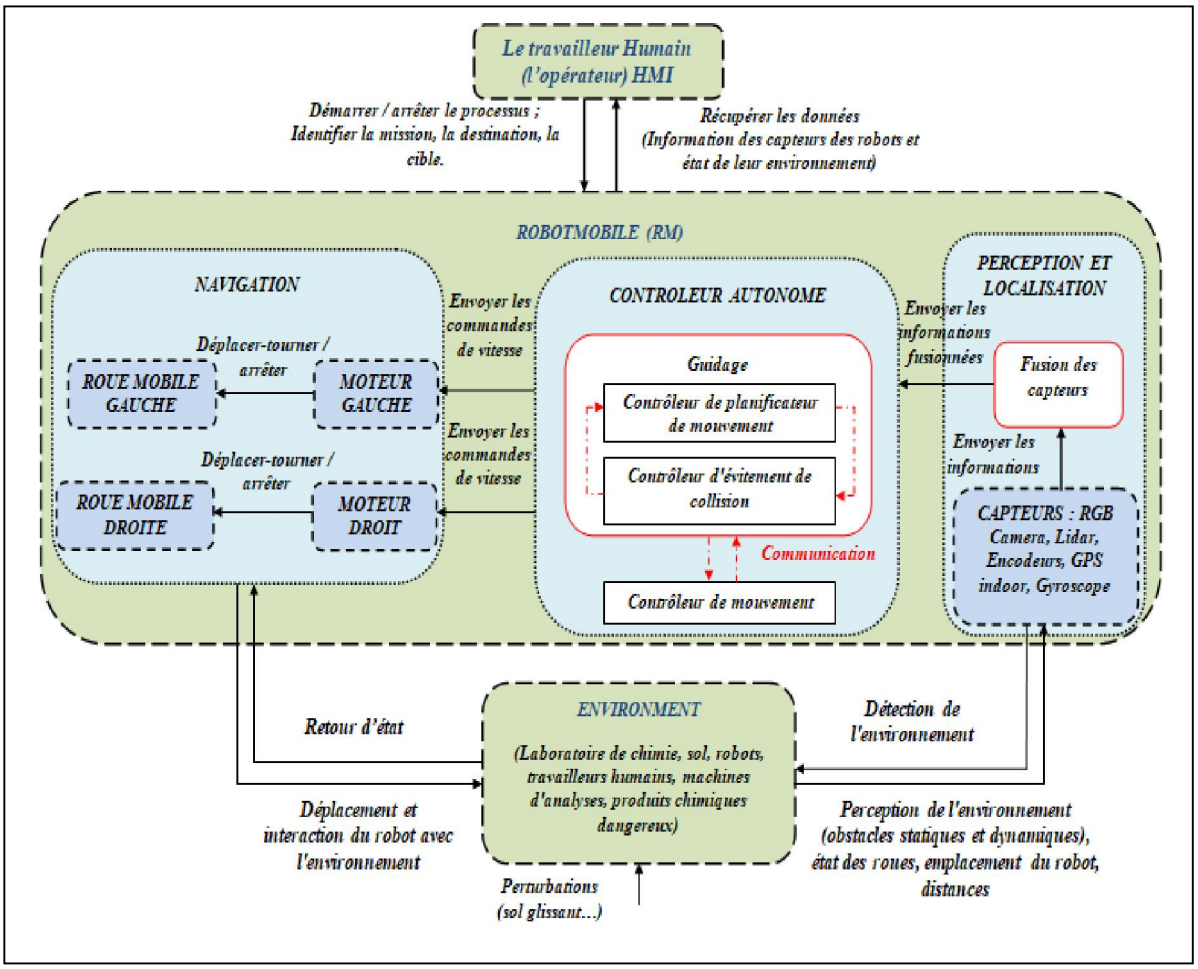


Figure III.23 Version détaillée de l'approche de contrôle d'un robot à deux roues différentielles

III.7.3 Étape 3 : Identification des actions de contrôle dangereuses et leurs facteurs de causalité

Le tableau III.13 présente l'ensemble des scénarios de dangers identifiés pour chaque fonctionnalité du contrôleur autonome des robots mobiles et ses facteurs causaux.

Tableau III.13 . Identification des scénarios de dangers pour chaque fonctionnalité du contrôleur

Action de contrôle / Communication	Mots-guides	Scenario (UCA)	S-lH	Facteurs causaux
Planifier et générer la trajectoire (depuis le contrôleur de planification de la trajectoire)	*Ne pas fournir (provoque un danger)*	**UCA1** : Le contrôleur ne calcule pas et ne génère pas le chemin.	**H5**	- Les unités de planification et de calculs ne remplissent pas leur fonction (défaillance des composants). - Informations insuffisantes pour prendre en charge le calcul (carte floue ou problème de capteurs). - Nombre élevé de calculs ou calcul bloqué en raison du grand nombre d'équations. - Saturation de la carte mémoire.
	Fournir (provoque un danger)	**UCA2** : Le contrôleur génère un chemin erroné, menant le robot à atteindre une destination erronée.	**H5**	- Informations de capteur insuffisantes. - Défaillance des capteurs. - Algorithme erroné. - Problème de programmation. - Ordre incorrect de l'opérateur.
		UCA3 : Le contrôleur génère une trajectoire longue mal optimisée de la position actuelle à la destination désirée.	**H5**	- Problème dans l'algorithme d'optimisation, approche inefficace, critères d'optimisation inappropriés.
		UCA4 : Le contrôleur ne met pas à jour la trajectoire dans un environnement dynamique.	**H1**	- Données de capteurs répétées. - Défaillance du contrôleur, des capteurs. - Algorithme inadéquat.
	Trop tôt, trop tard, hors service	**UCA5** : Trop de temps pour calculer et générer des trajectoires.	**H1, H2, H5**	- Trop de calculs intensifs. - Blocage de contrôleur. - Retard dans la transmission des informations capteurs. - Problèmes de fusion de données. - Blocage/arrêt intempestif du logiciel ou du calcul.

	Arrêté trop tôt, appliqué trop longtemps	**UCA6** : La planification de la trajectoire s'est arrêtée trop tôt.	**H1, H2, H5**	- Coupure instantanée des données. - Déchargement de la batterie.
Éviter les collisions (depuis le contrôleur d'évitement de collision)	*Ne pas fournir (provoque un danger)*	**UCA7** : La fonction d'évitement de collision n'est pas fournie pendant la navigation du robot.	**H1, H2, H4, H5**	- Défaillance des capteurs (n'indique pas s'il y a un obstacle). - Échec du contrôleur d'évitement de collision. - Algorithme de contrôle inadéquat (concernant les fonctionnalités). - Aucune dépendance entre les sous-contrôleurs.
	Fournir (provoque un danger)	**UCA8** : Emission de commandes incorrectes pour éviter la collision (accélérer/ralentir, arrêter, tourner à gauche, tourner à droite).	**H1, H2, H5**	- Étalonnage inadéquat des capteurs / fusion des données. - Données de capteurs ou données de communication erronées.
	Trop tôt, trop tard, hors service	**UCA9** : La fonction d'évitement d'obstacle est fournie trop tard (obstacle statique, autres robots ou humain).	**H1, H2**	- Retard des informations de capteurs. - Données manquantes des capteurs. - Manque de données lors de la communication (trop tard ou trop tôt). - Dépendance lâche entre les contrôleurs.
	Arrêté trop tôt, appliqué trop longtemps	**UCA10** : La fonction d'évitement de collision s'est arrêtée trop tôt pendant la navigation du robot.	**H1, H2, H5**	- Algorithme d'évitement des collisions inadéquat (non robuste). - Défaillance du contrôleur, défaillance du capteur détectant la distance entre les obstacles et le robot. - Calibrage inadéquat des capteurs.
	Ne pas fournir (provoque un danger)	**UCA11** : Ne fournit pas la dépendance entre les sous-contrôleurs (contrôleur de suivi de chemin ou de planification de chemin et contrôleur d'évitement de collision…).	**H1, H2, H5**	- Pas de données du capteur détectant les obstacles (panne des capteurs) ou données insuffisantes. - Algorithme de contrôle inadéquat.

Établir et maintenir la dépendance entre les sous-contrôleurs (logiciel)				- Défaillance du logiciel. -Echec du nœud connectant les sous-contrôleurs.
	Trop tôt, trop tard, hors service	**UCA12** : Fournit la dépendance trop tard.	**H1, H2, H5**	- Données des capteurs trop tard. - Trop de temps pour réaliser la fusion des données. - Bug logiciel.
	Arrêté trop tôt	**UCA13** : Perte de la dépendance entre les sous-contrôleurs.	**H1, H2, H5**	- Blocage du logiciel. - Corruption de programme. - Échec du nœud connectant les contrôleurs / ou perte du nœud. - Perte de la connexion avec le maître.
Établir et maintenir la communication entre robots	*Ne pas fournir (provoque un danger)*	**UCA14** : Ne fournit pas de communication entre les robots.	**H1**	- Pas de connexion entre les robots. - Défaillance des composants de communication.
	Fournir (provoque un danger)	**UCA15** : Fournit des informations insuffisantes. **UCA16** : Fournit beaucoup d'informations, même inutiles.	**H1, H5**	- Problèmes de cyber-sécurité.
	Trop tôt, trop tard, hors service	**UCA17** : Communication avec retard (trop tard).	**H1**	- Faible flux de réseau. - Flux important de données. - Perte de l'alimentation électrique.
	Arrêté trop tôt, appliqué trop longtemps	**UCA18** : Perte de la communication entre les robots.	**H1**	- Blocage du logiciel de communication. - Défaillance des composants de communication. - Informations reçues supérieures à la capacité du processeur. - Faible flux de réseau.
		UCA19 : La communication s'est arrêtée trop tôt.	**H1**	- Interruption du réseau.
	Ne pas fournir *(provoque un*	**UCA20** : Le contrôleur ne permet pas de suivre le chemin.	**H2, H5**	- Algorithme de contrôle de suivi de chemin inadéquat. - Défaillance d'un contrôleur de mouvement. - Défaillance des capteurs de

Suivre la trajectoire **(depuis le contrôleur de suivi de chemin)**	*danger)*			position. - Fusion de capteurs insuffisante. - Étalonnage inadéquat des capteurs. - Défaillance des actionneurs (blocage des roues).
	Fournir (provoque un danger)	**UCA21** : Suivi du chemin sans précision.	**H5**	- Algorithme de contrôle de suivi inadéquat. - Défaillance des capteurs, actionneurs. - Étalonnage inadéquat des capteurs. - Données de capteurs avec retard. - Fusion de données inadéquate.
	Arrêté trop tôt, appliqué trop longtemps	**UCA22** : Arrêt du suivi de chemin trop tôt (interruption).	**H5**	- Interruption des informations des capteurs. - Pas d'alimentation (panne de batterie ou décharge). - Défaillance des contrôleurs, capteurs ou actionneurs.
Envoyer la commande de vitesse aux roues **(depuis le contrôleur de mouvement après agrégation de l'ensemble des fonctionnalités)**	*Ne pas fournir (provoque un danger)*	**UCA23** : La commande de vitesse n'est pas fournie aux roues lorsque le robot est proche d'un obstacle dynamique (humain, autres robots).	**H1**	- Problème dans le bloc de communication (éditeur de commandes). - Algorithme d'agrégation inadéquat (problème de décision). - Défaillances des composants du contrôleur principal. - Défaillance du logiciel (des contrôleurs et capteurs). - Les informations des capteurs ne sont pas reçues par le contrôleur (problème dans les blocs d'abonnés). - Informations des capteurs mal fusionnées. - Défaillance des capteurs. - Défaillance du contrôleur des actionneurs (aucun signal fourni aux roues).

		UCA24 : Le contrôleur ne fournit pas la commande de vitesse à la roue droite / gauche pendant la navigation du robot.	**H5**	- Informations inadéquates sur les capteurs. - Défaillance du contrôleur des actionneurs (aucun signal fourni à la roue).
	Fournir (provoque un danger)	**UCA25** : Le contrôleur fournit une grande vitesse dans des situations inappropriées (robot transportant des produits chimiques, sol glissant, fumée, travail humain avec des robots dans la même pièce ...).	**H3, H4**	- Algorithme de contrôle inadéquat (le contrôleur ne s'adapte pas à ces situations). - Les capteurs ne détectent pas le glissement / la charge. - Calibrage inadéquat des capteurs. -Manque de capteurs.
		UCA26 : Le contrôleur fournit la même valeur de vitesse même si le robot est devant un obstacle.	**H1, H2, H3**	- Indication de capteurs manquante / ou fusion incorrecte - Blocage du logiciel / contrôleur
	Trop tôt, trop tard, hors service	**UCA27** : Envoie de la commande trop tard après un délai.	**H1, H2, H5**	-Envoyer les informations des capteurs trop tard (retard). - Problème du logiciel du contrôleur. - Saturation mémoire.
	Arrêté trop tôt, appliqué trop longtemps	**UCA28** : La commande d'envoi s'est arrêtée trop tôt.	**H1, H2**	- Défaillance du contrôleur principal / contrôleur des actionneurs, capteurs. - Informations de capteurs inadéquates (ne met pas à jour les informations sur l'environnement). - Perte de communication avec le maître.
		UCA 29 : La même valeur de commande est appliquée trop longtemps, y compris dans de nouvelles situations.	**H1, H2, H3**	- Défaillance des capteurs. - Informations inadéquates des capteurs. Le capteur indique le même état d'environnement (il ne met pas à jour les nouvelles données sur l'environnement).

III.7.4 Étape 4 : Génération des contraintes de sécurité et des exigences de sécurité importantes

Les contraintes de sécurité pour chaque action de contrôle non-sécurisée avec une exigence particulière sont présentées dans le tableau III.14. Son objectif est d'améliorer la partie « contrôle/commande » de chaque robot.

Tableau III.14 Tableau des contraintes et des exigences de sécurité

Action de contrôle / communication	UCA	Contraintes de sécurité	Exigences de sécurité suggérées
Planifier et générer la trajectoire	UCA1 / UCA3	Le contrôleur doit calculer et générer le chemin correct et optimisé.	Le contrôleur doit choisir la trajectoire sûre prenant le moins de temps et nécessitant de choisir le bon critère d'optimisation.
	UCA4	La planification doit toujours être adaptée aux changements d'environnement.	Le chemin doit être mis à jour après chaque action du robot, où il est nécessaire de réaliser la combinaison avec le contrôleur d'évitement d'obstacles.
	UCA5	Le contrôleur ne doit pas dépasser le temps de calcul spécifié par le programmeur.	Si le contrôleur dépasse un certain temps prédéfini lors de la planification, il est nécessaire d'arrêter manuellement le fonctionnement du contrôleur.
Éviter les collisions (depuis le contrôleur d'évitement de collision)	UCA7	Le contrôleur ne doit pas laisser le robot entrer en contact avec d'autres obstacles dynamiques ou statiques (objets, humains, robots) pendant sa navigation.	Le robot doit respecter une distance minimale suffisante n'est pas inférieur à 0.5 m (qui ne doivent pas être violées sous aucune condition) entre les robots et tout autre obstacle pendant sa navigation – ceci afin d'éviter tout contact.
	UCA8	Le contrôleur ne doit pas spécifier une commande incorrecte pour éviter la collision.	Le contrôleur doit vérifier toutes les directions autour du robot avant de spécifier la commande correcte d'évitement.
	UCA9	Le contrôleur d'évitement de collision ne doit pas laisser le robot entrer en contact avec des obstacles statiques ou dynamiques, en particulier lorsque le robot transporte un produit / un humain.	Le robot doit respecter les distances de sécurité spécifiées entre les autres obstacles statiques ou dynamiques pour éviter toute collision et il doit y avoir trois couches de distances de sécurité (zones) entourant le robot s'il y a un obstacle détecté sur la troisième. Le contrôleur commence à réduire

			la vitesse du robot et s'il n'est pas détecté jusqu'à la première zone, le contrôleur doit immédiatement arrêter le mouvement.
	UCA10	La fonction d'évitement de collision doit fonctionner tout le temps de navigation.	Un capteur de contact doit être en état de fonctionnement pour arrêter le robot, dans le cas d'un contact ou d'une collision.
Établir et maintenir la communication entre robots	UCA14	Les robots doivent communiquer et négocier entre eux avant de réaliser l'action.	Les tâches, mouvements et actions des robots doivent être organisés en assurant un échange continu d'informations inter-robots à l'aide de messages pour éviter les enchevêtrements et les actions indésirables et afin d'assurer une coopération efficace.
	UCA15 / UCA16	Il convient de préciser les informations suffisantes fournies par la communication.	Il faut préciser le type d'informations à échanger (positions des robots, vitesses, type de tâches, locaux occupés ou vides).
	UCA17	La communication doit être maintenue.	Il est nécessaire d'utiliser un logiciel multicouche comme ROS prenant en charge un grand nombre d'informations, et facilitant leur transmission. S'il y a une perte de connexion entre les nœuds, il est nécessaire d'en informer le maître.
Suivre la trajectoire	UCA20 / UCA23	Les robots ne doivent pas s'écarter du chemin spécifié pendant leur navigation.	Le contrôleur détecte tout écart par rapport au chemin spécifié à l'aide d'un système multi-capteurs caractérisant la position du robot (odomètre, télémètre laser…).
	UCA21	La précision doit être prise en compte dans la fonction de suivi.	- Utilisation de la redondance des capteurs (système multi-capteurs) pour minimiser le risque de panne. - Il est nécessaire de choisir le bon filtre pour les informations des capteurs afin d'augmenter la précision du suivi. - Le risque de défaut du capteur doit être minimisé par l'utilisation d'une approche tolérante aux fautes.

			- Un estimateur doit être utilisé pour minimiser le risque de non-observabilité.
Envoyer la commande de vitesse	UCA 23, 24, 25, 26, 27, 28, 29	La vitesse envoyée au robot doit être choisie correctement en fonction de la situation, tout en respectant les limites identifiées.	- Le programmeur doit spécifier des distances de sécurité à plusieurs niveaux : SD 1 pour les humains / SD 2 pour les robots / SD 3 pour les autres objets. - Détection des zones glissantes (en utilisant une caméra) ou réduction de la vitesse du robot. - Détection de la charge à l'aide d'un capteur de poids. - Décélération du robot lorsqu'il transporte des produits ou devant des humains ou d'autres robots.

III.7.5 Étape 5 : Intégration du RdP stochastique à l'analyse STPA

Cette section présente une intégration du réseau de Petri stochastique RdPS pour la modélisation et l'évaluation des scénarios de collision à partir du scénario de fonctionnement normal de deux robots.

III.7.5.1 Modélisation du fonctionnement normal des robots avec RdPS

Les figures III.24, III.25, III.26, III.27, III.28, III.29 illustrent un modèle représenté par RdPS, modélisé à l'aide du logiciel GRIF [123]. Ce modèle décrit le scenario de fonctionnement normal de deux robots (R1 et R2) dans un laboratoire d'analyses. Le laboratoire est composé d'une salle d'analyses, de deux salles de stockages de produits chimiques, d'une salle de chargement de batteries… (voir figure 2).

La partie 1, illustée par la figure III.24, présente la phase d'envoi des commandes et de préparation des robots pour une opération. Les deux robots représentés par deux places (P2 et P3), les deux marquages indiquent que les robots sont prêts, et qu'ils attendent la commande délivrée par la personne dans la salle d'analyse (Pa free) pour se déplacer. Les transitions 'demandes_S1' et 'demandes_S2' représentent les demandes de produits de la salle de stockage 1 (room1) et de la salle de stockage 2 (room 2) respectivement. La commande est réalisée selon les besoins des analyses (toutes les 4 heures, une demande est lancée pour chaque salle). Une liste est mise en place pour les demandes de produits pour la salle de stockage 1 et une autre pour la salle de stockage 2. Les places P5, P6 indiquent le nombre de demandes !D1 ,!D2 respectivement. Une demande étant lancée, la commande

est envoyée aux robots en fonction de la disponibilité de chaqu'un des deux robots (!Robot 1 = vrai ou !Robot 2 = vrai). Si les deux robots sont disponibles, une priorité est donnée au robot 1. Deux compteurs sont prévus afin de compter le nombre de cycles par robot (Nc1 = Nc1 + 1 et Nc2 = Nc2 + 1). S'il n'y a pas de robot dans la salle 1, la valeur de la variable room1 est fausse (!Room1 = false). Si l'un des robots entre dans la salle 1(resp. salle 2), la variable room 1 (resp. room 2), retourne la valeur« vrai ».

Pour identifier le robot entrant dans une salle, 4 variables sont définies comme suit :

- (!R11 = vrai) si le robot 1 se dirige vers la salle 1 ;
- (!R21 = vrai) si le robot 2 se dirige vers la salle 1 ;
- (!R22 = vrai) si le robot 2 se dirige vers la salle 2 ;
- (!R12 = vrai) si le robot 1 se dirige vers la salle 2.

Les parties 2 et 3, illustrées par les figures III.25 et III.26, présentent la phase de déplacement des robots pour le transport des produits. Les robots se déplacent de la salle d'analyses aux salles de stockage 1 et 2 respectivement. Les personnes des salles 1 et 2 (P1 et P2 respectivement) déposent les produits sur les robots. Une fois que les robots sortent de la salle 1 ou de la salle 2, les variables room1 ou room2 retournent à leurs états libres (! room 1= false, ! room 2= false), indiquant qu'il n'y a pas de robot dans les salles. Les robots reviennent à la salle d'analyses avec les produits. Les transitions (Tr7, Tr8, Tr9, Tr10, Tr11, Tr12, Tr13, Tr14) sont définient par une loi de dirac à délais déterministes, qui représentent les périodes de déplacement des deux robots.

Dans les parties 4 et 5, illustrées par les figures III.27 et III.28, une reconnaissance des robots (les deux robots sont définis par deux jetons) est effectuée pour les identifier et chaque robot peut retourner à sa place initiale. Si les robots réalisent un nombre de tours (Nc) supérieurs à Ncmax, alors ceux-ci partent à la salle de chargement de batterie avant d'être à nouveau disponibles et le compteur Nc retourne à la valeur 0.

Finalement, la partie 6, illustrée par la figure III.29, représente la phase de préparation des machines par la personne qui se trouve dans la salle d'analyses (Pa) pour effectuer celle-ci.

