STPA and Bowtie Risk Analysis Study for Centralized and Hierarchical Control Architectures Comparison

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

Alexandria Engineering Journal (2020) xxx, xxx–xxx

HOSTED BY

ELSEVIER

Alexandria University

Alexandria Engineering Journal

www.elsevier.com/locate/aej
www.sciencedirect.com

STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison

Chaima Bensaci [a], **Youcef Zennir** [b,*], **Denis Pomorski** [c], **Fares Innal** [b], **Yiliu Liu** [d], **Cherif Tolba** [e]

[a] *Université 20 Août 1955 Skikda, LGCES Laboratory, 21000 Skikda, Algeria*
[b] *Université 20 Août 1955 Skikda, Automatic Laboratory of Skikda, 21000 Skikda, Algeria*
[c] *Lille University, CRIStAL Laboratory – UMR 9189, 59000 Lille, France*
[d] *Department of Mechanical and Industrial Engineering Faculty of Engineering, NTNU University, NO-7491 Trondheim, Norway*
[e] *Université Badji Mokhtar –Annaba, B.P.12, 23000 Annaba, Algeria*

Received 18 January 2020; revised 14 April 2020; accepted 21 June 2020

KEYWORDS

Hazard identification;
System-theoretic process analysis;
Bowtie analysis;
Robotic systems;
Coordination structures

Abstract The industrial zones are increasingly invaded by groups of mobile robots that are the most capable to perform complex tasks by collaborating and cooperating together. The operation of a mobile robot within a dynamic and high-risk environment with strong interaction between robot-robot and human-robot is of a certain complexity of control and safety. Such type of systems requires a safety and hazard investigation to verify if it is able to operate under certain operating conditions, while still ensuring the control and collaboration between mobile robots and human. This paper presents an approach that combines aspects of System-Theoretic Process Analysis (STPA) and Bowtie for safety assessment purposes. The approach we propose is used for a case related to multi-robot systems considering the coordinating, cooperating and collaborating aspects. At first, a risk identification study is done using STPA to extract a set of risk scenarios related to different types of hierarchical coordination architectures in addition to their factors. Afterward, an evaluation of the obtained scenarios is performed by the Bowtie method. The aim of our study is to better compare different control approaches of a multi-agent system. The combination offers detailed hazard identification. It further provides a classification of risks which helps to improve STPA outcomes thus facilitate decision-making over the suitable approach.

* Corresponding author.
E-mail addresses: ch.bensaci@univ-skikda.dz (C. Bensaci), y.zennir@univ-skikda.dz (Y. Zennir), denis.pomorski@univ-lille.fr (D. Pomorski), fares.innal@univ-skikda.dz (F. Innal), yiliu.liu@ntnu.no (Y. Liu), cherif.tolba@univ-annaba.dz (C. Tolba).

Peer review under responsibility of Faculty of Engineering, Alexandria University.

1. Introduction

The continuous progress of industrialization has revealed the incapability of human to accomplish some hard and unsafe

https://doi.org/10.1016/j.aej.2020.06.036

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

missions which requires effort and stronger focus. Human made social robots with basic properties to meet some needs: like human simulation, cooperation and self-control, as well as interaction and collaboration between human and robots. Robots are actually widely spread in many industries, including automotive, medical, and power sectors. Although the use of cooperative mobile robots offers significant assistance to workers, severe consequences could be left if it is not appropriately structured and monitored. Hence, the emergence of mobile robotic entities within the field of industries which characterized by their dangerous zones like testing Labs that contain high-risk kinds of products (explosive, flammable, extremely toxic,...) requires a careful systematic investigation in order to aggregate all possible hazards and causes during the operation phase. It is worth noting that after robots acquired new features like autonomy, human-robot cooperation and intelligence skills [1,2] new hazards have appeared and traditional risk analysis becomes inadequate [3]. Various combination and improvements of hazard analysis methods have been proposed to better predict faults and hazards in the use of autonomous and collaborative robots. FMEA and FTA were used for collaborative robots in medical field [4,5]. A similar approach has been applied in [6] for a set of autonomous mobile robots working in a chemical laboratory. A variant of HAZOP was used for a therapeutic robot in [7] and for software in [8], Alexander et al., also have combined HAZOP and Functional Failure Analysis [9]. The authors, in [10], have developed a variant method of preliminary hazard analysis using new guidewords which called Environmental Hazard Analysis Survey ESHA. HAZOP-UML method focusing on human–robot interaction has been done in [11]. However, all these techniques are least able to consider specificities like the control structures and truly show all appropriate interactions between its components and encompassing the environment. To overcome these drawbacks, a method named System Theoretic Process Analysis STPA has been firstly created by Leveson [12], which provides guidewords like in HAZOP based on undesired interactions between components and multiple controllers. It has been applied to a robotic telesurgical system [13]. The same approach has been used successfully further for other complex systems such as automotive systems [14] and autonomous vessels [15]. Other research studies have been focused on risk analysis in multi-agent systems using System-Theoretic Accident Model and Processes (STAMP) and STPA approach described in [22,23]. It is true that researchers have obtained positive outcomes from applying STPA to those controlled systems, however, the analysis still insufficient since the method is fully qualitative.

Multi-agent systems require precise control which interest in coordination, cooperation, interaction aspects. Therefore, different organizational control approaches of an industrial system have been developed within the framework of a multi-agent system in the literature [16–21], where this multi-agent technology is seen as an important approach to the development of intelligent solutions (distributed or not) to control a complex industrial system. A multi-agent approach gives both different structures to a complex system and more organization, interaction, communication and collaboration between different agents (eg. robot in our case-study). Multi-agent systems can perform complex tasks with a certain level of security depending on the chosen approach [19]. These approaches are closely related to the complexity of the system and the mode of operation regarding its size and type of coordination and communication. Furthermore the collaboration feature is a very important behavior to ensure the stability and consistency of the whole system [19]. These different types of approaches are illustrated in the following figures (see Fig. 1).

In recent years, the distributed and hybrid control approaches become an attractive research area of the scientists' community. Kim et al. [18] proposed a hybrid approach for a system of planning and control based on an intelligent agent to solve the issue of order-picking within an industrial site, whereas hierarchical approach is used for communication and interaction in a computer network [20], according to the following figure (see Fig. 2).

Ben Othman [21] proposed a distributed multi-agent approach for Emergency Supply Chain Management (ESC), in which each area is controlled by an agent. In an operating process of an industrial system, the control must adjust and ensure the proper functioning in real time to execute the tasks in order to respond quickly and ensure the stability of the a posteriori plans, the operators and machines (robots in our case). These architectures have been selected according to several predefined criteria including application field, working state, materials cost, robustness...even safety and security aspects.

The present study will focus on N mobile robots (eg. 11 robots) collaborating with humans and cooperating to move dangerous chemicals in different parts of an analysis laboratory. The aim is to make a comparison between different types of hierarchical control approaches with a single level or multi-level according to safety and security aspects. This type of control approaches including centralized structure, hierarchical and modified hierarchical structures (Fig. 3) are suitable for the work of cooperative groups in common spaces like in our case. The strengths and weaknesses of the three structures are aggregated in Table 1 [16,17].

Figs. 3–5 depict each approach according to its properties.

The difference between the modified hierarchical approach and the basic hierarchical approach is communication between agents at the same level. The communication between agents at the same level is very necessary to control the system at these different levels and perform the tasks in each level. The lack of communication leads the studied system both to a risk situation and to an overall deficiency that requires a study of risk analysis of these two approaches.

In order to better compare the structures a hazard evaluation approach is proposed. We combined the STPA method which based on STAMP and Bowtie. STPA/STAMP is a qualitative method intended to identify risks provided by three different control architectures afterward a Bowtie analysis is used to visualize and contribute to evaluate the obtained scenarios. Thus, the combination assists to facilitate decision making over the suitable architecture.

The remainder of this document is structured as follows. An insight of the used methods is provided in Section 2. In Section 3, our case study, i.e. Multi-Mobile Robot System (MMRS) is presented. STPA application and the obtained results are detailed in Section 4. Section 5 is devoted to the hazard evaluation of hazard scenarios using the bowtie method. Finally, a conclusion is given in Section 6.

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

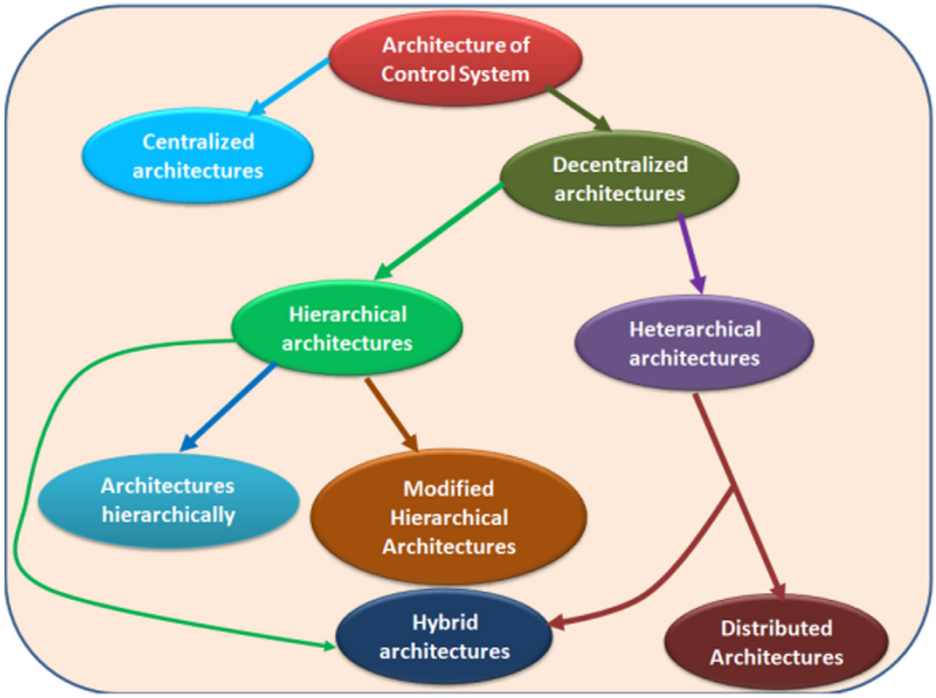

Fig. 1 Different architectures of industrial system control [16,17].

