Distributed vs. Hybrid Control Architecture Using STPA and AHP - Application to an Autonomous Mobile Multi-robot System

Chaima Bensaci, Youcef Zennir, Denis Pomorski, Fares Innal, Yiliu Liu

Distributed vs. Hybrid Control Architecture Using STPA and AHP - Application to an Autonomous Mobile Multi-robot System

Article *in* International Journal of Safety and Security Engineering · February 2021

DOI: 10.18280/ijsse.110101

CITATIONS
0

READS
57

5 authors, including:

Zennir Youcef
Université 20 août 1955-Skikda
75 PUBLICATIONS **135** CITATIONS
SEE PROFILE

Denis Pomorski
Université de Lille
112 PUBLICATIONS **714** CITATIONS
SEE PROFILE

Fares Innal
University of Batna 1
30 PUBLICATIONS **270** CITATIONS
SEE PROFILE

Yiliu Liu
Norwegian University of Science and Technology
95 PUBLICATIONS **530** CITATIONS
SEE PROFILE

International Journal of Safety and Security Engineering
Vol. 11, No. 1, February, 2021, pp. 1-12
Journal homepage: http://iieta.org/journals/ijsse

Distributed vs. Hybrid Control Architecture Using STPA and AHP - Application to an Autonomous Mobile Multi-robot System

Chaima Bensaci[1*], Youcef Zennir[2], Denis Pomorski[3], Fares Innal[2], Yiliu Liu[4]

[1] LGCES Laboratory, Université 20 Août 1955 Skikda, Skikda 21000, Algeria
[2] Automatic Laboratory of Skikda, Université 20 Août 1955 Skikda, Skikda 21000, Algeria
[3] CRIStAL Laboratory– UMR 9189, Lille University, Lille 59000, France
[4] Department of Production and Quality Engineering, Norweigian university of science and technology (NTNU), NO-7491 Trondheim, Norway

Corresponding Author Email: y.zennir@univ-skikda.dz

https://doi.org/10.18280/ijsse.110101

Received: 29 December 2020
Accepted: 9 February 2021

Keywords:
hazard analysis, STAMP model, system theoretic process analysis, distributed control architecture, hybrid control architecture, autonomous multi-mobile robots, analytic hierarchy process

ABSTRACT

Systems composed of a fleet of autonomous mobile robots are among the most complex control systems. This control complexity is at a high level especially when those robots navigate in hazardous and dynamic environments such as chemical analysis laboratories. These systems include different dangerous and harmful products (toxic, flammable, explosive...) with different quantity. In order to perform its mission on a regular basis, this multi-robot system can be controlled according to multiple architectures. We propose, firstly, to apply the System Theoretic Process Analysis (STPA) on two selected control architectures, namely distributed and hybrid architectures in order to obtain a set of loss scenarios for each kind of architecture. For further assessment, the Analytic Hierarchy Process (AHP) is used to choose the best architecture. The proposed approach provides a risk analysis and a more practical comparison between the two control architectures of a mobile multi-robot system and facilitates decision-making, even in complex situations.

1. INTRODUCTION

Nowadays, one of the biggest world challenges is ensuring the human work in complete safety, especially in dangerous environments such as nuclear power plants, hospitals, chemicals laboratories and so on. The use of a system consisting of a fleet of autonomous mobile robots seems to be an appropriate solution, but it is also one of the most complex systems to control. This complexity depends on several factors related to the complexity of the environment in which robots must operate and their knowledge about this unpredictable and changing environment. It also depends on the several features of robot such as the computing power, their moving capacities to reach target, the quality of communication and the number of collaborating robots [1, 2]. In a multi-agent system (multi-robot system: MRS), there are different ways to work together in a limited space and a hazardous environment with the existence of dangerous products. The fundamental technical aspects of MRS are coordination, cooperation, communication and interaction. These are crucial aspects to perform tasks correctly by a MRS. However, the misconception of these principles may constitute real sources of risk, for instance, collision between two robots carrying flammable, explosive or toxic products. Other risk sources may be induced by errors in the software used to control the MRS [3, 4]. With the technological advancement of sensors, intelligent controls, MRS are found in several application areas such as monitoring in a petroleum or nuclear facility, search and rescue in car accident (road or air transport), search for food in agriculture, exploration with drones from an agricultural field or risk zone, cooperative manipulation in a hospital or manufacturing industry, and transport of hazardous products in an analysis laboratory, among others [5]. Guiochet et al. [6], in their survey about safety-critical of robotic systems, mentioned that the risk and safety assessment of advanced robots has been treated in few research works. Sihai et al. [7], in order to increase worker safety and reduce asset losses, propose a standalone MRS to perform continuous inspection in power plants gasification integrated with biomass (BIGCC), where the maintenance of these plants is very crucial because of various hazards. Alexander et al. [8] studied the development of new advanced techniques for modeling and analysis of autonomous systems (AS) given the risks of interaction between the requirements and the ambiguity on the appropriate limits of the autonomous system. According to Saenz et al. [9], the involvement of MRS in the industrial field is slow due to the high security requirements and the lack of technical tools to analyze collaborative robotic (HRC) applications. These safety aspects are more or less high depending on the field of application. Okamura et al. [10] propose some key desired capabilities and technical achievements that a multi-robot system must have in the medical and health field in order to improve human health and well-being (socially assisted robotic system: SAR).

A strategy to manage human safety in a complex environment with the presence of a MRS is proposed by Lippi and Marino [11]. These robots are responsible for performing complex operations cooperating under appropriate functions. The authors propose safety control architectures regarding the increasing demand for close cooperation between humans and robots. They suggest the use of safety indices that depend both on the relative position, speed and trajectory of the human

operator and robots to ensure the safety of people. The robots considered in the previous study are robots manipulator type, unlike our case scenarios which are more complex with mobile robots where the variation of their positions and speeds and dynamics are similar to those of human operators.

Woodman et al. [3], discussed the safety issues related to the physical Human–Robot Interaction (pHRI) through the use of classical methods of risk analysis. The authors proposed a safety process to enhance the safety of autonomous personal robots. This process (protection of system security) is used to check the safety constraints observed in the risk analysis phase in order to control the execution of the robot action. In our case, this process is limited because of the strong interaction and cooperation between robots requiring a more general process to ensure the proper functioning of the system. Suwoong and Yamada [12], proposed a safety process for robotic systems with the human cooperation aspect (HCR) in automotive industry, where it is important to predetermine the required security level value, in order to design appropriate security functions and to analyze their validity. In our case, two control architectures of an MRS are used in order to propose safety functions for the functioning of the MRS.

Machin [13], proposed systematic methods for developing and justifying safety rules that take into account the versatility of autonomous systems like in our case (MRS). The human-robot interaction (HRI) is more and more of a topical issue because of the growth of the latter and the major risk it can cause to humans [14]. Guaranteeing a safe working environment for MRS requires a thorough study of potential risks and interaction architectures to control the operation of the MRS. Kazanzides [15] presented different security design strategy for medical robots with high-level security requirements, hazard analysis methods and security strategies. Fleming et al. [16] studied the improvement of the safety system of an air transport system regarding the technological advancement of today's aircraft using System Theoretic Accident Model and Processes (STAMP) and STPA methods. Dogzamadzi et al. [17] have developed a new structure of the Preliminary Risk Analysis (PHA) approach which explicitly aims to identify all undesirable and non-pre-work interactions determined by the use of new keywords sets. Böhm and Gruber [18], studied the application of Reliability, Availability, Maintainability and Safety (RAMS) analysis and the HAZard and OPerability analysis (HAZOP) method to a therapeutic robotic system for children, focusing on safety issues that are crucial for this specific therapeutic situation. Darmanin and Bugeja [5] worked on risk and safety analysis of a surgical platform with RAVEN II type robots, using the theoretical risk analysis technique (STPA) to identify potential risk scenarios and their causes.