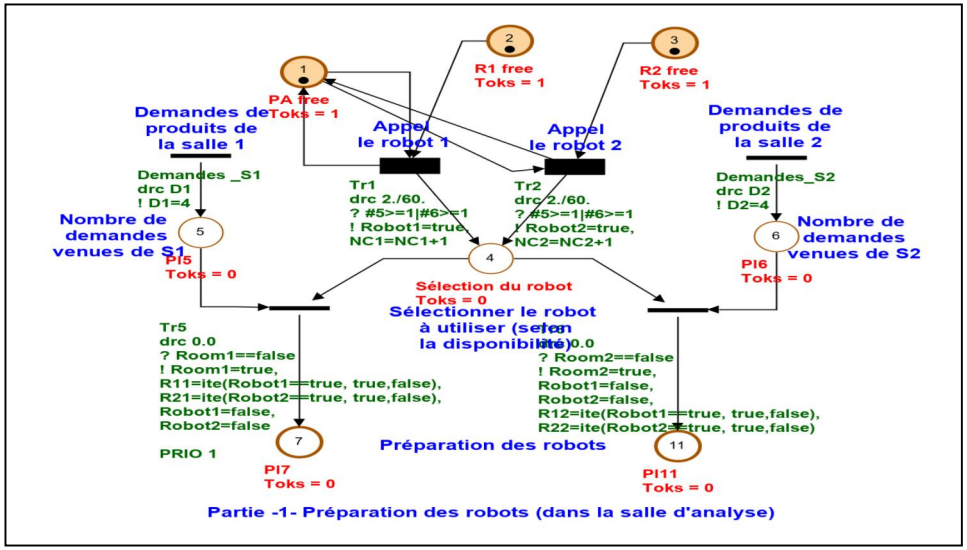


Figure III.24 Phase de préparation des robots

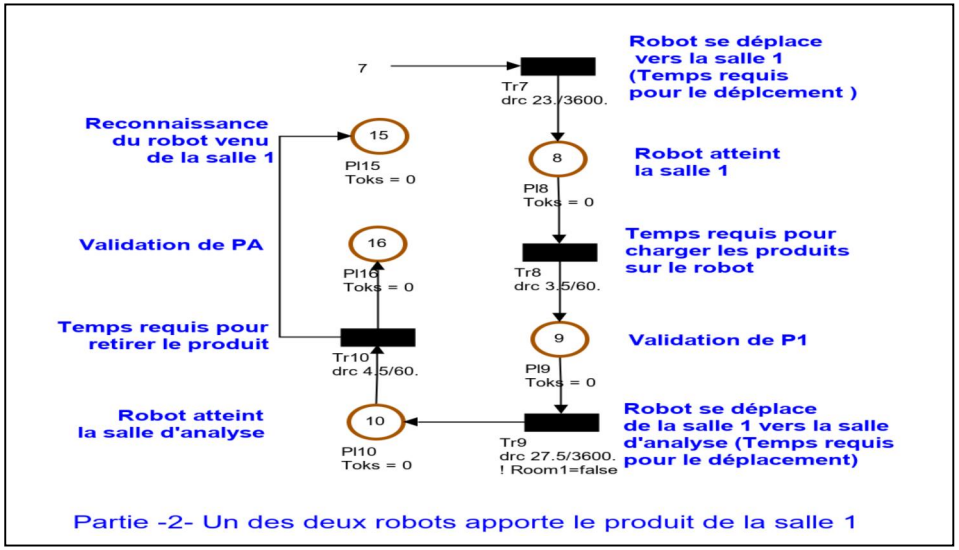


Figure III.25 Apport des produits de la salle 1

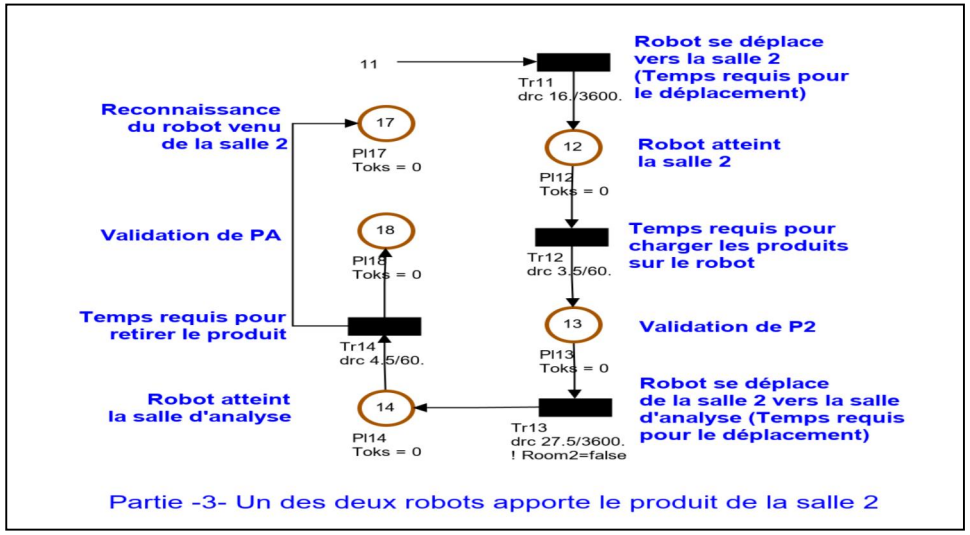


Figure III.26 Apport des produits de la salle 2

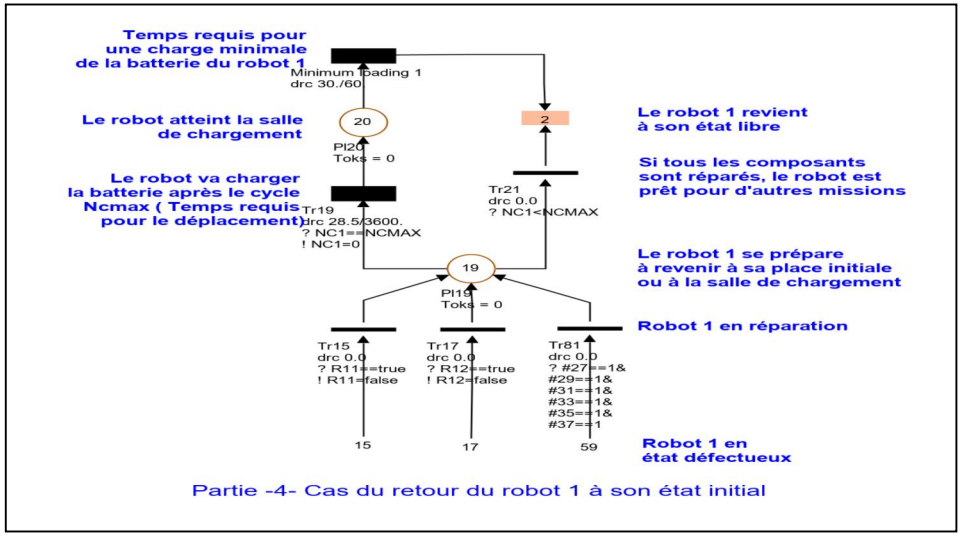


Figure III.27 Fin de tâche du robot 1

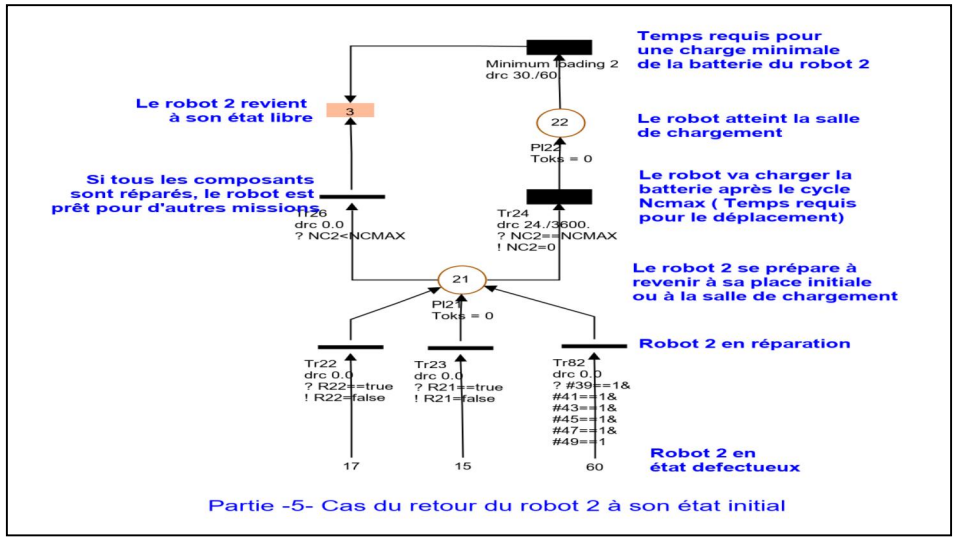


Figure III.28 Fin de tâche du robot 2

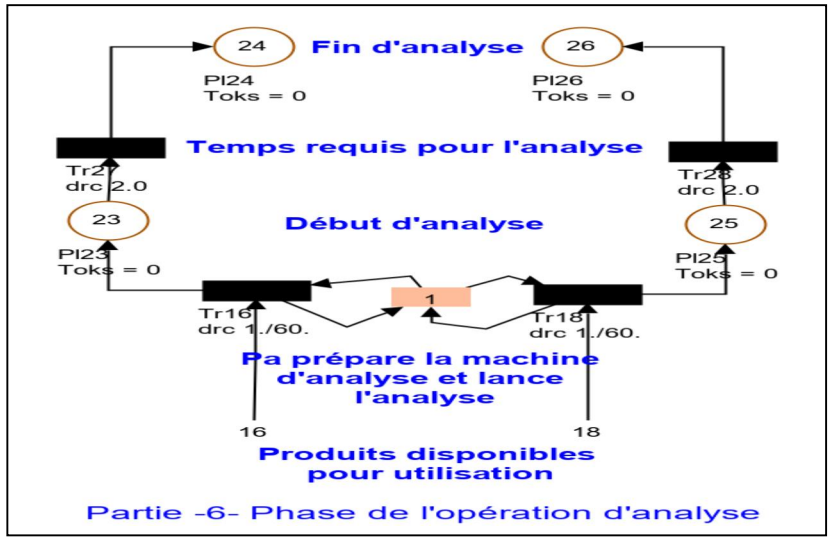


Figure III.29 Analyses

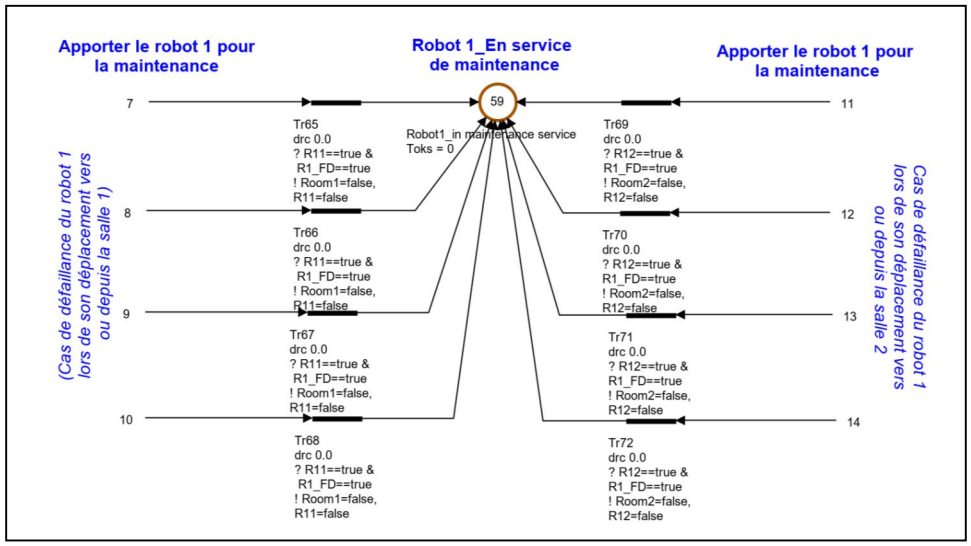


Figure III.30 Apport du robot 1 à la maintenance

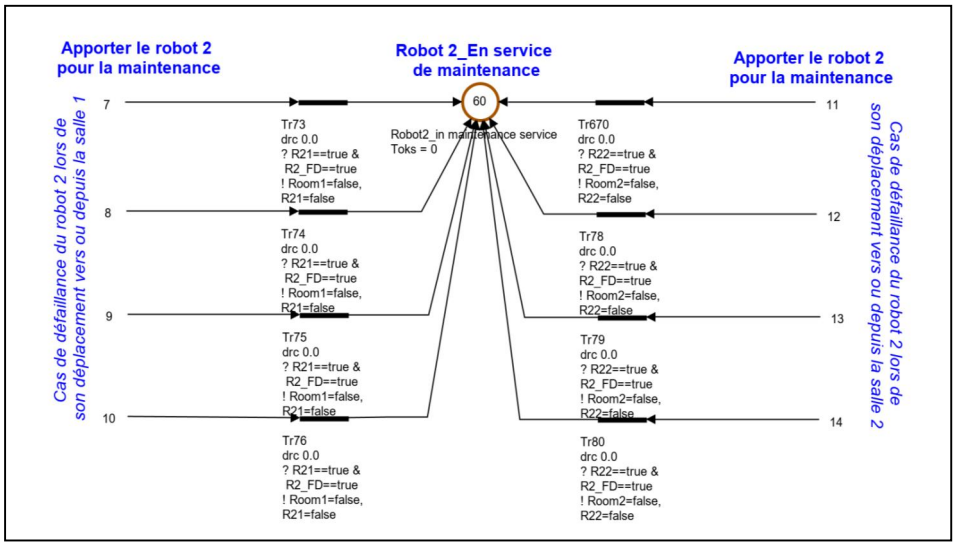


Figure III.31 Apport du robot 2 à la maintenance

III.7.5.2 Modélisation des scénarios de collision

La figure III.32 illustre le modèle RdPS pour les principaux scénarios de perte qui conduisent à un état de collision. Nous avons identifié les six causes principales à partir des résultats obtenus par la méthode STPA : défaillance du moteur de la roue gauche ou celui de la roue droite, défaillance du capteur scanner laser, défaillance du système de communication, défaillance de la carte de contrôle et problème de batterie. Notons que la défaillance des deux moteurs de chaque robot peut se produire indépendamment ou être causée par un événement de défaillance de cause commune (DCC). Nous avons intégré le modèle RdPS à la méthode STPA pour qu'on puisse évaluer la fréquence de collision selon les caractéristiques déterminées par notre système (i.e. laboratoire d'analyses robotisé).

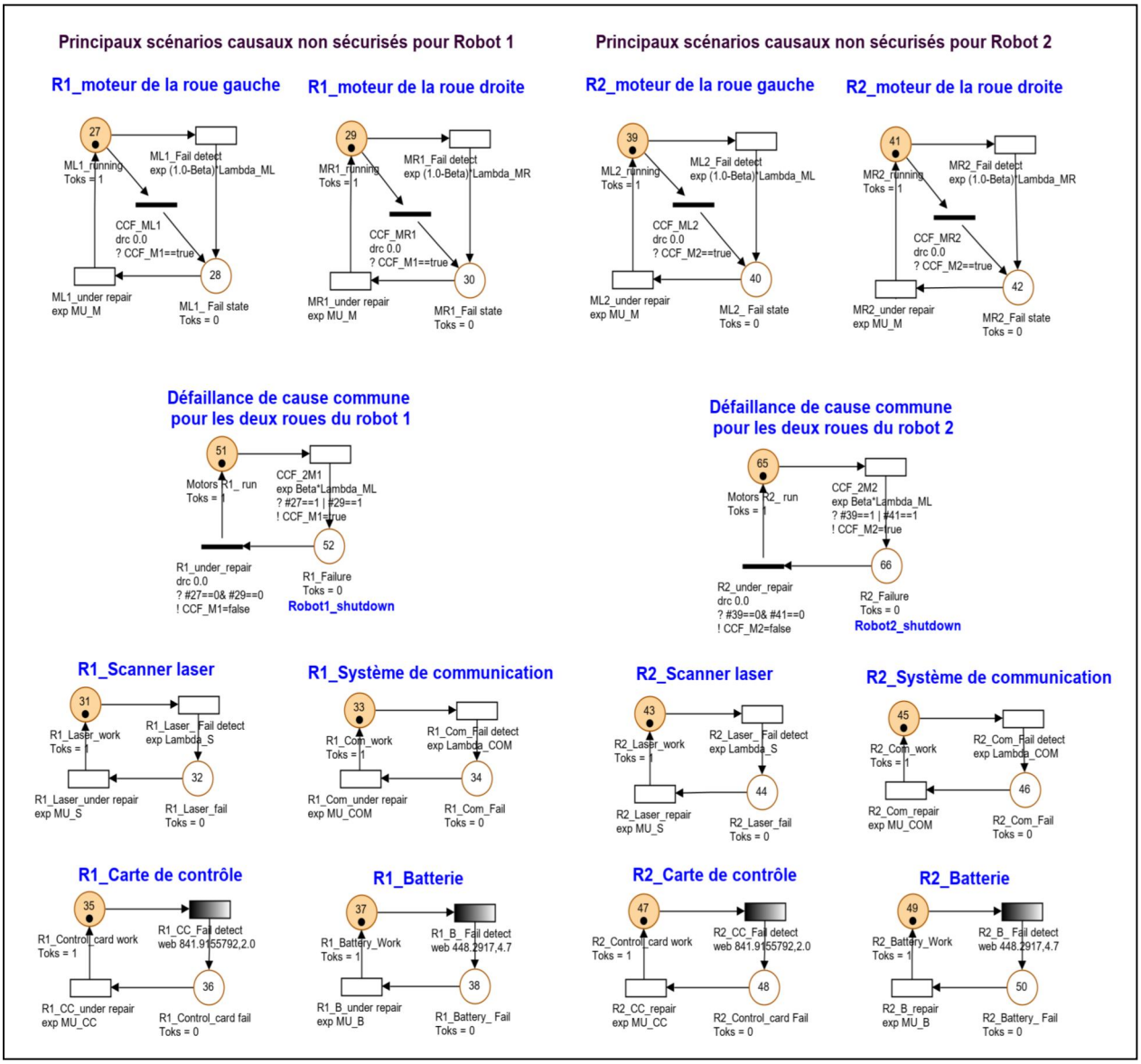


Figure III.32 Principaux scénarios causaux de collision pour les deux robots

Les jetons restent initialement aux places (P27, P29, P31, P33, P35, P37) pour le robot 1, et aux places (P39, P41, P43, P45, P47, P51) pour le robot 2, indiquant le bon fonctionnement des robots et tous leurs composants (jetons en P55 et P57 indiquant l'état sécurisé des deux robots, ce qui signifie qu'il n'y a pas de collision, voir la figure III.33).

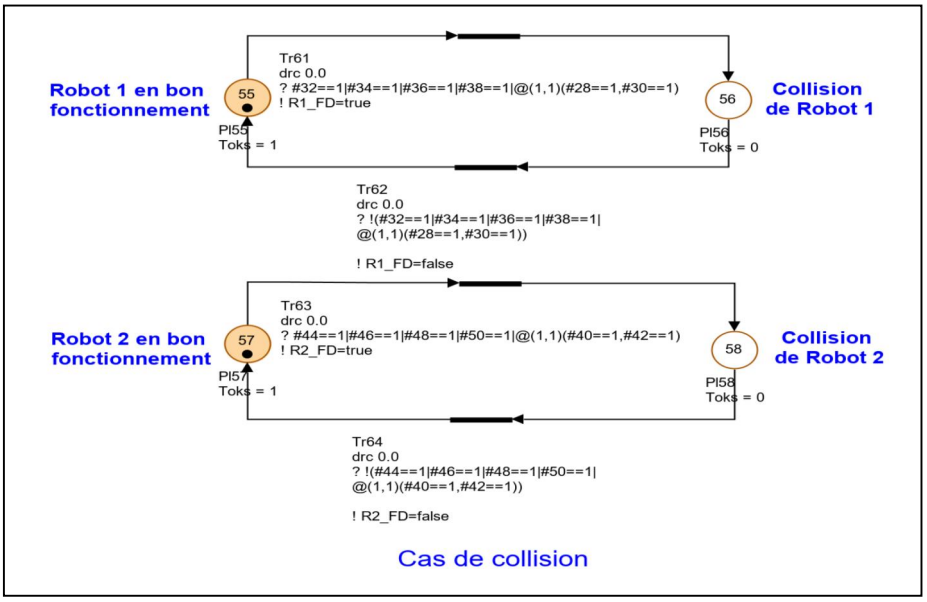


Figure III.33 Scénarios de collision

Lorsque les jetons franchissent les transitions de détection de panne et atteignent les places (P28, P30, P32, P34, P36, P38) pour le robot 1 ou les places (P40, P42, P44, P46, P48, P50) pour le robot 2, cela signifie que les robots sont en état non sécurisé à cause de la défaillance d'un ou de plusieurs de leurs composants, entraînant la collision (les jetons franchissent les transitions Tr 61 ou Tr 63 selon le prédicat «? # 32 == 1 | # 34 == 1 | # 36 == 1 | # 38 == 1 | @ (1,1) (# 28 == 1, # 30 == 1) » ou « ? # 44 == 1 | # 46 == 1 | # 48 == 1 | # 50 == 1 | @ (1,1) (# 40 == 1, # 42 == 1) », où les places 28, 30, 32, 34, 36, 38 représentent l'état de défaillance des composants du robot 1et les places 40, 42, 44, 46, 48, 50 représentent l'état de défaillance des composants du robot 2. Lorsque les jetons atteignent les places P56 ou P58 à partir de P55 ou P57,cela réalise l'assertion "«!R1_FD = true» si le robot 1 est défaillant ou «!R2_FD = true» si le robot 2 est défaillant".

Les robots défaillants sont transférés depuis les places (P7, P8, P9, P10, P11, P12, P13, P14) au service de maintenance (P59 ou P60). Ceci est illustré par les figures III.30 et III.31. Les jetons restent dans ces places jusqu'à ce que la réparation du problème soit complète. Lorsque les robots reviennent à leurs états initiaux à travers les transitions Tr62 et Tr64, les variables «R1_FD et R2_FD» seront fausses, les transitions Tr81 et Tr82 sont franchies pour atteindre les places P19 et P21 et poursuivre leurs missions.

III.7.6 Résultats et discussion

Les données de probabilités de défaillance récupérées des références [9 ; 124] sont réévaluées en fonction de nouvelles conditions de fonctionnement. Les événements de défaillance sont supposés être distribués selon deux lois de probabilités : la loi exponentielle et la loi de Weibull. La durée de l'expérience pour la simulation est quatre ans (34560 heures), le nombre d'histoires est de 10^6 histoires et l'intervalle de confiance est estimé à 90 %. La figure III.34 illustre la fréquence de collision pour une période de 4 ans avec les deux limites d'intervalle de confiance (IC) inférieure et supérieure.

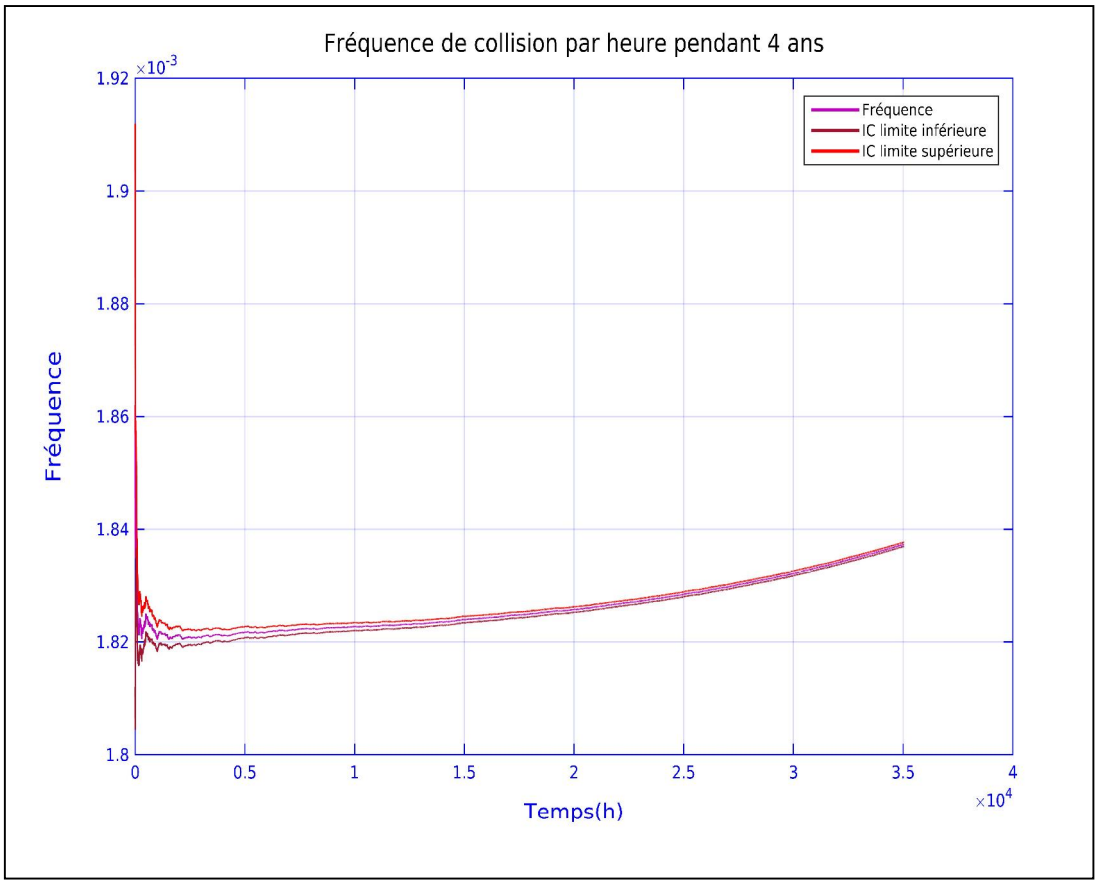


Figure III.34 Fréquence de collision par heure

La fréquence de collision a été calculée par simulation. Selon le graphe de la figure III.34, nous observons que sa valeur est comprise entre $1{,}82 \times 10^{-3}\, h^{-1}$ et $1{,}86 \times 10^{-3}\, h^{-1}$. Ce qui signifie que tous les 22 à 23 jours, il y a le risque que l'un des deux robots entre en collision dans le laboratoire.

III.8 Discussions et comparaison des résultats

Dans ce chapitre, plusieurs approches ont été élaborées pour fournir une analyse de risques détaillée d'un laboratoire d'analyses robotisé, tout en prenant en compte les dysfonctionnements des composants du système à l'échelle microscopique. En outre, nous considérons tout d'abord une architecture de contrôle de haut niveau d'un seul robot, en partant ensuite vers l'échelle macroscopique et en utilisant différentes architectures hiérarchiques de contrôle de l'ensemble du système multi-robots de haut niveau et de niveau détaillé. Enfin, nous effectuons deux types d'évaluation : une évaluation semi-quantitative, qui nous aident à sélectionner l'architecture de contrôle adéquate ; et une évaluation quantitative, qui nous aident à étudier les propriétés stochastiques d'un accident et donc d'estimer la fréquence du risque de collision. À notre connaissance, il existe actuellement très peu d'études autour de la sécurité des robots mobiles autonomes. En particulier, aucun article ne fournit les résultats de l'analyse de sécurité d'un système composé de plusieurs robots mobiles, en utilisant différents types d'architectures de contrôle.

La première approche consiste en une analyse préliminaire des modes de dysfonctionnement des principaux composants physiques d'un robot mobile. Cette approche est basée sur une combinaison de deux méthodes d'analyse : l'AMDEC et l'ADD. Pour assurer la sureté de fonctionnement des robots mobiles, un ensemble d'actions permettant la réduction de risque a été suggéré comme recommandations, faisant suite aux conclusions de l'analyse AMDEC. L'analyse de l'arbre de défaillance traite le mode opérationnel des robots mobiles en analysant le risque de collision. La combinaison des méthodes AMDEC et ADD est la plus utilisée dans le domaine de la robotique. Elle est notamment très utile pour l'identification des modes de défaillances de la partie physique du système.

La deuxième approche est basée sur la combinaison STPA/ADD. L'objectif est d'analyser les actions de contrôle dangereuses de l'architecture de contrôle de haut niveau d'un seul robot. Par la suite, une identification des scénarios de danger potentiels a été réalisée. L'analyse ADD aide à la modélisation de deux types d'accidents (collision robot-obstacle et collision robot-humain) consécutifs aux facteurs causaux obtenus par l'analyse STPA.

La troisième approche est une combinaison de l'analyse STPA et du nœud papillon. Cette approche a été appliquée pour l'analyse des différentes architectures hiérarchiques de

contrôle et coordination des systèmes multi-robots. Le résultat de cette analyse permet d'extraire un grand nombre de scénarios évalués semi-quantitativement. La combinaison du nœud papillon et de l'analyse STPA a permis une comparaison des architectures de contrôle. Une limitation de cette combinaison toutefois : Le nœud papillon est incapable de quantifier tous les scénarios potentiels et les facteurs de causalité obtenus par l'analyse STPA. Il est également incapable de différencier quantitativement certains scénarios : « lorsque l'action de contrôle n'est pas fournie, ou fournie trop tard ou trop tôt ». Il est enfin incapable de différencier les facteurs de causalité comme « mauvaise connexion ou connexion interrompue », considérées comme identiques dans notre évaluation.

La quatrième approche est une combinaison de la méthode STPA et du RdPS. Elle fournit une analyse détaillée des différentes fonctionnalités des contrôleurs des robots mobiles autonomes à l'aide d'une architecture de contrôle plus détaillée et en utilisant l'analyse STPA. Le résultat de cette analyse identifie des contraintes de sécurité nécessaires et propose également des exigences pour optimiser le contrôle de ces robots au sein d'environnements complexes à haut niveau de risques. Par ailleurs, le réseau de Petri stochastique RdPS contribue à modéliser le comportement des robots durant leur fonctionnement normal. Leurs scénarios de risque contribuent ainsi à évaluer quantitativement le risque de collision.

La propriété la plus marquée de l'analyse STPA est caractérisée par la possibilité d'extraire de nombreux ensembles d'événements dangereux, y compris ceux causés par des défaillances d'éléments du système, tels que les risques résultant d'interactions involontaires entre les éléments. En outre, l'analyse STPA nous fournit un grand nombre de scénarios potentiels, celle-ci ne traitant pas uniquement le système en modes de fonctionnement/dysfonctionnements, mais prenant également en compte le facteur de temps et son influence (action exécutée trop tard ou trop tôt).

III.9 Conclusion

Ce chapitre est consacré à l'élaboration d'une analyse des risques complète et détaillée dans le cadre d'un système complexe robotisé. Nous avons tout d'abord appliqué une approche pour identifier les modes de dysfonctionnements des systèmes robotiques mobiles. Dans un deuxième temps, nous avons élaboré une analyse des architectures de contrôle de haut niveau des robots en utilisant plusieurs architectures hiérarchisées. Enfin, l'analyse d'une architecture de contrôle de niveau plus détaillé a été réalisée afin de traiter

les actions de contrôle dangereuses pour chaque fonctionnalité des contrôleurs autonomes. Par ailleurs, une modélisation et une évaluation quantitative des scénarios de risque de collision sont effectuées. Cette analyse fournit une méthodologie très utile pour la gestion des risques des systèmes complexes robotisés. L'analyse conclut à un ensemble de contraintes et d'exigences de sécurité nécessaires dont les principaux objectifs sont : l'amélioration de la partie contrôle/commande des systèmes robotiques, l'assurance de leur sûreté de fonctionnement, l'optimisation de leur coopération tout en préservant la sécurité humaine et matérielle du système global.

Ci-dessous un résumé des principales conclusions :

La combinaison des analyses AMDEC et ADD est très utilisée dans le domaine de la robotique. Elle est très utile pour l'identification des modes de défaillances de la partie physique du système. L'analyse STPA est très utile pour les systèmes complexes automatisés et autonomes.

L'arbre de défaillances basé sur une analyse STPA fournit plus de détails comparativement à l'arbre de défaillances classique.

L'analyse STPA est une méthode purement qualitative. Par conséquent, une combinaison avec une autre technique est nécessaire pour une évaluation précise. A titre d'exemples, le diagramme nœud papillon et les réseaux de Petri peuvent être utilisés complémentairement.

Dans un environnement structuré et risqué tel notre exemple applicatif, l'architecture de contrôle la plus critique (et a fortiori, à éviter) d'un système multi-robots, est l'approche centralisée. C'est en particulier le cas lorsqu'un grand nombre de robots fonctionnent ensemble et en même temps. Afin de contrôler et de gérer le fonctionnement de nombreux robots dans un environnement complexe, l'utilisation d'une seule unité rend le système plus exposé aux accidents et aux dangers.

La structure hiérarchique présente un nombre moyen de scénarios de risques classés dans la zone intolérable. La structure hiérarchique modifiée est, quant à elle, la structure qui présente le moins de scénarios de risques classés dans la zone intolérable. Cette structure hiérarchique modifiée est par conséquent la plus appropriée dans le cadre d'un système multi-robots. Elle surpasse les autres architectures en raison de deux propriétés principales : le contrôle multi-niveaux et la communication inter-robots de même niveau.

Chapitre IV

Architecture de contrôle et sécurité des systèmes de robots mobiles

IV.1 Introduction

Un robot mobile à roues est un robot pouvant se déplacer de manière autonome d'un endroit à l'autre. Contrairement aux robots industriels conventionnels qui ne peuvent se déplacer que dans un espace de travail limité, les robots mobiles ont la particularité de se déplacer librement dans un espace de travail prédéterminé pour atteindre leurs objectifs [125]. Actuellement, leur autonomie nous permet de développer des lois et stratégies pour réguler leur comportement : ils sont à la fois autogérés et autorégulés. Par conséquent, ces robots ont la capacité de naviguer automatiquement par eux-mêmes sans l'intervention d'êtres humains, qui se concentrent sur la supervision [126– 127].

La navigation autonome nécessite un certain nombre de capacités hétérogènes, y compris la capacité d'exécuter des actions élémentaires pour atteindre un objectif, comme : atteindre un emplacement donné ; réagir en temps réel à des événements inattendus, éviter un obstacle inattendu; construire, utiliser et maintenir une carte de l'environnement proche ; déterminer la position du robot sur cette carte ; former des plans qui poursuivent des objectifs spécifiques ou éviter des situations indésirables ; s'adapter aux changements de l'environnement [128], etc. Un système de navigation autonome s'articule en trois principales tâches : la perception de l'environnement et la localisation, la planification et le contrôle du robot pour le suivi de trajectoire, comme illustrées sur la figure IV.1.

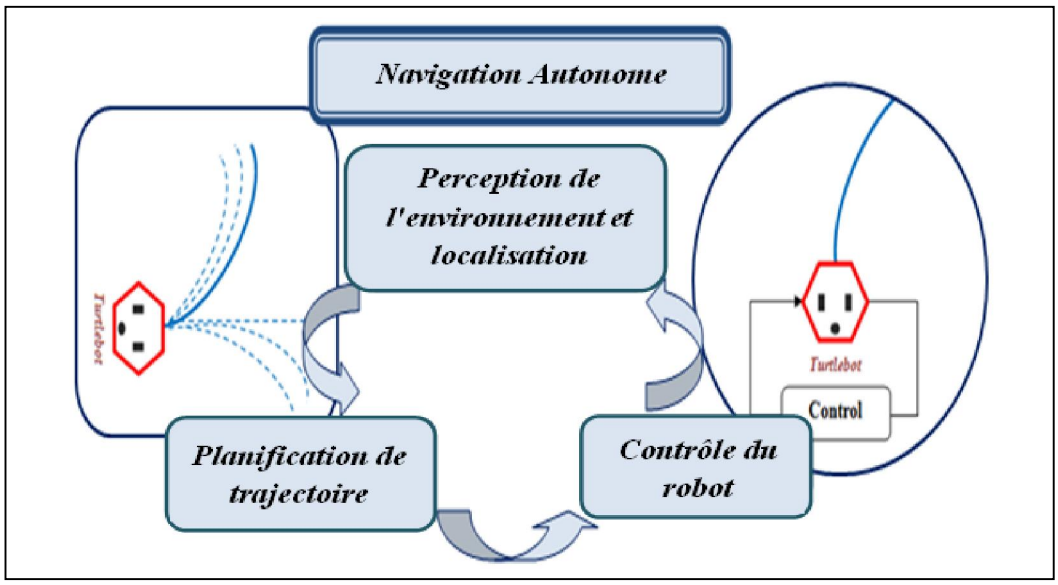


Figure IV.1 Système de navigation autonome

Dans ce travail, nous effectuons une navigation autonome de robots mobiles à roues en supposant des trajectoires planifiées prédéfinies et fixes. Par conséquent, un contrôleur de suivi de trajectoire a été développé dans le cadre d'un robot mobile à conduite différentielle à deux roues. Son architecture de contrôle comprend deux parties. La première est basée sur une commande cinématique non linéaire à retour d'état. La seconde partie consiste en un algorithme d'optimisation hors ligne permettant d'ajuster les paramètres du contrôleur pour obtenir les variables optimales de suivi de trajectoire. Nous avons choisi ce type de robot car il possède une structure mécanique simple nous permettant de mieux étudier sa propre navigation.

L'objectif de cette étude est de proposer une architecture de contrôle optimale qui assure la stabilité et augmente la précision du contrôle pour diverses formes de trajectoires complexes. Par ce biais, nous traitons et améliorons également la sécurité des systèmes robotiques mobiles dans les milieux industriels.

Une partie du contenu de ce chapitre est basée sur les conférences et les articles publiés suivants : ICAEPI 2017 [129], ICTAEE 2018 [130], AJSS 2017 [131].

IV.2 Modélisation cinématique des robots mobiles différentiels à deux roues

La cinématique des robots dépend de leur configuration dans leur environnement proche, des relations entre leurs paramètres géométriques et des contraintes imposées concernant les trajectoires. Le modèle cinématique consiste à trouver la relation géométrique du système de contrôle en étudiant le comportement mécanique du robot [132]. Par exemple, un robot mobile à roues peut avoir plusieurs roues avec ou sans contraintes dans leur mouvement [125]. Dans notre travail de thèse, nous avons utilisé le robot Turtlebot2, robot mobile à conduite différentielle d'entrainement à deux roues proposé par Willow Garage.

Ce type de robot se déplace suivant le modèle suivant :

Considérons $(O, \vec{X}, \vec{Y})$ un repère fixe global (qui peut être le repère initial du robot) et $(O', \overrightarrow{X_R}, \overrightarrow{Y_R})$ un repère mobile de coordonnées locales du robot, avec O' le milieu de son essieu. La pose du robot est exprimée en coordonnées cartésiennes dans le repère global :

$P = (x, y, \theta)^T$. La relation liant les deux repères mentionnés précédemment passe par la matrice de rotation suivante :

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{(IV.1)}$$

Où $R(\theta)$ est la matrice de rotation du repère local vers le repère global :

Cette matrice nous permet d'obtenir la vitesse du point P dans le repère global, notée $\dot{P}$, à partir de sa vitesse $\dot{P}'$ dans le repère local du robot selon l'équation :

$$\dot{P} = R(\theta).\dot{P}' \quad \text{(IV.2)}$$

La figure IV.2 représente le déplacement du robot dans son environnement, montrant la relation entre les deux repères.