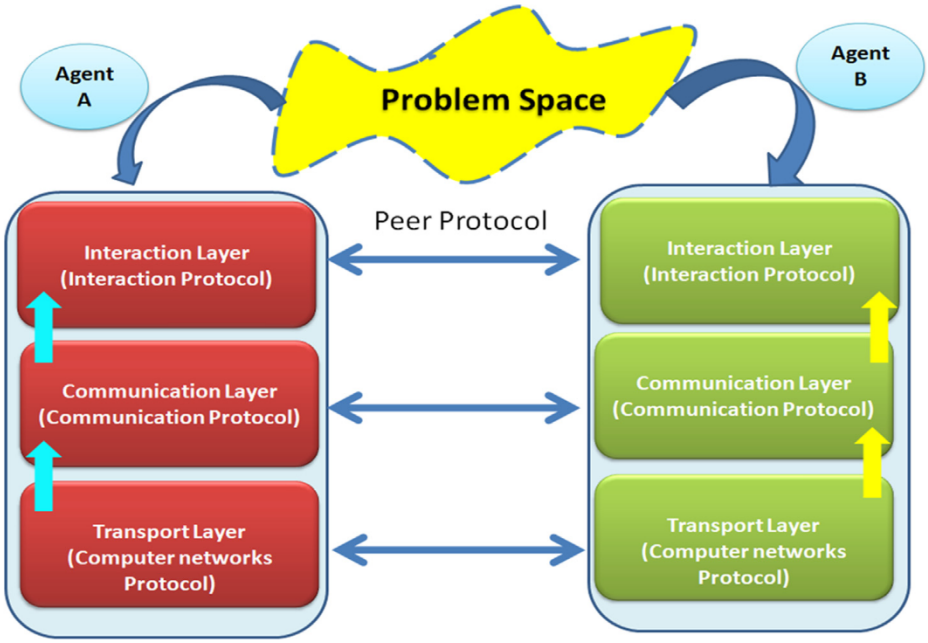

Fig. 2 Hierarchical model of the communication and interaction process among agents [22].

2. Methodology overview

Complex systems are systems that are composed of several interconnected components organized according to different structures of control and coordination. Such complexity increases according to two basic factors: their size and their functions, therefore, these systems as MMRS are considered among the critical advanced systems which are difficult to be analyzed. Systems theory brought a causation model of accidents known as a System-Theoretic Accident Model and Processes "STAMP", which is considered among the philosophical and intellectual basis of systems engineering [24,25]. STAMP technique depends upon three fundamental concepts [12], as depicted in Fig. 6. This technique has been

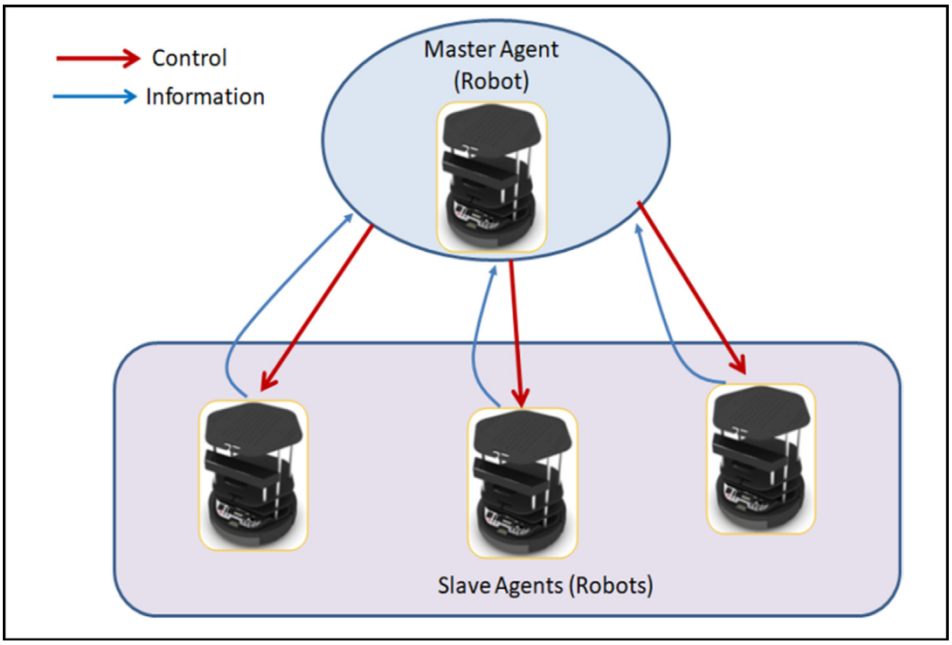

Fig. 3 Principle of Centralized Approach (CA).

Table 1 A table summarizing the important characteristics of the studied control aproaches.

Type of Structure	Benefits	Limitations
Centralized control approach (CA)	The master agent possesses an overall sight of all other slave robots by receiving sensors information and providing commands to manage the control of robots. Limited number of treatment and control units. Poor communication between robots.	The response time depends on the system size which means that the more slave agents, the slower communication. The slave agents are sensitive to the master faults. The master should receive continuous information of the whole system. It is difficult to modify the system structure.
Hierarchical control approach (HA)	Faster responses between masters/slaves coupling. It has more flexibility in comparison with the agents' number. It has great adaptability in comparison with the new states of agents. More Robust than the centralized one.	Coordination difficulties between robots at the same level. Each master unit of control should know all potential situations of their following agents. Any failure in the high-level controller affects the planning stage. To make structural changes, it should take into account the entire system.
Modified hierarchical control approach (MHA)	Faster responses between masters/slaves coupling. It has more flexibility in comparison with the agents' number. It has great adaptability in comparison with the new states of agents. More Robust than the centralized one. More communication allowed between robots and more coordination between the agents of the same level.	Each master unit of control should know all potential situations of their following agents. Any failure in the high-level controller affects the planning stage. To make structural changes, it should take into account the entire system.

selected as it is a method intended to analyze hazard scenarios provided by the control approach.

In the STAMP approach, systems are considered as components linked together in both ways in order to sustain a state of dynamic balance. Those interactions among system elements likewise among a system and other systems or operators are represented similar to a closed-loops of control in which the controllers provide control actions or transmit commands toward the monitored process as well they receive responses or feedbacks [1].

2.1. Systems-theoretic process analysis

STPA is among systematic hazard identification approaches dependent upon the causation model STAMP. Its point is to build up a new investigation strategy that conquers the limita-

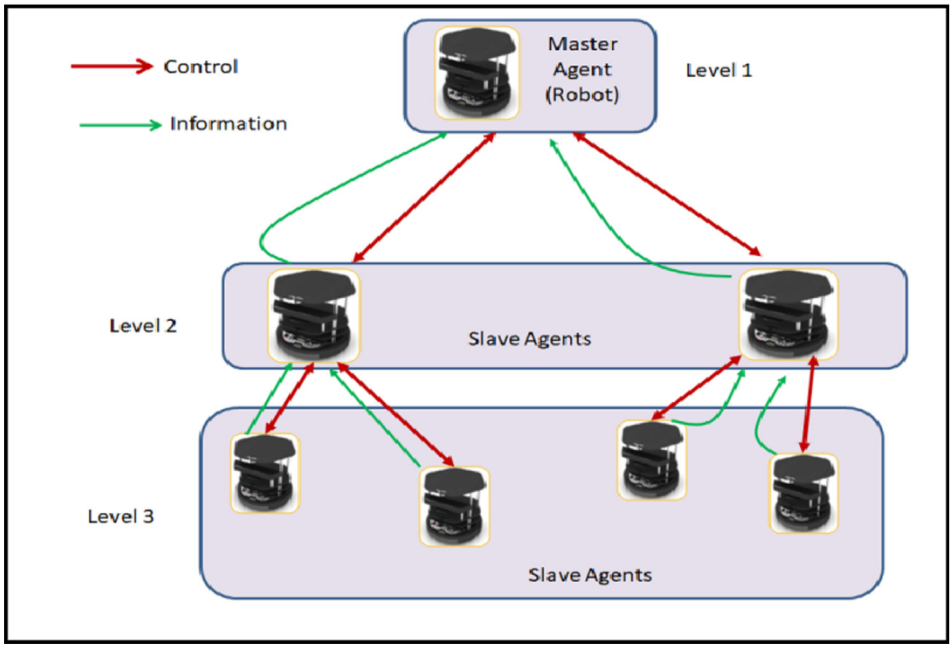

Fig. 4 Principle of Hierarchical Approach (HA).

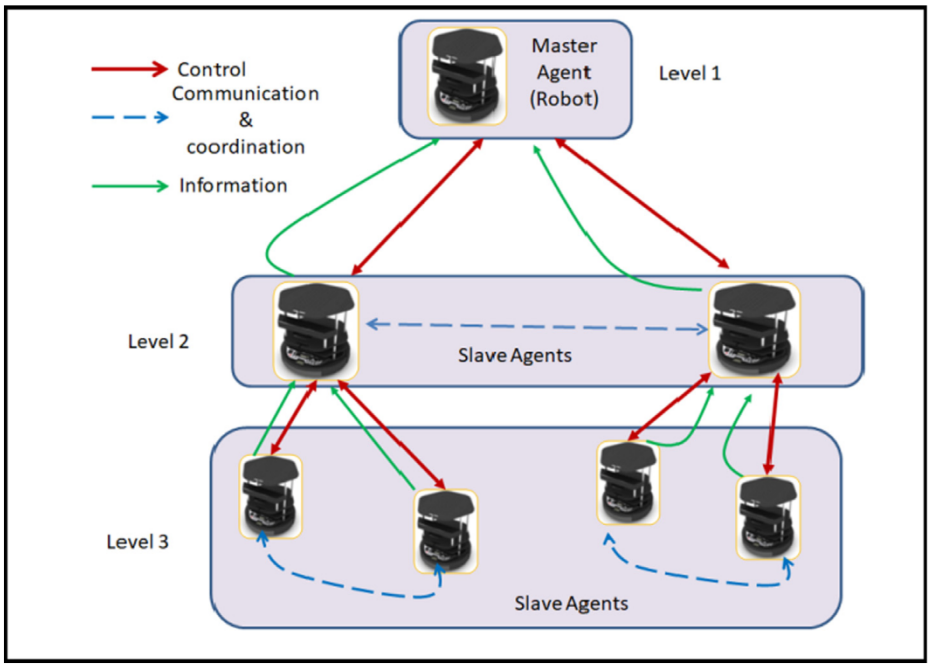

Fig. 5 Principle of Modified Hierarchical Approach (MHA).

tions of the classical hazard analysis in identifying a broader set of hazard scenarios and causal factors [14].

The analysis is performed according to four main steps. Firstly, STPA begins by defining the purpose of the analysis through identifying high-level accidents and hazards of the studied system, and then models the system's control structure in the form of a set of control loops in interaction. Once the control structure is built, the control actions are subject to an analysis using predefined guidewords by checking [12,26]:

- If any control action "**is provided**" could lead to a hazard;
- If a control action or measure necessary to prevent a danger is "**not provided**";
- If a control action "**is sent in incorrect timing**" **too soon or too late** could lead to a hazard;
- If "**Applying** a control action **for a long time or losing it earlier**" may produce a hazard.