Another approach has been developed by Martin-Guillerez et al. [19-21] to a mobile manipulator robot. They applied a modified HAZOP based on Unified Modeling Language (UML) description of human-robot interactions. A similar method was applied to an assistive robot [20]. However, these techniques could not adapt to take into account unwanted interactions between system components, interaction with environment and humans at the same time.

STPA method is developed by Leveson [22], which provides guide words like in HAZOP based on undesired interactions between components and multiple controllers, constitutes a useful alternative. It is true that the STPA method is a qualitative method and does not actually assess the risk quantitatively. However, it allowed us to provide a rigorous identification of hazardous scenarios of complex automated systems related to their control architectures. It has been applied to several safety extremely complex systems such as spacecraft [23], driving systems [24], aeronautical systems [25] and autonomous systems including robotic systems [4, 26, 27]. However, these studies do not consider the case of an autonomous multi-mobile robot. We already studied the safety aspects of a MSR with the Failure mode and effects analysis (FMEA) and Fault tree analysis (FTA) methods, and then we used a hierarchical STPA method combined with Bowtie approach [28-30].

In this paper, we consider N autonomous mobile robots all work in the same space and environment and have different or similar tasks. More specifically, the studied system could consist in transporting dangerous chemicals (toxic, flammable, explosive, infectious...) within a chemical analysis laboratory composed of one or more rooms, in the presence of analysis machines and workers. In order to fulfill its functions, this multi-robot system could be controlled according to several architectures (for instance, centralized, distributed, hierarchical and hybrid architecture). In order to ensure the safety of the system and the safety of the workers, we suggest the use of STPA while considering two control architectures, namely distributed architecture and hybrid architecture. The evaluation and selection of the best architecture will be performed thanks to the Hierarchical Analytical Process (AHP) which facilitates decision making in complex situations due to its efficiency for multi-criteria decision making process. The rest of this paper is organized as follows. Section 2 presents the Analysis carried out using STPA, which is a hazard investigation strategy, based on Systems-Theoretic Accident Model and Processes (STAMP). An overview on AHP is presented in Section 3. A first classification of the control architectures is proposed in Section 4. Section 5 is devoted to the risk analysis of the two types of control architecture with STPA. In Section 6, we present the decisions and the choice of the best control architecture using AHP. Finally, a discussion is presented before the conclusion in section 7.

2. STAMP/STPA HAZARD ANALYSIS

STPA is a hazard investigation strategy based on STAMP. This latter approach is based on causality model rather than reliability theory [31, 32]. STAMP is an accident model, which has been developed by Nancy Leveson [22, 33] based on system theory. In this conception of safety, accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately dealt by the control system. They result from lacking control or enforcement of safety-related constraints on the development, design, and operation of the system [34]. It has been well described in the studies [5, 32]. The STPA approach is fit for distinguishing potential perilous design blemishes, including software and hardware errors and unsafe interactions among various framework segments [35]. The main objective of STPA is to create a set of potentially hazardous scenarios [31]. STPA is more effective than the traditional hazard analysis such as FMEA and FTA, as mentioned by Nakao et al. [36]. Among its important benefits, it can be used to drive the earliest design decisions and then proceed in parallel with ensuing design decisions and design refinement, and its cost is potentially much cheaper than a

more conventional design process. In addition, Ishimatsu et al. [37] have shown the strength of utilizing STPA on complex systems by applying it to a transfer vehicle for aerospace exploration. A complex industrial system (multi-robot mobile system) is seen regarding the STPA method as a set of control loops with strong interactions. The study of the dependability and safety of the system begins first of all by the identification of the various possible hazards that can occur in order to translate them into high level safety constraints. Afterwards, a control structure (diagram) is proposed with a clear identification of the system components and the path of each control action and feedback.

Finally, this control structure will be used to analyze the safety of the system by associating to each control action guidewords and see whether they produce a hazard or not. For each control action, we should check if it is provided, not provided, provided too soon or too late or applying too long or losing too early could lead to a hazard, then each unsafe control action associated with their related major hazards. Inadequate actions, i.e. those that cause major hazards, will then be exploited to refine the system safety constraints. The safety analysis shows clearly the causes of potentially hazardous control actions. If the controls actions are inadequate, the recommendations will be essential in order to put in place additional mitigations measures [36, 37].

3. ANALYTICAL HIERARCHY PROCESS (AHP)

The hierarchical analytic process (AHP) is developed by Saaty [38]. This process is based on the decomposition of a complex multi-criteria decision-making problem into a hierarchical process. We find in the top level the objective of decision and in the lower levels the criteria and sub criteria. Decision Alternatives are found at the lowest level of this process [39, 40].

This theory is based on pairwise comparison and relies primarily on expert judgment to calculate priority scales. These comparisons are performed using a scale of absolute judgments. This judgment represents how much more one element dominates another with respect to a given attribute. In order to establish decision-making and the generation of priority, the decision must be broken down into several stages as follows:

First step: identify the problem and properly frame the knowledge sought.

Second step: proposal of a hierarchical decision structure from the top to bottom, with the decision object in the top, then the objectives in a broad perspective, through the intermediate levels (criteria on which the following elements depend) until lowest level (which is usually a set of alternatives decision), see Figure 1.

Third step: this step is based on the construction of pairwise comparisons matrices. A comparison pair consists of a top-level element (level number i) and a lower-level element (number i-1).

Last step: the priorities obtained from the comparisons will be used to weight the priorities in the level number (i-2). This operation must be repeated at all elements. At the end and for each element the global priority is deduced by adding these weighted values. The end of this process is determined by calculating the overall priorities of the alternative decisions.

The perfect application of this process requires a scale of numbers indicating the number of times one element is more important or dominant than another in relation to the criterion. For more details on this method, the reader could refer to the study [38].

Figure 1. Principal of AHP (hierarchical decision structure)

4. CLASSIFICATION OF DIFFERENT COMPLEX SYSTEMS' ARCHITECTURES

There are distinctive sorts of architectures to model complex systems control. From these architectures, structures for multi-agents are inspired.

The architecture of control of operation and organization of a complex industrial system differs according to its size and the complexity of the tasks to be carried out and also of the type of the system (production, service, etc. ...). The work done by Zennir [41], illustrates different architectures or structures of a production control system that have been proposed to improve the performance of existing industrial applications and meet the needs of future production systems. The different architectures are illustrated in the following Figure 2.

Zennir presented an adaptation of this type of architecture in order to control the coordination between the different agents (paw of a hexapod robot) [42]. In this study, we have opted for distributed architecture and hybrid architecture as depicted in the following Figures 3, 4.

The control of a robot's navigation can be simplified by breaking it up into several levels with certain independence according to the complexity of the task as shown in Figure 5. However, the simplification of the navigation control of a robot in increasing tasks complexity could lead to loss of information regarding the interaction between robots in the different levels.