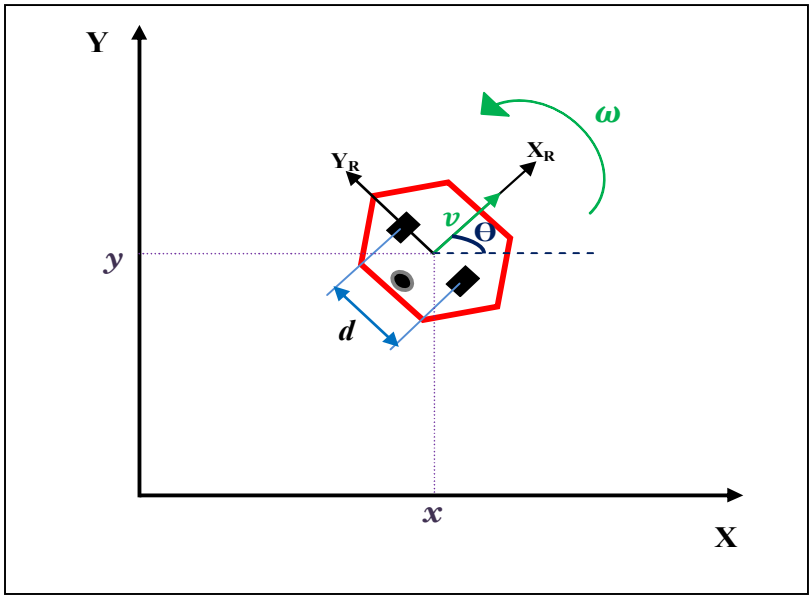


Figure IV.2 Schéma du robot Turtlebot2 dans son environnement

Où :

- x et y sont respectivement l'abscisse et l'ordonnée du point P par rapport au repère global $(O, \vec{X}, \vec{Y})$.
- θ est l'angle d'orientation de l'axe des abscisses du repère local du robot $(O', \overrightarrow{X_R}, \overrightarrow{Y_R})$ par rapport à l'axe des abscisses du repère global $(O, \vec{X}, \vec{Y})$.
- d est la distance entre les roues.
- v est la vitesse linéaire du robot mobile définie dans son repère.

- ω est la vitesse angulaire du robot mobile définie dans son repère.

L'entraînement différentiel est l'entraînement mécanique le plus simple car il ne nécessite pas la rotation d'un essieu vers la direction souhaitée. Ce type d'entrainement se compose de deux roues motorisées fixes, installées sur les côtés gauche et droit de la plate-forme du robot. Les deux roues sont entraînées indépendamment. Une ou deux roues pivotantes passives (i.e. roues folles) sont utilisées pour l'équilibre et la stabilité du robot. Lorsque les deux roues tournent à la même vitesse, le robot se déplace tout droit. Il peut ainsi avancer ou reculer en ligne droite sur un plan horizontal sans défaut. Si une roue tourne plus vite que l'autre, le robot suit une trajectoire courbe. Le virage vers la droite est réalisé en actionnant la roue gauche à une vitesse supérieure à celle de la roue droite et vice-versa pour tourner à gauche. Il peut également tourner sur lui-même en actionnant une roue vers l'avant et la deuxième roue dans le sens opposé avec la même vitesse [125].

Les roues du robot Turtlebot2 sont caractérisées par des contraintes non holonomes. La contrainte non holonome rencontrée en robotique mobile est la contrainte de mouvement d'un disque qui roule sur un plan sans glissement (figure IV.3). Autrement dit, la vitesse relative de la roue par rapport au sol au point de contact est nulle. En théorie, pour vérifier cette condition, les hypothèses suivantes doivent être remplies :

- Le contact entre la roue et le sol est ponctuel ;
- Les roues sont indéformables, de rayon r.

En raison de la condition de non glissement, les coordonnées de vitesse de roue généralisées sont contraintes par les équations (IV.3) et (IV.4) suivantes, considérant que ϵ représente l'angle de rotation de la roue.

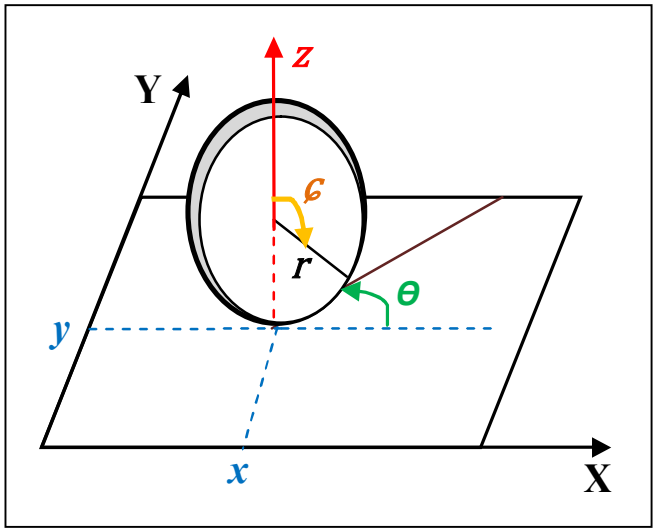


Figure IV.3 Représentation d'une roue dans un système de coordonnées cartésiennes

$$\dot{x} = \mathrm{r}\,\dot{\varphi}\cos\theta\ ,\ \dot{y} = \mathrm{r}\,\dot{\varphi}\sin\theta \tag{IV.3}$$

En éliminant la vitesse de la roue $v = \mathrm{r}\,\dot{\varphi}$ de l'équation (IV.3), on obtient :

$$\dot{x}\sin\theta - \dot{y}\cos\theta = 0 \tag{IV.4}$$

La relation entre les vitesses du robot (v, ω) et les vitesses des roues droite et gauche respectivement (ω_d, ω_g) s'exprime par ces deux équations :

$$v = r.\left(\frac{\omega_d + \omega_g}{2}\right) \tag{IV.5}$$

$$\omega = r.\left(\frac{\omega_d - \omega_g}{2}\right) \tag{IV.6}$$

Equations cinématiques :

Supposons que le robot soit dans une pose courante notée $P_c = (x_c, y_c, \theta)^T$et que la distance entre sa pose courante et la pose désirée $P_d = (x_d, y_d, \beta)^T$ est définie par rapport au repère global comme indiquée sur la figure IV.4.

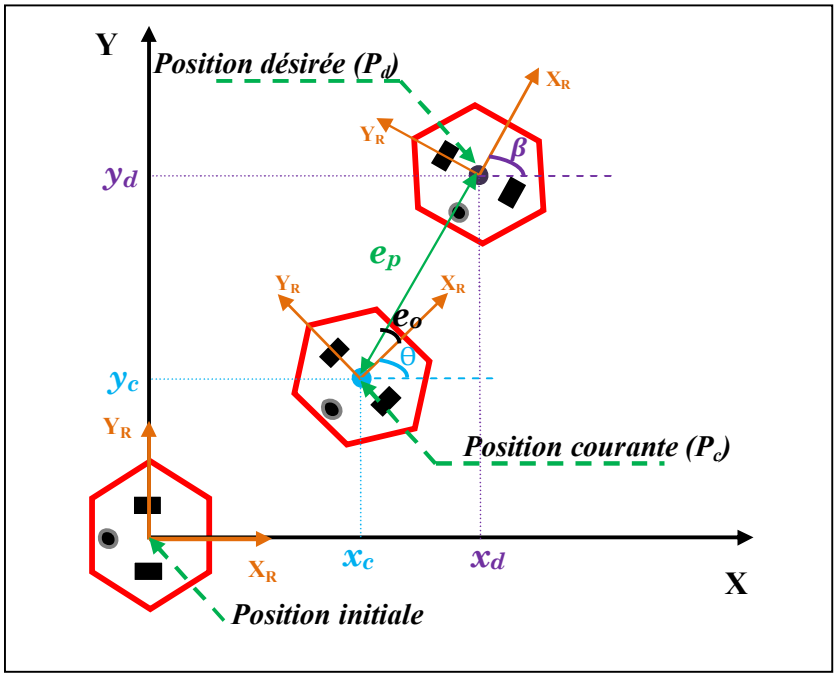


Figure IV.4 Déplacement du robot mobile

Etant donné que ce robot ne peut se déplacer que dans une seule direction, perpendiculaire à l'axe des roues et que son centre de masse correspond au milieu de l'essieu, le modèle cinématique du robot est décrit par l'équation (IV.7) :

$$\dot{P} = \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \end{bmatrix} = \begin{bmatrix} \cos\theta & 0 \\ \sin\theta & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v \\ \omega \end{bmatrix} \tag{IV.7}$$

L'équation (IV.7) peut se réécrire de la façon suivante :

$$\begin{cases} \dot{x} = v\cos\theta \\ \dot{y} = v\sin\theta \\ \dot{\theta} = \omega \end{cases} \tag{IV.8}$$

La pose du robot peut également être représentée en coordonnées polaires avec une erreur de position $e_p > 0$ et une erreur d'orientation $e_o = \beta - \theta$:

$$\begin{cases} \dot{e_p} = -v\cos(\beta-\theta) = -v\cos e_o \\ \dot{\beta} = v\frac{\sin(\beta-\theta)}{e_p} = v\frac{\sin e_o}{e_p} \\ \dot{\theta} = \omega \end{cases} \tag{IV.9}$$

Considérant que :

- e_o représente l'angle mesuré entre l'axe des abscisses de référence ($\overrightarrow{O'X_R}$) et l'axe e_p.
- e_p représente la distance entre la pose courante P_c et la pose désirée P_d, exprimée par l'équation suivante :

$$e_p = \sqrt{(x_d - x_c)^2 + (y_d - y_c)^2} \tag{IV.10}$$

Les équations cinématiques obtenues à partir des coordonnées polaires sont :

$$\begin{cases} \dot{e_p} = & -v\cos e_o \\ \dot{e_o} = & -\omega + v\frac{\sin e_o}{e_p} \\ \dot{\beta} = & v\frac{\sin e_o}{e_p} \end{cases} \quad \text{avec :} \quad e_p \neq 0 \tag{IV.11}$$

IV.3 Commande de suivi de trajectoire

La commande de mouvement des robots mobiles à roues a été, et reste, un axe de recherche attrayant [133–139] en raison des contraintes de non-holonomie. L'amélioration des techniques de contrôle hautement non linéaires est un challenge. Le suivi de trajectoire est l'une des problématiques les plus fréquentes du contrôle de mouvement des robots. Il s'agit de la conception d'un contrôleur qui force le robot mobile à roues à suivre une trajectoire géométrique planifiée à travers le calcul de signaux de commande, conduisant à une convergence asymptotique nulle de l'erreur entre la pose du robot et celle désirée [132].

De nombreuses recherches ont été menées pour étudier le problème du contrôle de suivi de trajectoire de ce type de robots en utilisant plusieurs stratégies de contrôle/commande. Citons à titre d'exemple, la commande adaptative [133–134 ; 139], la commande par mode glissant [132 ; 140], la commande backstepping [141], la commande par retour d'état linéarisant [142], la commande basée sur la logique floue [143–144], la commande basée sur les réseaux de neurones [145], la commande d'apprentissage itératif [146], la commande basée sur la théorie de Lyapunov [147]. Des études complètes des divers problèmes de contrôle du mouvement des robots à roues ont été réalisées dans [148–149].

Dans cette étude, nous avons proposé une commande cinématique basée sur le théorème de Lyapunov, similaire à celle proposée par [147 ; 150]. Différentes formes de trajectoires sont planifiées pour le suivi. Après une optimisation des paramètres de la loi de commande, une comparaison des résultats des deux travaux termine cette section.

IV.3.1 Architecture de contrôle proposée

L'architecture de contrôle proposée dans le cadre de notre étude est représentée sur la figure (IV.5). Il s'agit d'une commande de vitesses linéaire et angulaire à retour d'état.

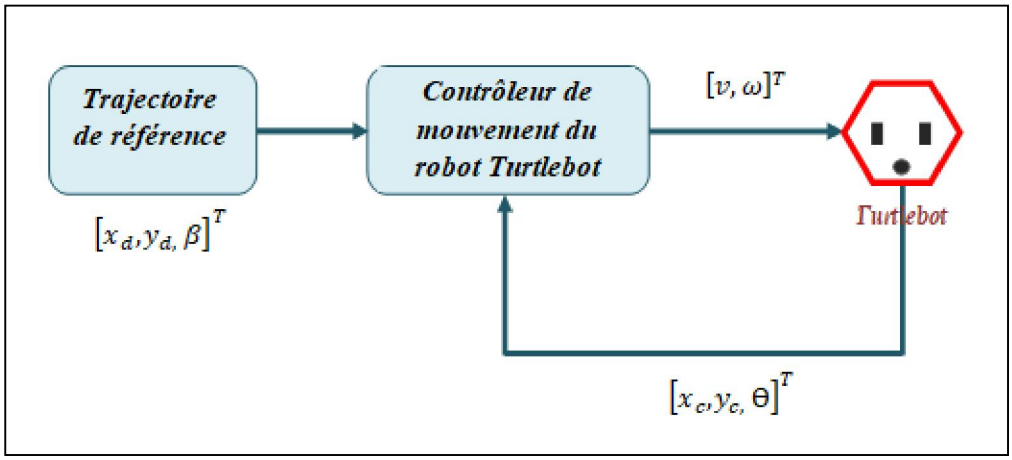


Figure IV.5 Architecture de contrôle proposée pour le suivi de trajectoire

IV.3.2 Trajectoires de référence et acquisition des données des capteurs

La trajectoire de référence est une trajectoire prédéfinie permettant de relier la pose initiale à la pose désirée du robot. Le contrôleur est testé sur différentes trajectoires complexes afin d'éprouver la loi de commande utilisée. L'acquisition des données est réalisée par estimation odométrique en récupérant les valeurs de position le long des axes x et y et l'orientation du robot à chaque instant.

IV.3.3 Loi de commande et stabilité

L'algorithme de contrôle doit être conçu pour déplacer le robot de sa configuration actuelle à sa configuration souhaitée. Nous imposons donc au robot des commandes cinématiques de vitesses linéaire et angulaire $u = [v \quad \omega]^T$ jusqu'à ce que le robot atteigne la pose souhaitée.

La loi de commande proposée dépend de l'état, c'est-à-dire $[v \quad \omega]^T = f(e_p, e_o, \beta)$, ce qui garantit que l'état se déplace vers $(0,0,\beta)$ sans atteindre $e_p = 0$ dans un intervalle de temps fini.

L'une des méthodes les plus couramment utilisées pour étudier le comportement asymptotique est basée sur la théorie de la stabilité de Lyapunov. Considérons une forme quadratique définie positive simple de la fonction de Lyapunov avec, respectivement, e_p et e_o, les erreurs de position et d'orientation :

$$V = V_1\,(e_p) + V_2\,(e_0) = \frac{1}{2}{e_p}^2 + \frac{1}{2}{e_o}^2 \tag{IV.12}$$

Sa dérivée par rapport au temps est donnée par :

$$\dot{V} = \dot{V_1} + \dot{V_2} = \dot{e_p}.e_p - \dot{e_o}.e_o \tag{IV.13}$$

En utilisant les équations cinématiques (IV.11) :

$$\dot{V} = e_p.(-v\cos e_o) + e_o.(-\omega + v\,\frac{\sin e_o}{e_p}) \tag{IV.14}$$

Le premier terme peut être non positif, permettant de mettre la vitesse linéaire sous la forme :

$$\begin{cases} v = & K_p e_p \cos e_o \text{ avec} K_p > 0 \\ \dot{V_1} = & e_p\,(-K_\rho e_p \cos^2 e_o) \\ \dot{V_1} = & -K_p {e_p}^2 \cos^2 e_o \leq 0 \end{cases} \tag{IV.15}$$

Cela signifie que le terme $(\dot{V_1})$ est toujours une fonction non croissante dans le temps. Par conséquent, il converge asymptotiquement vers une limite finie non négative. De même, le deuxième terme peut être non positif. Par conséquent, la vitesse angulaire est mise sous la forme :

$$\begin{cases} \omega = & K_p \sin e_o \cos e_o + K_o e_o \text{ avec} K_o > 0 \\ \dot{V_2} = & e_o\,(-K_p \sin e_o \cos e_o - K_o e_o - \frac{K_p e_p \sin e_o \,.\, \cos e_o}{e_p}) \\ \dot{V_2} = & -K_o {e_o}^2 \leq 0 \end{cases} \tag{IV.16}$$

Enfin, l'expression de la dérivée temporelle de la fonction de Lyapunov (V) devient :

$$\dot{V} = \dot{V_1} + \dot{V_2} = -K_p\,{e_p}^2 \cos^2 e_o - K_o {e_o}^2 \leq 0 \tag{IV.17}$$

Le résultat est sous forme semi-négative. En appliquant le lemme de Barbalat, il s'ensuit que (V) converge nécessairement vers zéro en un temps limité. Ce qui implique que le vecteur d'état converge de (e_p, e_o, θ) vers $(0,0,\beta)$.

Nous concluons donc que les expressions des vitesses linéaire et angulaire suivantes rendent le mouvement du robot lisse et stable.

$$\begin{cases} v = & K_p e_p \cos e_o \\ \omega = & K_p \sin e_o \cos e_o + K_o e_o \end{cases} \quad \text{(IV.18)}$$

IV.4 Optimisation des paramètres à l'aide d'outils issus de l'intelligence artificielle

L'optimisation désigne un processus permettant de détecter les solutions optimales qui minimisent ou maximisent le rendement avec une fonction de coût minimale. L'optimalité de la solution est basée sur un ou plusieurs critères (fonction objectif), qui dépendent généralement du problème et de l'utilisateur [151]. Le processus d'optimisation d'un problème commence par la sélection des variables de conception et la formulation des contraintes et des fonctions « objectifs ». Le but principal de la fonction objectif est de fixer une valeur à des variables sélectionnées en fonction des contraintes données, permettant de produire la meilleure réponse. Selon le nombre de solutions disponibles pour un problème donné, ces méthodes d'optimisation peuvent être divisées en méthodes d'optimisation continues ou combinatoires. Les méthodes continues ont des solutions infinies, tandis que les méthodes combinatoires ont des solutions limitées. Dans le cas de méthodes combinatoires, afin de trouver la meilleure solution, différents paradigmes d'optimisation doivent être utilisés pour traiter divers problèmes calculatoires [152].

IV.4.1 Aperçu des méthodes d'optimisation

L'objectif principal de l'optimisation est d'essayer d'obtenir le meilleur résultat possible parmi les solutions potentielles pour un problème donné. Cependant, cela dépend du contexte ou de l'environnement. Le résultat optimal peut être exprimé sous la forme d'une valeur maximale ou minimale. Dans la plupart des cas, l'optimisation est conduite, soit pour trouver une sortie maximale, représentée par une fonction de qualité ; soit pour trouver une sortie minimale, tout en minimisant un coût [153]. Il existe de nombreuses méthodes d'optimisation qui peuvent être utilisées pour résoudre une ou plusieurs fonctions variables, avec ou sans contrainte. Selon la littérature, les méthodes d'optimisation peuvent être classées en plusieurs catégories, comme le montre la figure IV.6. La plupart des méthodes d'optimisation conventionnelles sont fondées et résolues numériquement. Elles sont basées sur des algorithmes de recherche permettant de trouver la meilleure solution. Ces méthodes sont plus adaptées aux fonctions « objectifs » uni modales simples. Cependant, elles ne sont pas efficaces pour les problèmes complexes multimodaux [152], c'est-à-dire pour les problèmes admettant plusieurs minima locaux.

Afin de compenser les limitations inhérentes à l'optimisation basée sur des calculs numériques, des méthodes d'optimisation intelligentes dites méta-heuristiques ont été développées. Les méthodes méta-heuristiques sont des méthodes stochastiques inspirées de phénomènes naturels et biologiques. Ces méthodes peuvent être divisées en deux catégories principales :

Les méthodes à population de solutions, appelées également « algorithmes évolutionnaires ». Ces algorithmes améliorent une population de solutions, tels les algorithmes génétiques, les stratégies d'évolution, la programmation évolutionnaire ou les algorithmes à essaim.

Les méthodes à solution unique *:* ces méthodes commencent la recherche à partir d'une solution unique, qui circule en générant une trajectoire dans l'espace de recherche. Parmi ces méthodes, citons la méthode du recuit simulé, la méthode GRASP, la méthode de descente, la recherche tabou et la recherche locale itérée [154].

De nos jours, les méthodes stochastiques sont couramment utilisées pour résoudre les problèmes d'optimisation [155]. Récemment, les algorithmes heuristiques naturels ont prouvé leur capacité à résoudre les problèmes d'optimisation numérique de manière plus appropriée. Ces méthodes d'optimisation intelligentes ont surpassé les méthodes classiques par leur aptitude à résoudre les problèmes à variables multiples [153].

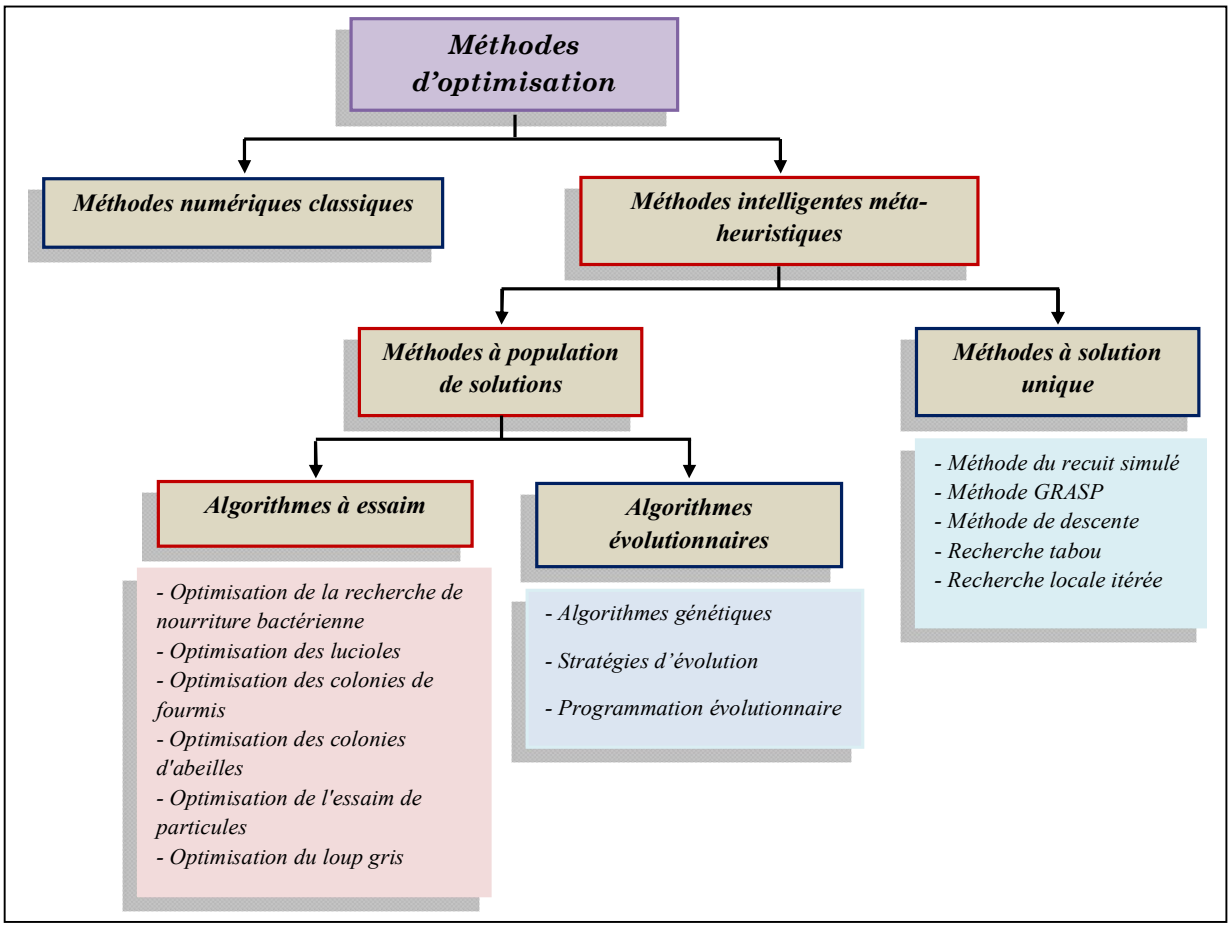


Figure IV.6 Classification des méthodes d'optimisation

Dans la section suivante, nous décrivons les techniques d'optimisation de l'intelligence en essaim, plus efficaces pour résoudre un problème linéaire / non linéaire, comparativement à d'autres techniques.

IV.4.2 Techniques d'optimisation de l'intelligence en essaim

L'intelligence en essaim est une discipline d'auto-organisation dans laquelle la structure apparaît au niveau global à partir de la coordination des agents individuels. Il s'agit d'une discipline contemporaine de l'intelligence artificielle, principalement dédiée à la conception de systèmes multi-agents avec des applications telles l'optimisation, la robotique, etc.

Les techniques d'optimisation de l'intelligence en essaim sont des algorithmes stochastiques développés sur la base du comportement collectif d'agents individuels, qui peuvent communiquer directement ou indirectement pour effectuer des tâches complexes dans la nature. Certaines de ces techniques efficaces, qui imitent les comportements d'animaux ou d'insectes (oiseaux, fourmis, abeilles, mouches et même germes), sont

appelées « algorithmes inspirés de la nature », et sont utilisés pour le réglage automatique des contrôleurs [155].

Dans la littérature, il existe plusieurs algorithmes d'optimisation basés sur l'intelligence de l'essaim, comme les volées d'oiseaux, de fourmis, de poissons, d'abeilles, etc. où les individus sont simples, de nature homogène et autonomes [152]. Parmi les algorithmes les plus couramment utilisés et les plus efficaces pour le calcul des paramètres, nous rencontrons la méthode d'optimisation de l'essaim de particules PSO, présentée dans la section suivante.

IV.4.3 Méthode d'optimisation de l'essaim de particules (Particle Swarm Optimisation PSO)

L'optimisation de l'essaim de particules (PSO) est une technique d'optimisation stochastique basée sur la population inspirée du comportement social des oiseaux ou des poissons. Elle a été introduite pour la première fois par Eberhart et Kennedy en 1995. Par la suite, elle a été appliquée avec succès dans différents domaines, notamment la conception, les télécommunications, le contrôle, et en particulier le contrôle non linéaire [156–157] et l'optimisation combinatoire. De nombreux ajustements de contrôleurs PID (proportionnel, intégral, dérivé) basés sur PSO pour diverses applications ont été réalisés dans [157–160].

Avec l'algorithme PSO, au lieu d'utiliser des opérateurs évolutifs comme la mutation et le croisement pour manipuler des algorithmes, un troupeau de particules est placé dans l'espace de recherche d-dimensionnel avec des vitesses et des positions choisies au hasard, connaissant leurs valeurs optimales. La vitesse et la position de chaque particule sont ajustées en fonction de sa propre expérience de vol et de l'expérience de vol des autres particules [157]. La description de l'algorithme PSO est donnée à la section IV.5.1.

IV.5 Contrôle optimal de la navigation d'un robot dans un environnement inconnu à risques

L'objectif principal de cette partie est de proposer une architecture de contrôle convenable et optimale permettant d'assurer une navigation autonome précise et sécurisée des robots mobiles au sein d'environnements à risques.

Après avoir défini la loi de commande utilisée dans cette étude (voir la section IV.3.3), une approche d'ajustement des paramètres de contrôle (K_p et K_o) utilisant l'algorithme d'optimisation de l'essaim de particules PSO est proposée afin d'obtenir les variables optimales de suivi de trajectoire. L'objectif est d'optimiser les performances de contrôle (précision, rapidité et stabilité), améliorant ainsi la sécurité du système. L'approche globale proposée est illustrée sur la figure IV.7.

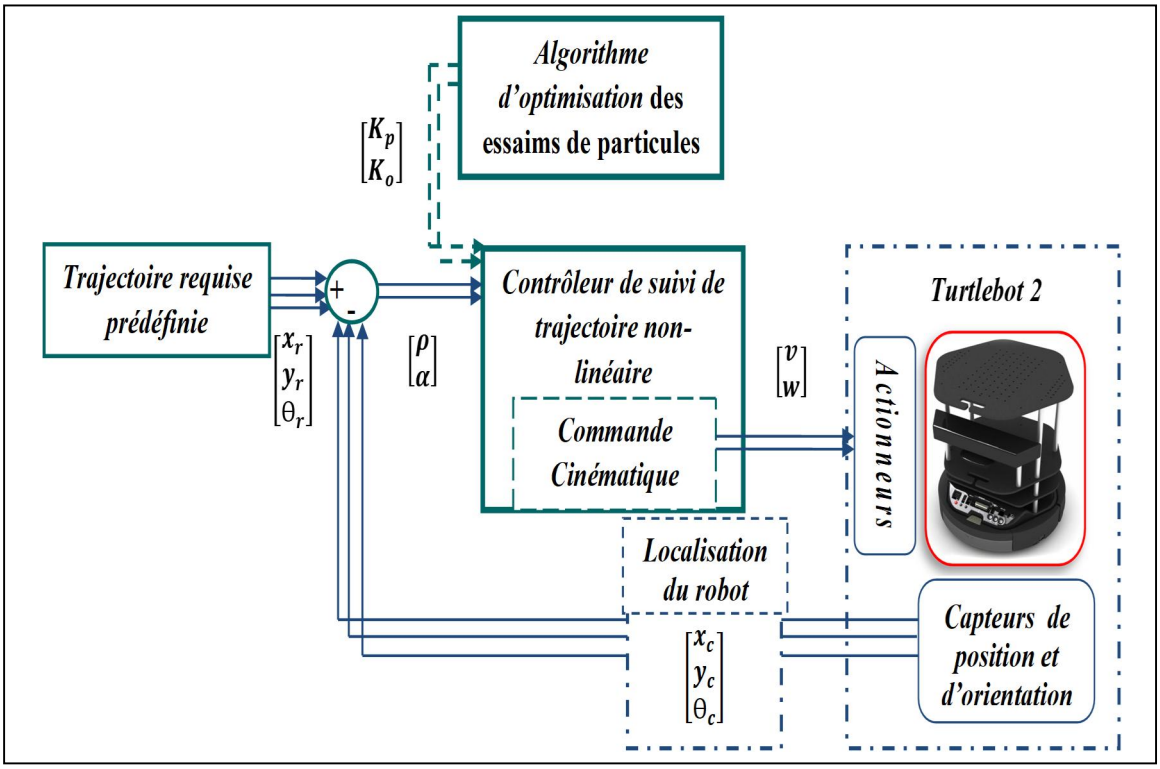


Figure IV.7 Architecture de contrôle globale proposée pour le suivi de trajectoire

IV.5.1 Optimisation des paramètres K_p et K_o par PSO

Cette partie décrit les différentes étapes suivies pour l'obtention des deux paramètres de contrôleur K_p et K_o en utilisant l'algorithme PSO. La figure IV.8 illustre les différentes étapes de l'algorithme d'optimisation de l'essaim de particules.