Finally, the last step is to extract the causal factors of each hazardous action.

STPA methodology is presented below in Fig. 7. The STPA technique has a similar objective as any hazard analysis method. Thus, it is clearly to extract a set of hazard scenarios [28].

2.2. STPA analysis comparison with other classical methods

The benefit of STPA contrary to other methods appears obviously in its capability of identifying a large number of possible hazards whether it is caused by failure or by other reasons like environment condition or organizational effects. This approach is at the first level built on the theory of systems and their properties instead of theory of reliability where it is allowed us to focus on interactions arisen between system components and to look at the system from different sides. Therefore, the hazard in STPA appears due to two main reasons: unsafe and inadvertent interactions between the system components or from inadequate safety constraints enforcement. The other methods such as Failure Mode and Effects Analysis (FMEA), Process Hazard Analysis (PHA) and Fault tree analysis (FTA) do the analysis on system design instead of system control functions [12]. It should be mentioned that the HAZOP method focuses the analysis on the physical part of control loops only contrary to STPA which focuses on control actions. This is what makes the traditional approaches focus on system's component failure and do not look at the unsafe/insecure behavior itself and the other factors including social and organizational ones. Thus the interest of STPA approach headed from "preventing failures" to "preventing unsafe actions and operations by applying safety constraints to system behavior".

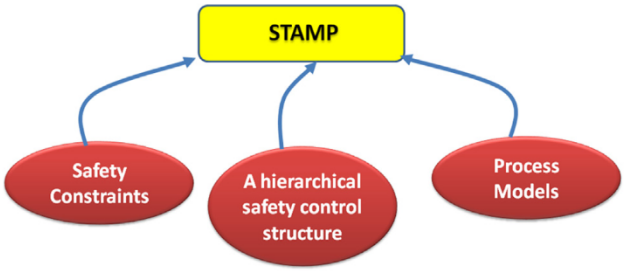

Fig. 6 Concepts of STAMP.

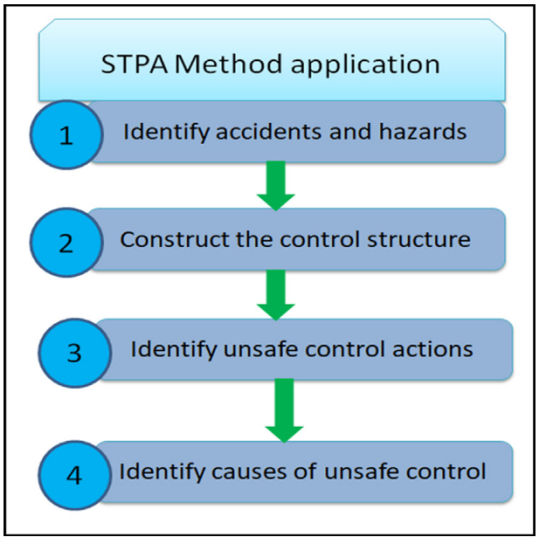

Fig. 7 Organizational chart of the STPA analysis.

Although failure is a problem that requires more care to deal with, other involuntary causes need also to be highlighted in order to be controlled [17,28]. With regard to the limitations, that analysis method requires more focus and rigor during the investigation, more than with other conventional methods where a team of specialized experts will be required [10]. In addition, the approach is still fully qualitative without any quantification due to the difficulty of assessing some scenarios, even though the importance of assessment in risk analysis.

2.3. Bowtie method

Bowtie analysis is a method that combines between the benefits of the two analysis techniques called Fault tree analysis (FTA) and Event Tree Analysis (ETA) for identifying the dreaded event; its causes and consequences in addition to barriers. It is well suited to provide a global and a broad view of hazard scenarios that could occur to the system [27–32]. The Bowtie analysis are selected for a combination with STPA as bow-

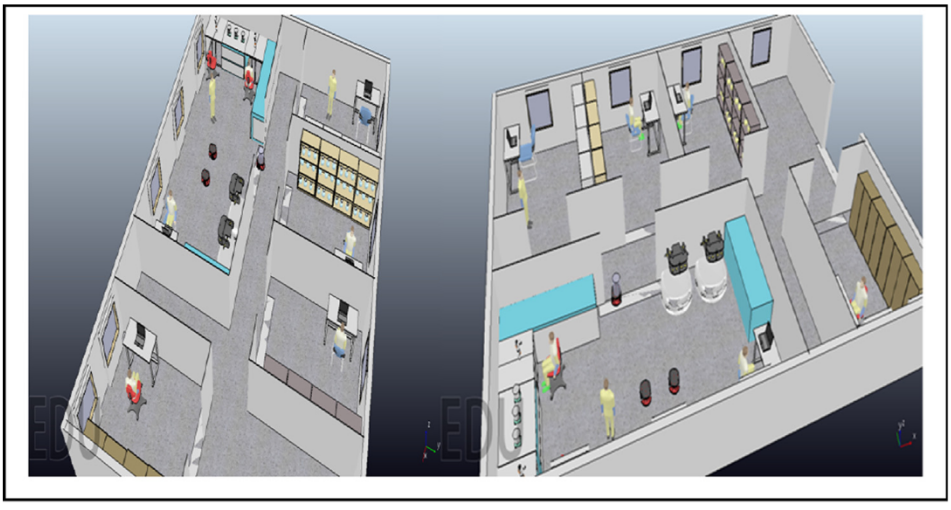

Fig. 8 Representation of a robotic chemical analysis laboratory.

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

tie offers a good visualization of STPA outcomes and it is capable to evaluate hazard scenarios obtained by STPA.

3. A robotic chemical analysis laboratory

The studied system is comprised of a group of eleven robots coordinating together in order to move chemical products within the analysis laboratory as shown in Fig. 8.

The laboratory area devided on different rooms (analysis room, product storage room, loading room for robots, reception room, foreclosure room). The robots are in the loading room and they wait for orders. The robots move between the different rooms.

3.1. Development of the hierarchical control structures using STAMP modeling

In this step, different control structures diagrams are established depending on STAMP modeling. The structures show clearly interrelationships and interactions between the various

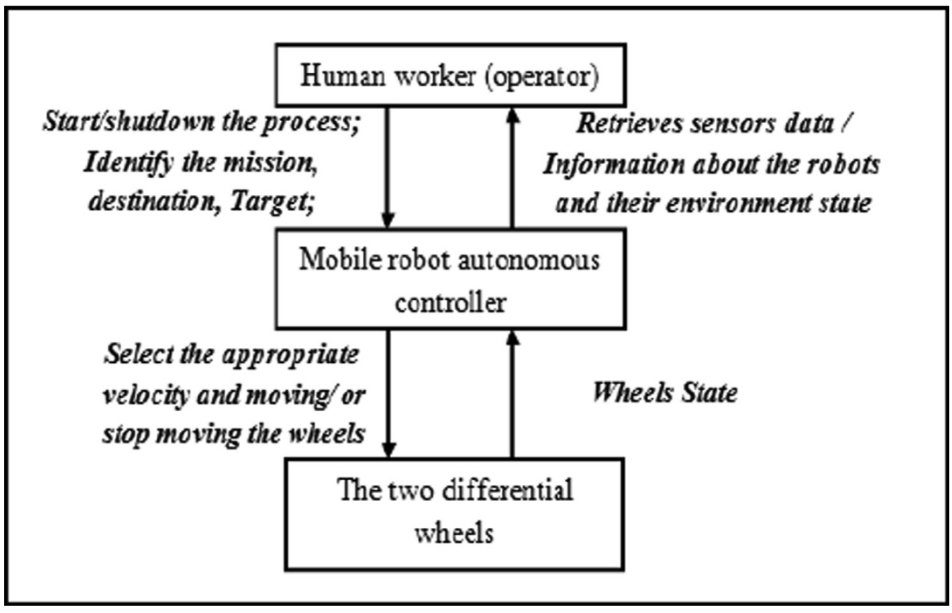

Fig. 9 The high-level control structure for a differential mobile wheeled robot.

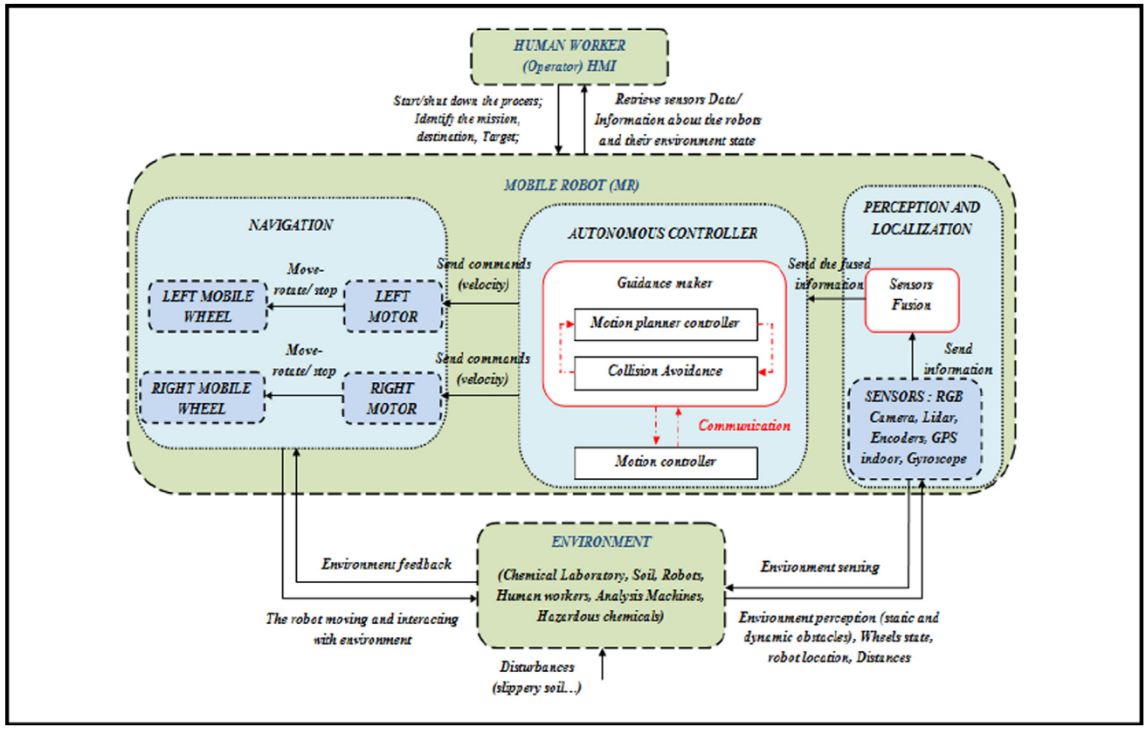

Fig. 10 The detailed version of the control structure for a single – two differential wheels robot.

system components. The set of actions, commands and feedback are identified. It is also important to describe environmental disturbances that may affect the system and its operation.

