ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/357852571

A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System

Article · January 2019

CITATIONS
10

READS
132

3 authors:



Zennir Youcef
Université 20 août 1955-Skikda
113 PUBLICATIONS **404** CITATIONS
SEE PROFILE



Chaima Bensaci
Université 20 août 1955-Skikda
14 PUBLICATIONS **78** CITATIONS
SEE PROFILE



Denis Pomorski
Université de Lille
120 PUBLICATIONS **1,056** CITATIONS
SEE PROFILE

All content following this page was uploaded by Zennir Youcef on 19 January 2022.

The user has requested enhancement of the downloaded file.



A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System

Youcef Zennir, Chaima Bensaci, Denis Pomorski

▶ **To cite this version:**

Youcef Zennir, Chaima Bensaci, Denis Pomorski. A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System. WSEAS Transactions on Computers, World Scientific and Engineering Academy and Society (WSEAS), In press. hal-03508542

HAL Id: hal-03508542

https://hal.archives-ouvertes.fr/hal-03508542

Submitted on 3 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Comparative Study of STPA Hierarchical Structures in Risk Analysis: The case of a Complex Multi-Robot Mobile System

Youcef ZENNIR, Chaima BENSACI, Denis POMORSKI
Université 20 Août 1955 Skikda, LGCES Laboratory, Skikda, ALGERIA
Université 20 Août 1955 Skikda, Automatic Laboratory of Skikda, Skikda, ALGERIA
Université de Lille, CRIStAL Laboratory – UMR9189, Lille, FRANCE
ch.bensaci@univ-skikda.dz, y.zennir@univ-skikda.dz, denis.pomorski@univ-lille.fr

Abstract— Autonomous multi-robot systems are among the most complex systems to control, especially when those robots navigate in fully hazardous and dynamic environments such as chemical analysis laboratories which include dangerous and harmful products (poisonous, flammable, explosive...). This paper presents an approach for systems-complex and theoretic safety assessment, also it considers their coordinating, cooperating and collaborating using different control architectures (centralized, hierarchical and modified hierarchical). We classified at first those control architectures according to their properties using Bowtie analysis method, and then we used a systems-theoretic hazard analysis technique (STPA) to identify the potential safety hazard scenarios and their causal factors.

Keywords— Risk Analysis, STAMP Method, STPA Method, Bowtie method, Multi-Robot Mobile System, Control Architectures.

1 Introduction

Due to the continuous progress of industrialization and the inability of worker to accomplish some hard and unsafe missions, which requires effort and stronger focus, human created so-called by robots and he added to them a set of properties that enable human simulation, like self-control and cooperation. Robotics now is widely spread in many industries, including automotive, medical, and power sectors. The use of autonomous cooperative mobile robots in industrial field is a double-edged sword. Although it has a great benefit, it has also serious effects if it is not well controlled, especially when these industrial areas are risky dynamic environments such as chemical analysis laboratories with dangerous chemicals (poisonous, flammable, explosive...). All these factors would increase the control system complexity. Therefore, before including those robots in such environments, a thorough analytical study of all potential risk scenarios likely to be created and their causal factors is needed. After robots acquired new features like autonomy, human-robot cooperation and intelligence skills [1] new hazards are appeared and traditional risk analysis becomes inadequate. Various analysis methods have been used and combined to predict faults and hazards in autonomous and collaborative robots. FMEA and FTA were used for collaborative robots by both (Kazanzides, 2009; Suwoong and Yamada, 2012) [2, 3] in medical field. A similar approach has been applied in [4] for a set of autonomous mobile robots working in chemical laboratory. A variant of HAZOP was used for a therapeutic robot in [5] and for software in [6], (Alexander et al, 2009) also combined between HAZOP and FFA (Functional Failure Analysis) in [7]. (Dogramadzi et al, 2014) [8] developed a specific method named ESHA (Environmental Survey Hazard Analysis). HAZOP-UML method focusing on human–robot interaction has been done by (Guiochet, 2015) in [9] but all those techniques could not adapt to take into account specificities like the control structures and unwanted interaction between controller and the controlled process. A method called STPA (System Theoretic Process Analysis) has been developed by Leveson [10], which provides guide words like in HAZOP based on undesired interactions between components and multiple controllers.It has been applied to a robotic telesurgical systemby (Alemzadeh et al, 2015) in [11]. The same approach has beenapplied to the operation of fully autonomous vessels by (Jiahui Zou, 2018) in [12].