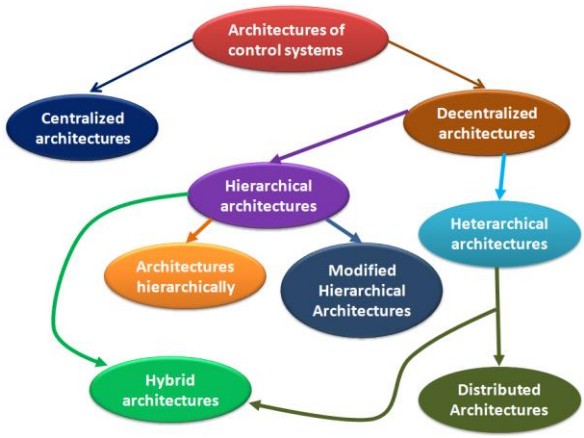


Figure 2. Different architectures [41]

Table 1. Advantages and disadvantages of distributed and hybrid architectures

Architecture type	Advantages	Disadvantages
Distributed architecture	Improving system flexibility (ability to easily add or remove robots) Increasing robustness Improving adaptation to changes Each robot is controlled independently of the others Sharing local and global information	Communication may become very complex Coordination between robots is very important and complex The achievement of the overall goal is based on local goals and it is very difficult to be ensured The overall performance of the system depends on the choice of local rules and negotiation protocols between the entities
Hybrid architecture	The central robot has a global view of the system (receives sensor information and issues commands for the robot control) Increasing robustness Good coordination between robots Sharing local information between them and global information to the central robot	The problem of finding the right compromise between hierarchical supervision and the degree of autonomy attributed to hierarchic levels. This compromise ensures stability and adaptation to the changing of the complex environment

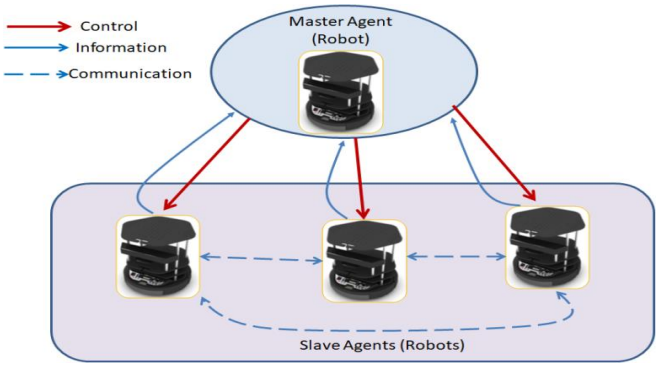


Figure 3. Hybrid architecture

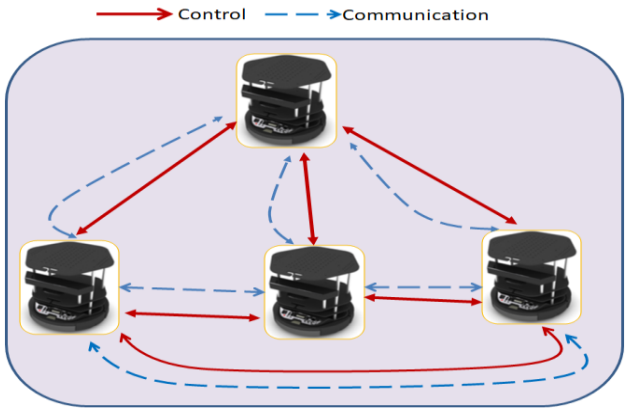


Figure 4. Distributed architecture

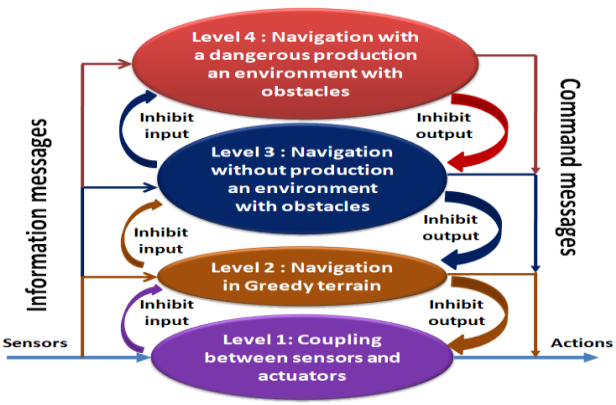


Figure 5. Control architecture for one robot

The strengths and weaknesses of distributed and hybrid architectures are illustrated in Table 1, which have collected from existing literature [41, 42].

The distributed architecture in multi-robot systems characterized by providing more autonomy in control for each robot which increases the robustness and flexibility of the system, however, in order to coordinate between robots' actions, inter-robots communication is required. All robots must communicate with each other to share and collect information (their positions, speeds, locations…) also to negotiate. This characteristic complicates the communication process and may cause problems especially in the case of a large number of robots; whereas, the hybrid architecture minimizes autonomy of the system and reduces inter-robot communication due to hierarchical control and centralized communication, which facilitate the coordination task.

The difficulty in hybrid control is to find the right compromise between hierarchical supervision and the degree of autonomy.

According to the properties that characterize each architecture, they can be classified depending on problems severity in three levels: the architecture which gives the minimum number of hazardous situations presents a low hazard, that which has the maximum number of hazardous situations presents a high hazard and the intermediate state between these two extremes presents a medium hazard. In our case, the two architectures present a medium hazard depending on problems severity.

5. HAZARD ANALYSIS OF THE TWO TYPES OF CONTROL ARCHITECTURES WITH STPA

This section illustrates the use of STPA on our system. It is composed of eleven mobile robots which transport hazardous chemicals between rooms within a chemical analysis laboratory as shown in Figure 6. For applying the STPA technique on this system, we start by recognizing the system accidents likely to happen and its hazards. Table 2 below presents accidents and hazards identification. After the hazards identification, the two types of control structures must be selected. There are several architectures to coordinate the control of these multi-robots. In this paper, as mentioned before, we propose to analyze the distributed and hybrid architectures.

Figure 6. Scenario related to eleven mobile robots within a chemical analysis laboratory

5.1 The distributed architecture

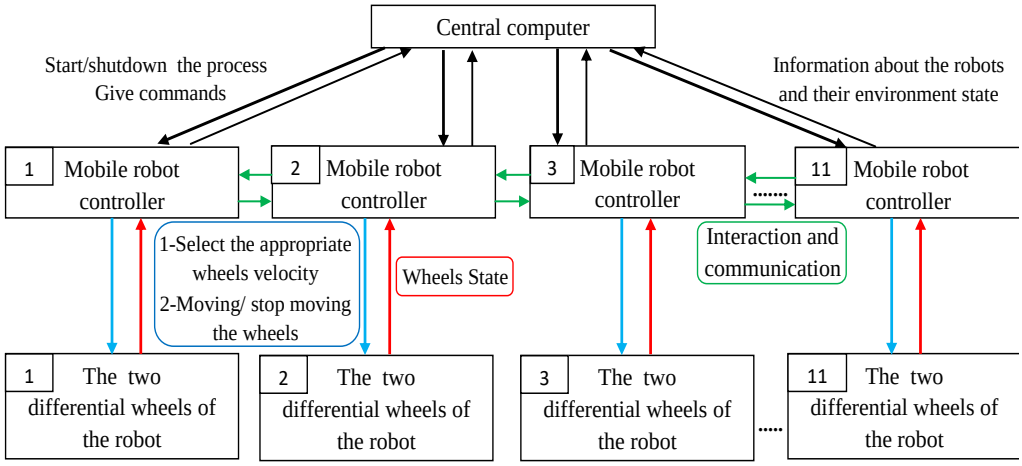
Figure 7 shows the distributed control architecture, which means that each mobile robot have total sensory and decisional autonomy. All robots are at the same level where they can communicate and coordinate with each other [41, 42].