– **The Case of a single robot (High-level and detailed one)**

Figs. 9 and 10 show the high-level and a more detailed fully autonomous control structure for a differential mobile wheeled robot respectively, in which the operator starts the process and identifies the robot task or the target. The robot controller merges the sensors data, calculates feasible paths, and chooses the optimal path to its mission and control the motion of the wheels.

– **The Case of a multi-robot system**

There are several steering approaches. We can use them to coordinate the control of the different robotic entities, manage their motion and organize its tasks [17,18]. Among them three approaches are analyzed in this paper:

- *The centralized approach (CA)*. As shown in Fig. 11, a control unit controls all the other robots and has decision-making power. It maintains the overall information of all the activities of the multi-robot system. This unit manages, processes events in real time, synchronizes and coordinates all tasks.
- *The hierarchical approach (HA)*. Fig. 12 represents the hierarchical control approach. The robots are linked by master–slave relations. This hierarchy has been studied extensively and has been widely used and deployed in industry since the 1970s [18]. In this type of approach, management decisions are made by the high level leader, which must necessarily have all the information necessary to make decisions allowing good overall performance.
- *The Modified hierarchical approach (MHA)*. There is another form of hierarchical approach where robots at the same level can coordinate with each other and communicate. This type of approach is called a modified hierarchical approach (Fig. 13).

4. STPA hazard analysis results

In order to perform the STPA analysis on the system under consideration [14,25], we should continue with the two last steps shown in the organizational chart of Fig. 7.

- Step 3: the obtained results in terms of possible hazards are gathered in Table 3.
- Step 4: the possible causes of the obtained hazards are summarized in Table 4.

Before starting with STPA analysis, losses, high level accidents and hazards of the system likely to be occurred should be identified. Table 2 details the set of hazards, their resulting accidents and losses. Each hazard is associated with its severity value, the hazards severities have been evaluated according to their accidents losses severities.

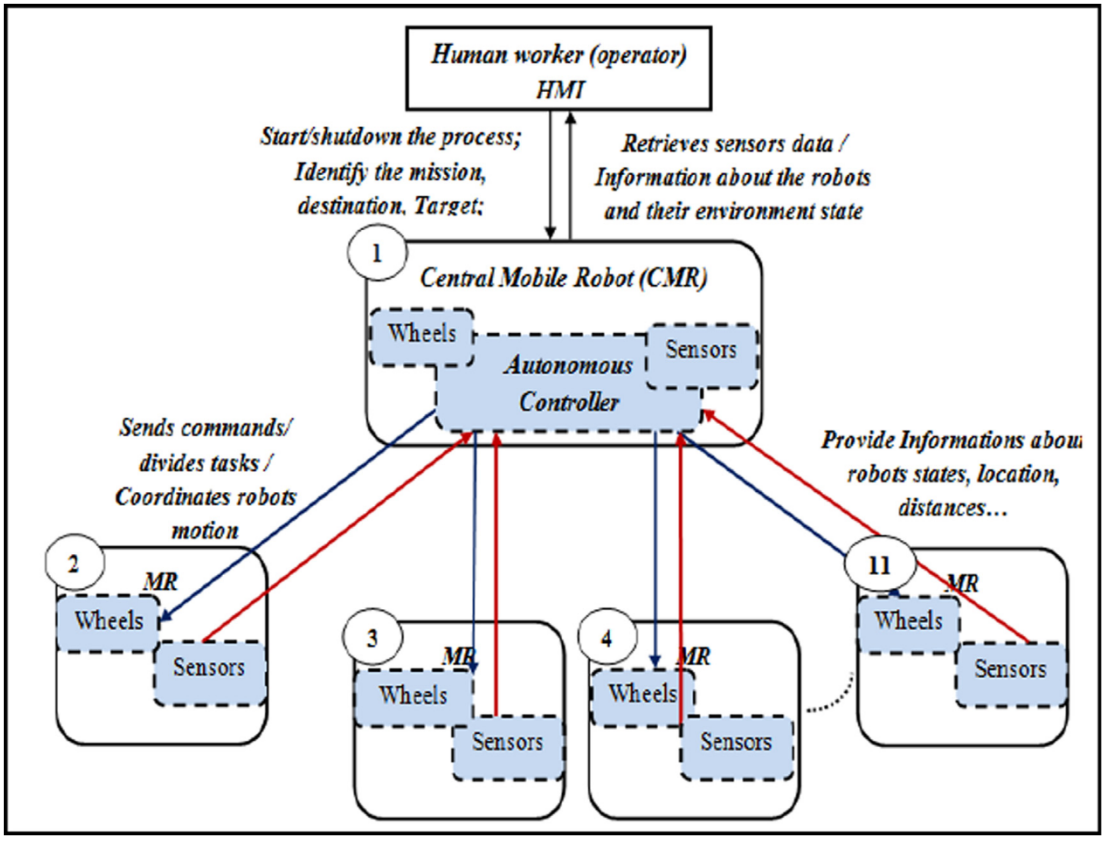

Fig. 11 Centralized control structure for MMRS (Blue arrow for sending commands, red arrow for receiving feedback).

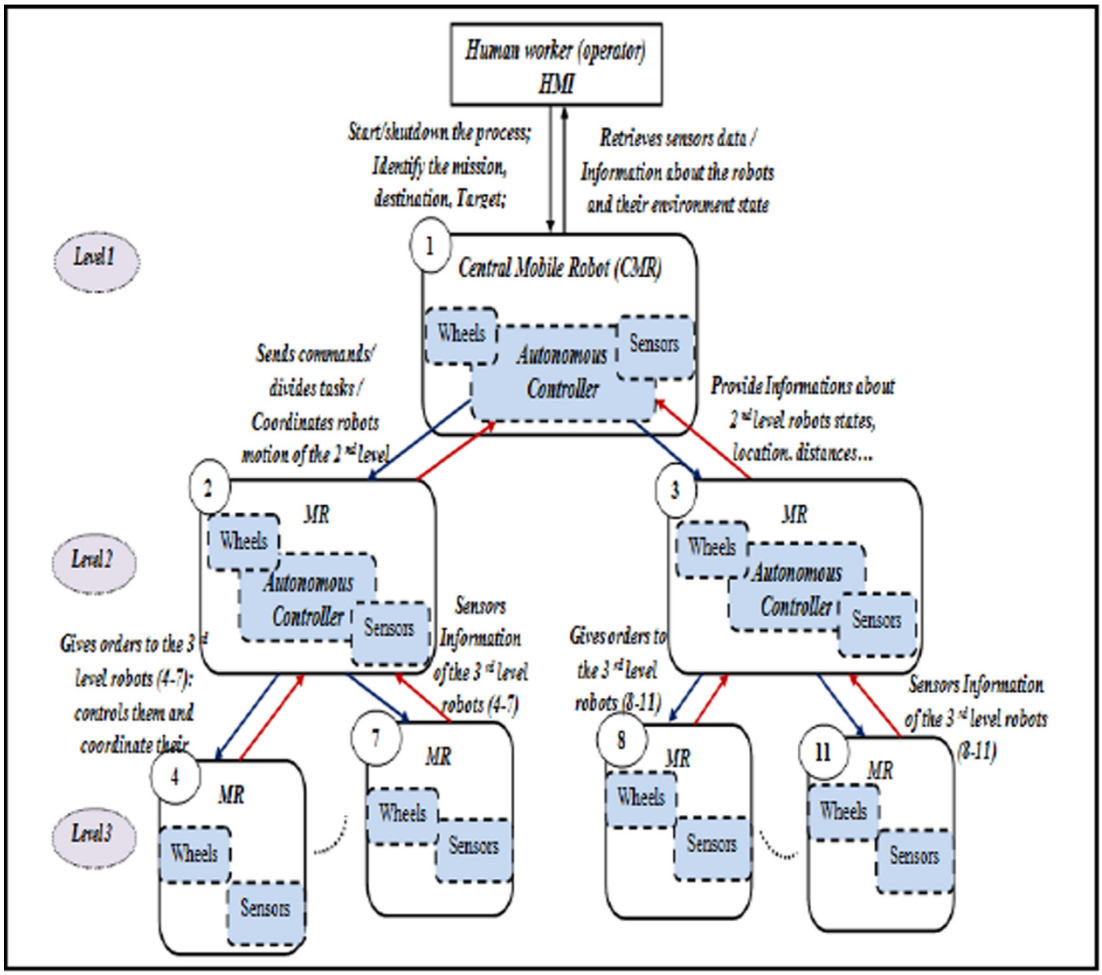

Fig. 12 Hierarchical control structure for MMRS (Blue arrow for sending commands, red arrow for receiving feedback).

4.1. Identification of hazard scenarios by STPA

The STPA technique allows us to extract hazardous scenarios that would occur in the different situations mentioned above in Section 2.1. The corresponding risk events and their causal factors can be found in Tables 3 and 4. This step assist to extract a large number of scenarios, their causes, moreover relate each scenario by the hazard that it results from the list obtained in Table 2.

To bring more importance to the analysis and to make scenarios resulting by STPA more meaningful, a semi quantitative evaluation was made based on Bowtie outcomes (see Section 5, Figs. 17–19). This assessment gives us a classification according to the criticality of each scenario.

5. Hazards evaluation with bowtie method

5.1. Hazard analysis using bowtie method

We used the Graphical interface for reliability forecasting (GRIF) software to develop the different bowtie models [33,34]. The bowties represented in Figs. 14–16 includes risk scenarios of bad control for each approach, respectively. We identify causes that could lead to hazard and their effects. The middle node of each bowtie represents the same unwanted event which is losing control by leader.

The use of bowtie method assists to:

- Visualize the outcomes of STPA (the frequent causes for each architecture and hazards);
- Offer further details about the causal factors obtained by STPA;
- Define the existing safety barriers for each structure;
- Finally assess the hazards using the risk classification matrix by combining the frequency of the unwanted event obtained from the frequencies of causes with the severity of each hazard.

5.2. Risk classification of hazard scenarios

The criticality assessment is done according to the risk matrix that we have defined in GRIF software. This is carried out by the combination of the frequency of consequences and their severity. The following figures (Figs. 17–19) show the risk classification matrices of the three kind of approaches.