In the literature, different architectures have been proposed to solve the problem of control and coordination of multi-agents. These architectures are of two types to model the control of complex systems: centralized and decentralized (hierarchical and distributed). In this paper, we are going to analyze the centralized and hierarchical types. Various research studies have analyzed the evolution of the different existing structures [13, 14-18]. Table 1 presents three architectures with their advantages

Extended version from EECS 2018

and disadvantages. Our study will be conducted on eleven mobile robots collaborating with human and cooperating with each other in order to move dangerous chemicals from one lab room to another or within the same room. This multi-robot system can use several control architectures to carry out its functions. In this paper, we will analyze this three architectures (centralized, hierarchical and modified hierarchical) using two analysis methods Bowtie and STPA.

The remainder of the paper is organized as follows. An overview of the used methodology is presented in section 2. The case study is presented in section 3. Hazard analysis and accident identification with Bowtie method is explained in section 4. Section 5 is devoted to the application of STPA method and their results. Finally, conclusion is made in Section 6.

TABLE 1. ADVANTAGES AND DISADVANTAGES OF THE THREE CONTROL ARCHITECTURES [19,18]

Architecture	***Advantages***	***Disadvantages***
Centralized architecture	- The central robot has a global view of the system (it receives sensor information and issues commands for the robot control). - Low communication between robots. - A limited number of control units, processing means and information management.	- The response speed depends on the size of the system (i.e. when the number of robots increases, the speed of communications decreases). - The system is not robust because it is sensitive to faults of the central robot. - The central robot must have global information at all times, which is not always realistic. - It is hard to change the system.
Hierarchical architecture	- Faster answers through master / slave coupling between the robots. - Robustness is more important than that in the centralized architecture. - The architecture is more flexible compared to the number of robots and adaptive compared to the new situations of robots.	- Coordination problems between agents at the same level. - To make structural changes you have to overhaul the entire system. - Each robot "controller" must consider all possible situations of the components of levels below him. - Unexpected disruption problem, such as a failure of a resource that makes planning and scheduling for the high-level controller invalid. - Robustness problem when the high-level central controller fails. This situation requires the total shutdown of the system.
Modified hierarchical architecture	- Faster answers through master / slave coupling between the robots. - Robustness is more important than that in the centralized architecture. - The architecture is more flexible compared to the number of robots and adaptive compared to the new situations of robots.	- To make structural changes you have to overhaul the entire system. - Each robot "controller" must consider all possible situations of the components of levels below him. - Unexpected disruption problem, such as a failure of a resource that makes planning and scheduling for the high-level controller invalid. - Robustness problem when the high-level central controller fails. This situation requires the total shutdown of the system.

2 Methodology overview

Systems theory provides the philosophical and intellectual underpinnings of systems engineering and for a new, more inclusive accident causality model called STAMP (System-Theoretic Accident Model and Processes) [20]. In addition to the basic notions of systems theory, the STAMP analysis is based on three concepts [10]:

- Safety constraints: Events that could cause loss of or harm arise only because safety constraints were not successfully enforced. In our days, the difficulty in identifying and enforcing safety constraints in design and operations has increased because of the intelligent systems and their control complexity.
- A hierarchical safety control structure: In systems theory, the systems are classified as hierarchical structures, where each level imposes constraints on the activity of the level below. Control processes operate between levels to control the processes at lower levels in the hierarchy. The structure components communicate with each other (giving orders, receiving conditions and behaviors).
- Process models: Any controller, human or automated, needs a model of the process to control it effectively.

In the STAMP approach, systems are interrelated components maintained in a state of dynamic equilibrium by feedback control loops. The interactions between system components and operators are modeled as control loops composed of the actions or commands that a controller takes/sends to a controlled process and the response or feedback that the controller receives from the controlled process [1].