Table 2. Identification of accidents and hazards

System Accidents	System Hazards
A1- Human worker die or become injured (collision of robots loaded with dangerous chemicals or between robot and human)	**H1-** Robots enters prohibited area / Dangerous chemicals spill
A2- Collision between robots (two or more)	**H2-** Robots violate the safer distance between them
A3- Robot crash to wall or falling down	**H3-** Robots enters uncontrolled state or unsafe attitude
A4- Explosion/ Fire	**H4-** Robots collide when they transport explosive /flammable chemicals, explosive/flammable chemicals spill

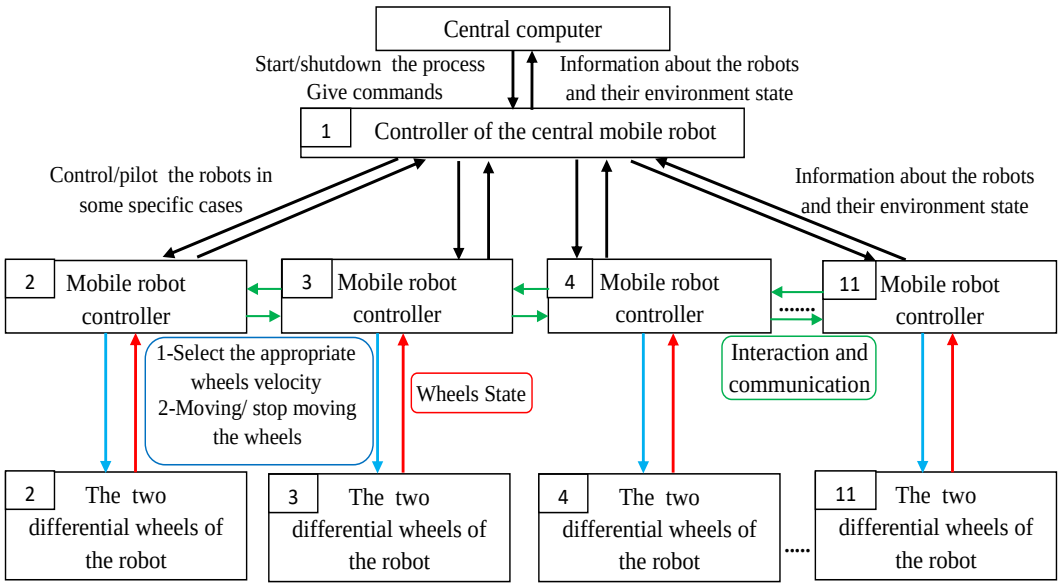
5.2 The hybrid architecture

Figure 8 shows the hybrid control architecture combining both centralized and distributed aspects. Centralized control is applied to give the strategies and general orders of the tasks to be executed, whereas the distributed control takes into account navigation and local actions. Communication and coordination between robots are provided, morover communication between the central robot and other slave robots [41, 42].



Note : Blue arcs refer to orders, the red ones refer to feedback and the green ones refer to communication

Figure 7. The distributed architecture for the studied system



Note : Blue arcs refer to orders, the red ones refer to feedback and the green ones refer to communication

Figure 8. The hybrid architecture for the studied system

Table 3. STPA hazard analysis table-part 1

	Control Actions	Unsafe control actions	Hazard	Hazard N°
The distributed architecture	**Start / shutdown the process by central computer**	- The start command **is provided** (**or not provided**) by the central computer to robots or to one of them.	**No Hazard**	
	Send commands (moving, stop moving)	- The controller **does not provide** the moving command to the wheels in front of a dynamic obstacle (human, the other robots).	**Yes**	**H1**
		- The controller **provides** the moving command to the wheels of a robot while the operator loads it by chemicals; or while there is an analysis machine or other robots stand in front of it.	**Yes**	**H2**
		- The controller **provides** a moving command to the wheels to turn in a wrong direction.	**Yes**	**H3**
		- The controller **provides** a moving command to the wheels **after a delay time**.	**Yes**	**H4**
		- The controller **stops providing** the moving command of the wheels **too soon** in front of other robots while they are transporting.	**Yes**	**H5**
		- The controller **does not provide** the stop moving command to the wheels when a dynamic/static obstacle moves/ stand (human- robots / analysis machine …) in front of it.	**Yes**	**H6**
		- The controller **provides** the stop moving command to the wheels in front of a dynamic obstacle (human, the other robots).	**Yes**	**H7**
		- The controller **provides** a stop moving command to the wheels **after a delay time**.	**Yes**	**H8**
		- The controller **stops providing /applies** the stop moving command of the wheels **too soon/too long** in front of the other robots while they are transporting.	**Yes**	**H9**
	Select velocity	- The controller **does not select** the appropriate velocity during navigation task (very high).	**Yes**	**H10**
		- The controller **changes** the velocity value **in an incorrect time** (**too early or too late**).	**Yes**	**H11**
	Communicate to coordinate robots actions	- **Provide** an interrupted communication inter-robots	**Yes**	**H12**
		- Inter-robots communication **not provided** or **provided too late**	**Yes**	**H13**

Table 3. STPA hazard analysis table-part 2

The hybrid architecture	**Start / shutdown the process by central computer**	**- The initial command** provided (or not provided) **by the central computer to the central robot.**	**No Hazard**	
	Send commands from master controller to other slave controllers to coordinate actions	- The master controller **does not provide** commands to other robots in emergency cases.	**Yes**	**H14**
		- The master controller **issues** a false command to the robots.	**Yes**	**H15**
		- The master controller **issues** a command **after a delay time** to robots in emergency cases.	**Yes**	**H16**
		- The master robot **provides** several commands to the same robot or repeats the same command to the same robot at the same time.	**Yes**	**H17**
	Send commands from controllers (moving, stop moving)	- The controller **does not provide** the moving command to the wheels in front of a dynamic obstacle (human, the other robots).	**Yes**	**H18**
		- The controller **provides** the moving command to the wheels of a robot while the operator loads it by chemicals; or while there is an analysis machine or other robots stand in front of it.	**Yes**	**H19**
		- The controller **provides** a moving command to the wheels to turn in a wrong direction.	**Yes**	**H20**
		- The controller **provides** a moving command to the wheels **after a delay time**.	**Yes**	**H21**
		- The controller **stops providing /applies** the stop moving command of the wheels **too soon/too long** in front of the other robots while they are moving.	**Yes**	**H22**
	Select velocity	- The controller **does not select** the appropriate velocity during navigation task (very high).	**Yes**	**H23**
		- The controller **changes** the velocity value **in an incorrect time (too early or too late)**.	**Yes**	**H24**
	Communicate to coordinate robots actions	- **Provide** an interrupted communication from master.	**Yes**	**H25**
		- Communication between master and other robots **not provided** or **provided too late.**	**Yes**	**H26**
		- **Provide** an interrupted communication inter-robots at the same level.	**Yes**	**H27**
		- Inter-robots communication **not provided or provided too late**.	**Yes**	**H28**

5.3 Obtained result from STPA application

Table 3 presents an assessment of the control actions provided in the multi-robot system design with STPA method using the two control architectures presented in Figures 7 and 8 in order to determine the potential for inadequate controls leading to hazardous situations.