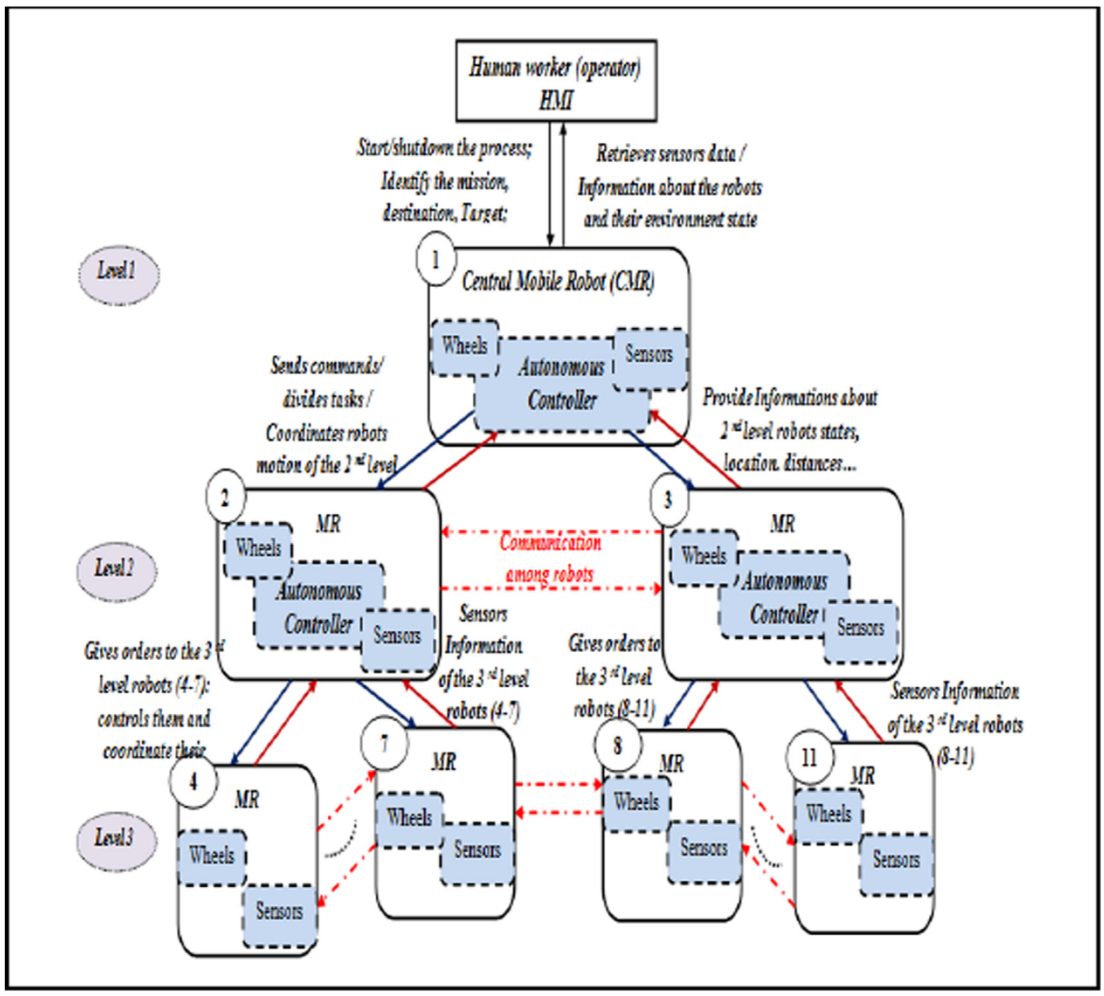

Fig. 13 Modified hierarchical control structure for MMRS.

Table 2 A table of losses, Accidents and hazards.

Losses	System-level accidents	System-level hazards
L-1 Human worker become injured (Get harmed to humans) Severity value = 3	**SlA-1**Collision of two/more robots without chemicals. (**L-4, L-5**)	**S-lH1** Robots violate the distance required for safety (**SlA-1, SlA-2, SlA-3, SlA-4, SlA-5**) (Very serious)
L-2 Minor injury to human Severity value = 2	**SlA-2**Collision between two/more robots while they moving products (**L-3, L-4, L-5, L-6**)	**S-lH2** Robots speeding (exceed the safety speed) (**SlA-1, SlA-2, SlA-3, SlA-4**) (Very serious)
L-3 Loss of chemical products Severity value = 2	**SlA-3** Collision between one / more than one robot and human. (**L-2, L-3, L-4, L-5**)	**S-lH3** Robots have a problem in their behaviors (abnormal operation of robots) (**SlA-1, SlA-2, SlA-4**) (Very serious)
	SlA-4 Collision between one / more than one robot carrying products and human. (**L-1, L-3, L-4, L-5,L-6**)	
L-4 Loss of mission Severity value = 2	**SlA-5** Robots crashes to wall or static objects (analysis machines) falls down on floor. (**L-3, L-4, L-5**)	**S-lH4** Unexpected shut-down of robots operation (**SlA-6**) (Serious)
L-5 Damage to robots, machines Severity value = 2	**SlA-6** Interrupted operation of analysis machines (**L-4**)	**S-lH5** High risk chemical products spill (Flammable, Toxic...) (**SlA-7**) (Very serious)
L-6 Damage to the working environment: Toxic dust, gas, burns... Severity value = 3	**SlA-7** Fire, poisoning (area, gas emission) (**L-3, L-4, L-5, L-6**)	**S-lH6** Abnormal operation of robots without products (**SlA-1, SlA-3, SlA-5**) (Serious)

Table 3 Hazard scenarios identification Table by STPA.

Control Actions	*Unsafe Scenarios (US)*	*System-level Hazard(S-lH)*		
		CA	*HA*	*MHA*
Launch/ shut down the process (by operator)	**US1:**The operator launches wrong program or two different programs at the same time to the master robot	S-lH6	S-lH6	S-lH6
	US2: The operator does not shut down the process in emergency cases which requires his intervention or too late	S-lH3	S-lH3	S-lH3
Control and coordinating unit				
Send commands, coordinate robots motion(by master , 1st level)	**US3:** The controller provides the guidance command to a slave robots ,of the 2nd level, with no precision	S-lH3	S-lH3	S-lH3
	US4: The controller provides the wrong execution command to avoid obstacles (wrong direction)	S-lH3	S-lH3	S-lH3
	US5: Operation command provided to robots intermittently	S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5
	US6: Operation command does not provided to robots ,of the 2nd level, unexpectedly (interrupted operation)	S-lH1 S-lH4	S-lH1 S-lH4	S-lH1 S-lH4
	US7: stop command doesn't provided when it is needed /The avoidance command does not provided by the master to a slave robots ,of the 2nd level, in front of a dynamic or static obstacle	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US8: The controller provides the right command but too late	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US9: The same command value provided for a long time	S-lH1 S-lH5	S-lH1 S-lH5	S-lH1 S-lH5
	US 10: The master doesn't coordinate the motion between the two robots, of the 2nd level, or the coordination is provided too late	S-lH3	S-lH3	S-lH3
Send orders, commands & coordinate robots motion(by controllers , 2nd level)	**US11:** The controllers ,of the 2nd level, provides the guidance command to a slave robots , of the 3rd level ,with no precision	N/A	S-lH3	S-lH3
	US12: Operation command provided to robots intermittently		S-lH1 S-lH3 S-lH5	S-lH1 S-lH3 S-lH5
	US13: Operation command does not provided to robots , of the 3rd level , unexpectedly (interrupted operation)		S-lH1 S-lH4	S-lH1 S-lH4
	US14: The avoidance command does not provided by the master to a slave robots, of the 3rd level, in front of a dynamic or static obstacle		S-lH1 S-lH5	S-lH1 S-lH5
	US15: The controller provides the right command but too late		S-lH1	S-lH1
	US16: The master controller issues a wrong order		S-lH1 S-lH3	S-lH1 S-lH3
	US17:A command signal issued by the controller too late		S-lH1 S-lH5	S-lH1 S-lH5
	US18: Command signal interrupted or provided for a long time		S-lH1 S-lH5	S-lH1 S-lH5
	US 19: The master doesn't coordinate the motion between robots , of the 3rd level , or the coordination is provided too late		S-lH3	S-lH3
Select the appropriate speed (speed up, speed down)	**US 20:**The controller provides a high speed value to robots in a slippery floor (spill of chemicals on floor)	S-lH1 S-lH2 S-lH3	S-lH1 S-lH2 S-lH3	S-lH1 S-lH2 S-lH3
	US 21: Robots are moving without respect of speed constraints	S-lH1 S-lH2 S-lH5	S-lH1 S-lH2 S-lH5	S-lH1 S-lH2 S-lH5

These risk matrices contain four risk categories: No impact where the risk is acceptable (green color), incorporate risk reduction measures where the risk is reasonable (yellow color), manage for continuous improvement where the risk is unacceptable (orange color) and intolerable risk (red color), from the lower to the higher impact respectively. An effect which is classified in the lower level of criticality presents a low danger; otherwise an effect which is classified in the higher level of criticality presents a high danger. From the Bowtie risk classification that was done above, four hazards reached the intolerable risk column for the system characterized by the centralized control approach. The system organized according to a modified hierarchical structure is the one that contains two hazards included in the red zone, whereas the system char-

Table 4 The causative factors of identified danger scenarios table.