L'algorithme est initialisé avec une population de solutions aléatoires et recherche des optimums en mettant à jour des générations. Dans PSO, les solutions potentielles, appelées particules, volent à travers l'espace du problème en suivant les particules optimales actuelles. Dans le système PSO, chaque individu ajuste son vol en fonction de sa propre expérience de vol et de l'expérience de vol de son compagnon. Chaque particule garde la trace de ses coordonnées dans l'espace du problème, associées à la meilleure solution (fonction de fitness) qu'elle a obtenue jusqu'à présent. Cette valeur est appelée

« *pbest* ». Une autre « meilleure » valeur de chaque particule, suivie par l'optimiseur de l'essaim de particules, est la meilleure valeur obtenue par la particule jusqu'à présent. Ce meilleur rapport « qualité-prix » est appelé « meilleur global », et est noté « *gbest* ».

À chaque itération, chaque particule est mise à jour en utilisant ces deux « meilleures » valeurs. Après avoir trouvé les deux meilleures valeurs, la particule met à jour sa vitesse et ses positions à travers les équations (IV.19) et (IV.20).

$$v_{ij}^{(k+1)} = \mathrm{W} \times v_{ij}^{(k)} + c_1 r_1 \times (pbest_{ij} - x_{ij}^{(k)}) + c_2 r_2 \times (gbest_j - x_{ij}^{(k)}) \quad \text{(IV.19)}$$

$$x_{ij}^{(k+1)} = x_{ij}^{(k)} + v_{ij}^{(k+1)} \quad \text{(IV.20)}$$

Où :

- $x_{ij}^{(k)}$ est la particule actuelle (la solution) ;
- W est une constante, appelée « coefficient d'inertie » appartenant au segment [0 ; 1], généralement varie de 0,5 à 0,9 ;
- $v_{ij}^{(k)}$est la vitesse de la particule ;
- r_1, r_2 sont des nombres aléatoires appartenant au segment [0 ; 1] ;
- c_1, c_2 sont des facteurs d'apprentissage :
  - c_1 indique le degré de confiance de la particule elle-même,
  - c_2 indique le degré de confiance que la particule a sur ses voisins.
  - Leurs valeurs optimales sont trouvées empiriquement. Généralement, il est proposé que ces deux constantes d'accélération soient égales à la valeur 2 : $c_1 = c_2 = 2$;
- $pbest_{ij}$ et $gbest_j$ sont définis comme indiqué précédemment [161].

IV.5.2 Définition de la fonction de fitness (Fitness function)

Dans les méthodes de conception des contrôleurs PID, l'un des critères de performance les plus importants est l'erreur. L'utilisation de ce critère d'erreur comme fonction de fitness de l'algorithme d'optimisation entraîne un léger dépassement avec un temps de stabilisation long. En général, les fonctions de fitness sont basées sur des équations d'erreur. Les quatre équations suivantes : l'erreur quadratique intégrée (ISE), l'erreur absolue intégrée (IAE), l'erreur absolue de temps intégral (ITAE) et l'erreur

quadratique de pondération temporelle intégrée (ITSE) indiquent les fonctions de fitness les plus couramment utilisées [162] :

$$\text{ISE} = \int e(t)^2 . dt \tag{IV.21}$$

$$\text{IAE} = \int |e(t)| . dt \tag{IV.22}$$

$$\text{ITAE} = \int t . |e(t)| . dt \tag{IV.23}$$

$$\text{ITSE} = \int t . [e(t)^2] . dt \tag{IV.24}$$

Les fonctions de fitness ne sont pas réellement limitées aux équations ci-dessus. Les ingénieurs peuvent fournir des fonctions de fitness personnalisées en fonction de la conception de la cible et du système de contrôle. Les performances globales (vitesse de convergence et précision d'optimisation) des algorithmes évolutifs dépendent de la fonction de fitness adoptée pour suivre la recherche d'optimisation.

Dans notre étude, nous utilisons trois types d'optimisation :

- Optimisation PSO mono-objectif en utilisant une fonction de fitness F monocritère.
- Optimisation PSO multi-objectifs Pareto en utilisant une fonction de fitness F multicritères de coefficients de pondération égaux. Selon l'approche d'agrégation de l'équation (IV.25), une combinaison des fonctions à optimiser f_i est obtenue.

$$\text{F} = \sum_{i=1}^{n} w_i f_i \ (x) \tag{IV.25}$$

Avec : w_i le coefficient de pondération relatif à la fonction objectif « f_i ».

Les coefficients de pondération relatifs à n fonctions objectifs sont égaux : $w_1 = w_2 = \ldots = w_n$ et $\sum_i^n w_i = 1$.

- Optimisation PSO multi-objectifs non Pareto en utilisant une fonction de fitness F multicritère de coefficients de pondération distincts, c'est-à-dire $w_1 \neq w_2 \neq \ldots \neq w_n$ où w_i est choisi aléatoirement $0 \leq w_i < 1$ et $\sum_i^n w_i = 1$ [154].

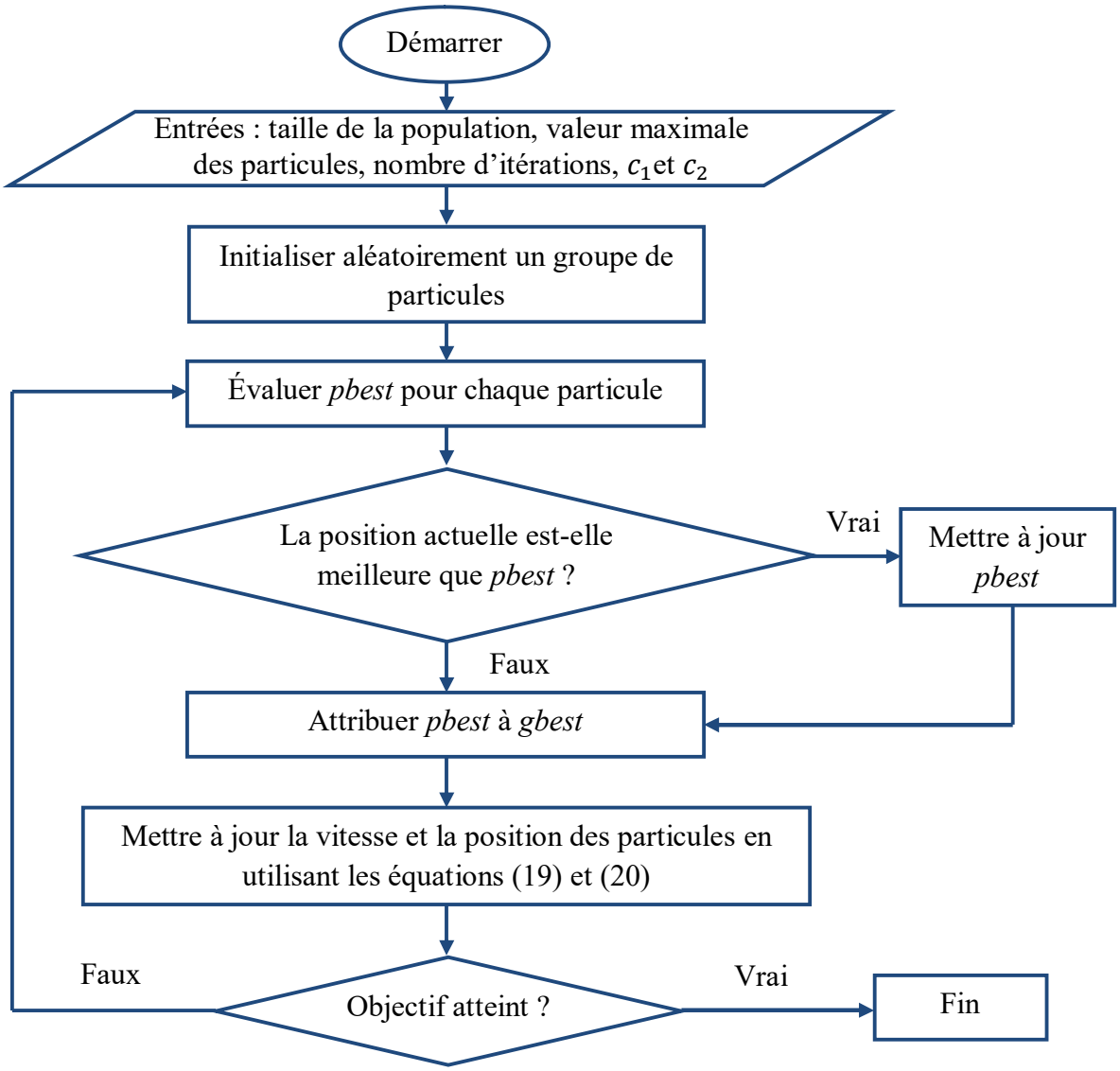


Figure IV.8 Les différentes étapes de l'algorithme d'optimisation de l'essaim de particules

Les paramètres de simulation sélectionnés pour l'algorithme PSO sont définis dans le tableau IV.1 comme suit :

Tableau IV.1 Paramètres d'entrées pour la simulation de l'algorithme PSO

Paramètres d'entrée	**Valeurs**
Nombre d'itérations	iter = de 10 à 50
Taille de la population (de l'essaim)	N = de 10 à 50

IV.6 Simulation et expérimentations

Le but de la simulation et de l'expérimentation est ici d'étudier l'efficacité et les performances du contrôleur non linéaire cinématique proposé, celui-ci étant basé sur l'application de l'algorithme d'optimisation PSO en un robot mobile différentiel à deux roues de type Turtlebot2. L'algorithme a été développé sous l'environnement Matlab™/Simulink (voir la figure IV.9). Une simulation sous le logiciel Gazebo a été effectuée et un ensemble d'expérimentations ont été réalisées sur le robot réel Turtlebot2 en prenant en compte différents types de trajectoires.

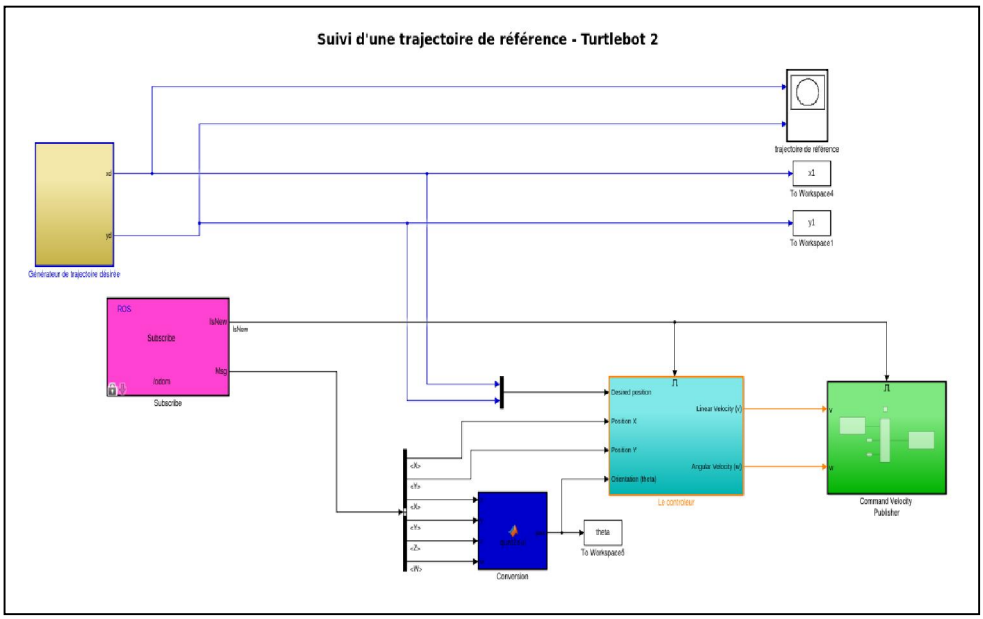


Figure IV.9 Modélisation sous Simulink du suivi de trajectoire

IV.6.1 Protocole et matériels

Afin de contrôler la base Kobuki du robot Turtlebot2 à distance, à travers un ordinateur dénommé ici « Workstation » de type Windows, nous devons créer une relation de type « Maître-Esclave » entre la Workstation et le netbook du robot (muni du système d'exploitation Ubuntu/ROS).

IV.6.1.1 Création d'une relation Maître/Esclave

Afin de créer cette relation entre les deux ordinateurs, ceux-ci doivent être définis sur le même réseau. La Workstation doit être identifiée en tant que Maître (nœud « master » dans la terminologie de ROS) à partir de Matlab. Nous pouvons alors créer un nœud ROS global qui communique avec le nœud ROS du netbook de chaque robot Turtlebot2.

IV.6.1.2 Publication des vitesses

Afin de contrôler le robot Turtlebot2 à distance, nous devons nous enregistrer en tant qu'éditeur (terminologie « publisher » sous ROS) sur le topic de commande des vitesses à l'aide du block Simulink de la figure IV.10 et créer un message au format utilisé par ce topic. Enfin, nous devons envoyer les valeurs de vitesses par message. Les vitesses réglables sur le robot Turtlebot2 sont *la vitesse linéaire X* et *la vitesse angulaire Z*, lui permettant ainsi d'avancer et de tourner.

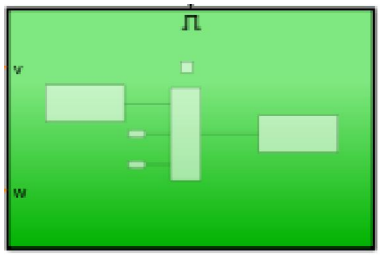


Figure IV.10 Bloc Simulink permettant la publication sous ROS

IV.6.1.3 Acquisition des données des capteurs

Pour acquérir les données des capteurs (odomètre, gyroscope...) à distance via Matlab, nous devons nous inscrire (terminologie « subscriber » sous ROS) sur le topic d'odométrie en tant qu'abonné à l'aide du bloc Simulink de la figure IV.11.

Figure IV.11 Bloc Simulink permettant de souscrire sous ROS

IV.6.1.4 Utilisation du logiciel de simulation Gazebo

Gazebo est un simulateur robotique tridimensionnel pour les environnements de types indoor ou outdoor. Il est capable de simuler une population de robots, de capteurs et d'objets. Il génère à la fois un retour de capteur réaliste et des interactions physiquement plausibles entre les objets (il comprend une simulation précise de la physique des corps rigides). En simulant de manière réaliste des robots et des environnements, le code conçu pour faire fonctionner un robot physique peut être exécuté sur une version artificielle. De nombreux chercheurs ont également utilisé Gazebo pour développer et exécuter des expériences uniquement dans un environnement simulé. La simulation orchestrée par Gazebo peut être considérée comme une copie expérimentale d'un robot réel dans un monde virtuel [163].

Dans notre travail, avant de passer à l'expérimentation et à l'implémentation sur le robot réel, nous nous proposons d'implémenter la loi de commande sur le robot Turtlebot2 simulé dans « Gazebo World » pour la simulation en trois dimensions. Les deux versions du robot Turtlebot2 (simulée et réelle) sont présentées sur la figure IV.12. Une description succincte du robot Turtlebot2 est fournie en annexe.

Figure IV.12 Robot Turtlebot2 simulé en trois dimensions sous Gazebo (à gauche) – Robot réel (à droite)

IV.6.2 Partie simulation

Dans ce qui suit, nous présentons les résultats obtenus à partir de simulations basées sur différentes formes de trajectoires de référence illustrées sur la figure IV.13.

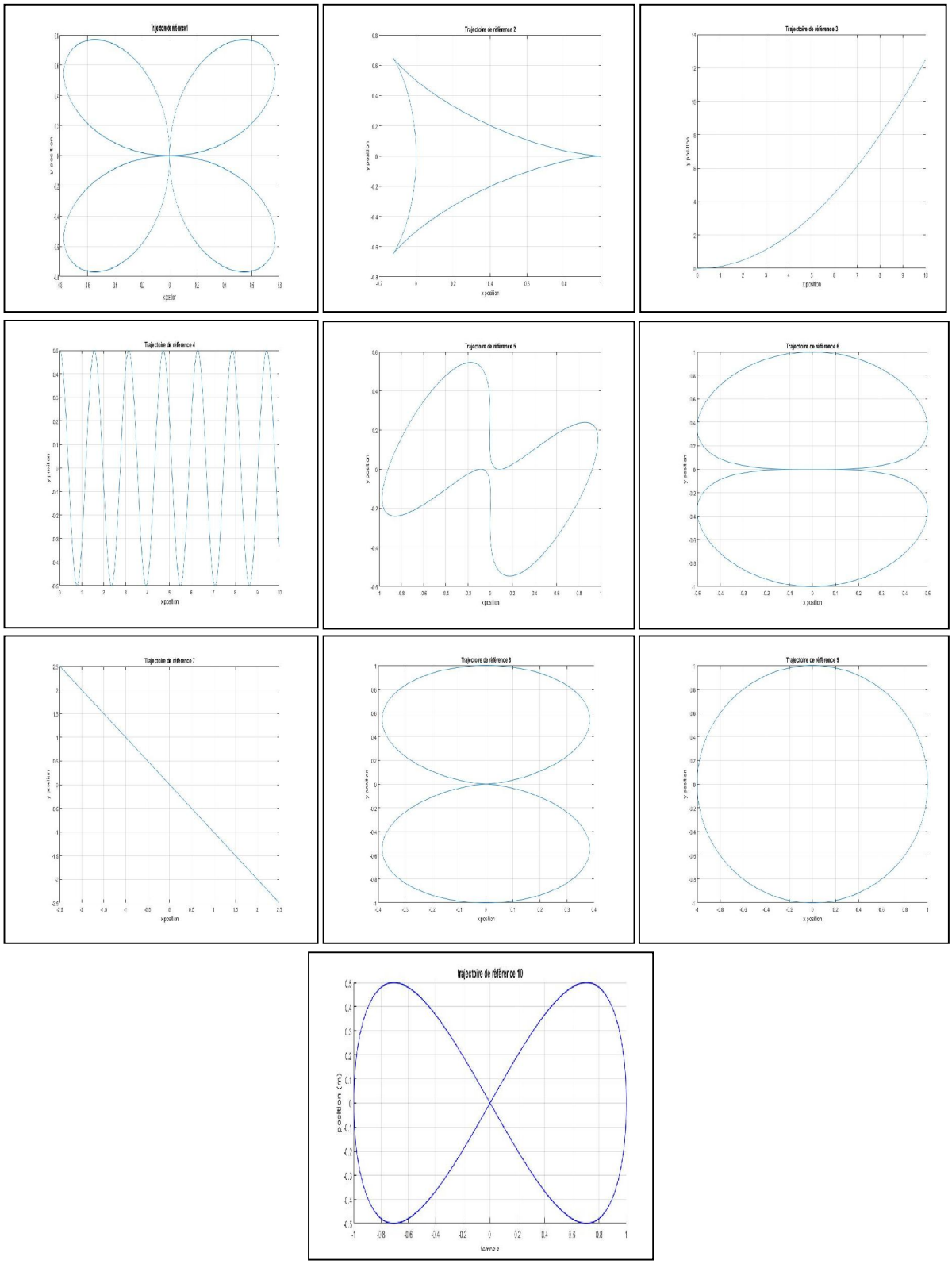


Figure IV.13 Différentes trajectoires de référence

IV.6.2.1 Résultats de simulation

Nous proposons d'exécuter cinq formules d'erreur pour différentes configurations d'itérations afin d'évaluer la performance des fonctions de fitness et de trouver les meilleurs paramètres de simulation, avec une durée de simulation totale de 20 secondes.

Avec :

- *T1* le temps d'optimisation ;
- *G* la fonction de gain.

Les simulations ont été réalisées avec la trajectoire de référence 2.

1- Simulation selon la fonction IAE, où : F 1=sum(abs(e(2,:)))

Tableau IV.2 Résultats de simulation pour la fonction IAE

N	***iter***	***Kp***	***Ko***	***T1***	***G***	e_p	e_o
10	10	43.1679	15.9838	436.4424	296.8823	0.006356	0.008417
20	20	89.2852	23.6772	1.6162e+03	143.3313	0.002881	0.004423
40	40	100	61.7625	7.0800e+03	126.8477	0.002555	0.003087
50	50	100	72.7369	1.0224e+04	126.8387	0.002555	0.002891

2- Simulation selon la fonction ISE, où : F 2=sum(e(2,:).*e(2,:))

Tableau IV.3 Résultats de simulation pour la fonction ISE

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
10	10	82.0693	15.1113	432.8688	7.4103	0.008358	0.005154
20	20	97.8299	12.0378	1.6344e+03	5.2281	0.007034	0.004551
40	40	100	34.3553	6.2320e+03	4.9703	0.006884	0.003721
50	50	100	74.3589	9.8445e+03	4.9634	0.006884	0.002867

3- Simulation selon la fonction ITAE, où : F 3=sum(t(2,:).*abs(e(2,:)))

Tableau IV.4 Résultats de simulation pour la fonction ITAE

N	***iter***	***Kp***	***Ko***	***T1***	***G***	e_p	e_o
10	10	49.2856	5.5698	974.9977	6.2257e+03	0.005889	-2.783
20	20	85.4699	4.1495	3.7489e+03	3.5833e+03	0.003057	-2.988
40	40	100	45.7209	1.4816e+04	3.0603e+03	0.002555	0.003428
50	50	100	89.0859	2.2572e+04	3.0596e+03	0.002555	0.00264

4- Simulation selon la fonction ITSE, où : F 4= sum (t(2,:) .*e(2,:) .*e(2,:))

Tableau IV.5 Résultats de simulation pour la fonction ITSE

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
10	10	38.9352	13.3800	943.6091	65.9671	0.007139	0.009512
20	20	100	30.4910	3.7567e+03	9.9092	0.002555	0.003829
40	40	99.0787	31.2165	1.4839e+04	10.0924	0.002580	0.003835
50	50	100	100	2.2702e+04	9.8957	0.002555	0.002496

5- Simulation selon la fonction MO Pareto, où : $F5_1$=0.25*(F1+F2+F3+F4)

Tableau IV.6 Résultats de simulation pour la fonction MO Pareto

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
10	10	49.6503	1.0633	420.3797	714.4240	0.01364	0.00986
20	20	98.4095	1.6997	1.5940e+03	356.5796	0.006993	0.004995
40	40	100	48.8846	6.7980e+03	350.1810	0.006884	0.003358
50	50	100	1.6768	9.5865e+03	350.8462	0.006884	0.004918

6- Simulation selon la fonction MO non Pareto

Où : $F5_2$=w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.2148 ; w2 = 0.6371 ; w3 = 0.0644 ; w4 = 0.0837.

Tableau IV.7 Résultats de simulation pour la fonction MO non Pareto $F5_2$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
10	10	53.0999	12.0962	423.3855	3.8185e+03	0.01278	0.007711
20	20	100	3.6028	1.9967e+03	2.0218e+03	0.006884	0.004826
40	40	100	52.5954	6.0430e+03	2.0201e+03	0.006884	0.003276
50	50	100	31.6590	9.1365e+03	2.0204e+03	0.006884	0.003798

7- Simulation selon la fonction MO non Pareto

Où : $F5_3$= w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.1323 ; w2 = 0.4492 ; w3 = 0.2634 ; w4 = 0.1551.

Tableau IV.8 Résultats de simulation pour la fonction MO non Pareto $F5_3$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	89.2851	1.1593e+04	585.6219	0.006883	0.002641

8- Simulation selon la fonction MO non Pareto

Où : $F5_4$=w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.3407 ; w2 = 0.1135 ; w3 = 0.1678 ; w4 = 0.3780.

Tableau IV.9 Résultats de simulation pour la fonction MO non Pareto $F5_4$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	2.2838	1.1613e+04	191.2640	0.006883	0.004888

9- Simulation selon la fonction MO non Pareto

Où : $F5_5$=w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.1800 ; w2 = 0.1680 ; w3 = 0.0232 ; w4 = 0.6287.

Tableau IV.10 Résultats de simulation pour la fonction MO non Pareto $F5_5$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	1.6642	1.0465e+04	241.7294	0.006883	0.004918

10- Simulation selon la fonction MO non Pareto

Où : $F5_6$= w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.2081 ; w2 = 0.3524 ; w3 = 0.2456 ; w4 = 0.1939.

Tableau IV.11 Résultats de simulation pour la fonction MO non Pareto $F5_6$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	87.0321	1.0438e+04	473.4081	0.006883	0.002673

11- Simulation selon la fonction MO non Pareto

Où : $F5_7$=w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.3659 ; w2 = 0.0828 ; w3 = 0.4586 ; w4 = 0.0926.

Tableau IV.12 Résultats de simulation pour la fonction MO non Pareto $F5_7$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	66.9673	1.0439e+04	152.3079	0.006883	0.002994

12- Simulation selon la fonction MO non Pareto

Où : $F5_8$=w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.3125 ; w2 = 0.1875 ; w3 = 0.3125 ; w4 = 0.1875.

Tableau IV.13 Résultats de simulation pour la fonction MO non Pareto $F5_8$

N	*iter*	*Kp*	*Ko*	*T1*	*G*	e_p	e_o
50	50	100	74.2149	1.0429e+04	278.4948	0.006883	0.002869

13- Simulation selon la fonction MO non Pareto

Où : $F5_9$ = w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.125 ; w2 = 0.375 ; w3 = 0.125 ; w4 = 0.375.

Tableau IV.14 Résultats de simulation pour la fonction MO non Pareto $F5_9$

N	***iter***	***Kp***	***Ko***	***T1***	***G***	e_p	e_o
50	50	100	1.2107	4.0158e+04	493.5986	0.006883	0.004940

14- Simulation selon la fonction MO non Pareto

Où : $F5_{10}$ =w1*F1+w2*F2+w3*F3+w4*F4 avec : w1 = 0.375 ; w2 = 0.125 ; w3 = 0.375 ; w4 = 0.125.

Tableau IV.15 Résultats de simulation pour la fonction MO non Pareto $F5_{10}$

N	***iter***	***Kp***	***Ko***	***T1***	***G***	e_p	e_o
50	50	100	2.3278	1.0593e+04	207.9258	0.006883	0.004886

Temps total de simulation : 20 secondes.

Rassemblons les meilleurs résultats obtenus à partir de la simulation dans le tableau IV.16 :

Tableau IV.16 Tableau récapitulatif des meilleurs résultats obtenus par simulation

La fonction de fitness	*N*	*iter*	*Kp*	*Ko*	*T1*	*G*	*Valeur moyenne* e_p	*Valeur moyenne* e_o
F1=sum(|e|) IAE	50	50	100	53.4293	1.7219e+04	130.98	0.0102	6.5e-05
	50	50	100	72.7369	1.0224e+04	126.8387	0.0102	5.5955e-05
F2=sum(e^2) ISE	50	50	100	74.3589	9.8445e+03	4.9634	0.0102	5.5434e-05
F3=sum(t*|e|) ITAE	50	50	100	89.0859	2.2572e+04	3.0596e+03	0.0102	5.1117e-05
F4=sum(t*e^2) ITSE	50	50	100	100	2.2702e+04	9.8957	0.0102	4.8328e-05
$F5_3$ = sum(w_i*F_i) i =1…4, w1 = 0.1323, w2 = 0.4492, w3 = 0.2634, w4 = 0.1551.	50	50	100	89.2851	1.1593e+04	585.6219	0.0102	5.1063e-05

Le tableau IV.17 suivant montre les différentes valeurs des erreurs de distance et de direction obtenues pour chaque trajectoire de référence selon différents critères d'optimisation (ITSE, ITAE, ISE, IAE et F5).

Tableau IV.17 Tableau récapitulatif des résultats de simulation pour chaque trajectoire

IAE PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
***Kp* =100**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0154	0.0197	0.0064	-0.0239	0.1259	9.9782e-05	0.0169	8.3924e-04	0.0089	0.0066
***Ko* =53.4293**	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	6.2997e-05	0.0450	0.0015	0.0088	-0.0047	0.0101	0.0066	0.0097	3.6808e-05
IAE PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
***Kp* = 100**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0154	0.0175	0.0064	-0.0206	0.1259	8.8632e-05	0.0169	-2.5958e-05	0.0089	0.0058
***Ko* =72.7369**	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	5.5955e-05	0.0456	0.0088	0.0088	-0.0285	0.0101	0.0059	0.0097	-2.7660e-04
ISE PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
***Kp* = 100**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0154	0.0177	0.0064	-0.0592	0.1259	8.7807e-05	0.0171	0.0017	0.0090	0.0058
***Ko* =74.3589**	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	5.5434e-05	0.0456	0.0088	0.0088	-0.0037	0.0101	0.0058	0.0097	-2.7395e-04
ITAE PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
***Kp* = 100**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0154	0.0160	0.0064	-0.0207	0.1259	8.0970e-05	0.0169	8.3043e-06	0.0089	0.0053
***Ko* =89.0859**	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	5.1117e-05	0.0450	0.0042	0.0088	-0.0045	0.0101	0.0054	0.0097	-2.7395e-04

F5 PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
***Kp* = 100**	0.0154	0.0160	0.0064	-0.0207	0.1259	8.0885e-05	0.0169	8.5612e-06	0.0089	0.0053
	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
***Ko* = 89.2851**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	5.1063e-05	0.0450	0.0042	0.0088	-0.0045	0.0101	0.0054	0.0097	-2.4896e-04
ISTE PSO	Trajectoire de référence 1		Trajectoire de référence 2		Trajectoire de référence 3		Trajectoire de référence 4		Trajectoire de référence 5	
	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
***Kp* = 100**	0.0154	0.0152	0.0064	-0.0207	0.1259	7.6553e-05	0.0169	2.0557e-05	0.0089	0.0051
	Trajectoire de référence 6		Trajectoire de référence 7		Trajectoire de référence 8		Trajectoire de référence 9		Trajectoire de référence 10	
***Ko* = 100**	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o	e_p	e_o
	0.0102	4.8328e-05	0.0450	0.0042	0.0088	-0.0050	0.0101	0.0051	0.0097	-2.3163e-04

IV.6.2.2 Discussion et comparaison des résultats de simulation

Nous constatons que l'optimisation des paramètres du contrôleur PID avec l'algorithme PSO, en prenant en compte différentes trajectoires, a donné des résultats très satisfaisants, que ce soit par rapport à l'erreur de position (précision) ou par rapport à l'erreur d'orientation.

Nous pouvons également conclure que, quel que soit le critère d'optimisation utilisé (ISTE, ITAE, ISE, IAE ou F5), les meilleurs résultats par rapport aux deux erreurs (position et orientation) sont obtenus avec les trajectoires de référence 5 et 8.

Les résultats obtenus dans le cadre de ce travail sont nettement meilleurs comparativement aux résultats obtenus par Wehbi [150] (PID classique, avec une erreur autour de10^{-2}).