After carring out the STPA method, we conclude that:

- A lot of the problems may be arise from unintended interactions between system components and due to bad controllers communication.
- Among the conditions that must be respected for the proper functioning of complex systems is timing and appropriate velocity (good control of speed, speed limits) in addition to ensure instruments integrity,which are used for control, communication moving and sensing.
- Hybrid architecture is the architecture that has a minimum severity;it represents the least risk compared with distributed architecture.

Distributed architecture is the most dangerous with ten hazard scenarios with high severity from thirteen hazards. Hybrid architecture presents just four hazard scenarios with high severity from fifteen hazard scenarios.

6. SELECTING THE BEST CONTROL ARCHITECTURE USING AHP

In the following we will determine what type of architecture would be best and safer to coordinate the control of the autonomous multi-robot system: either to choose a distributed architecture or hybrid architecture. According to AHP methodology, we start by identifying the overall objective of the decision and choosing the main criteria, the sub-criteria if they exist and the alternatives. In our case, we have identified six main criteria namely: flexibility, adaptation to changes, coordination, communication, achieving the overall goal and robustness.

These criteria reflect the main and necessary characteristics for the good and safe functioning of multi-robots and therefore the safety of human beings and their environment. Safety was not explicitly considered as a decision criterion because it is implicit regarding each used factor or criterion (flexibility, communication …). The failure in ensuring one of the specified criteria impacts directly the safety of potential targets (people ...).

Each criterion is explained below:

- Flexibility: the possibility to easily add or remove robots, this choice is necessary in a multi-robot system in order to ensure the overall task, that is to say if a robot fails the other robots must ensure the execution of the overall task.
- Adaptation to changes: each robot must have a behavior that allows it to adapt to changes in the environment: static obstacles (analysis machines, doors, walls, etc.), dynamic obstacles (other robots and workers), different loads and tasks to be carried out.
- Coordination: very crucial criterion for a mobile robotic system. The coordination is essential to carry out a complex task and avoid accidents while mobile robots are moving in the same environment.
- Communication: it is an important criterion for other criteria such as coordination, we cannot ensure it if we do not have good communication and we cannot adapt to the change of the environment if communication is bad or failing.
- Achieving the overall goal: each system has a global objective, for example a certain number of analyzes per day, each robot ensures its local objective and with coordination it ensures the global objective. It is very important to achieve the overall goal.
- Robustness: a multi-robot system should be able to continue achieving the required tasks under internal perturbations (e.g. motors or sensors failures) or external ones (e.g. trajectory modification or loads).

The hierarchical decision structure is shown in Figure 9.

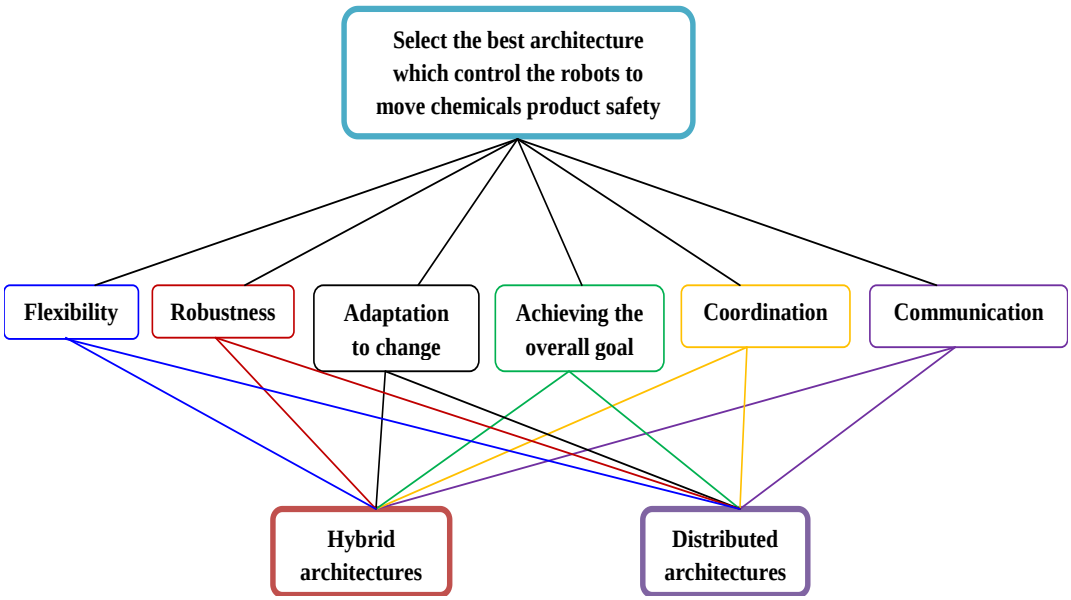


Figure 9. Hierarchical decision structure for the multi-robot systems

Table 4. AHP scale for combinations

Numerical scale	Definition	Explanation
1	Equal significance of the two elements	Two elements contribute equally to the property
3	Low significance of one element compared to another	Experience and personal assessments favor one element slightly over another
5	Strong significance of one element compared to another	Experience and personal assessments favor one element strongly over another
7	Confirmed dominance of one element over another	One element is strongly favored and its dominance is borne out in practice
9	Absolute dominance of one element over another	The evidence favoring one element over another appears irrefutable
2, 4, 6 and 8	Intermediate values between two neighboring levels	The assessment falls between two levels
Reciprocals (1/x)	A value attributed when activity i is compared to activity j becomes the reciprocal when j is compared to i	

6.1 Criteria and alternatives pairwise comparison

The elements of each hierarchical level must be subjected to pairwise comparisons with respect to each element of the higher hierarchical level. This step makes it possible to build matrices of comparisons. The values of these matrices are obtained by transforming the judgments into numerical values according to the Saaty scale (Scale of Binary Comparisons, see Table 4) [43, 44]. The evaluation of criteria was based on the experience of experts in the field.

Comparison matrices of criteria and alternatives are written in the following form:

$$M = [a_{ij}] = \begin{array}{c} criteria \\ c_1 \\ c_2 \\ \vdots \\ c_n \end{array} \begin{array}{c} \begin{array}{cccc} c_1 & c_2 & \dots & c_n \end{array} \\ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{pmatrix} \end{array} \quad (1)$$

where, M is the criteria comparison matrix, a_{ij} is the value that is in the intersection of the cell i column and j line, c_1, c_2 to c_n are the comparison criteria.

The comparison matrix of alternatives has the same form as comparison matrix of criteria in Eq. (1).

6.2 Priority vector and consistency

6.2.1 Priority vector

Through the evaluations obtained (the previous step), the determination of elements priorities of each matrix is done by solving the eigenvector problem as follows:

- Normalize the comparison matrices making the sums of each column then divide each element of the matrix by the total of the column.
- Calculate the average of the elements of each row of the matrix, the result is called priority vector W.