Number of Unsafe Scenario (US)	*Causative factors of danger*		
	CA	*HA*	*MHA*
US1-US2	– Human lose focus, extreme tiredness…	The same as CA	The same as CA
US3, US11US 16	– Erroneous data from sensors which detect position (position sensors failure, steering angle sensor failure, receiving sensors information with delay, inadequate sensors calibration, Inadequate data fusion) – Failure of wheels	– Erroneous data from sensors which detect position (position sensors failure, steering angle sensor failure, inadequate sensors calibration, Inadequate data fusion) – Failure of wheels	The same as HA
US4, US12	– No indication of obstacles from distance sensors (tiny obstacles not observable by sensors, shining surfaces of obstacles, inaccuracies in measures). – Failure of obstacle detection sensor. – Inappropriate or insufficient calibration of sensors. – Failure of wheels	The same as CA	The same as CA
US5/US8 **US13** **US 17**	– Failed connection – Low battery level – Slow execution of commands because of the huge number of received information at once – Lock of program or software. – Feedback arrived to the controller after a delay time.	– Failed connection – Low battery level – Lock of program or software.	– Failed connection – Low battery level – Lock of program or software.
US6 **US 14**	– Lock of software – Failure of actuators (Motors, wheels) – Failure of actuators controllers – Failure of master controller – Failure of communication components of the slave robots (slave robot receiver). – Failed connection – Limited capacity of memory card.	– Lock of software – Failure of actuators (Motors, wheels) – Failure of actuators controllers – Failure of main controllers – Failure of communication components – Interrupted connection	The same as HA
US7 US15	– Failure of obstacle avoidance sensor – Wrong/ no indication of obstacles from distance sensors (tiny obstacles not observable by sensors, shining surfaces of obstacles, inaccuracies in measures). – Inadequate or wrong program or algorithm of control (requirement does not properly defined in the program file). – Lock of software	The same as CA	The same as CA
US9 US18	– Slow execution of commands because of the huge number of received information at once – Failure of obstacle avoidance sensor – Wrong/ no indication of obstacles from distance sensors (tiny obstacles not observable by sensors, shining surfaces of obstacles, inaccuracies in measures). – Inadequate or wrong program or algorithm of control (requirement does not properly defined in the program file). – Poor connection – Lock of software	– Failure of obstacle avoidance sensor – Wrong/no indication of obstacles from distance sensors (tiny obstacles not observable by sensors, shining surfaces of obstacles, inaccuracies in measures). – Inadequate or wrong program or algorithm of control (requirement does not properly defined in the program file). – Lock of software – Poor connection	The same as HA
US10 US 19	– Wrong sensors data (inadequate calibration, failure of sensors) – Lock of software	The same as CA – No communication between groups	The same as CA – Poor connection/invalid communication among robot groups

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

Table 4 (*continued*)

Number of Unsafe Scenario (US)	*Causative factors of danger*		
	CA	*HA*	*MHA*
US20	– Spill of chemicals or water on the floor/hygiene problem	The same as CA	The same as CA
US21	– Failure of speed sensor	The same as CA	The same as CA
US22 US23	– Inadequate or incomplete control algorithm (safe distance between robots not enough for emergencies, problem of coordination) – Slow execution of commands because of the huge number of received information at once	– Inadequate or incomplete control algorithm (safe distance between robots not enough for emergencies, problem of coordination) – Slow connection	The same as HA
US24 US25 US26	– Failure of speed sensor – Slow execution of commands because of the huge number of received information at once – Lock of software	– Failure of speed sensor – Lock of software	– Failure of speed sensor – Lock of software
US 27	– Wrong Sensors data (Failure of sensors or inadequate calibration) – Data Wrongly fused	The same as CA	The same as CA
US28	– A huge number of sensors information provided to the master robot – Poor connection, slow software execution	– Poor connection, – Slow software execution	The same as HA
US29	– Motors failure, actuators controller failure, wrong command, low battery voltage	The same as CA	The same as CA
US30	– Inadequate control and coordination algorithm – Failure of software, sensors	The same as CA	The same as CA
US31 US32	– Interrupted/failed connection – Failure of communication components – Lock of software	The same as CA	The same as CA
US33 US34	No communication provided	No communication provided	Loose/slow connection between robots, Failure of connection components

acterized by the hierarchical approach has one hazard reached the intolerable zone see Table 5.

A comparison of the three architectures was made (see Table 5). This comparison based on outcomes obtained from the evaluation of risk scenarios resulting from STPA/Bowtie combination, some remarks are summarized below:

- According to Table 5 below, we can conclude that the most critical approach is the centralized approach followed by the hierarchical one.
- The modified hierarchical approach has outperformed the other approaches, due to two main properties: the multi-level control and the inter-robots communication in the same level, so that the master could be freed from the huge flow of incoming information.

5.3. Recommendation

After applying STPA and bowtie methods, we can establish the following remarks:

Based on STPA/ Bowtie outcomes, the modified hierarchical approach is that which is limited by a lower constraints number comparing with the other studied structures. Therefore, it can be considered as the most suitable for multi-robot systems (see Table 6).

It is true that Bowtie method is not very useful for control approaches however its addition to STPA assists to enhance the analysis and makes it more effective. It provides an overview of the system hazard scenarios and contributes to better evaluate them and therefore facilitated our comparison.

As we make a comparison between different approaches quite complex we cannot rely on conventional and non-specialized methods, the advantage of the STPA is that it is based on control actions between controllers. The application of STPA provides a large set of hazard scenarios and causal factors including software, human environmental and technical problems. Moreover, the obtained scenarios from STPA are more detailed than other classical methods. In addition, it gives more importance to the controlling part; we can even propose barriers at the level of the control algorithm (software).

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

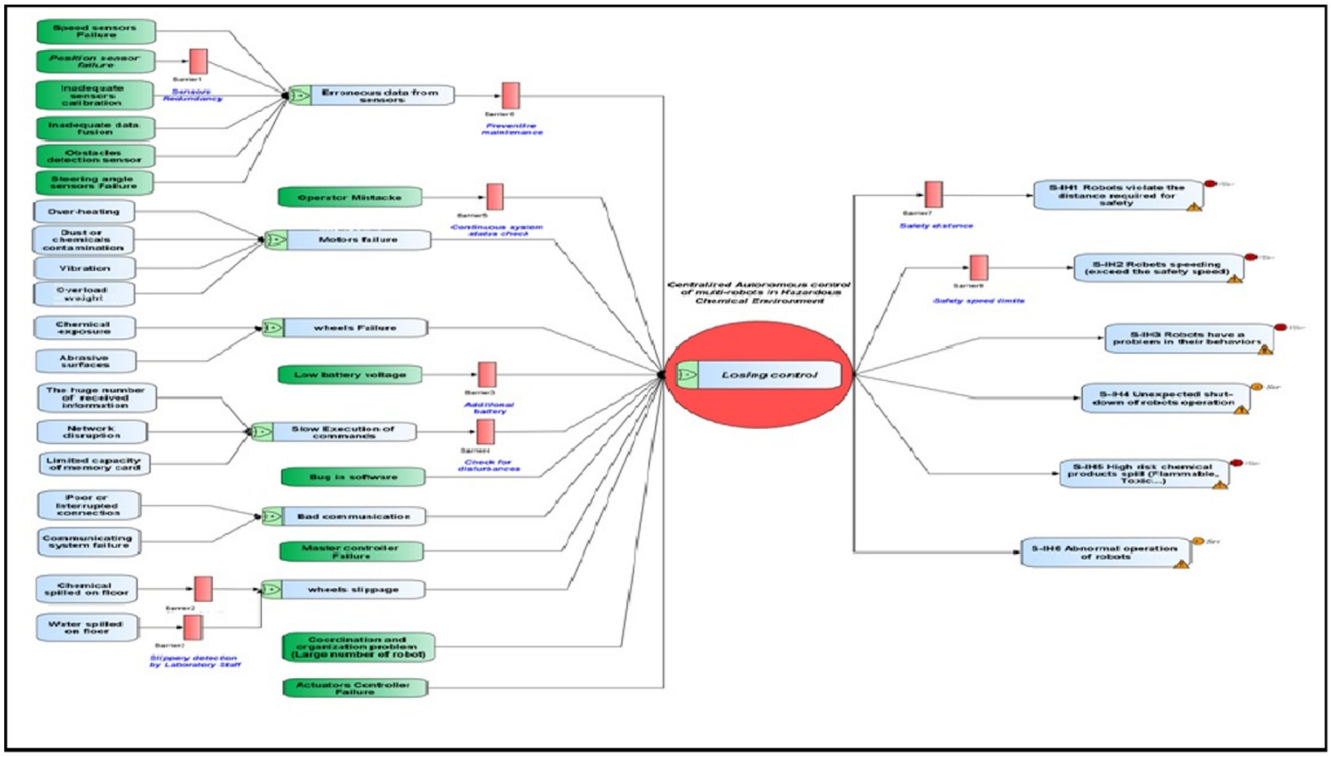

Fig. 14 Bowtie model for the centralized approach.

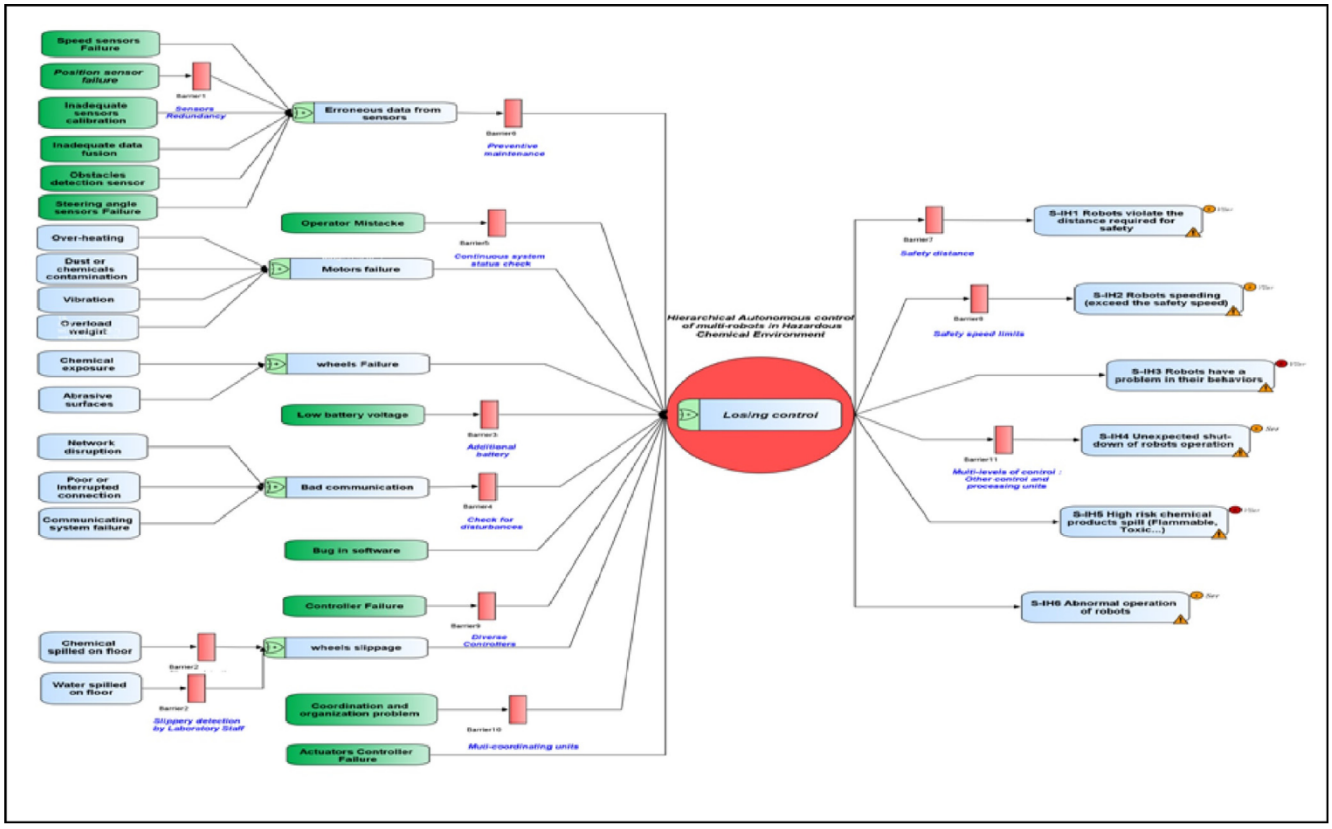

Fig. 15 Bowtie model for the hierarchical approach.