IV.6.3 Partie simulation sous Gazebo

Pour Te = 0.001 seconde, les résultats obtenus sont illustrés sur les figures suivantes :

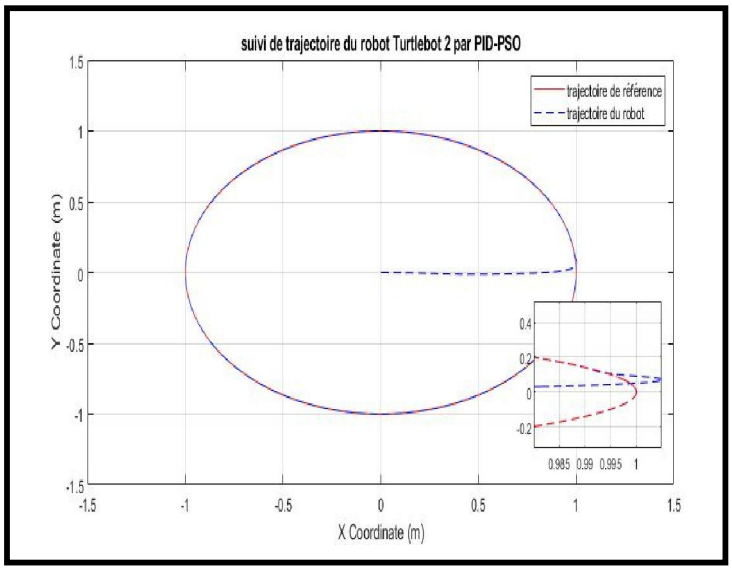


Figure IV.14 Trajectoire de référence et trajectoire de sortie

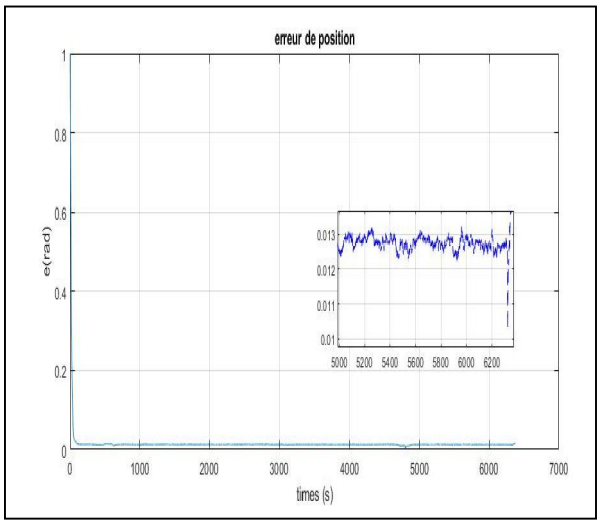


Figure IV.15 Erreur de position

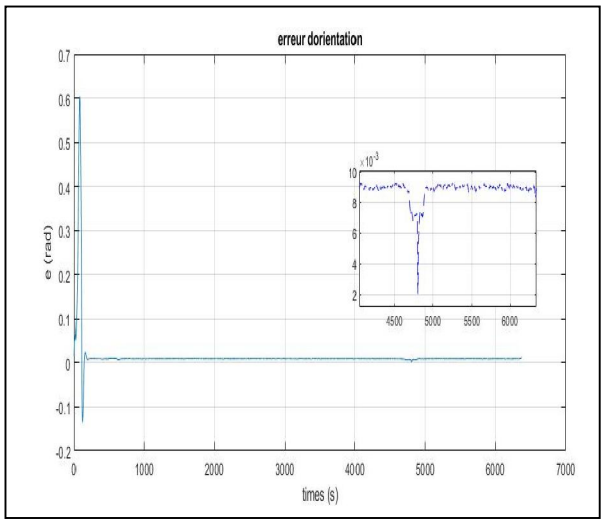


Figure IV.16 Erreur d'orientation

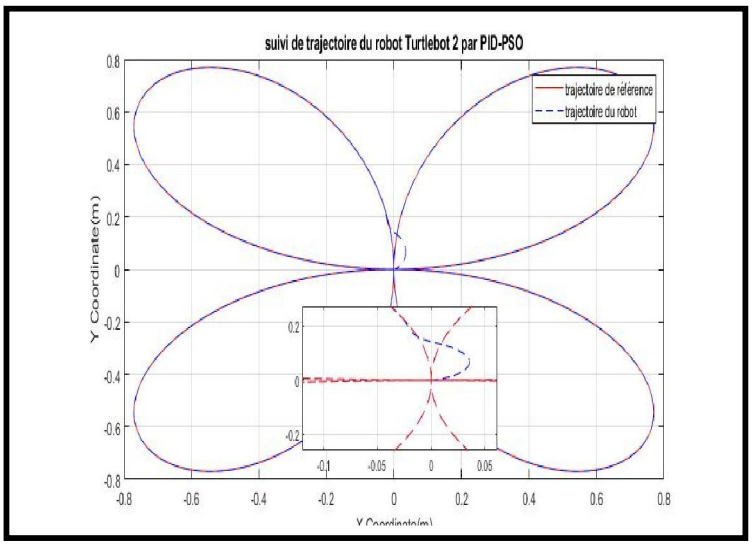


Figure IV.17 Trajectoire de référence et trajectoire de sortie

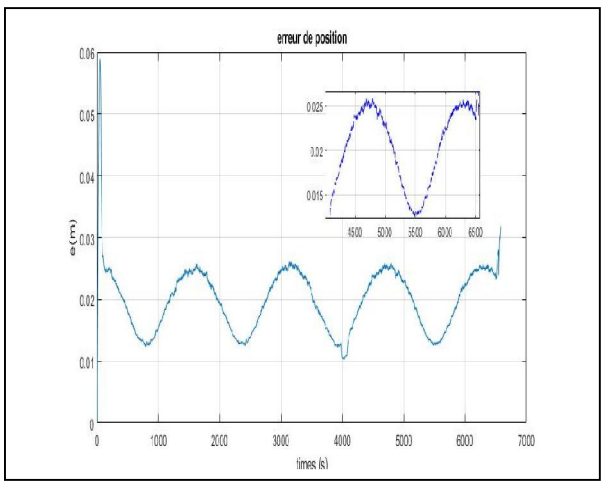


Figure IV.18 Erreur de position

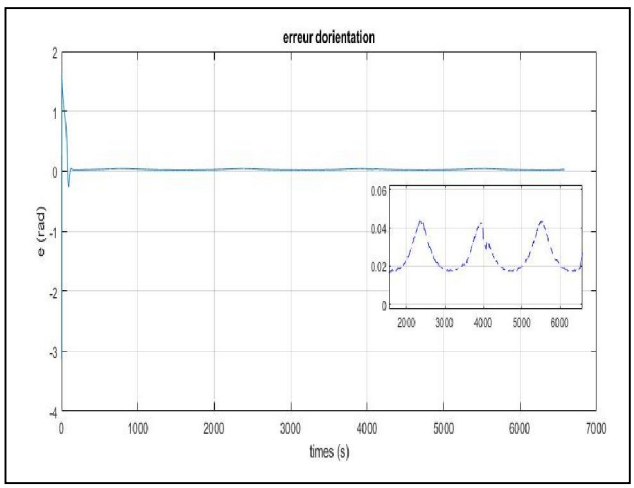


Figure IV.19 Erreur d'orientation

Pour Te=0.01 seconde :

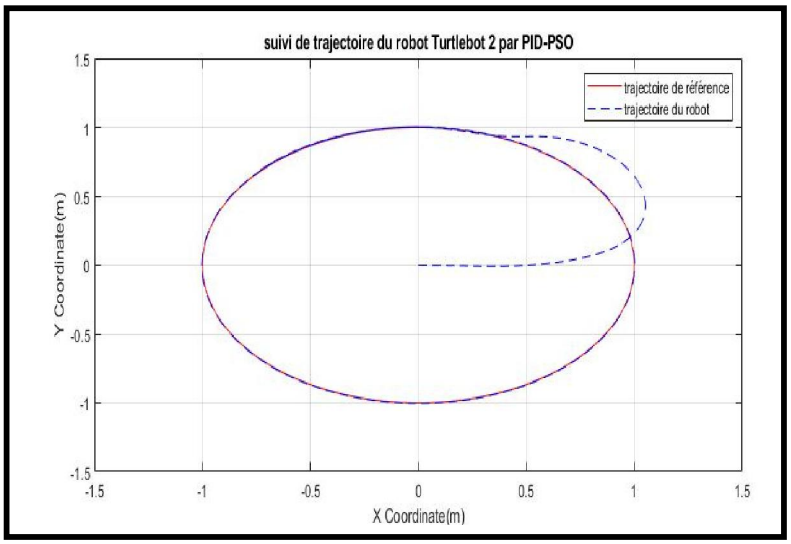


Figure IV.20 Trajectoire de référence et trajectoire de sortie

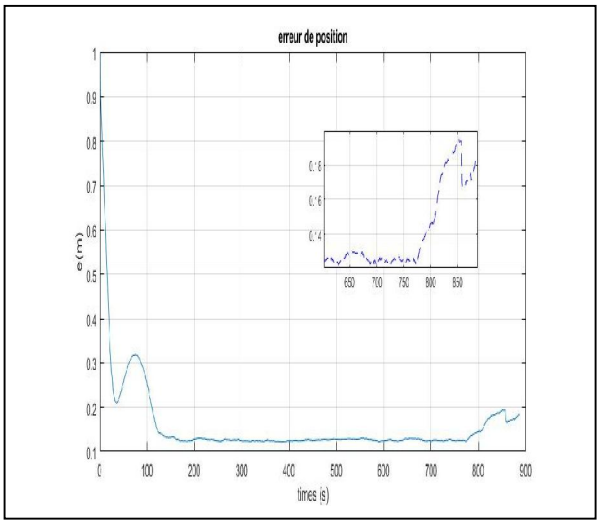


Figure IV.21 Erreur de position

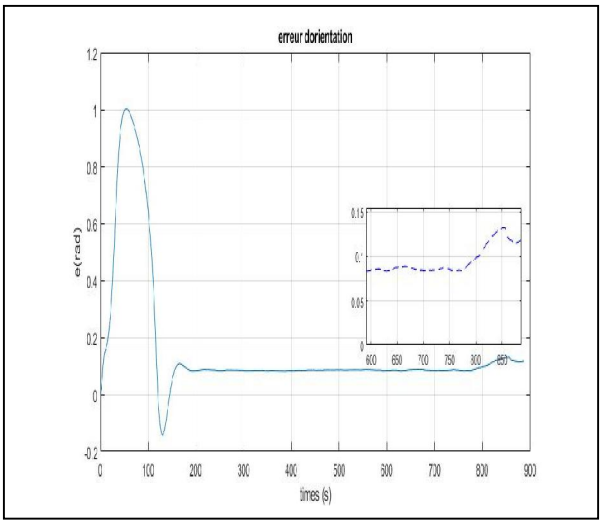


Figure IV.22 Erreur d'orientation

Remarquons que les erreurs de position et d'orientation sont nettement diminuées quelle que soit la trajectoire (entre 10^{-2} et 10^{-3}). Avec une période Te = 10^{-3} seconde, le suivi est nettement amélioré suite à l'optimisation des paramètres du contrôleur, obtenue avec l'algorithme PSO.

IV.6.4 Résultats d'expérimentations

Dans ce qui suit, nous présentons la partie expérimentale développée en prenant en compte les différentes formes de trajectoires illustrées sur la figure IV.13.

Le tableau ci-dessous montre les paramètres optés pour la simulation :

Tableau IV.18 Paramètres de simulation utilisés pour l'expérimentation

Paramètres	K_P	K_o	Te	Fonction
Algorithme PSO	1	0.5343	0.01/0.001/ 0.0001/0.005	Différentes fonctions

Les résultats expérimentaux en utilisant différentes périodes d'échantillonnages sont illustrés sur les figures ci-dessous :

Pour une période d'échantillonnage Te = 0.0001 seconde :

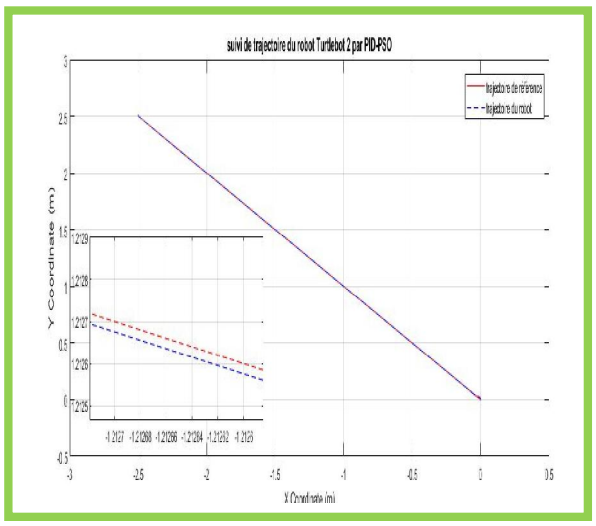


Figure IV.23 Trajectoire de référence et trajectoire de sortie

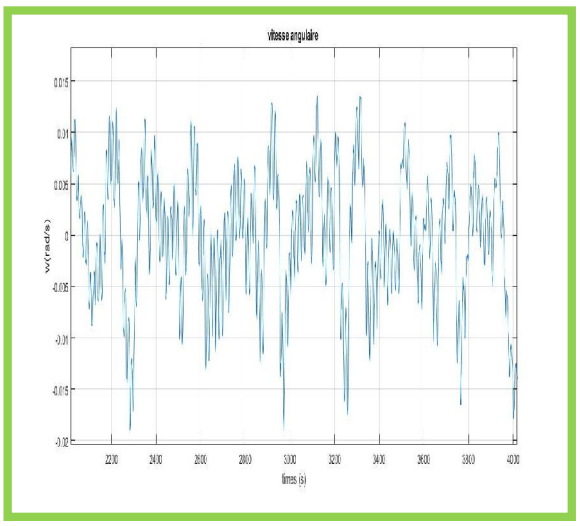


Figure IV.24 Vitesse angulaire en fonction du temps

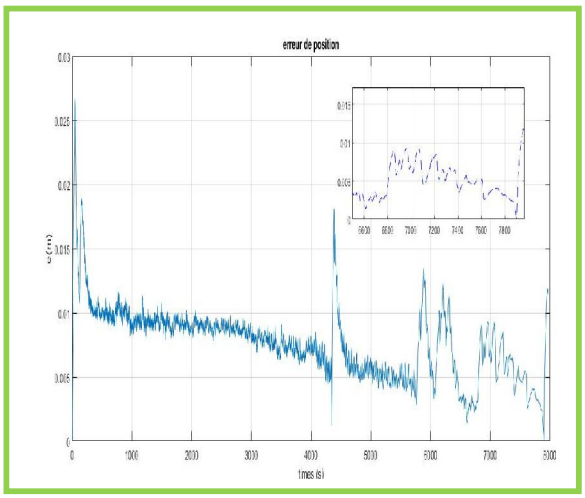


Figure IV.25 Erreur de position

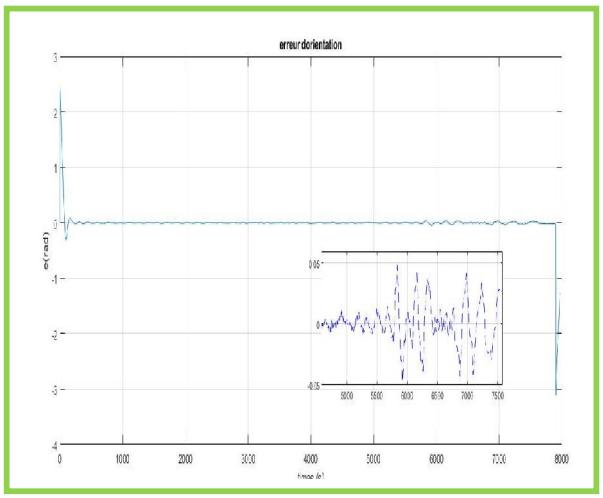


Figure IV.26 Erreur d'orientation

Pour une période d'échantillonnage Te = 0.001 seconde :