6.2.2 Calculating the average (λ_{max})

In order to calculate the maximum eigen-value of matrix Mc, λ_{max}, we have to follow these steps:

- Determine a weight sums vector, Ws using Eq. (2):

$$\{Ws\} = [M] . \{W\} \quad (2)$$

- Find consistency vector by Eq. (3):

$$\{consis\} = \{Ws\} . \{1/W\} \quad (3)$$

- Determine the average of the elements of$\{consis\}$: λ_{max}.

6.2.3 Checking for consistency

The consistency of judgments can be evaluated using Eq. (4):

- Determining the Consistency Ratio (CR):

$$CR = \frac{CI}{RC} \quad (4)$$

With:

- CI stands for Consistency Index that it is calculated by Eq. (5):

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (5)$$

- RC (Random Consistency index) can be acquired from Table 5:

Table 5. Table of random consistency index

n	1	2	3	4	5
RC	0	0	0.58	0.9	1.12
n	6	7	8	9	10
RC	1.24	1.32	1.41	1.45	1.49

where, n is the criterion number.

- If RC ≤ 10%, the matrix is considered to be sufficiently consistent.
- In the other case, where this value exceeds 10%, the assessments may require certain revisions.

6.2.4 Calculating the final aggregation

The final step is to distribute the relative weights for each level of the hierarchy in order to calculate the overall priorities using Eq. (6).

$$[FR]^T \times \{W\} \quad (6)$$

FR (Final Rating matrix) is a matrix n∗m that contains the average values of each row of the normalized alternatives matrix with respect to each criterion where *n* is the criterion number and *m* is the number of alternatives.

6.3 Obtained result from AHP application

The criteria matrices, alternatives criteria and different

parameters for AHP methods used for comparing different control architecture are illustrated in the Tables 6, 7, 8, 9.

Then, we can find the value $Fr^T \times W$ for the two types of architectures as follow:

Case of distributed architecture

$$Fr^T \times w = 0.161975327 \quad (7)$$

Case of hybrid architecture

$$Fr^T \times w = 0.588024673 \quad (8)$$

Table 6. Table of criteria matrix

Criteria matrix						
Criteria	**Flexibility**	**Adaptation to changes**	**Coordination**	**Communication**	**Achieving the overall goal**	**Robustness**
Flexibility	1	3	0.2	0.2	0.1111	0.3333
Adaptation to changes	0.3333	1	0.2	0.2	0.1111	0.3333
Coordination	5	5	1	1	0.2	5
Communication	5	5	1	1	0.2	5
Achieving the overall goal	9	9	5	5	1	9
Robustness	3	3	0.2	0.2	0.1111	1

Table 7. Table of alternatives matrix

Alternatives matrix								
	Flexibility			***Adaptation to changes***			***Coordination***	
Alternatives	**Distributed architecture**	**Hybrid architecture**	**Alternatives**	**Distributed architecture**	**Hybrid architecture**	**Alternatives**	**Distributed architecture**	**Hybrid architecture**
Distributed architecture	***1***	***5***	***Distributed architecture***	*1*	*9*	**Distributed architecture**	*1*	*0.2*
Hybrid architecture	***0.2***	***1***	***Hybrid architecture***	*0.111111111*	*1*	**Hybrid architecture**	*5*	*1*
Sum of each column	**1.2**	**6**	**Sum of each column**	1.111111111	10	**Sum of each column**	6	1.2
	Communication			***Achieving the overall goal***			***Robustness***	
Alternatives	**Distributed architecture**	**Hybrid architecture**	***Alternatives***	***Distributed architecture***	***Hybrid architecture***	**Alternatives**	***Distributed architecture***	***Hybrid architecture***
Distributed architecture	1	0.111111111	**Distributed architecture**	1	0.2	**Distributed architecture**	1	0.333333333
Hybrid architecture	9	1	**Hybrid architecture**	5	1	**Hybrid architecture**	3	1
Sum of each column	10	1.111111111	**Sum of each column**	6	1.2	**Sum of each column**	4	1.333333333

Table 8. Table of Fr transpose

Fr transpose						
Alternatives/ Criteria	Flexibility	Adaptation to changes	Coordinantion	Communication	Achieving the overall goal	Robustness
Distributed architecture	0.833333333	0.9	0.166666667	0.1	0.166666667	0.25
Hybrid architecture	0.166666667	0.1	0.833333333	0.9	0.833333333	0.75

Table 9. Checking consistency

Ws vector	Consistency vector	Criteria Weights (W)	1/w	Result
0.2168914	5.960500305	0.036388117	27.481499	Lamda 6.562072329
0.14623	6.302664379	0.023201304	43.101027	CI 0.1124145
0.8868899	6.908106812	0.128383925	7.7891371	RI 1.25
0.8868899	6.908106812	0.128383925	7.7891371	CR 0.0899316
2.662864	6.961589207	0.382508069	2.6143239	CR<0.1 consistent
0.3237574	6.331466459	0.05113466	19.556207	

The first pair wise comparison was made among the parameters of the six criteria influencing the top level in the hierarchy, see the histogram in Figure 10. The objective is to determine at first which criteria are more important than others.

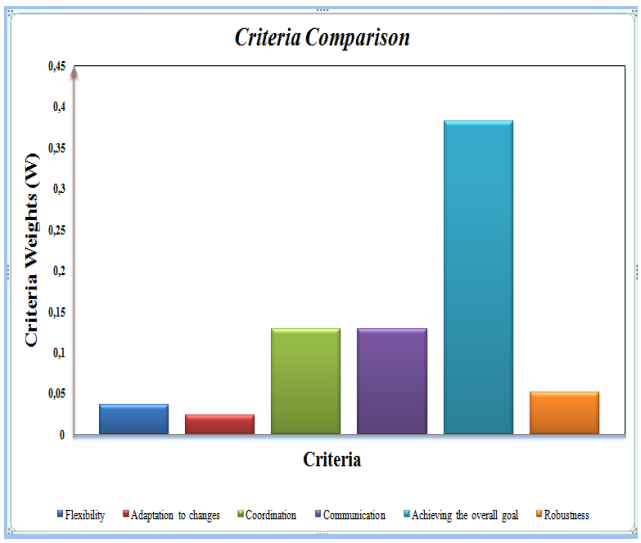


Figure 10. Criteria comparison

In order to ensure the consistency of the judgments in criteria matrix, consistency ratio (CR) was calculated using Eqns. (1) to (4). The result is shown in Table 10:

Table 10. Parameters used with AHP methods

λ_{max}	*RC*	*CI*	*CR*
6.562	**1.24**	**0.112**	**0.091< 0.1**

The value of CR is lower than 0.1 (CR <10%) so our ranking is consistent.

The second pairwise comparison has been made between the two alternatives (distributed and hybrid architectures) in order to select which architecture is more important for each criterion. The comparison result is presented in Figure 11.