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036

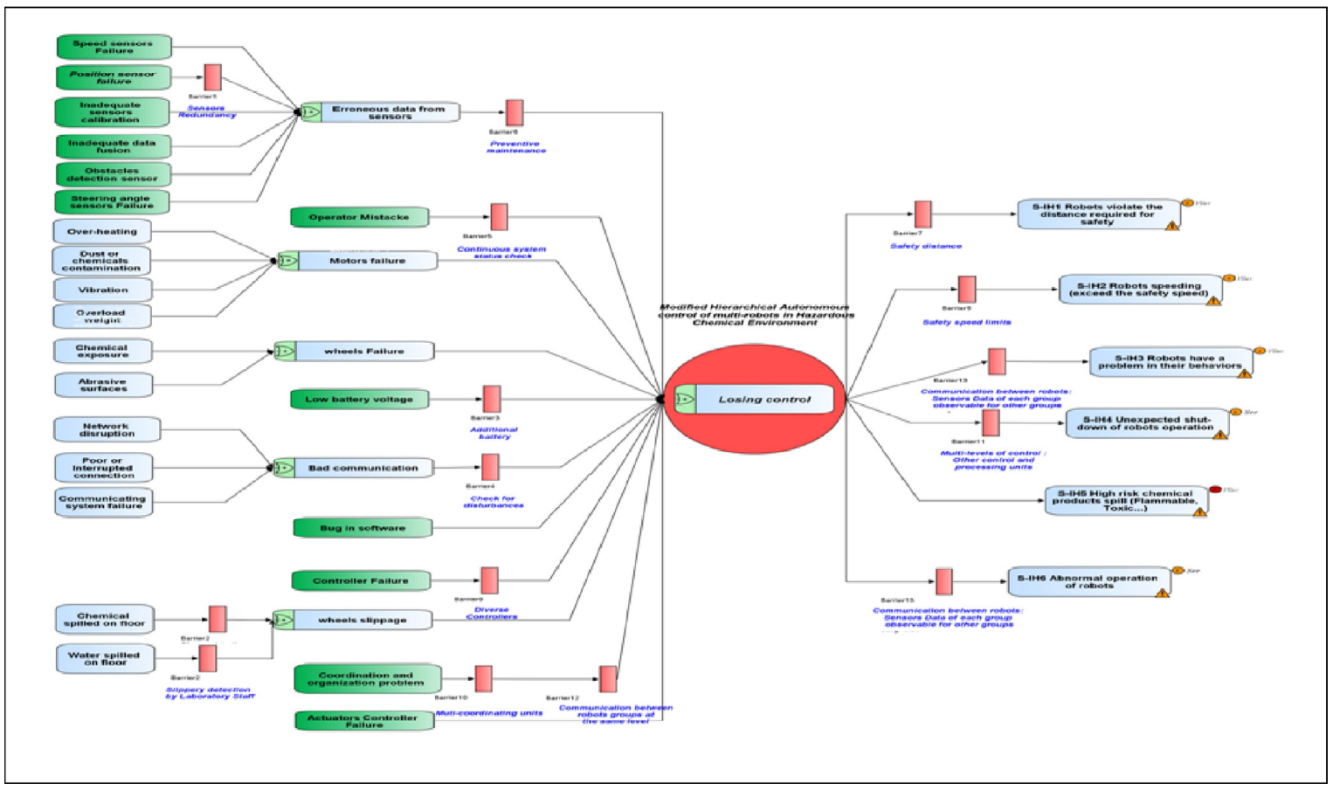

Fig. 16 Bowtie model for the modified hierarchical approach.

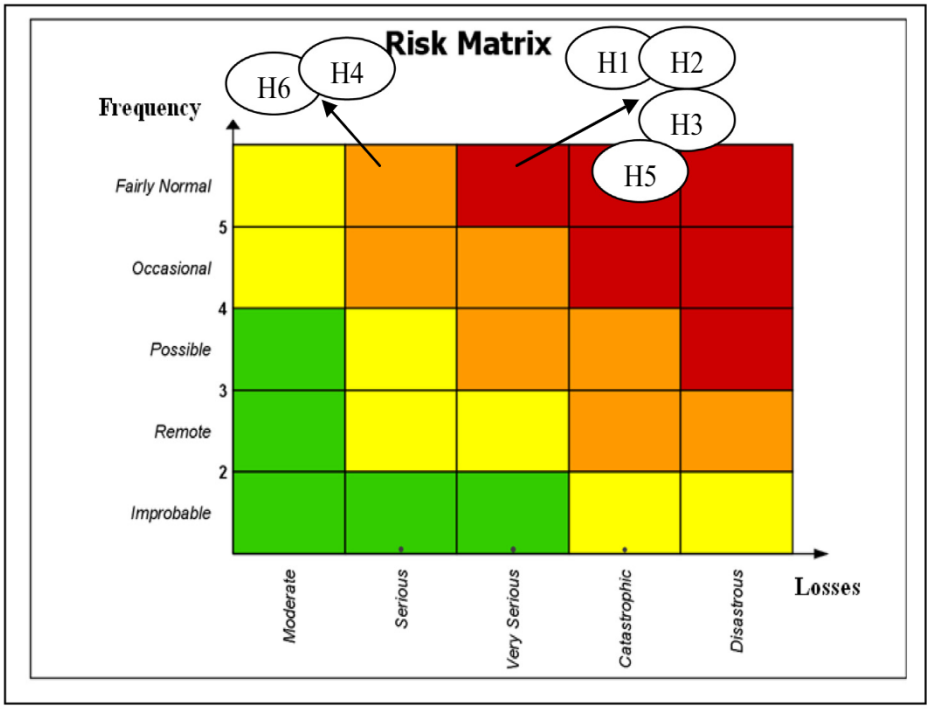

Fig. 17 Risk classification for centralized approach.

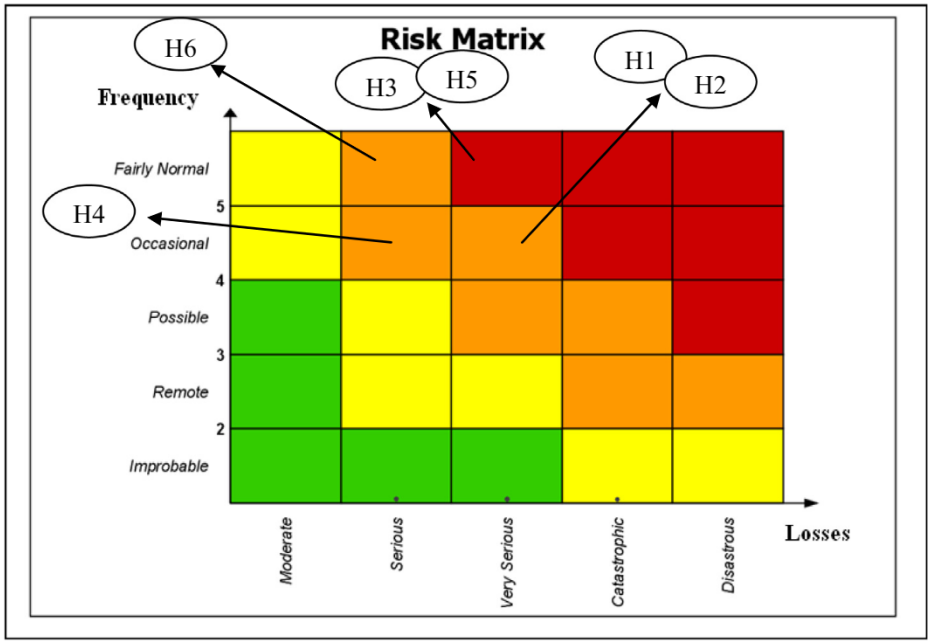

Fig. 18 Risk classification for hierarchical approach.

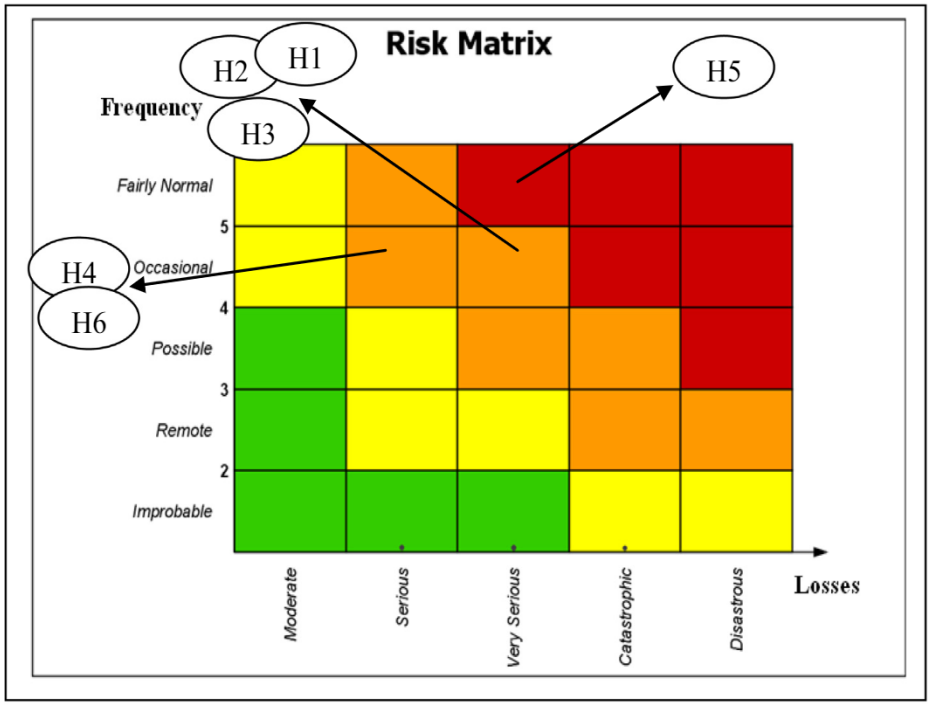

Fig. 19 Risk classification for modified hierarchical approach.