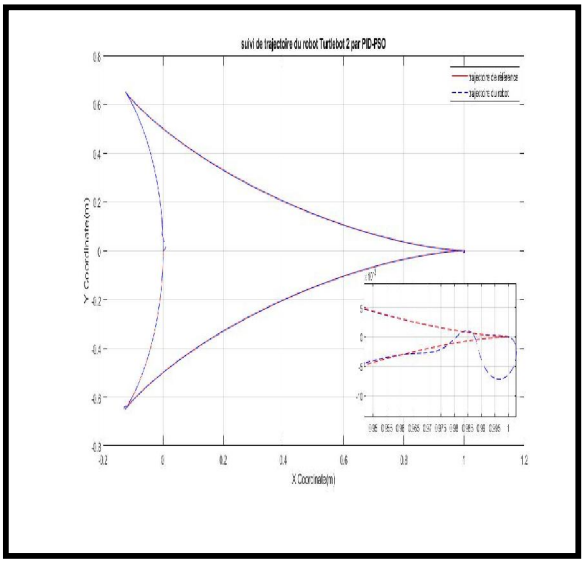


Figure IV.27 Trajectoire de référence et trajectoire de sortie

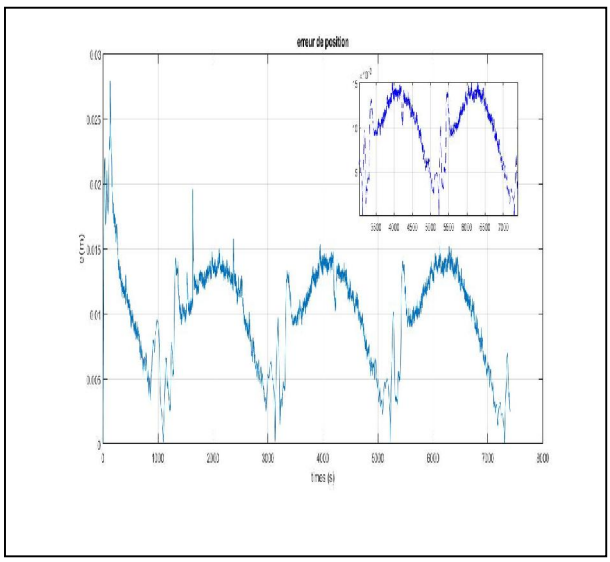


Figure IV.28 Erreur de position

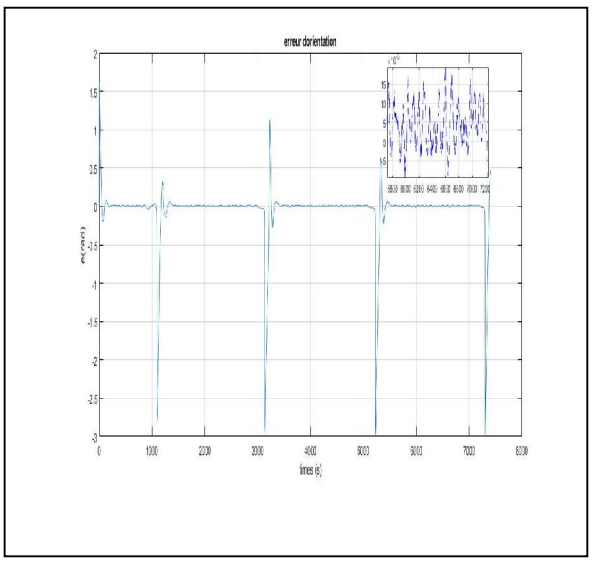


Figure IV.29 Erreur d'orientation

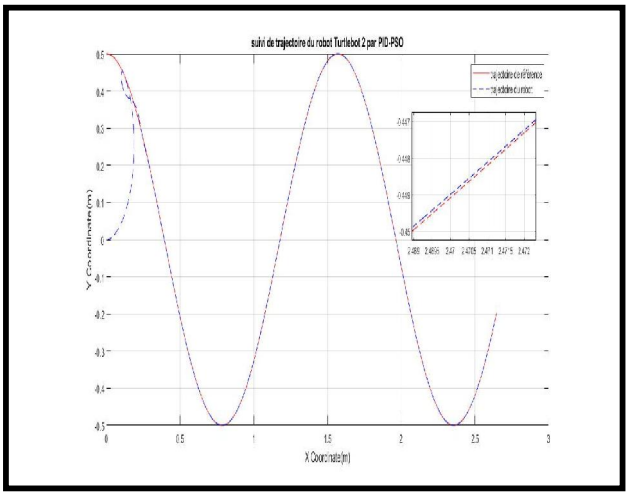


Figure IV.30 Trajectoire de référence et trajectoire de sortie

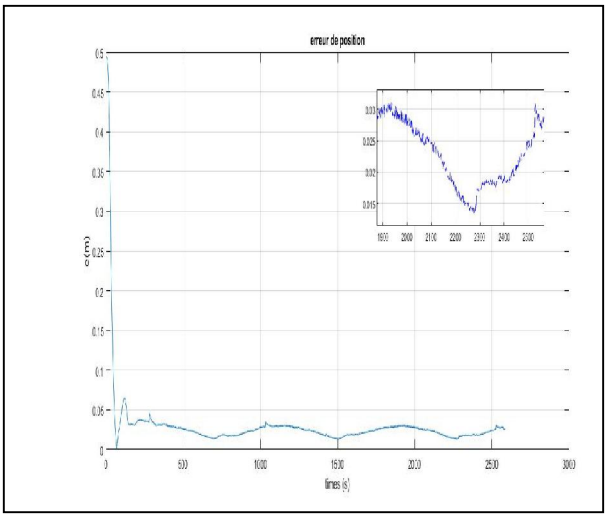


Figure IV.31 Erreur de position

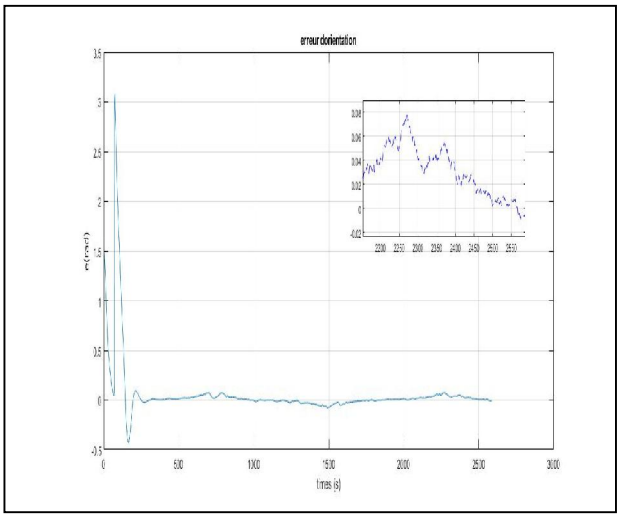


Figure IV.32 Erreur d'orientation

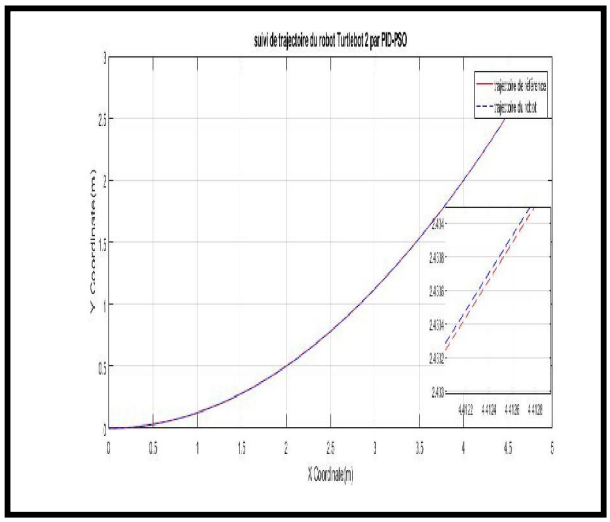


Figure IV.33 Trajectoire de référence et trajectoire de sortie

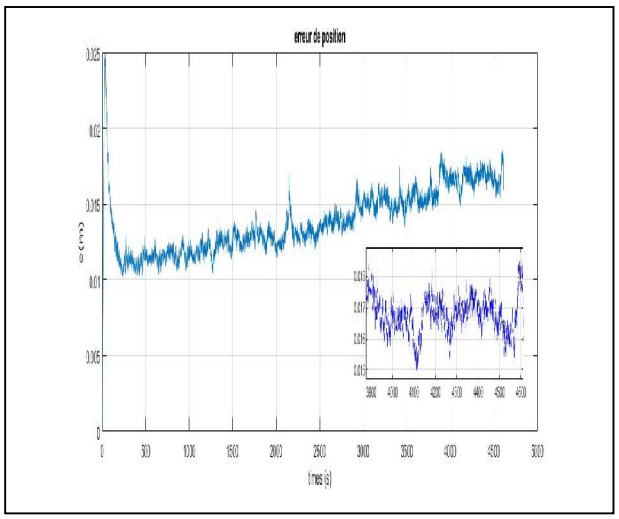


Figure IV.34 Erreur de position

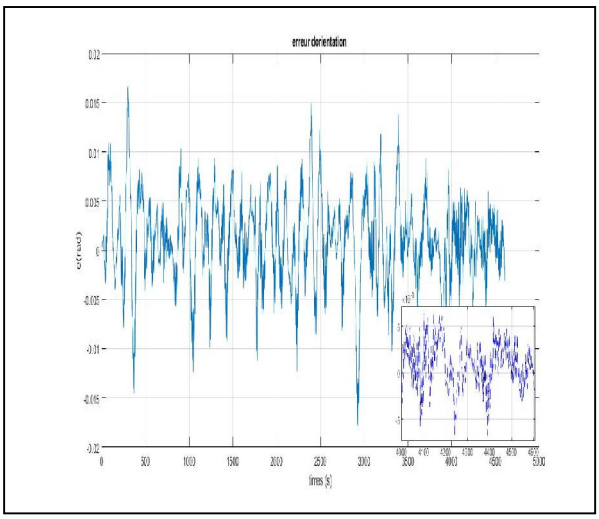


Figure IV.35 Erreur d'orientation

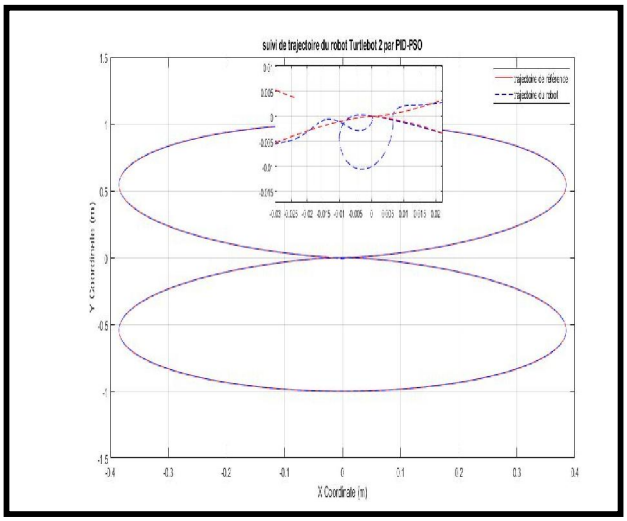


Figure IV.36 Trajectoire de référence et trajectoire de sortie

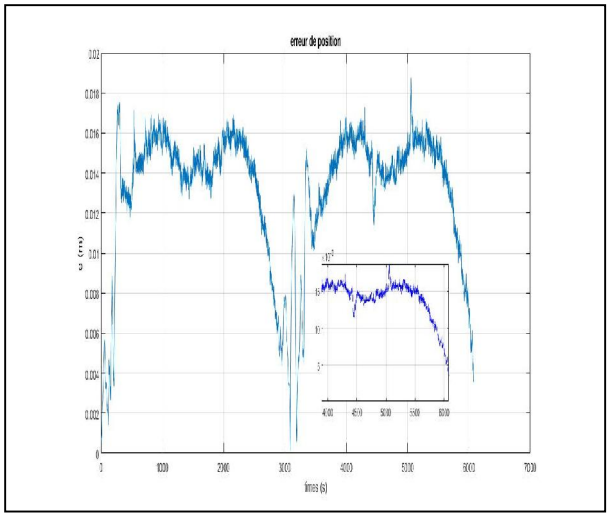


Figure IV.37 Erreur de position

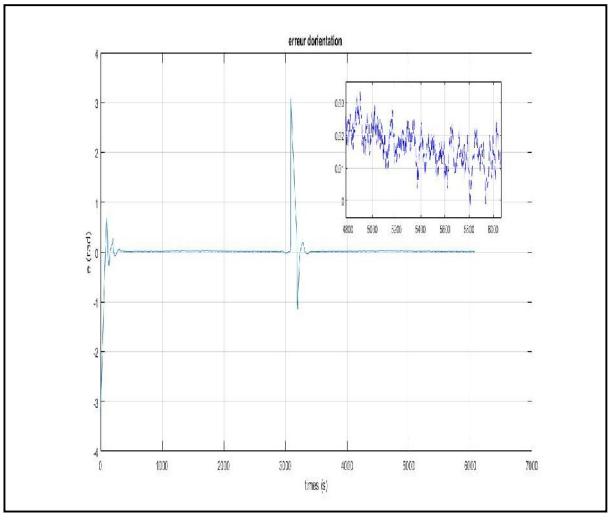


Figure IV.38 Erreur d'orientation

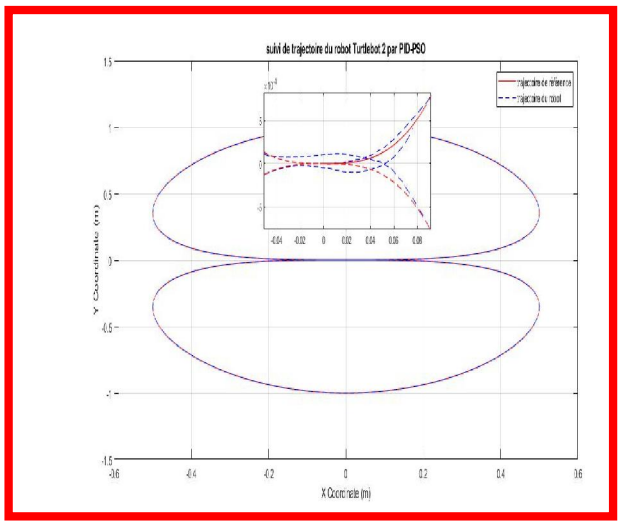


Figure IV.39 Trajectoire de référence et trajectoire de sortie

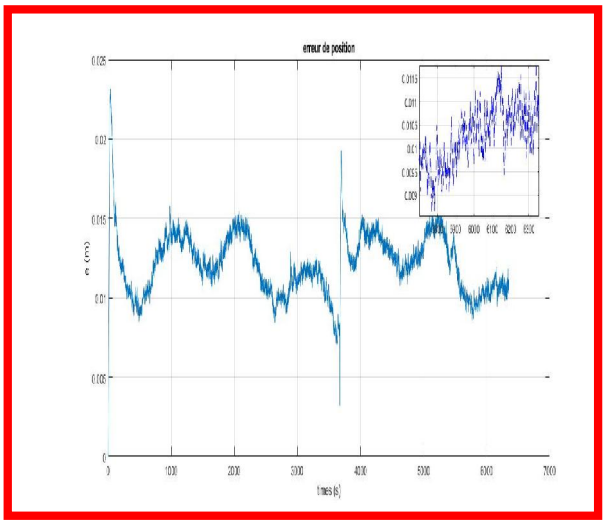


Figure IV.40 Erreur de position

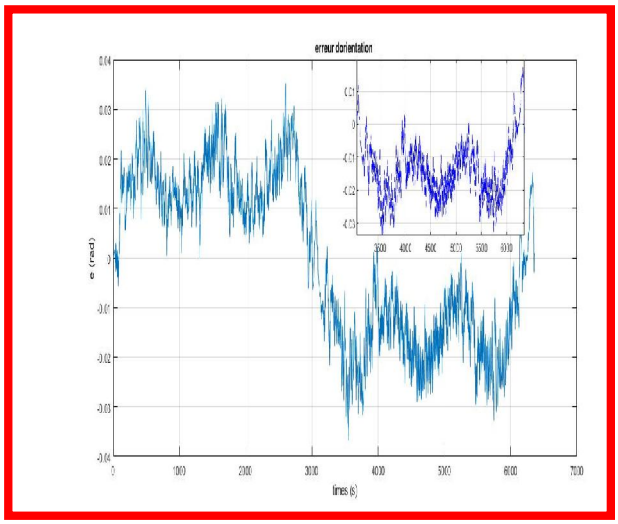


Figure IV.41 Erreur d'orientation

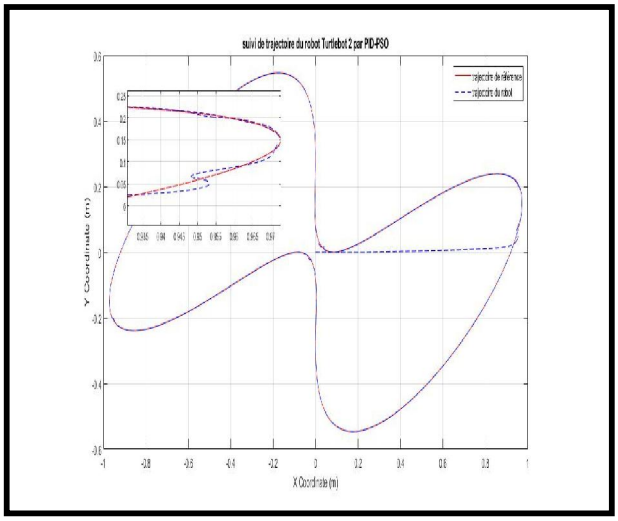


Figure IV.42 Trajectoire de référence et trajectoire de sortie

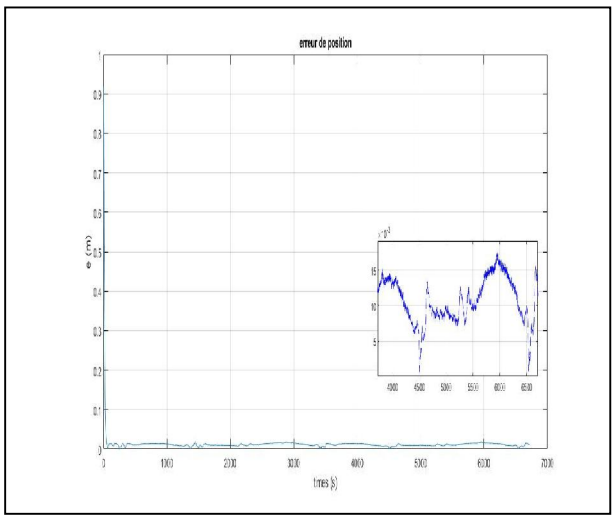


Figure IV.43 Erreur de position

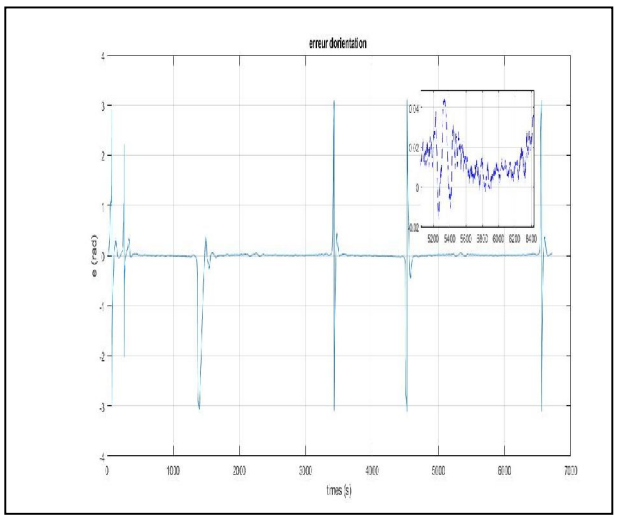


Figure IV.44 Erreur d'orientation

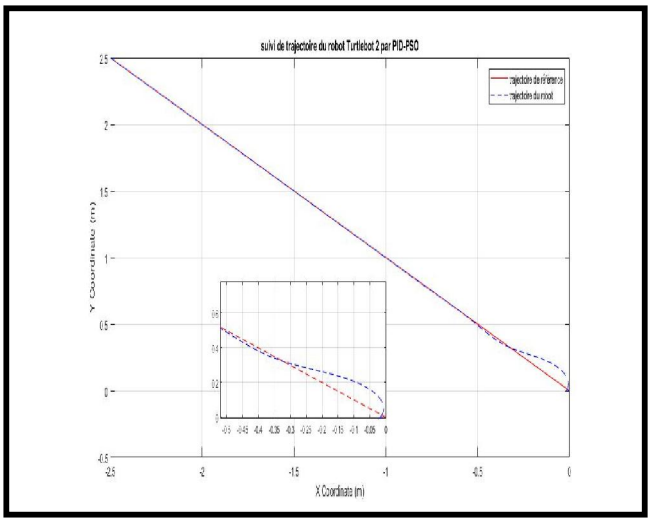


Figure IV.45 Trajectoire de référence et trajectoire de sortie

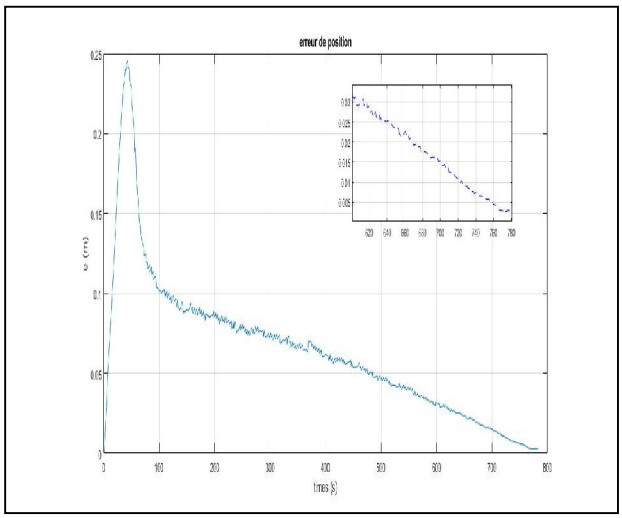


Figure IV.46 Erreur de position

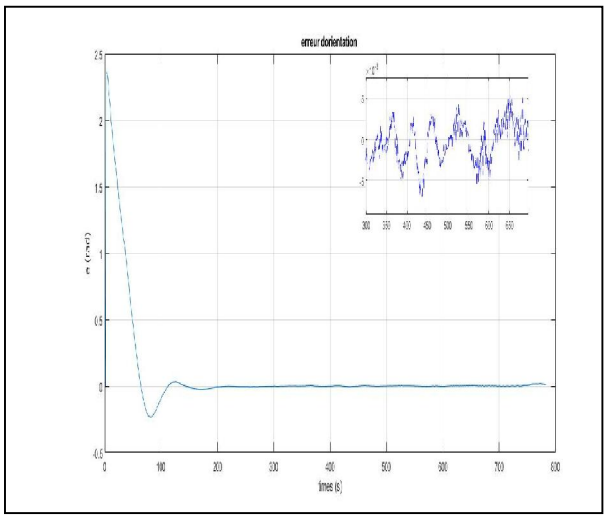


Figure IV.47 Erreur d'orientation

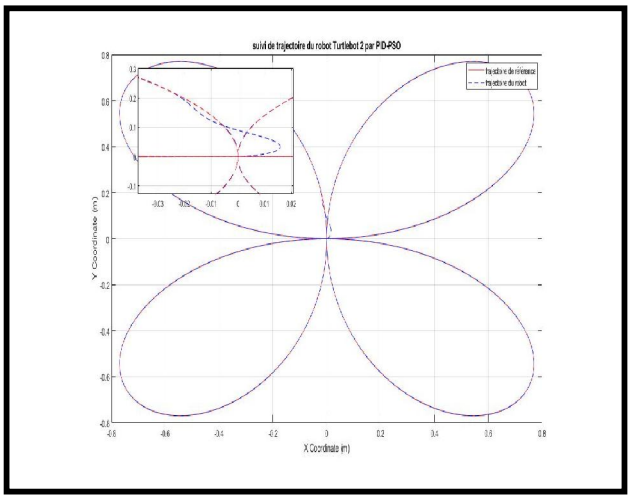


Figure IV.48 Trajectoire de référence et trajectoire de sortie

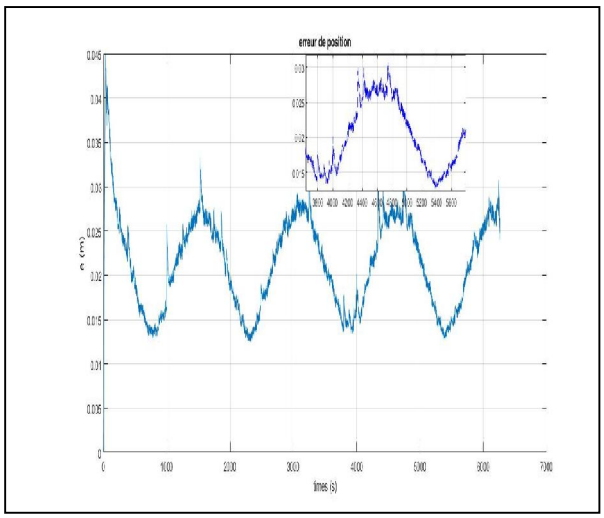


Figure IV.49 Erreur de position

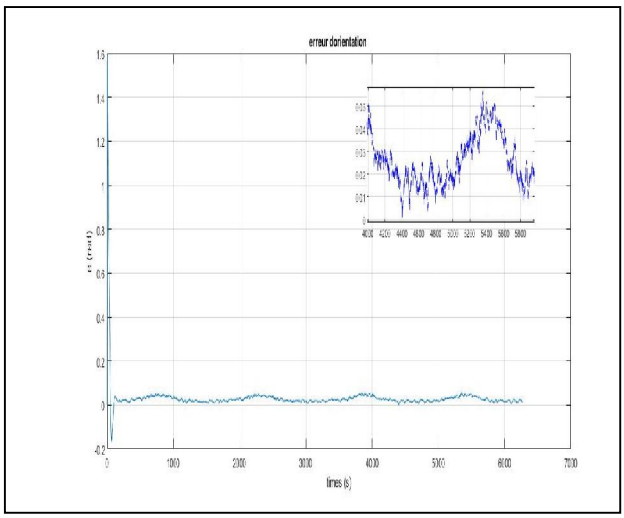


Figure IV.50 Erreur d'orientation

Pour une période d'échantillonnage Te = 0.01 seconde :

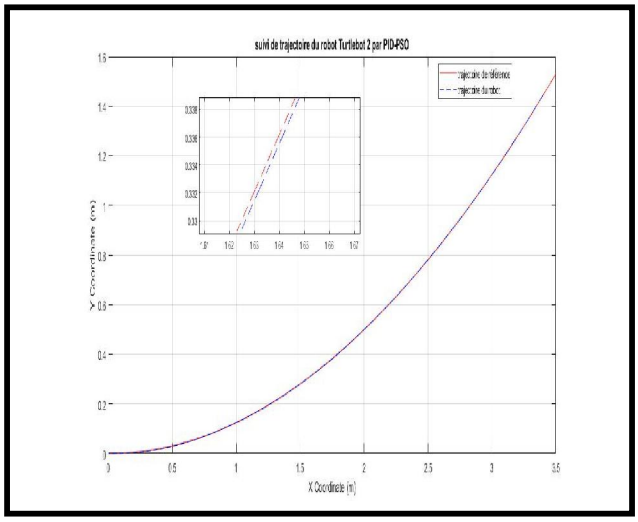


Figure IV.51 Trajectoire de référence et trajectoire de sortie

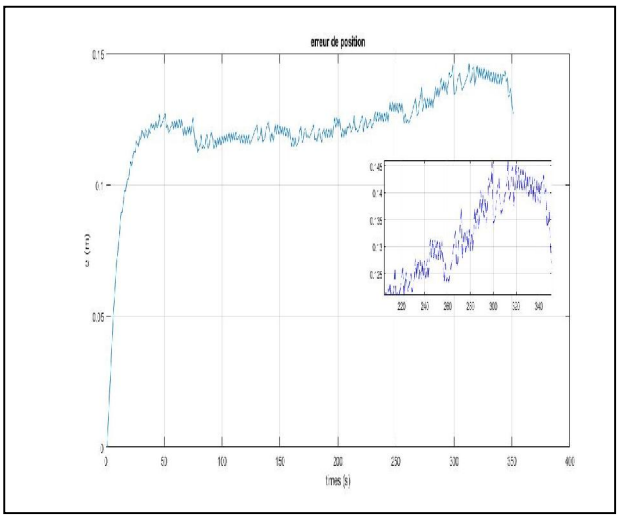


Figure IV.52 Erreur de position

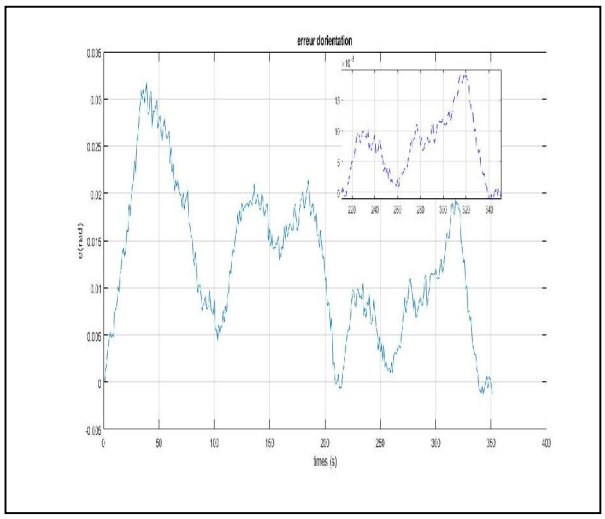


Figure IV.53 Erreur d'orientation

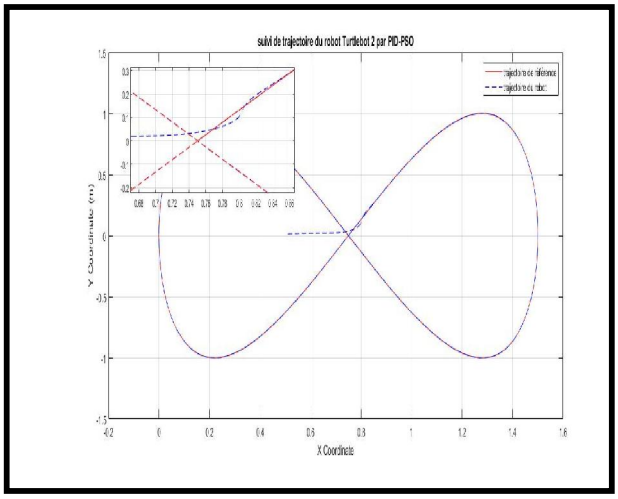


Figure IV.54 Trajectoire de référence et trajectoire de sortie

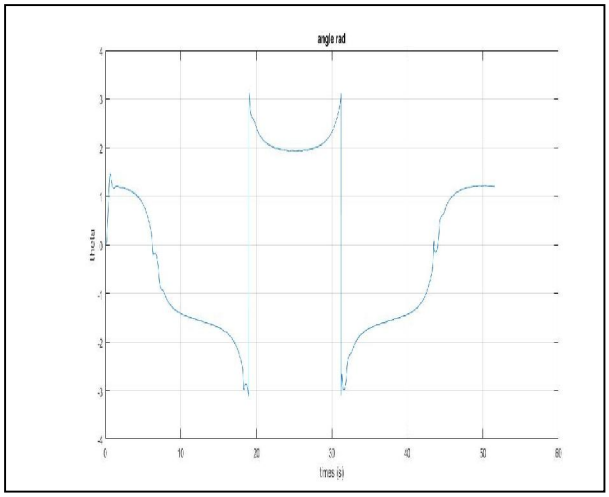


Figure IV.55 Angle d'orientation

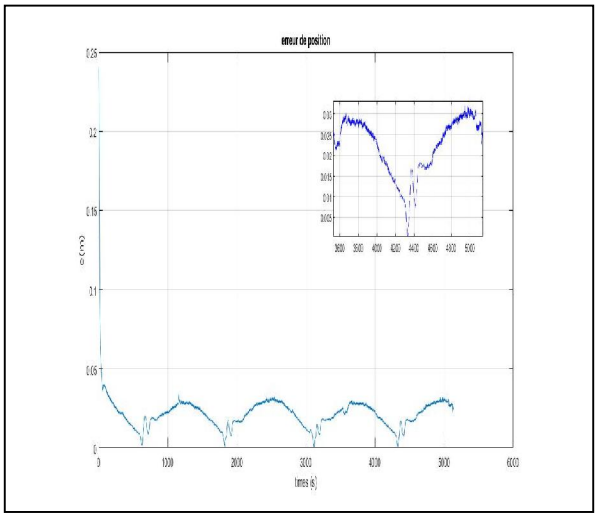


Figure IV.56 Erreur de position

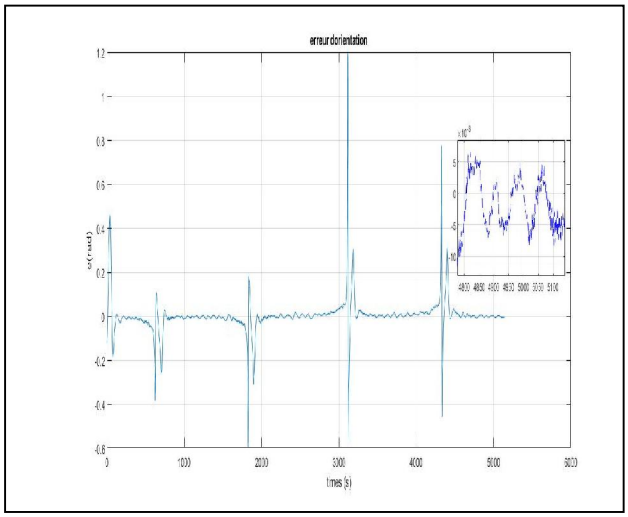


Figure IV.57 Erreur d'orientation

Pour une période d'échantillonnage Te = 0.005 seconde :

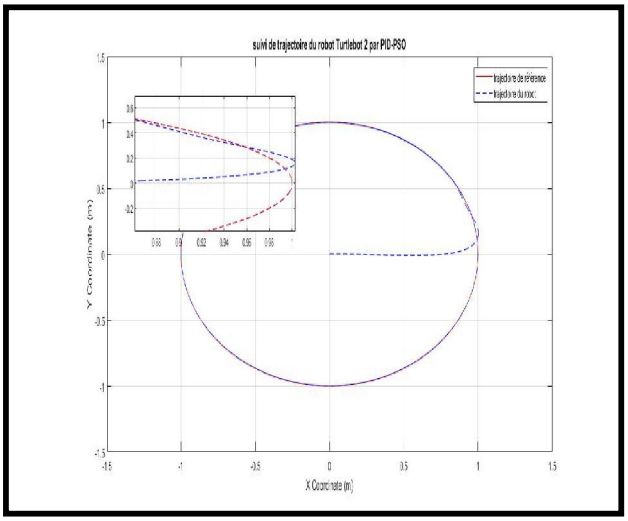


Figure IV.58 Trajectoire de référence et trajectoire de sortie

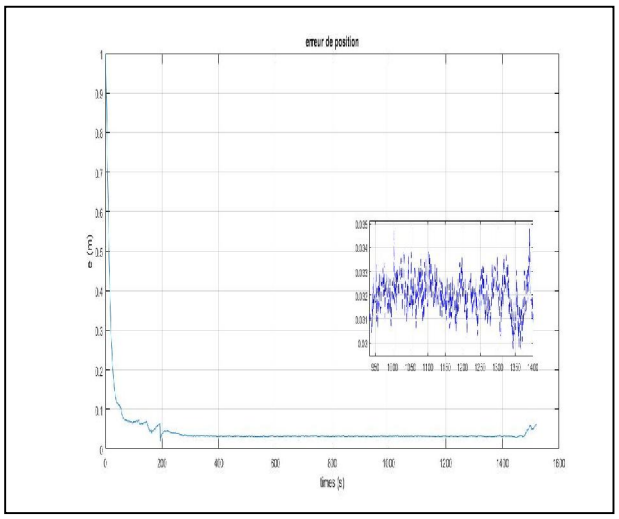


Figure IV.59 Erreur de position

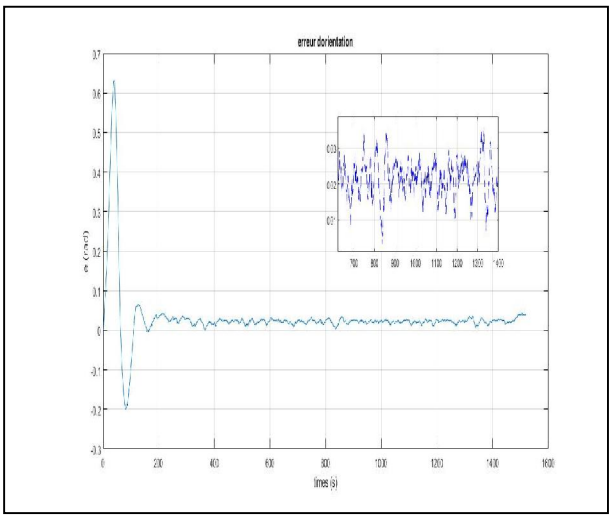


Figure IV.60 Erreur d'orientation

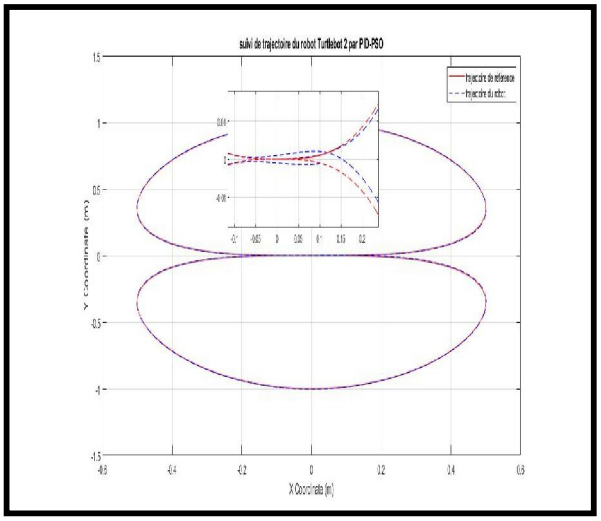


Figure IV.61 Trajectoire de référence et trajectoire de sortie

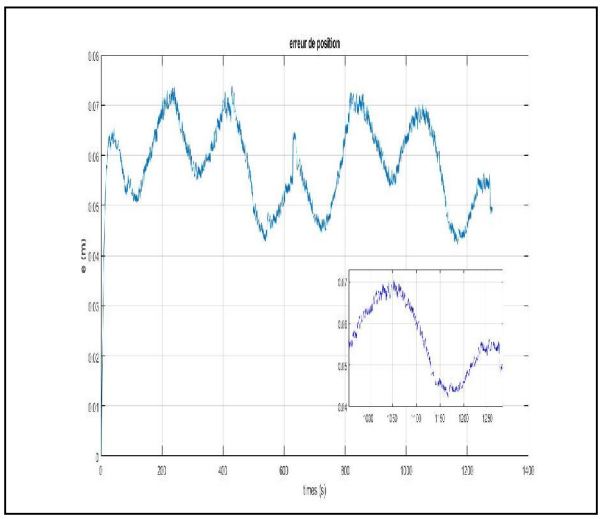


Figure IV.62 Erreur de position

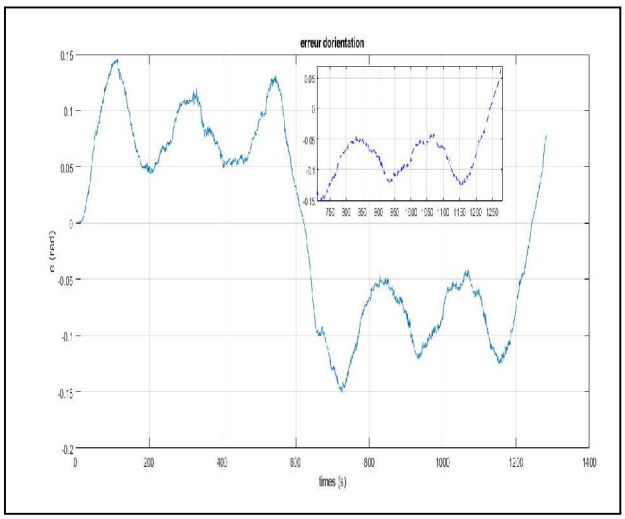


Figure IV.63 Erreur d'orientation

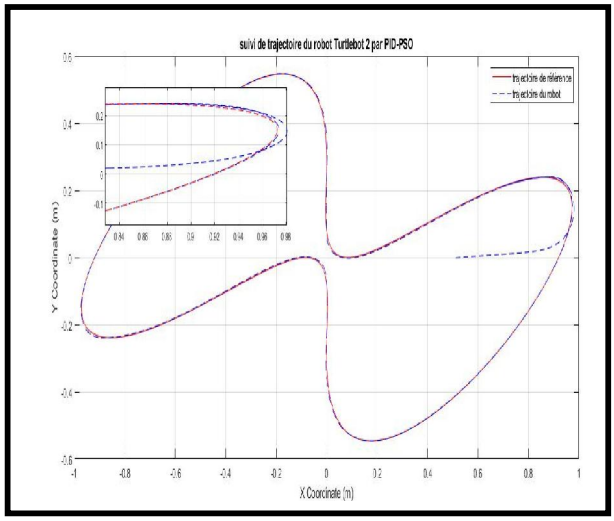


Figure IV.64 Trajectoire de référence et trajectoire de sortie

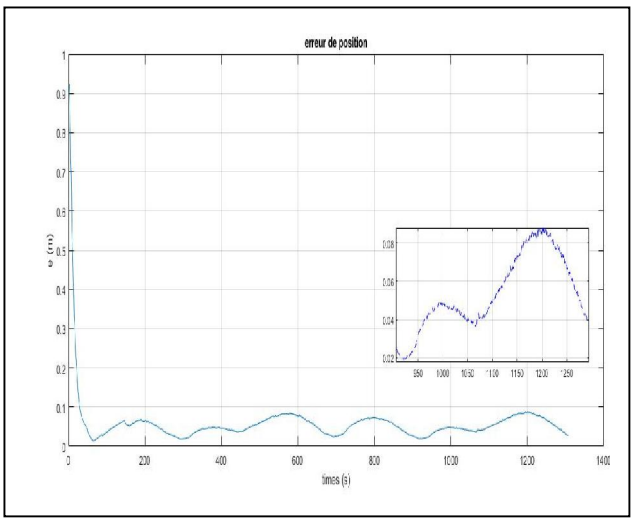


Figure IV.65 Erreur de position

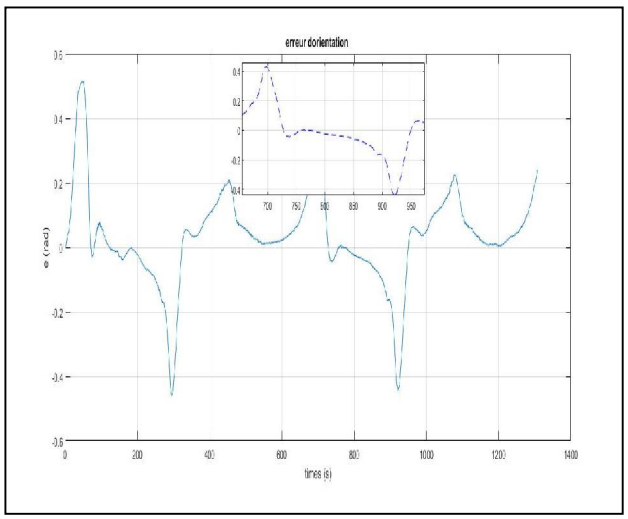


Figure IV.66 Erreur d'orientation

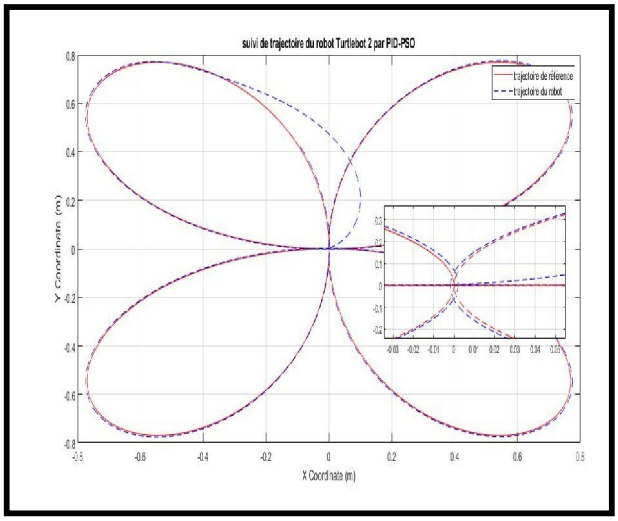


Figure IV.67 Trajectoire de référence et trajectoire de sortie

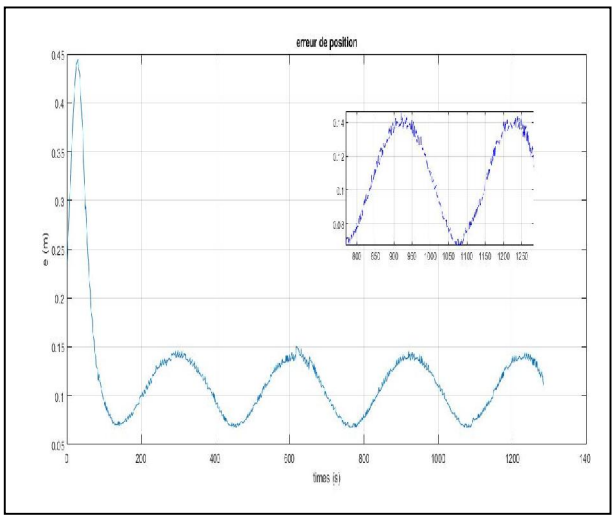


Figure IV.68 Erreur de position

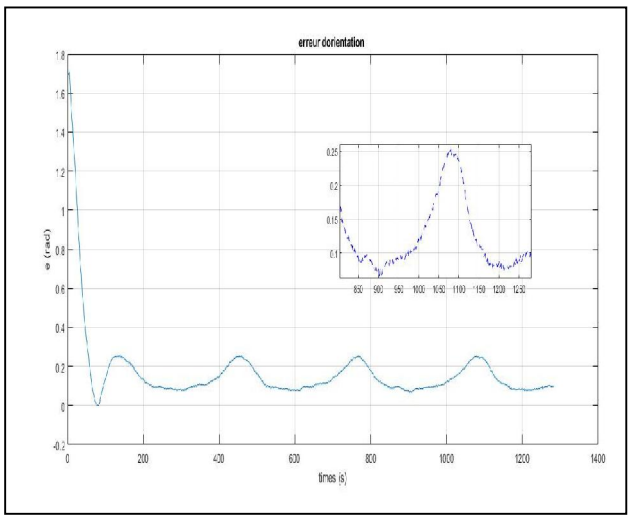


Figure IV.69 Erreur d'orientation

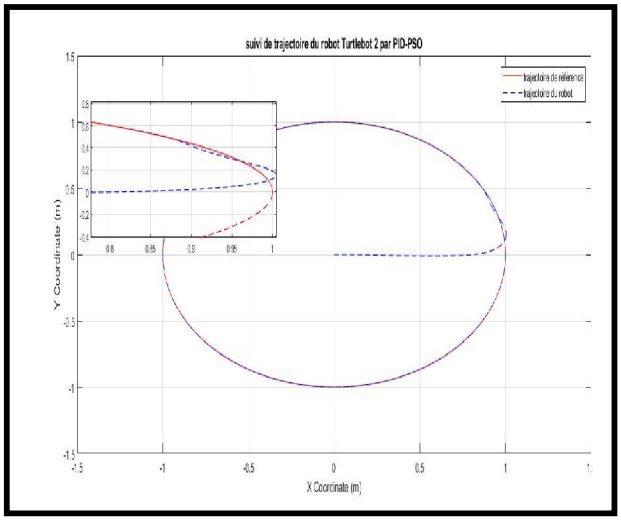


Figure IV.70 Trajectoire de référence et trajectoire de sortie

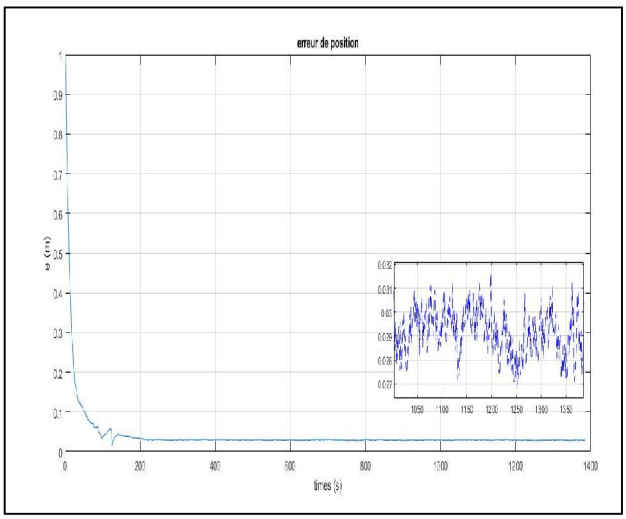


Figure IV.71 Erreur de position

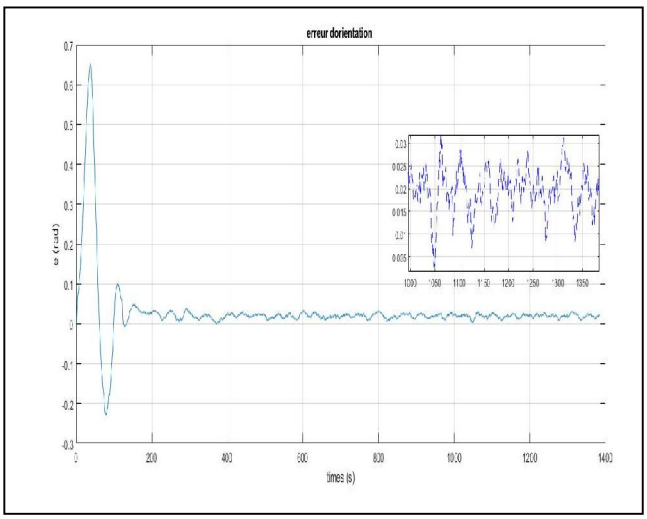


Figure IV.72 Erreur d'orientation

IV.6.5 Discussion et comparaison des résultats expérimentaux

Une comparaison des résultats obtenus est récapitulée dans le tableau IV.19 :