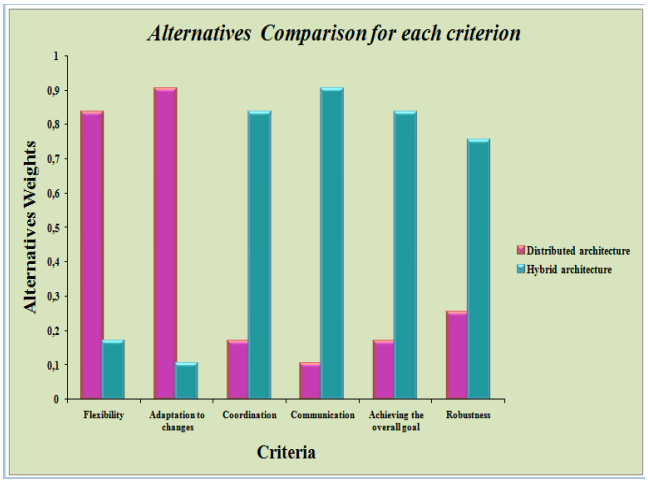


Figure 11. Alternatives comparison for each criterion

The final result of the comparison between the two control architectures with AHP method is presented in Figure 12.

From the results of the pairwise comparisons, we observe that:

- The criterion "achieving the overall goal" is the most important one, then the "coordination" one and finally "communication".
- The distributed architecture is more flexible and more suitable to changes than the hybrid one, whereas the hybrid is better in 4 criteria: communication, coordination, robustness and reaching the overall goal.
- The final result shows that the hybrid architecture is three times better than the distributed one according to the selected criteria.

After performing the STPA and AHP methods, the hybrid architecture is considered as the best choice to control the considered multi-robot system in a safe way.

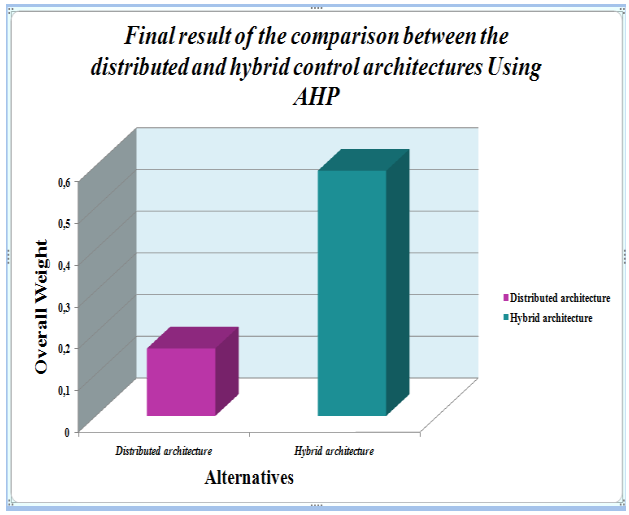


Figure 12. Final ranking for the two control architectures

7. CONCLUSION

The main goal of this paper was to compare two control architectures, i.e. distributed and hybrid, in order to determine the one that should be used to manage the multi-robot system in a safe way. For this reason, we performed two types of analysis: STPA and AHP. STPA is a hazard analysis method used to identify the hazard scenarios that would take place in the event when undesired control actions are provided. The AHP is a multi-criteria decision-making method used for selections and evaluations. As a first step, we analyzed both architectures using the STPA risk analysis method. We identified all the dangerous control measures and assessed the severity of the associated risks. In a second step using AHP, we determined the best architecture to control the multi-robot system according to different criteria. Based on the results of STPA and AHP, we concluded that hybrid architecture is the best choice we should implement to control the multi-robot system navigation. In fact, that architecture is the most robust and the best in terms of coordination and communication. This helps robots to cooperate and achieve their goal effectively and safely. This study has clearly shown the adaptation and application of risk analysis methods to two control architectures of a multi-robot mobile system with very specific parameters and constraints. Its generalization is possible with the change of these constraints.

REFERENCES

[1] Laouici, Z. (2015). La modélisation d'un système de coopération et communication dans la navigation des robots mobiles. PhD Thesis, Modèle de données

avancées et réseaux émergents (in frensh), PhD thesis, University of Oran 1, Algeria, 121 pages.

[2] Van Tuan, L. (2010). Cooperation dans les systèmes multi-robots: Contribution au maintien de la connectivité et à l'allocation dynamique de rôles. Robotique (in frensh). PhD Thesis. University of Caen, France, 137 pages.

[3] Woodman, R., Winfield, A.F., Harper, C., Fraser, M. (2012). Building safer robots: Safety driven control. Internatioanl Journal of Robotics Research, 31(13): 1603-1626. https://doi.org/10.1177/0278364912459665

[4] Alemzadeh, H., Chen, D., Lewis, A., Kalbarczyk, Z., Raman, J., Leveson, N., Iyer, R. (2015). Systems-theoretic safety assessment of robotic telesurgical systems. In Proceedings of the 34th international conference on Computer Safety, Reliability, and Security (SAFECOMP'15), Delft, The Netherlands, pp. 213-227. https://doi.org/10.1007/978-3-319-24255-2_16

[5] Darmanin, R.N., Bugeja, M.K. (2017). A review on multi-robot systems categorised by application domain. 25th Mediterranean Conference on Control and Automation (MED), July 3-6, Valletta, Malta, pp. 701-706. http://doi.org/10.1109/MED.2017.7984200

[6] Guiochet, J., Machin, M., Waeselynck, H. (2017). Safety-critical advanced robots: A survey. Robotics and Autonomous Systems, 94: 43-52. http://doi.org/10.1016/j.robot.2017.04.004

[7] Sihai, A., Farshad, A., Simon, W., Barry, L. (2019). Development of a multi-robotic system for exploration of biomass power plants. Personal paper, pp. 1-5.

[8] Alexander, R., Kelly T., Herbert, N. (2009). Deriving safety requirements for autonomous systems. In Proceedings of the 4th SEAS DTC Technical Conference, Edinburgh, pp. 1-8.

[9] Saenz, J., Elkmann, N., Gibaru, O., Neto, P. (2018). Survey of methods for design of collaborative robotics applications- Why safety is a barrier to more widespread robotics uptake. Proceedings of the 2018 4th International Conference on Mechatronics and Robotics Engineering, pp. 95-101. http://doi.org/10.1145/3191477.3191507

[10] Okamura, A.M., Mataric, M.J., Christensen, H.I. (2010). Medical and health-care robotics achievements and opportunities. IEEE Robotics & Automation Magazine, 17(3): 26-37.

[11] Lippi, M., Marino, A. (2018). Safety in human-multi robot collaborative scenarios: A trajectory scaling approach. IFAC-PaperOnLine, 51(22): 190-196. http://doi.org/10.1016/j.ifacol.2018.11.540

[12] Suwoong, L., Yamada, Y. (2012). Risk assessment and functional safety analysis to design safety function of a human-cooperative robot. In Human Machine Interaction - Getting Closer, Mr Inaki Maurtua (Ed.). Intech, 18 pages.

[13] Machin, M. (2015). Synthèse de règles de sécurité pour des systèmes autonomes critiques (in frensh). PhD Thesis. University of Toulouse 3 Paul Sabatier, France, 120 pages.