In this context, we may note some preventive measures to ensure greater efficiency of the control approach and reduce the level of hazards:

- Ensure the confidence level of the controlling part and the reliability of its components.
- Validate all programs.
- Software and hardware integrities should be checked.
- No changes are allowed in programs without permission accorded.
- Add sensors that detect slippery and differentiate between human being and other robots like camera.
- Add several safety constraints (safety distances for human, robots and other objects, tracking accuracy, operating conditions) at the level of the control / command algorithm.

Table 5 Table summarizes the result obtained by risk classification matrices.

Architecture type	*Risk classification of system-level Hazards*
CA	(H1, H2, H3, H5) Intolerable risk zone (severity: very serious, frequency: fairly normal) (H4, H6) unacceptable risk zone (severity: serious, frequency: fairly normal)
HA	(H3, H5) Intolerable risk zone (severity: very serious, frequency: fairly normal) (H1, H2) unacceptable risk zone (severity: very serious, frequency: occasional) H4 unacceptable risk zone (severity: serious, frequency: occasional) H6 unacceptable risk zone (severity: serious, frequency: fairly normal)
MHA	H5 Intolerable risk zone (severity: very serious, frequency: fairly normal) (H1, H2, H3) unacceptable risk zone (severity: very serious, frequency: occasional) (H4, H6) unacceptable risk zone (severity: serious, frequency: occasional)

Table 6 Comparison of results obtained by risk classification.

Architecture Type	*CA*	*HA*	*MHA*
Risk classification of Hazard scenarios obtained by STPA	– 21/23 scenarios reach Intolerable risk level – 2/23 scenarios reach Unacceptable risk level	– 22/32 scenarios reach Intolerable risk level – 10/32 scenarios reach Unacceptable risk level	– 9/34 scenarios reach Intolerable risk level – 25/34 scenarios reach Unacceptable risk level

6. Conclusions

This paper presented a combination of two types of hazard analysis, the STPA and Bowtie methods. The proposed approach has been applied to an autonomous multi-mobile robots work in an analysis laboratory. In addition, a comparison between STPA and other conventional methods mentioned above; described the main concepts differences between them. The most dominant point in STPA is defined as the method which could extract many and various sets of hazard events even the ones caused by failures of system elements, such as the risks resulting from inadvertent interactions among elements. Furthermore, the STPA analysis is more suitable for automated systems analysis due to its attachment to the structures of control, and that is why it has been used in this paper. Three kinds of hierarchical approaches have been selected for mobile robots coordination (centralized, hierarchical and modified hierarchical control approach). These approaches are analyzed with STPA, evaluated and classified according to their criticality using Bowtie.

It is true that the STPA analysis resulted in a larger set of risk scenarios that affect the system safety. However, it is still a purely qualitative method, and hence its use is insufficient for our case. The combination of bowtie with STPA has assisted to offer a good visualization and evaluation of hazards obtained by STPA since there is no clear systematic step for that.

The analysis results show clearly that the most critical control approach which we should avoid in such structured and risky environment is the centralized approach especially in the case of a large number of robots operating together at the same time. The idea of using a single unit, to control and manage the operation of many robots in a complex environment, makes the system more exposed to accidents and hazards. The hierarchical structure presents a medium number of risk scenarios classified in the intolerable zone, whereas the modified hierarchical structure is the one that presents the lower number of risk scenarios classified in the intolerable zone. Therefore, the modified hierarchical structure is the most suitable for multi-robot systems, due to its two main properties: the multi-level control and the inter-robots communication in the same level.

One limitation of this combination is that bowtie still incapable to quantify all potential scenarios and causal factors obtained by STPA. Another limitation is related to the struggle to quantitatively differentiate between some scenarios, such as "when control action is not provided and provided too late or too early", and between causal factors like "poor connection and interrupted connection" which we considered the same in our evaluation.

Declaration of Competing Interest

The authors declared that there is no conflict of interest.

References

[1] H. Alemzadeh, D. Chen, A. Lewis, Z. Kalbarczyk, J. Raman, N. Leveson, R. Iyer, Systems-theoretic Safety Assessment of Robotic Telesurgical Systems, Springer International Publishing, Switzerland, 2015, pp. 213–227.
[2] I. Sohail, F. Shahzad, S. Khuram, M. AsadWaqar, M.H. Mian, H. Osman, Secure Surgi NET: A framework for ensuring security in telesurgery, Int. J. Distrib. Sens. Netw. 15 (9) (2019) 1–12.
[3] T. Pawlicki, A. Samost, D.W. Brown, R.P. Manger, G.Y. Kim, N.G. Leveson, Application of systems and control theory based hazard analysis to radiation oncology, Med. Phys. 43 (3) (2016) 1514–1530.
[4] P. Kazanzides, Safety design for medical robots, in: Annual International Conference of the IEEE Engineering in Medicine and Biology Society 2009, 2009, pp. 7208–7211.

[5] S. Lee, Y. Yoji, Risk assessment and functional safety analysis to design safety function of a human-cooperative robot, Hum. Mach. Interact. – Getting Closer (2012) 140–154.
[6] C. Bensaci, Y. Zennir, D. Pomorski, E. Mechhoud, Complex safety study of intelligent multi-robot navigation in a risk's environment, International Carnahan Conference on Security Technology, Madrid, Spain, 2017, pp. 6.
[7] P. Böhm, T. Gruber, A novel HAZOP study approach in the RAMS analysis of a therapeutic robot for disabled children, in: International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2010, 2010, pp. 15–27.
[8] R. Woodman, A.F. Winfield, C. Harper, M. Fraser, Building safer robots: safety driven control, Int. J. Robot. Res. (2012) 1603–1626.
[9] R. Alexander, N. Herbert, T. Kelly, Deriving safety requirements for autonomous systems, in: 4th SEAS DTC Technical Conference – Edinburgh 2009, 1–8.
[10] S. Dogramadzi, M.E. Giannaccini, C. Harper, M. Sobhani, R. Woodman, J. Choung, Environmental hazard analysis – a variant of preliminary hazard analysis for autonomous mobile robots, J. Intell. Robot. Syst. 76 (1) (2014) 73–117.
[11] J. Guiochet, Hazard analysis of human–robot interactions with HAZOP–UML, Saf. Sci. 84 (2016) 225–237.
[12] N.G. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, 2012, p. 555.
[13] M. Rejzek, N.G. Leveson, B. Antoine, C. Hilbes, M. Grossmann, D. Meer, 2012. Evaluation of STPA in the safety analysis of the gantry 2 proton radiation therapy system: talk, in: 1st MIT STAMP Workshop, 2012, 1–22.
[14] A. Abdulkhaleq, M. Baumeister, H. Böhmert, S. Wagner, Missing no interaction – using STPA for identifying hazardous interactions of automated driving systems, Int. J. Saf. Sci. 2 (1) (2018) 115–124.
[15] K. Wróbel, J. Montewka, P. Kujala, Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, Reliab. Eng. Syst. Saf. 178 (2018) 209–224.
[16] Y. Zennir, Apprentissage par renforcement et systèmes distribués: application à l'apprentissage de la marche d'un robot hexapode, PhD thesis, INSA Lyon, 2004, 180.
[17] D.M. Dilts, N.P. Boyd, H.H. Whorms, The evolution of control approaches for automated manufacturing systems, J. Mfg. Sys. 10 (1) (1991) 79–93.
[18] K. Byung-In, S.H. Sunderesh, J.G. Robert, S.O. Art, A hybrid scheduling and control system approach for warehouse management, IEEE Trans. Robot. Autom. 9 (6) (2003) 991–1001.
[19] W. Shen, Q. Hao, J.Y. Hynn, H.N. Douglas, Applications of agent-based systems in intelligent manufacturing: An updated review, Adv. Eng. Inf. 20 (4) (2006) 415–431.
[20] J. Zhang, Multi-agent-based: Production Planning and Control, Shanghai Jiao Tong University, China, 2017, p. 414.
[21] Othman S. Ben, H. Zgaya, M. Dotoli, S. Hammadi, An agent-based decision support system for resources'. Scheduling in emergency supply chains, Control Eng. Pract. 59 (2017) 27–43.
[22] D. Oueidat, F. Guarnieri, E. Garbolino, E. Rigaud, Evaluating the safety operations procedures of an LPG storage and distribution plant with STAMP, in: 3rd European STAMP workshop, Procedia Engineering, vol. 128, 2015, pp. 83–92.
[23] F. Guarnieri, E. Garbolino, Safety dynamics: evaluating risk in complex industrial systems, in: Advanced Sciences and Technologies for Security Applications, Springer, 2019, p. 240.
[24] T. Ishimatsu, N.G. Leveson, J.P. Thomas, C.H. Fleming, M. Katahira, Y. Miyamoto, R. Ujiie, H. Nakao, N. Hoshino, Hazard analysis of complex spacecraft using systems-theoretic process analysis, J. Spacecraft Rock. 51 (2) (2014) 509–522.
[25] M. Rejzek, S.H. Björnsdóttir, S.S. Krauss, Modelling multiple levels of abstraction in hierarchical control structures, Int. J. Saf. Sci. 2 (1) (2018) 94–103.
[26] M. Rejzek, C. Hilbes, S.S. Krauss, Safety driven design with UML and STPA, in: STAMP Workshop, 2015, Boston, pp. 23.
[27] R.W. Mcleod, P. Bowie, Bowtie Analysis as a prospective risk assessment technique in primary healthcare, J. Policy Pract. Health Saf. 16 (2) (2018) 17.
[28] M.M. Chatzimichailidou, J. Ward, T. Horberry, P.J. Clarkson, A comparison of the bow-tie and STAMP approaches to reduce the risk of surgical instrument retention, Risk Anal. (2017) 20.
[29] A. de Ruijter, F. Guldenmund, The bowtie method: A review, Saf. Sci. 88 (2016) 218–425.
[30] H.C. Merrett, J.J. Horng, A. Piggot, A. Qandour, C.W. Tong, Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system, in: MATEC Web of Conferences, 2019, p. 18.
[31] R. Burgess-Limerick, T. Horberry, L. Steiner, Bow-tie analysis of a fatal underground coal mine collision, Ergon. Austr. 10 (2) (2014) 5.
[32] V. De Dianous, C. Fiévez, ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance, J. Hazard. Mater. 130 (3) (2006) 220–233.
[33] GRIF-Workshop, Graphical interface for reliability forecasting software, 2019. Available at: http://grif-workshop.fr/.
[34] C. Folleau, C. Vinuesa, S. Collas, F. Doux, Nouvel outil d'évaluation des fréquences d'occurrence pour les études de risque Congrès Lambda Mu 21 "Maîtrise des risques et transformation numérique: opportunités et menaces, 2018, pp. 6.

Please cite this article in press as: C. Bensaci et al., STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison, Alexandria Eng. J. (2020), https://doi.org/10.1016/j.aej.2020.06.036