Tableau IV.19 Comparaison des résultats expérimentaux obtenus

<table>
<tr><th>Périodes d'échantillonnage</th><th>Valeur moyenne de l'erreur de position</th><th>Valeur moyenne de l'erreur d'orientation</th></tr>
<tr><td>Te = 0.01 seconde</td><td>Comprise entre 2.18×10^{-2} mètre et 1.217×10^{-1} mètre pour les différentes trajectoires (figures IV.52 et IV.56)</td><td>Comprise entre 2.1×10^{-3} radian et 1.26×10^{-2} radian pour les différentes trajectoires (figures IV.42 et IV.46)</td></tr>
<tr><td>Te = 0.005 seconde</td><td>Comprise entre 4.12×10^{-2} mètre et 1.2×10^{-1} mètre pour les différentes trajectoires (figures IV.59, IV.62, IV.65, IV.68 et IV.70)</td><td>Comprise entre 3.05×10^{-2} radian et 1.6×10^{-1} radian pour les différentes trajectoires (figures IV.60, IV.63, IV.66, IV.69 et IV.72)</td></tr>
<tr><td rowspan="2">Te = 0.001 seconde</td><td>Comprise entre 9.8×10^{-3} mètre et 6.47×10^{-2} mètre pour les différentes trajectoires (figures IV.31, IV.34, IV.37, IV.40, IV.43, IV.46 et IV.49)</td><td>Comprise entre 7.036×10^{-6} radian et 8.27×10^{-2} radian pour les différentes trajectoires (figures IV.32, IV.35, IV.38, IV.41, IV.44, IV.47 et IV.50)</td></tr>
<tr><td colspan="2">La trajectoire donnant les meilleurs résultats est celle dont les figures sont entourées par un cadre rouge (figures IV.39, IV.40 et IV.41)</td></tr>
<tr><td rowspan="2">Te = 0.0001 seconde</td><td>Egale à 7.6×10^{-3} mètre (figure IV.25)</td><td>Egale à 9.6×10^{-3} radian (figure IV.26)</td></tr>
<tr><td colspan="2">La trajectoire donnant les meilleurs résultats est celle dont les figures sont entourées par un cadre vert (figures IV.24, IV.25 et IV.26)</td></tr>
</table>

D'après le tableau IV.19, les meilleurs résultats sont obtenus avec Te = 10^{-4} seconde, que ce soit vis-à-vis de l'erreur de position ou de l'erreur d'orientation.

Nous pouvons également conclure que les valeurs de paramètres du contrôleur obtenus avec l'algorithme PSO ont donné des résultats très satisfaisants en pratique, comme en simulation (erreur autour de 10^{-3} et 10^{-4}) comparativement aux résultats obtenus par [150] (PID classique avec une erreur autour de 10^{-2}). Nos résultats pourraient être encore améliorés via l'utilisation d'autres algorithmes d'optimisation, comme l'optimisation GWO (acronyme de « Grey Wolf Optimizer ») ou l'optimisation ACO (acronyme de « Ant Colony Optimization »).

IV.7 Conclusion

Dans ce chapitre, nous avons traité du problème de la navigation autonome de robots mobiles dans des environnements non structurés à risques. Cependant, pour des raisons de sécurité, la trajectoire est supposée prédéfinie et planifiée à l'avance. Par conséquent, notre étude a été consacrée au suivi de différentes formes de trajectoires de référence complexes : circulaire, infinie, linéaire… Une commande cinématique optimisée a été proposée dans le cadre d'un robot mobile à conduite différentielle à deux roues (robot de type Turtlebot2). L'objectif est de réaliser une architecture de contrôle ayant des performances optimales. Cette architecture comprend deux parties. La première est basée sur une commande cinématique non linéaire à retour d'état. La seconde partie comprend un algorithme d'optimisation de l'essaim de particules (PSO), qui permet d'ajuster les paramètres du contrôleur pour obtenir les variables optimales de suivi de trajectoire. Cette démarche permet de préserver la sureté de bon fonctionnement des robots et la sécurité humaine et matérielle, au sein de ces environnements complexes. Diverses simulations et expérimentions ont été effectuées pour évaluer les performances du contrôleur proposé en utilisant la version simulée sous Gazebo du robot, ainsi que sa version réelle.

Les résultats obtenus montrent l'efficience et l'efficacité de la stratégie de contrôle du mouvement. Les résultats de simulation ont débouché sur une précision accrue, grâce à la rapidité de transmission des données au simulateur.

Conclusion générale et Perspectives

Conclusion générale et Perspectives

Dans cette thèse, nous avons traité le problème de l'intégration d'un système de robotique mobile autonome dans un environnement industriel à haut niveau de risques. Cette étude s'est concentrée sur la sureté et la sécurité de l'environnement. La navigation de ces robots passe par la prise en compte d'un contrôle optimal, d'une interaction et d'une coordination précises des différentes entités robotiques, à travers diverses architectures de commande multi-contrôleurs.

Dans un premier temps, nous nous sommes focalisés sur une étude bibliographique de la maitrise de risques et de la sécurité des systèmes industriels robotisés. Cette étude réalise un aperçu général du processus de gestion des risques dans l'objectif d'optimiser et de préserver la sécurité industrielle. Ainsi, nous mettons en évidence l'ensemble des normes de sécurité adoptées dans le domaine de la robotique industrielle. Nous présentons les différentes techniques appliquées à l'analyse et à l'évaluation des risques. Une classification de ces méthodes est présentée.

Dans un deuxième temps, une description théorique des différentes méthodes d'analyse utilisées dans le cadre de notre travail est réalisée. A partir de celle-ci, une méthodologie reposant sur quatre approches est proposée. Elle permet de réaliser une analyse complète et détaillée des scénarios de risques dans un laboratoire d'analyses robotisé. La première approche consiste en une analyse préliminaire des modes de dysfonctionnement des principaux composants physiques d'un robot mobile. La deuxième approche permet d'analyser les actions de contrôle dangereuses menant aux risques de collision. La troisième approche permet d'analyser différentes architectures hiérarchiques de contrôle et de coordination d'un système multi-robots. La quatrième approche fournit une analyse détaillée des différentes fonctionnalités des contrôleurs des robots mobiles autonomes. Par ailleurs, nous proposons une évaluation des scénarios de risque de collision basée sur un modèle de fonctionnement du système. La méthodologie proposée nous a permis de fournir une analyse détaillée des systèmes industriels complexes équipés de robots mobiles autonomes, de collecter également un grand nombre de scénarios de risques probables, de modéliser le comportement du système durant son fonctionnement normal et son dysfonctionnement, et enfin, d'évaluer le risque de collision. Ainsi, des exigences de

sécurité et des recommandations ont été suggérées pour résoudre les problèmes de navigation et de contrôle des robots mobiles à roues différentielles, tout en préservant la sûreté et la sécurité de l'ensemble du laboratoire.

Finalement, nous avons solutionné un problème de navigation autonome d'un robot mobile en environnement complexe à risques. Toutefois, pour des raisons de sécurité, la trajectoire est supposée prédéfinie et planifiée par avance. Nous avons développé une architecture de contrôle optimale d'un robot mobile à roues différentielles, assurant la stabilité et l'amélioration de la précision du suivi de diverses formes de trajectoires complexes. Cette architecture contribue, par conséquent, à l'amélioration de la sécurité d'un système de robotique mobile en milieu industriel. Cette architecture de contrôle se décompose en deux parties. La première est basée sur une commande cinématique non linéaire à retour d'état ; la seconde partie consiste en un algorithme d'optimisation de l'essaim de particules (PSO), qui permet d'ajuster les paramètres du contrôleur pour obtenir les variables optimales de suivi de trajectoire. Nous avons montré l'efficience et l'efficacité de la stratégie proposée par une simulation 3D sous Gazebo d'une part, et une application temps réel sur un robot mobile de type Turtlebot2 d'autre part.

Durant notre travail de thèse, nous nous sommes imposés certaines limitations. Elles peuvent être considérées comme des points de réflexion à développer dans de futurs travaux :

Comme mentionné ci-dessus, l'analyse STPA est encore considérée comme l'une des méthodes purement qualitatives en raison de la difficulté d'évaluer certains scénarios. Par conséquent, son utilisation n'est pas suffisante pour une analyse plus rigoureuse. Dans un travail ultérieur, il serait préférable de la combiner à une autre méthode quantitative, permettant d'obtenir une quantification plus concrète des scénarios de dangers résultants.

L'analyse semi-quantitative utilisée à travers la combinaison STPA / nœud papillon est incapable d'évaluer tous les scénarios potentiels et les facteurs causaux obtenus par STPA. Cette combinaison ne peut également différencier quantitativement certains scénarios : « lorsque l'action de contrôle n'est pas fournie, ou est fournie trop tard ou trop tôt », ou certains facteurs causaux comme « mauvaise connexion et connexion interrompue ». Dans un travail futur, nous souhaitons nous orienter vers un outil estimant cette différentiation.

Dans l'étude de cas de la quatrième approche, nous avons limité le nombre de robots à deux, dû à la complexité élevée du modèle de réseau de Petri. Le but est de faciliter la compréhensibilité du modèle d'une part, et de minimiser le temps de simulation d'autre part. De plus, nous avons considéré que les scénarios de collision étaient causés par les défaillances des composants des robots, tout en ignorant d'autres facteurs, tels l'erreur humaine, le fonctionnement dégradé des composants... Dans un travail futur, pour avoir une quantification plus rigoureuse des scénarios de perte, il sera préférable de prendre en compte chaque action de contrôle non sécurisée.

Ainsi, dans un travail de futur, nous nous envisageons de généraliser et d'appliquer la méthodologie proposée à d'autres systèmes industriels complexes (e.g. systèmes pétrochimiques).

Finalement, nous nous efforcerons de prendre en considération les exigences suggérées pour améliorer la robustesse de l'algorithme de contrôle. En particulier, les solutions proposées pour améliorer la fonctionnalité d'évitement de collision et le traitement des informations bruitées doivent être utilisées. Nous espérons également éprouver et généraliser l'architecture de contrôle à deux robots ou plus en prenant en considération la communication.

Annexes

Annexe 1 : Description succincte du robot mobile Turtlebot2™

Le robot mobile TurtleBot2™ est l'un des robots non holonomes proposés par Willow Garage dans le cadre du développement du système d'exploitation ROS dédié à la robotique. Il est notamment équipé d'une caméra de type Kinect™, d'un netbook, de plateaux pour l'installation de ces deux composants et d'une base Kobuki™, comme illustré sur la figure A.1[130].

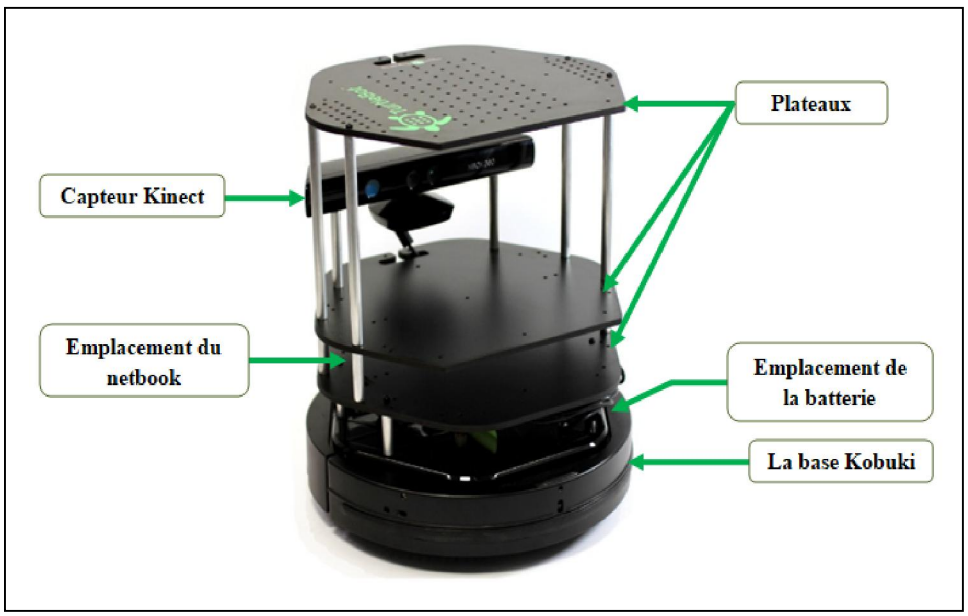


Figure A.1 Les différents composants du TurtleBot2™

1. **Le netbook :** Sa tâche principale est d'interagir avec les différents éléments du robot (actionneurs/capteurs). Il est muni d'un système de communication wifi afin de recevoir et d'envoyer des données via une station de travail, opérant par exemple sous Matlab.
2. **La base Kobuki™ :** Elle constitue la base mobile du Turtlebot2™. Les roues, non directrices, sont commandées par l'application d'un différentiel de vitesses sur celles-ci. La base contient également des capteurs de proximité, des encodeurs de roues et un gyromètre pour chaque axe. La base Kobuki™ permet également d'alimenter des capteurs externes (capteur à ultrasons, capteur infrarouge, scanner

laser, Kinect™ ou autres caméras...) ou des actionneurs (moteurs, servomoteurs…). La figure suivante montre les vues du dessus et du dessous de la base Kobuki™.

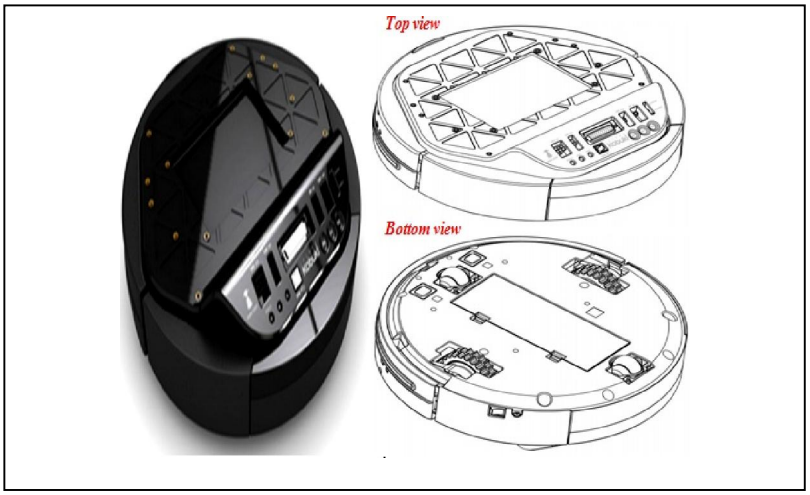


Figure A.2 La base Kobuki™

Les principaux capteurs de la base Kobuki™ sont les suivants [130]:

- **Encodeurs :** les encodeurs sont des capteurs attachés à un objet en rotation (e.g. une roue) afin de mesurer sa rotation. Son déplacement, sa vitesse et son accélération peuvent ainsi être déterminés. On parle alors de localisation par odométrie. Celle-ci, basée sur la mesure individuelle du mouvement de chaque roue, nous permet de reconstituer le mouvement global du robot : A partir d'une position initiale connue et en intégrant les déplacements mesurés, il est alors possible de calculer la position actuelle du robot mobile à chaque instant.
- **Gyroscope :** Le gyroscope est un capteur permettant de connaître les vitesses angulaires selon les trois axes$x$, y et z.
- **Capteurs de pare-chocs :** Trois capteurs de pare-chocs sont répartis entre la partie gauche, le centre et la partie droite de la base.
- **Capteurs de vide :** De même, trois capteurs sont répartis entre la partie gauche, la partie centrale et la partie droite de la base.
- **Capteurs de descente de roue :** Un capteur sur chacune des roues gauche et droite.

3. **Caméra Kinect™ :** La figure ci-dessous illustre ce capteur.

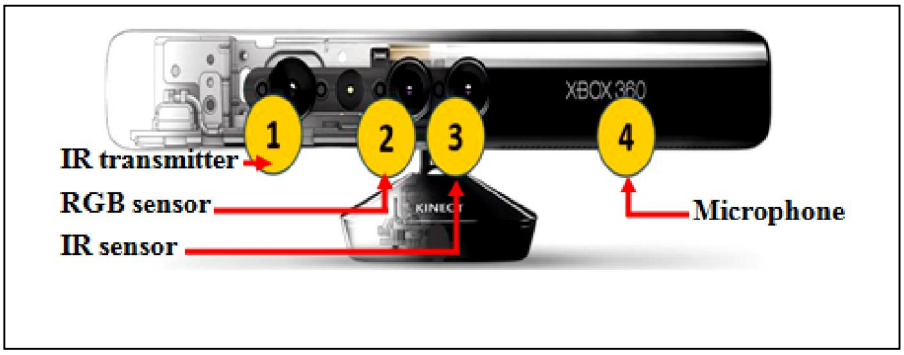


Figure A.3 Les composants de la caméra Kinect™ XBOX360™

Les principaux composants de la caméra Kinect™ sont [130]:

- **Une caméra RVB (rouge, vert, bleu) :** Elle stocke les données sur trois canaux avec une résolution de 1280 x 960 pixels, permettant la capture d'une image couleur.
- **Un émetteur / récepteur infrarouge (IR) :** L'émetteur émet un signal IR et le capteur de profondeur reçoit le signal IR réfléchi par les différents obstacles rencontrés. La distance parcourue par le signal IR permet de mesurer la distance entre l'obstacle et le capteur. Cette technologie permet ainsi la capture d'une image de profondeur.

Annexe 2 : Echelles d'estimation de risque et données de probabilités

Afin de pouvoir évaluer le risque à travers la matrice de risque, des échelles ont été définis pour estimer ses éléments. Dans ce qui suit, nous définissons les échelles, Adaptées des travaux de Guiochet [13] et Rausand [20], que nous avons utilisées dans l'évaluation.

1. Echelle de gravité :

Le tableau A.1 suivant définit l'échelle de gravité.

Tableau A.1 Echelle de gravité

Gravité	Personnel	Environnement	Biens
1. Perte minime	Blessures légères	Aucun déversement	Impact inaperçu sur les performances de production
2. Perte mineure	Blessures mineures	Déversement faible	Dommages partiels des biens, ce qui entraîne une réduction des performances de production à court terme, cout de récupération réduit
3. Perte importante	Blessures ou maladies graves	Déversement mineure, impact interne	Dommages totales des biens, ce qui entraîne une réduction des performances de production à court terme, cout de récupération réduit
4. Perte majeure	Décès d'une personne	Déversement mineure, impact externe	Dommages totales des biens, ce qui entraîne une réduction des performances de production à long terme, cout de récupération réduit
5. Perte catastrophique	Plusieurs décès	Déversement majeure	Dommages totales des biens, ce qui entraîne une réduction des performances de production à long terme, cout de récupération important

2. Echelle de fréquence :

Le tableau A.2 suivant définit l'échelle de fréquence.

Tableau A.2 Echelle de fréquence

Catégorie	Fréquence
1. Improbable	> 100 ans
2. Rare	> 10 ans
3. Probable	1 ans- 10 ans
4. Occasionnelle	2 mois- 1 ans
5. Fréquente	< 2 mois

3. Echelle de détectabilité :

Le tableau A.3 suivant définit l'échelle de détectabilité.

Tableau A.3 Echelle de détectabilité

Probabilité	Détectabilité
1	Facilement détectable
2	Détection à l'autocontrôle
3	Détection visuelle
4	Détection difficile
5	Indétectable

4. Données de probabilités :

Le tableau A.4 suivant présente les taux de défaillance des composants et les distributions de probabilité que nous avons adoptés pour notre étude.

Tableau A.4 Données de probabilités

Composants	Distribution de probabilité
Moteur électrique	Exp (9×10^{-6})
Scanner laser	Exp (5×10^{-6})
Système de communication	Exp (9×10^{-4})
Carte de contrôle	Web (2, 9.5×10^{4})
Batterie	Web (4.7, 4.9×10^{4})

Bibliographie

Bibliographie

[1] "The CARLoS Project," *Cooperative mobile robotics, Project supported by the European Commission under the 7th Framework Programme, 2012–2014*. http://carlosproject.aimen.es/. [Accessed: 03-Oct-2020].

[2] "Welcome | RoboSafe.org," *Trustworthy Robotic Assistants, EPSRC-funded project, 2013. UK*. http://robosafe.csc.liv.ac.uk/. [Accessed: 03-Oct-2020].

[3] "SIMERO," *Safety strategies for human-robot cooperation, Project partially funded by the German Research Foundation*. https://www.ai3.uni-bayreuth.de/de/forschung/simero/index.php. [Accessed: 03-Oct-2020].

[4] J. A. G. Junior, C. M. Busso, S. C. O. Gobbo, and H. Carreão, "Making the links among environmental protection, process safety, and industry 4.0," *Process Safety and Environmental Protection*, vol. 117, pp. 372–382, 2018. https://doi.org/10.1016/j.psep.2018.05.017

[5] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," *European Journal of Operational Research*, vol. 253, no. 1, pp. 1–13, August 2016. https://doi.org/10.1016/j.ejor.2015.12.023

[6] J. Guiochet, M. Machin, and H. Waeselynck, "Safety-critical advanced robots: A survey," *Robotics and Autonomous Systems*, vol. 94, pp. 43–52, Aug. 2017. https://doi.org/10.1016/j.robot.2017.04.004

[7] D. C. Hendershot, "Lessons from human error incidents in process plants," *Process Safety and Environmental Protection*, vol. 84, no. 3, pp. 174–178, 2006. https://doi.org/10.1205/psep.05184

[8] CEI 60300-3-9 standard. "Gestion de la sûreté de fonctionnement-Partie 3: Guide d'application-Section 9: Analyse du risque des systèmes technologiques", *Commission électrotechnique internationale*, Ed.1, 67 pages, Geneva, Switzerland,1995.

[9] IEC 61508 standard. "Functional safety of electrical/ electronic/ programmable electronic safety-related systems- Parts 1 to 7," *International Electrotechnical Commission*, Geneva, Switzerland, 2010.

[10] ISO/CEI Guide 51. "Aspects liés à la sécurité — Principes directeurs pour les inclure dans les normes," ISO/CEI , Ed.3, 16 pages, Avril 2014.

[11] OHSAS 18001, Occupational health and safety management systems - specification. British Standards Institute (BSI), England, 1999.

[12] J. C. Laprie *et al.*, *Guide de la Sûreté de Fonctionnement*, 324 pages, Cépaduès Editions, Toulouse, France, 1995.

[13] J. Guiochet, "Safety management of service robot systems-UML approach based on

system risk analysis." PhD thesis, Institut National des Sciences Appliquées de Toulouse, France, 2003.

[14] N. Margossian, *Risques et accidents industriels majeurs: Caractéristiques, réglementation, prévention*. Collection : Technique et ingénierie, Dunod, 280 pages, Jan. 2006.

[15] N.G. Leveson, *Safeware: system safety and computers*. Addison-Wesley, Reading, MA, 680 pages , 1995.

[16] D. Macdonald, *Practical industrial safety, risk assessment and shutdown systems*. Elsevier, 384 pages, ISBN: 9780750658041, 2003. https://doi.org/10.1016/B978-0-7506-5804-1.X5000-9

[17] M. Fumey, "Méthode d'évaluation des risques agrégés: application au choix des investissements de renouvellement d'installations," PhD thesis, Institut National Polytechnique de Toulouse, France, 2001.

[18] C. Morneau, "La gestion des risques d'accidents industriels majeurs: état de la situation sur le territoire de la pointe-de-l'île," CSSS de la Pointe-de-l'île, 67 pages , 2011.

[19] Y. Bai and W.-L. Jin, *Chapter 38 - Risk Assessment Methodology*. In: Bai, Y. & Jin, W.-L. (eds.) Marine Structural Design (2nd ed.). Oxford: Butterworth-Heinemann, pp. 709–723, 2016.

[20] M. Rausand, *Risk assessment: theory, methods, and applications*, vol. 115, John Wiley & Sons, 635 pages, 2013. ISBN: 1118281101

[21] 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." PhD thesis, Université Bordeaux 1, France, 2008.

[22] B.S. Dhillon and O.C. Anude, "Robot safety and reliability: A review," *Microelectronics Reliability*, vol.33, no.3, pp.413–429, 1993. https://doi.org/10.1016/0026-2714(93)90030-3

[23] H. Dezfuli, A. Benjamin, C. Everett, C. Smith, M. Stamatelatos, and R. Youngblood, "Nasa system safety handbook. *volume 1; system safety framework and concepts for implementation*," National Aeronautics and Space Administration, vol. 1, 102 pages, Washington, États-Unis, Nov.2011.

[24] G. Zwingelstein, "Sûreté de fonctionnement-Principaux concepts," *Automatique et ingénierie système*. Techniques de l'Ingénieur, *Ref. TI660*, mars.2019.

[25] M.H. Mazouni, "Pour une meilleure approche du management des risques: de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision." PhD thesis, Institut National Polytechnique de Lorraine, France, 2008.

[26] ISO 31000 standard. "*Risk management,*" *International Organization for Standardization*, Ed. 2, 16 pages, 2018.

[27] F.I. Khan, P.R. Amyotte, and Md.T. Amin, "Chapter One - Advanced methods of risk assessment and management: An overview,"Methods in Chemical Process Safety, vol. 4, pp.1-34, Elsevier, 2020. https://doi.org/10.1016/bs.mcps.2020.03.002

[28] P.R. Garvey and Z.F. Lansdowne, "Risk matrix: an approach for identifying, assessing, and ranking program risks," *Air Force Journal of Logistics*, vol. 22, no. 1, pp. 18–21, 1998.

[29] H. Ni, A. Chen, and N. Chen, "Some extensions on risk matrix approach," *Safety Science*, vol. 48, no. 10, pp. 1269–1278, 2010. https://doi.org/10.1016/j.ssci.2010.04.005

[30] B. Ruge, "Risk matrix as tool for risk assessment in the chemical process industries," *Probabilistic Safety Assessment and Management*, pp. 2693–2698, 2004. https://doi.org/10.1007/978-0-85729-410-4_431

[31] Conseil d'orientation pour l'emploi, "Automatisation, numérisation et emploi, Tome 1: les impacts sur le volume, la structure et la localisation de l'emploi," *rapport,189 pages, France, janvier* 2017.

[32] A. Sghaier and P. Charpentier, "La problématique de l'utilisation des robots industriels en matière de sécurité," *Annales des Mines- Réalités industrielles*, vol. février 2012, no. 1, pp. 24–31, 2012. https://doi.org/10.3917/rindu.121.0024

[33] J.A. Corrales, G.J.G. Gomez, F. Torres, and V. Perdereau, "Cooperative tasks between humans and robots in industrial environments," *International Journal of Advanced Robotic Systems*, vol. 9, no. 3, p. 94, 2012. https://doi.org/10.5772/50988

[34] ISO 10218-2 standard. "Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration", *International Organization for Standardization*, Ed. 1, 79 pages, 2011.

[35] T. Malm, "Guidelines to make safe industrial robot systems," VTT Technical research centre of Finland Ltd, Research report, 30 pages, 1 March 2017.

[36] R.N. Shea. "Collaborative robot technical specification ISO/TS 15066 update," *International collaborative robots workshop by robotic industries association (ria)*, Boston, US, 3-4 May 2016.