[14] Goodrich, M.A., Schultz, A.C. (2007). Human-robot interaction: A survey. Foundations and Trends in Human-Computer Interaction, 1(3): 203-275. http://doi.org/10.1561/1100000005

[15] Kazanzides, P. (2009). Safety design for medical robots. In Proceedings of the 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS), Minneapolis, Minnesota, USA, pp. 7208-7211. http://doi.org/10.1109/IEMBS.2009.5335275

[16] Fleming, C.H., Spencer, M., Thomas, J., Leveson, N., & Wilkinson, C. (2013). Safety assurance in NextGen and complex transportation systems. Safety Science, 55: 173-187. http://doi.org/10.1016/j.ssci.2012.12.005

[17] Dogramadzi, S., Giannaccini, M.E., Harper, C., Sobhani, M., Woodman R., Choung, J. (2014). Environmental hazard analysis - A variant of preliminary hazard analysis for autonomous mobile robots. Journal of Intelligent & Robotic Systems, 76(1): 73-117. http://doi.org/10.1007/s10846-013-0020-7

[18] Böhm, P., Gruber, T. (2010). A novel HAZOP study approach in the RAMS analysis of a therapeutic robot for disabled children. In Proceedings of the 29th international conference on Computer Safety, Reliability, and Security (SAFECOMP'10), pp. 15-27. http://doi.org/10.1007/978-3-642-15651-9_2

[19] Martin-Guillerez, D., Guiochet, J., Powell, D., Zanon, C. (2010). An UML-based method for risk analysis of human-robot interactions, 2nd International Workshop on Software Engineering for Resilient Systems, pp. 32-41. http://doi.org/10.1145/2401736.2401740

[20] Guiochet, J. (2015). Trusting robots: Contributions to dependable autonomous collaborative robotic systems. Embedded Systems. PhD thesis. University of Toulouse 3 Paul Sabatier, France, 150 pages.

[21] Guiochet, J. (2016). Hazard analysis of human–robot interactions with HAZOP–UML. Safety Science, Elsevier, 84: 225-237. http://doi.org/10.1016/j.ssci.2015.12.017

[22] Leveson, N.G. (2011). Engineering a safer world: Systems thinking applied to safety. Cambridge, MA: The MIT Press, 555 pages. http://doi.org/10.7551/mitpress/8179.001.0001

[23] Ishimatsu, T., Leveson, N.G., Thomas, J.P., Fleming, C.H., Katahira, M., Miyamoto, Y., Ujiie, R., Hakao, H., Hoshino, N. (2014). Hazard analysis of complex spacecraft using systems-theoretic process analysis. Journal of Spacecraft and Rockets, 51(2): 509-522. http://doi.org/10.2514/1.A32449

[24] Abdulkhaleq, A., Baumeister, M., Böhmert, H., Wagner, S., (2018). Missing no interaction—Using STPA for identifying hazardous interactions of automated driving systems. International Journal of Safety Science, 2(1): 115-124. http://doi.org/10.24900/ijss/0201115124.2018.0301

[25] Plioutsias, A., Karanikas, N. (2015). Using STPA in the evaluation of fighter pilots training programs. Procedia Engineering, 128: 25-34. http://doi.org/10.1016/j.proeng.2015.11.501

[26] Wróbel, K., Montewka, J., Kujala, P. (2018). Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliability Engineering & System Safety, 178: 209-224. http://doi.org/10.1016/j.ress.2018.05.019

[27] Banda, O.A.V., Kannos, S. (2017). Hazard analysis process for autonomous vessels. Technical report, p. 69.

[28] Bensaci, C., Zennir, Y., Pomorski. D. (2018). A comparative study of STPA hierarchical structures in risk analysis: The case of a complex multi-robot mobile system. 2nd IEEE European Conference on Electrical

Engineering & Computer Science, EECS 2018, Bern, Switzerland, pp. 1-6. http://doi.org/10.1109/EECS.2018.00080

[29] Bensaci, C., Zennir, Y., Pomorski, D., Mechhoud, E. (2017). Complex safety study of intelligent multi-robot navigation in risk's environment. IEEE/AESS ICCST, The 51st International Carnahan Conference on Security Technology, Madrid, Spain, pp. 1-6. http://doi.org/10.1109/CCST.2017.8167809

[30] Bensaci, C., Zennir, Y., Pomorski, D., Innal, F., Liu, Y. Tolba, C. (2020). STPA and bowtie risk analysis study for centralized and hierarchical control architectures comparison. Alexandria Engineering Journal, 59(5): 3799-3816. https://doi.org/10.1016/j.aej.2020.06.036

[31] Young, W., Leveson, N.G. (2014). Inside risks - An integrated approach to safety and security based on systems theory - Applying a more powerful new safety methodology to security risks. Communications of the ACM, 57(2): 31-35.

[32] Ishimatsu, T., Leveson, N., Thomas, J., Katahira, M., Miyamoto, Y., Nakao, H. (2010). Modeling and hazard analysis using STPA. In Proceedings of the 4th IAASS Conference, Making Safety Matter. European Space Agency Publications-Esa Sp, 680: 31 pages.

[33] Leveson, N.G. (2004). A new accident model for engineering safer systems. Safety Science, 42(4): 237-270. http://doi.org/10.1016/S0925-7535(03)00047-X

[34] Leveson, N.G. (2009). Software challenges in achieving space safety. Journal of the British Interplanetary Society (JBIS), 62(7/8): 15 pages.

[35] Stringfellow, M.V., Leveson, N.G., Owens, B.D. (2010). Safety-driven design for software-intensive aerospace and automotive systems. In Proceedings of the IEEE, 98(4): 515-525. http://doi.org/10.1109/JPROC.2009.2039551

[36] Nakao, H., Katashira, M., Miyamoto, Y., Leveson, N. (2011). Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. In Proceedings of the 5th International Conference of the Association for the Advancement of Space Safety (IAASS), 5 pages.

[37] Ishimatsu, T., Leveson, N.G., Fleming, C.H., Katahira, M., Miyamoto, Y., Nakao, H. (2011). Multiple controller contributions to hazards. In Proceedings of the 5th IAASS Conference. European Space Agency Publications - Esa Sp, 699: 76 pages.

[38] Saaty, T.L. (2008). Decision making with the analytic hierarchy process. International Journal of Services Sciences, 1(1): 83-98. http://doi.org/10.1504/IJSSCI.2008.017590

[39] Triantaphyllou, E. (2000). Multi-criteria decision making methods: A comparative study. Springer Science+Business Media Dordrecht, 44: 306 pages. http://doi.org/10.1007/978-1-4757-3157-6

[40] Pohekar, S.D., Ramachandran, M. (2004). Application of multi-criteria decision making to sustainable energy planning - A review. Renewable and Sustainable Energy Reviews, 8(4): 365-381. http://doi.org/10.1016/j.rser.2003.12.007

[41] Zennir, Y. (2004). Apprentissage par renforcement et systèmes distribués: Application à l'apprentissage de la marche d'un robot hexapode (in frensh). PhD Thesis. INSA de Lyon, France, 180 pages.

[42] Adouane, L. (2005). Architectures de contrôle comportementales et réactives pour la coopération d'un groupe de robots mobiles (in frensh). PhD Thesis. University of Franche-Comté, France, 220 pages.

[43] Aminbakhsh, S., Gunduz, M., Sonmez., R. (2013). Safety risk assessment using analytic hierarchy process (AHP) during planning and budgeting of construction projects. Journal of Safety Research, 46: 99-105. http://dx.doi.org/10.1016/j.jsr.2013.05.003

[44] Brunelli, M. (2015). Introduction to the analytic hierarchy process. Springer Briefs in Operations Research, 1-83. http://doi.org/10.1007/978-3-319-12502-2