[37] ANSI/RIA R15.06 standard. "The industrial robot safety standard", *American National Standards Institute*, 2012.

[38] B.S. Dhillon and A.R.M. Fashandi, "Safety and reliability assessment techniques in robotics," *Robotica*, vol. 15, no. 6, pp. 701–708, 1997. https://doi.org/10.1017/S0263574797000829

[39] I. D. Walker and J. R. Cavallaro, "Failure mode analysis for a hazardous waste clean-up manipulator," *Reliability Engineering & System Safety*, vol. 53, no. 3, pp. 277–290, 1996. https://doi.org/10.1016/S0951-8320(96)00055-5

[40] M. L. Visinsky, J. R. Cavallaro, and I. D. Walker, "Robotic fault detection and fault tolerance: A survey," *Reliability Engineering & System Safety*, vol. 46, no. 2, pp. 139–158, 1994. https://doi.org/10.1016/0951-8320(94)90132-5

[41] P. Kazanzides, "Safety Design for medical robots," *International Conference of the IEEE Engineering in Medicine and Biology Society: Engineering the Future of Biomedicine, EMBC 2009*, pp. 7208–7211, 2009. https://doi.org/10.1109/IEMBS.2009.5335275

[42] S. Lee and Y. Yam, "Risk Assessment and Functional Safety Analysis to Design Safety Function of a Human-Cooperative Robot," *Human Machine Interaction - Getting Closer*, Mr Inaki Maurtua (Ed.), ISBN: 978-953-307-890-8, InTech, 2012. https://doi.org/10.5772/37821

[43] P. Böhm and T. Gruber, "A novel HAZOP study approach in the RAMS analysis of a therapeutic robot for disabled children," In: Schoitsch E. (eds) Computer Safety, Reliability, and Security. SAFECOMP2010. Lecture Notes in Computer Science, vol. 6351, Springer, Berlin, Heidelberg, pp. 15–27, 2010. https://doi.org/10.1007/978-3-642-15651-9_2

[44] R. Alexander, N. Herbert, and T. Kelly, "Deriving safety requirements for autonomous systems," *4th SEAS DTC Technical Conference*, 2009.

[45] R. Woodman, A.F.T. Winfield, C. Harper, and M. Fraser, "Building safer robots: Safety driven control," *International Journal of Robotics Research*, vol. 31, no. 13, pp. 1603–1626, 2012. https://doi.org/10.1177/0278364912459665

[46] S. Dogramadzi, M.E. Giannaccini, C. Harper, M. Sobhani, R. Woodman, and J. Choung, "Environmental Hazard Analysis - a Variant of Preliminary Hazard Analysis for Autonomous Mobile Robots," *Journal of Intelligent and Robotic Systems: Theory and Applications*, vol. 76, no. 1, pp. 73–117, 2014. https://doi.org/10.1007/s10846-013-0020-7

[47] D. Martin-Guillerez, J. Guiochet, D. Powell, and C. Zanon, "A UML-based method for risk analysis of human-robot interactions," *International Workshop on Software Engineering for Resilient Systems*, pp. 32–41, 2010. https://doi.org/10.1145/2401736.2401740

[48] M. Machin, "Synthèse de règles de sécurité pour des systèmes autonomes critiques." PhD thesis, Université de Toulouse, Université Toulouse III-Paul Sabatier, France,2015.

[49] J. Guiochet, "Hazard analysis of human–robot interactions with HAZOP–UML," *Safety science*, vol. 84, pp. 225–237, 2016. https://doi.org/10.1016/j.ssci.2015.12.017

[50] A. Scarinci, A. Quilici, D. Ribeiro, F. Oliveira, D. Patrick, and N.G. Leveson, "Requirement generation for highly integrated aircraft systems through STPA: An application," *Journal of Aerospace Information Systems*, vol. 16, no. 1, pp. 9–21, 2019. https://doi.org/10.2514/1.I010602

[51] N.G. Leveson, *Engineering a safer world: Systems thinking applied to safety*, The MIT press, ISBN 9780262016629, Cambridge, 560 pages, 2011.

[52] N.G. Leveson and J.P. Thomas, *STPA handbook*, Online document, vol. 3, 188 pages, March 2018.

[53] A. Abdulkhaleq, M. Baumeister, H. Böhmert, and S. Wagner, "Missing no Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems," *International Journal of Safety Science*, vol. 02, no. 01, pp. 115–124, March 2018. https://doi.org/10.24900/ijss/0201115124.2018.0301

[54] A. Plioutsias and N. Karanikas, "Using STPA in the Evaluation of Fighter Pilots Training Programs," *Procedia Engineering*, vol. 128, pp. 25–34, Dec.2015.

https://doi.org/10.1016/j.proeng.2015.11.501

[55] C. H. Fleming, M. Spencer, J. Thomas, N. Leveson, and C. Wilkinson, "Safety assurance in NextGen and complex transportation systems," *Safety science*, vol. 55, pp. 173–187, 2013. https://doi.org/10.1016/j.ssci.2012.12.005

[56] T. Ishimatsu *et al.*, "Hazard analysis of complex spacecraft using systems-theoretic process analysis," *Journal of Spacecraft and Rockets*, vol. 51, no. 2, pp. 509–522, 2014. https://doi.org/10.2514/1.A32449

[57] H. Alemzadeh *et al.*, "Systems-theoretic safety assessment of robotic telesurgical systems," *International conference on computer safety, reliability, and security*, pp. 213–227, 2014. https://doi.org/10.1007/978-3-319-24255-2_16

[58] K. Wróbel, J. Montewka, and P. Kujala, "Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels," *Reliability Engineering and System Safety*, vol. 178, pp. 209–224, 2018. https://doi.org/10.1016/j.ress.2018.05.019

[59] O.A.V. Banda and S. Kannos, "Hazard Analysis Process for Autonomous Vessels," Novia University of Applied Sciences, 69 pages, 2017.

[60] B. Rokseth, O. I. Haugen, and I.B. Utne, "Safety Verification for Autonomous Ships," *MATEC Web of Conferences*, vol. 273, No. 02002, p. 15, 2019. https://doi.org/10.1051/matecconf/201927302002

[61] S. Khan, S. Madnick, and A. Moulton, "Cybersafety analysis of a central utilities plant (CUP) gas turbine using STPA-SEC," MIT Sloan Research Paper, no. 5726-18, 40 pages, 15 Apr. 2019. http://dx.doi.org/10.2139/ssrn.3370560

[62] A. Rachman and R.M.C. Ratnayake, "Implementation of system-based hazard Analysis on physical safety barrier: A case study in subsea HIPPS," *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 11–15, 2015. https://doi.org/10.1109/IEEM.2015.7385598

[63] H. Kim and M.A. Lundteigen, A. Hafver, F.B. Pedersen, "Application of STPA to the isolation of Subsea wells: Opportunities and Challenges of Applying STPA to Subsea Operations". *Offshore Technology Conference*, 2018. https://doi.org/10.4043/28830-MS

[64] J. Zhang, H. Kim, Y. Liu, and M.A. Lundteigen, " Combining system-theoretic process analysis and availability assessment: A subsea case study. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2019. https://doi.org/10.1177/1748006X18822224

[65] K. Hardy and F. Guarnieri, "Using a systemic model of accident for improving innovative technologies: application and limitations of the STAMP model to a process for treatment of contaminated substances," *The 15th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI*, 2011.

[66] M. Rodríguez Hernández and F.I. Díaz Moreno, "System theory based hazard analysis applied to the process industry," *International Journal of Reliability and Safety*, vol. 10, no. 1, pp. 72–86, 2016. https://doi.org/10.1504/IJRS.2016.076355

[67] Y. Song, "Applying system-theoretic accident model and processes (STAMP) to

hazard analysis." PhD Thesis, MC Master university, Canada. 2012.

[68] J. Thomas, F. Lemos, and N.G. Leveson, "Evaluating the safety of digital instrumentation and control systems in nuclear power plants," *NRC Technical Researcy Report2013*, 2012.

[69] D.-A. Lee, J. S. Lee, S. W. Cheon, and J. Yoo, "Application of system-theoretic process analysis to engineered safety features-component control system," *Proc. of the 37th Enlarged Halden Programme Group (EHPG) meeting*, 2013.

[70] D. Uesako, "STAMP applied to Fukushima Daiichi nuclear disaster and the safety of nuclear power plants in Japan.", PhD Thesis, Massachusetts Institute of Technology,Cambridge, UK, 2016.

[71] T. Ishimatsu, N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, and H. Nakao, "Modeling and hazard analysis using STPA," Proceedings of the 4th IAASS Conference, Making Safety Matter, 19–21 May 2010, Huntsville, Alabama, USA SP-680, 2010.

[72] H. Nakao, M. Katahira, Y. Miyamoto, and N.G. Leveson, "Safety guided design of crew return vehicle in concept design phase using STAMP/STPA," *Fifth International Association for the Advancement of Space Safety Conference, Versailles, France,* pp. 17–19, 2011.

[73] J J. Tixier, G. Dusserre, O. Salvi, and D. Gaston, "Review of 62 risk analysis methodologies of industrial plants," *Journal of Loss Prevention in the process industries*, vol. 15, no. 4, pp. 291–303, 2002. https://doi.org/10.1016/S0950-4230(02)00008-6

[74] ISO/IEC 31010 standard, " Gestion des risques — Techniques d'évaluation des risques", ISO/ CEI, Ed. 1, 176 pages, 2009

[75] D. Noyes and F. Pérès, "Analyse des systèmes-Sûreté de Fonctionnement," *Techniques de l'ingénieur*, Ref : AG3520, 2007.

[76] G. Zwingelstein, "Évaluation de la criticité des équipements. Méthodes analytiques," *Sécurité et gestion des risques,* Techniques de l'ingénieur, *Ref : TI112* , Jul. 2014.

[77] IEC 60812 standard. "Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)" , *International Electrotechnical Commission*, Ed. 2. 93 pages, Geneva, Switzerland, 2006.

[78] BS EN 31010 standard. " Risk management. Risk assessment techniques" British Standards Institution, 2010.

[79] M. Rusu and I. Soare, "Comparative risk assessment in applicative aerospace projects using different approaches," *INCAS Bulletin*, vol. 10, no. 2, pp. 233–246, 2018.

[80] Y. Mortureux, *Amde (c). Sécurité et gestion des risques*, Ed. Techniques Ingénieur, *Ref : SE4040 v1*, 2005.

[81] C.A. Ericson and C. Li, "Fault tree analysis," *System Safety Conference, Orlando, Florida*, vol. 1, pp. 1–9, 1999. https://doi.org/10.1016/j.cosrev.2015.03.001

[82] S.M. Sulaman, A. Beer, M. Felderer, and M. Höst, "Comparison of the FMEA and STPA safety analysis methods–a case study," *Software Quality Journal*, vol. 27, no. 1, pp. 349–387, 2019. https://doi.org/10.1007/s11219-017-9396-0

[83] IEC 61025 standard. " Fault tree analysis (FTA)", *International Electrotechnical Commission*, Ed. 2, 103 pages, Geneva, Switzerland, 2006.

[84] W.E. Vesely, F.F. Goldberg, N.H. Roberts and D.F. Haasl, *Fault tree handbook*, Nuclear Regulatory Commission Washington DC, Vol.13, no.10, Réf: 13671554, 211 pages , USA, Jan.1981.

[85] Y. Mortureux, "Arbres de défaillance, des causes et d'événement," *Sécurité et gestion des risques*, Ed. Techniques Ingénieur, *Ref: SE4050 v1*, 2002.

[86] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," *International Conference on Computer Safety, Reliability, and Security*, pp. 310–325, 2014. https://doi.org/10.1007/978-3-319-10506-2_21

[87] M. Rejzek, S. H. Björnsdóttir, and S. S. Krauss, "Modelling multiple levels of abstraction in hierarchical control structures," *International Journal of Safety Science*, vol. 2, no. 01, pp. 94–103, 2018.

[88] M. Rejzek, S.S. Krauss, and C. Hilbes, "Safety driven design with UML and STPA," *4th MIT STAMP Workshop, Boston MA, USA, 23-26 March 2015*, 2015. 10.24900/ijss/020194103.2018.0301

[89] A.A. Adesina, Q. Hussain, S. Pandit, M. Rejzek, and A.M. Hochberg, "Assessing the value of system theoretic process analysis in a pharmacovigilance process: an example using signal management," *Pharmaceutical Medicine*, vol. 31, no. 4, pp. 267–278, 2017. https://doi.org/10.1007/s40290-017-0195-5

[90] M. Rejzek, N. Leveson, B. Antoine, C. Hilbes, M. Grossmann, and D. Meer, "Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System," *STAMP Workshop-Massachusetts Institute of Technology*, vol. 2012, April. 2012.

[91] D.M. Dilts, N.P. Boyd, and H.H. Whorms, "The evolution of control architectures for automated manufacturing systems," *Journal of manufacturing systems*, vol. 10, no. 1, pp. 79–93, 1991. https://doi.org/10.1016/0278-6125(91)90049-8

[92] M.M. Chatzimichailidou, J. Ward, T. Horberry, and P.J. Clarkson, "A comparison of the bow-tie and STAMP approaches to reduce the risk of surgical instrument retention," *Risk Analysis*, vol. 38, no. 5, pp. 978–990, 2018. https://doi.org/10.1111/risa.12897

[93] V. De Dianous and C. Fievez, "ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance," *Journal of Hazardous Materials*, vol. 130, no. 3, pp. 220–233, 2006. https://doi.org/10.1016/j.jhazmat.2005.07.010

[94] R.W. McLeod and P. Bowie, "Bowtie Analysis as a prospective risk assessment technique in primary healthcare," *Policy and Practice in Health and Safety*, vol. 16, no. 2, pp. 177–193, 2018. https://doi.org/10.1080/14773996.2018.1466460

[95] H.C. Merrett, J.J. Horng, A. Piggot, A. Qandour, and C.W. Tong, "Comparison of STPA and Bow-tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System," *MATEC Web of Conferences*, vol. 273, no.02008, p.18, 2019. https://doi.org/10.1051/matecconf/201927302008

[96] R. Burgess-Limerick, T. Horberry, and L. Steiner, "Bow-tie analysis of a fatal underground coal mine collision," *Ergonomics australia*, vol. 10, no. 2, 2014.

[97] O. Iddir, "Le nœud papillon: une méthode de quantification du risque majeur," *Sécurité et gestion des risques*, *Techniques de l'ingénieur.* Ref: SE4055, 2008.

[98] J.P. SIGNORET, "Analyse des risques des systèmes dynamiques: réseaux de Petri-Exemples de modélisation," *Sécurité et gestion des risques*, *Techniques de l'ingénieur.* Ref: SE4072 v1, 2008.

[99] J. Wang, "Chapter 15, Petri nets," in : *Handbook of finite state based models and applications (1 st ed.)*. Computer Science, Mathematics & Statistics, Chapman and Hall/CRC, 409 pages, 2012. https://doi.org/10.1201/b13055

[100] S. K. Andreadakis and A. H. Levis, "Synthesis of distributed command and control for the outer air battle," Massachusetts inst of tech cambridge lab for information and decision systems, Technical report , 13 pages, July.1988.

[101] D. Milutinovic and P. Lima, "Petri net models of robotic tasks," *Proceedings - IEEE International Conference on Robotics and Automation (Cat. No.02CH37292)* , *Washington*, *DC*, *USA*, vol.4, pp. 4059–4064, 2002. https://doi.org/10.1109/ROBOT.2002.1014376

[102] J. Wang, "Charging information collection modeling and analysis of GPRS networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 4, pp. 473–481, 2007. https://doi.org/10.1109/TSMCC.2007.897338

[103] M. Malhotra and K. S. Trivedi, "Dependability Modeling Using Petri-Nets," *IEEE Transactions on Reliability*, vol. 44, no. 3, pp. 428–440, 1995. https://doi.org/10.1109/24.406578

[104] Y. Dutuit, E. Châtelet, J.P. Signoret, and P. Thomas, "Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases," *Reliability Engineering & System Safety*, vol. 55, no. 2, pp. 117–124, 1997. https://doi.org/10.1016/S0951-8320(96)00108-1

[105] J. P. Signoret, "Dependability & safety modeling and calculation: Petri nets," *IFAC Proceedings Volumes (IFAC-PapersOnline)*, vol. 42, no. 5, pp. 203–208, 2009. https://doi.org/10.3182/20090610-3-IT-4004.00040

[106] V. Kumar and K. K. Aggarwal, "Petri net modelling and reliability evaluation of distributed processing systems," *Reliability Engineering & System Safety*, vol. 41, no. 2, pp. 167–176, 1993. https://doi.org/10.1016/0951-8320(93)90029-X

[107] X. Yang, J. Li, W. Liu, and P. Guo, "Petri net model and reliability evaluation for wind turbine hydraulic variable pitch systems," *Energies*, vol. 4, no. 6, pp. 978–997, 2011. https://doi.org/10.3390/en4060978

[108] G. Kumar, V. Jain, and O. P. Gandhi, "Reliability and availability analysis of

mechanical systems using stochastic petri net modeling based on decomposition approach," *International Journal of Reliability, Quality and Safety Engineering*, vol. 19, no. 01, p. 1250005, 2012. https://doi.org/10.1142/S0218539312500052

[109] S. Jian, W. Shaoping, and S. Yaoxing, "Petri-nets based availability model of fault-tolerant server system," in *2008 IEEE conference on robotics, automation and mechatronics*, pp. 444–449, 2008. https://doi.org/10.1109/RAMECH.2008.4681434

[110] J. P. Signoret, Y. Dutuit, P. J. Cacheux, C. Folleau, S. Collas, and P. Thomas, "Make your Petri nets understandable: Reliability block diagrams driven Petri nets," *Reliability Engineering and System Safety*, vol. 113, no. 1, pp. 61–75, 2013. https://doi.org/10.1016/j.ress.2012.12.008

[111] IEC 62551 standard. " Analysis techniques for dependability - Petri net techniques ", International Electrotechnical Commission, Ed.1, 136 pages, Geneva, Switzerland, 2012.

[112] H. Blume, T. von Sydow, D. Becker, and T. G. Noll, "Application of deterministic and stochastic Petri-Nets for performance modeling of NoC architectures," *Journal of Systems Architecture*, vol. 53, no. 8, pp. 466–476, 2007. https://doi.org/10.1016/j.sysarc.2006.11.001

[113] C. Girault and R. Valk, *Petri nets for systems engineering: a guide to modeling, verification, and applications*. Springer Science & Business Media, Ed.1, 607 pages, 2013. https://doi.org/10.1007/978-3-662-05324-9

[114] W. Reisig, *Understanding petri nets: modeling techniques, analysis methods, case studies.* Springer, 230 pages, 2013. https://doi.org/10.1007/978-3-642-33278-4

[115] G. S. Hura, "Use of Petri nets for system reliability evaluation," *Fundamental Studies in Engineering*, Elsevier, vol. 16, pp. 339–368, 1993. https://doi.org/10.1016/B978-0-444-81660-3.50018-6

[116] C. Bensaci, Y. Zennir, D. Pomorski, F. Innal, Y. Liu, and C. Tolba, "STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison," *Alexandria Engineering Journal*, vol. 59, no. 5, pp. 3799–3816, October 2020. https://doi.org/10.1016/j.aej.2020.06.036

[117] C. Bensaci, Y. Zennir, and D. Pomorski, "A New Approach to System Safety of human-multi-robot mobile system control with STPA and FTA." *Algerian Journal of Signals and Systems (AJSS)*, vol.5, no.1, ISSN: 2543-3792 – EISSN: 2676-1548, March 2020.

[118] C. Bensaci, Y. Zennir, D. Pomorski, and E.-A. Mechhoud, "Complex safety study of intelligent multi-robot navigation in risk's environment," *International Carnahan Conference on Security Technology*, Madrid, Spain, October 2017. https://10.1109/CCST.2017.8167809

[119] C. Bensaci, Y. Zennir, D. Pomorski, "Safety Study of Industrial Multi-Robot Navigation using Bow Tie Risk Analysis Method", International Conference on Maintenance and Industrial Safety (CIMSI), Skikda, Algeria, 20-21 November 2017.

[120] C. Bensaci, Y. Zennir, and D. Pomorski, "A Comparative Study of STPA

Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System," in *2018 2nd European Conference on Electrical Engineering and Computer Science (EECS)*, pp. 400–405, Bern, Switzerland, Dec 2018. https://10.1109/EECS.2018.00080

[121] W. Shen, Q. Hao, H.J. Yoon, and D.H. Norrie, "Applications of agent-based systems in intelligent manufacturing: An updated review," *Advanced engineering INFORMATICS*, vol. 20, no. 4, pp. 415–431, 2006. https://doi.org/10.1016/j.aei.2006.05.004

[122] B.-I. Kim, S.S. Heragu, R.J. Graves, and A.St Onge, "A hybrid scheduling and control system architecture for warehouse management," *IEEE Transactions on Robotics and Automation*, vol. 19, no. 6, pp. 991–1001, Jan. 2004. https://10.1109/TRA.2003.819735

[123] GRIF-Workshop, "Graphical interface for reliability forecasting software",2020. Available at: http://grif-workshop.fr/

[124] H. Fazlollahtabar and S. T. A. Niaki, "Integration of fault tree analysis, reliability block diagram and hazard decision tree for industrial robot reliability evaluation," *Industrial Robot*, vol. 44, no. 6, pp. 754–764, 2017. https://doi.org/10.1108/IR-06-2017-0103

[125] S.G. Tzafestas, *Introduction to mobile robot control*. Elsevier, 2013. https://doi.org/10.1016/C2013-0-01365-5

[126] G.T. Fokam, "Commande et planification de trajectoires pour la navigation de véhicules autonomes." PhD thesis, Université de Technologie de Compiègne, France, 2014.

[127] L. Steels, "When are robots intelligent autonomous agents?," *Robotics and Autonomous systems*, vol. 15, no. 1–2, pp. 3–9, 1995. https://doi.org/10.1016/0921-8890(95)00011-4

[128] J. Cao, "Vision techniques and autonomous navigation for an unmanned mobile robot." , Thesis of Master of Science, University of Cincinnati, 1999.

[129] C. Bensaci, Y. Zennir, and D. Pomorski, "Turtlebot 2 Autonomous Navigation Under the Virtual World Gazebo," *International Conference on Advanced Engineering in Petrochemical Industry (ICAEPI'17), Skikda, Algeria*, 2017.

[130] C. Bensaci, Y. Zennir, and D. Pomorski, "Nonlinear Control of a differential wheeled mobile robot in real time-Turtlebot 2," in *International Conference on Advanced Technologies and ElectricalEngineering (ICTAEE'18), Skikda, Algeria. pp.12-14, 2018.* hal-02014895.

[131] C. Bensaci and Y. Zennir, "Control of mobile robot navigation under the virtual world Matlab-Gazebo," *Algerian journal of signals and systems (AJSS)*, vol. 2, no. 4, 2017.

[132] B. Abci, "Approche informationnelle pour la navigation autonome tolérante aux défauts: application aux systèmes robotiques mobiles," PhD thesis, université de Lille ,France, 2019.

[133] K. Shojaei, A.M. Shahri, A. Tarakameh, and B. Tabibian, "Adaptive trajectory

tracking control of a differential drive wheeled mobile robot," *Robotica*, vol. 29, no. 3, pp. 391–402, 2011. https://doi.org/10.1017/S0263574710000202

[134] M. Oya, C.-Y. Su, and R. Katoh, "Robust adaptive motion/force tracking control of uncertain nonholonomic mechanical systems," *IEEE Transactions on Robotics and Automation*, vol. 19, no. 1, pp. 175–181, 2003. https://doi.org/10.1109/TRA.2002.807528

[135] X. Liang, H. Wang, Y.-H. Liu, W. Chen, and T. Liu, "Formation control of nonholonomic mobile robots without position and velocity measurements," *IEEE Transactions on Robotics*, vol. 34, no. 2, pp. 434–446, 2017. https://10.1109/TRO.2017.2776304

[136] P. Morin and C. Samson, "Trajectory tracking for non-holonomic vehicles: overview and case study," *Proceedings of the Fourth International Workshop on Robot Motion and Control (IEEE Cat. No. 04EX891)*, pp. 139–153, 2004. https://10.1109/ROMOCO.2004.240574

[137] C. Samson, "Control of chained systems application to path following and time-varying point-stabilization of mobile robots," *IEEE transactions on Automatic Control*, vol. 40, no. 1, pp. 64–77, 1995. https://10.1109/9.362899

[138] C.C. De Wit, "Quasicontinuous stabilizing controllers for nonholonomic systems: Design and robustness considerations," *3rd European Control Conference*, pp. 2630–2635, 1995.

[139] Z. Shen, Y. Ma and Y. Song, "Robust adaptive fault-tolerant control of mobile robots with varying center of mass," *IEEE Transactions on industrial electronics*, vol. 65, no. 3, pp. 2419–2428, 2017. https://10.1109/TIE.2017.2740845

[140] A. Stotsky and X. Hu, "Sliding mode control of a car-like mobile robot using single-track dynamic model," *Variable structure systems, sliding mode and nonlinear control*, Springer, pp. 181–191, 1999. https://doi.org/10.1016/S1474-6670(17)56103-0

[141] U. Kumar and N. Sukavanam, "Backstepping based trajectory tracking control of a four wheeled mobile robot," *International Journal of Advanced Robotic Systems*, vol. 5, no. 4, p. 38, 2008. https://doi.org/10.5772/6224

[142] G. Oriolo, A. De Luca, and M. Vendittelli, "WMR control via dynamic feedback linearization: design, implementation, and experimental validation," *IEEE Transactions on control systems technology*, vol. 10, no. 6, pp. 835–852, 2002. https://10.1109/TCST.2002.804116

[143] S.G. Tzafestas, K.M. Deliparaschos, and G.P. Moustris, "Fuzzy logic path tracking control for autonomous non-holonomic mobile robots: Design of System on a Chip," *Robotics and Autonomous Systems*, vol. 58, no. 8, pp. 1017–1027, 2010. https://doi.org/10.1016/j.robot.2010.03.014

[144] H. Yu, G.-Y. Tang, H. Su, C.-P. Tian, and J. Zhang, "Trajectory tracking control of wheeled mobile robots via fuzzy approach," *Proceedings of the 33rd Chinese Control Conference*, pp. 8444–8449, 2014. DOI: 10.1109/ChiCC.2014.6896417

[145] J. Ye, "Tracking control of a non-holonomic wheeled mobile robot using improved compound cosine function neural networks," *International Journal of Control*, vol.

88, no. 2, pp. 364–373, 2015. https://10.1080/00207179.2014.953590

[146] X. Lu and J. Fei, "Velocity tracking control of wheeled mobile robots by fuzzy adaptive iterative learning control," *Chinese Control and Decision Conference (CCDC)*, pp. 4242–4247, 2016.https://10.1109/CCDC.2016.7531726

[147] S.K. Malu and J. Majumdar, "Kinematics, localization and control of differential drive mobile robot," *Global Journal of Research In Engineering*, Vol 14, No 1-H, 2014. Online ISSN: 2249-4596.

[148] I. Kolmanovsky and N.H. McClamroch, "Developments in nonholonomic control problems," *IEEE Control systems magazine*, vol. 15, no. 6, pp. 20–36, 1995. https://10.1109/37.476384

[149] A. De Luca, G. Oriolo, and M. Vendittelli, "Control of wheeled mobile robots: An experimental overview," in *Ramsete*, Springer, pp. 181–226, 2001. https://doi.org/10.1007/3-540-45000-9_8

[150] F. Wehbi, "Architecture logicielle et matérielle pour fusion tolérantes au fautes pour systèmes multi-robots sous ROS," *Master report*, University of Lille, France, University of Lebanon-Lebanon, 64 pages, 2015.

[151] K.E. Parsopoulos and M.N. Vrahatis, *Particle Swarm Optimization and Intelligence*, Information Science Reference, Hershey, Now-York, 329 pages, 2010.

[152] K.K. Vardhini et T. Sitamahalakshmi, A review on nature-based swarm intelligence optimization techniques and its current research directions. *Indian Journal of Science and Technology*, vol. 9, no 10, pp. 1-13, 2016.

[153] S. Slami, *Introduction à l'optimisation Méta-heuristique*, Ed: OPU, Algeria, 2019. ISBN: 978-9961-0-2113-2.

[154] R. Madiouni, "Contribution à la synthèse et l'optimisation multi-objectif par essaims particulaires de lois de commande robuste RST de systèmes dynamiques," PhD thesis, Université Paris-Est, France, Juin 2016.

[155] B. Saleh, A. Al-aqbi, and A. Saedi, "Comparative Study of Inspired Algorithms for Trajectory-Following Control in Mobile Robot," *International Journal of Modern Education and Computer Science*, vol. 10, pp. 1–10, Jan. 2018.

[156] L. Zhang, "Simplex method based optimal design of PID controller. *Information and Control*, " vol. 33, no 3, p. 376-379, 2004.

[157] S. Ghosal, R. Darbar, B. Neogi, A. Das, and D. N. Tibarewala, "Application of Swarm Intelligence Computation Techniques in PID Controller Tuning: A Review," *Proceedings of the International Conference on Information Systems Design and Intelligent Applications (INDIA 2012)*, Visakhapatnam, India, pp. 195–208, 2012. https://doi.org/10.1007/978-3-642-27443-5_23

[158] M. Zamani, M. Karimi-Ghartemani, N. Sadati, and M. Parniani, "Design of a fractional order PID controller for an AVR using particle swarm optimization," *Control Engineering Practice*, vol. 17, no. 12, pp. 1380–1387, Dec. 2009. https://doi.org/10.1016/j.conengprac.2009.07.005

[159] A. Oonsivilai and B. Marungsri, "Stability Enhancement for Multi-machine Power

System by Optimal PID Tuning of Power System Stabilizer using Particle Swarm Optimization.", *WSEAS transactions on power systems*, vol. 3, pp. 465-474, 2008.

[160] A. Jalilvand, A. Kimiyaghalam, A. Ashouri, and M. Mahdavi, "Advanced particle swarm optimization-based PID controller parameters tuning," *IEEE INMIC 2008: 12th IEEE International Multitopic Conference - Conference Proceedings*, pp. 429–435, 2008. DOI: 10.1109/INMIC.2008.4777776

[161] R.N. PATEL, "Application of artificial intelligence for tuning the parameters of an AGC, " *International Journal of Mathematical, Physical and Engineering Sciences*, vol. 1, no 2, p. 34-40, 2007.

[162] A. Almabrok, M. Psarakis, and A. Dounis, "Fast Tuning of the PID Controller in An HVAC System Using the Big Bang-Big Crunch Algorithm and FPGA Technology," *Algorithms*, vol. 11, no. 10, 146 pages, 2018. https://doi.org/10.3390/a11100146

[163] W. Qian *et al.*, "*Manipulation Task Simulation using ROS and Gazebo*", *IEEE International Conference on Robotics and Biomimetics (ROBIO 2014)*. pp. 2594-2598, 2014. https://10.1109/ROBIO.2014.7090732