2.1 System-Theoretic Process Analysis STPA

This theoretical basis STAMP allowed creating new and more powerful techniques of safety analysis and design. System-Theoretic Process Analysis (STPA) is one of the new risk analysis techniques based on STAMP causality model. The analysis is performed on the functional control structure of the system. The system is modeled as a collection of interacting control loops.

Once the control structure created, the first step of the STPA analysis is to identify potentially dangerous control actions with the help of 4 main guidewords:

- *providing* a control action that leads to a danger;
- *not providing* a control measure necessary to prevent a hazard;
- *providing* a control action *too early* or *too late* or *out of sequence*;
- *continuing* a control action *too long* or *stopping it too early*.

Once the unsafe control actions have been identified, the second step is to examine the system's control loops (using a structured and guided process) to identify scenarios that can lead to the identified unsafe control actions. The organizational chart of STPA is represented in Figure 1.

The STPA objective is the same as any hazard analysis: it is to create a set of potentially hazardous scenarios [19].

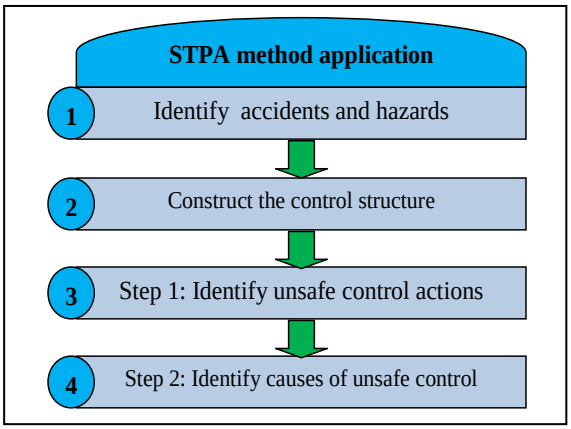


Fig. 1. Organizational chart of the STPA analysis.

2.2 Comparison between the STPA analysis and the old methods (FTA, FMEA, HAZOP, ETA...)

The STPA analysis has the same goal as the old methods like FTA, FMEA and HAZOP, which is to clarify the set of hazardous scenarios of a system. The STPA analysis includes a broader set of potential scenarios, including those for which no failures occur, the problems arising due to unsafe and unintended interactions between the system components or from inadequate safety constraints enforcement.

Most risk and vulnerability analysis techniques like HAZOP and FMEA use physical system models rather than functional system models. Thus, they focus on physical failures rather than dysfunctional (unsafe or insecure) behaviors, and broader social and organizational factors. Therefore,

the STPA analysis is a risk analysis technique based on systems theory rather than reliability theory. In the STPA approach, the focus shifts from "preventing failures" to "applying safety constraints to system behavior". Although the application of safety constraints may require the processing of component failures, other unintended causes have also to be controlled [20; 1; 13; 21]. Nevertheless, this method, like any other analysis method, has advantages and disadvantages, among them:

For safety issues in a wide variety of industries, the STPA analysis is currently used. Careful assessment and comparisons with traditional risk analysis techniques revealed that STPA finds the loss scenarios found by traditional approaches (such as the failure tree analysis, the failure modes and the analysis of effects), as well as many others that do not involve component failures. Surprisingly, while the STPA analysis is more powerful, it also seems to require fewer resources, including time. Another benefit of using a model-based tool is that it can be applied earlier in the design process and in situations where specific component data is not available. The analysis can begin as soon as the system's high-level baseline objectives are identified and design decisions are evaluated for their impact on safety and security before expensive reshuffling is required. With regard to the disadvantages, this method requires that those involved in the analysis be open-minded, more than with other traditional methods. Since the STAMP methods identify more causal scenarios, it is essential that information / results and control structure templates are carefully controlled and updated with the actual system design (configuration control / data control). In addition, depending on the system analyzed, a team of subject matter experts will be required to ensure that all scenarios are analyzed. These are not strictly disadvantageous with the method itself, but in its application [8-13].

3 Case Study : A Robotic Chemical Analysis Laboratory

Our system is composed of eleven mobile robots transports dangerous chemicals into a chemical analysis lab as shown in Figure 2.

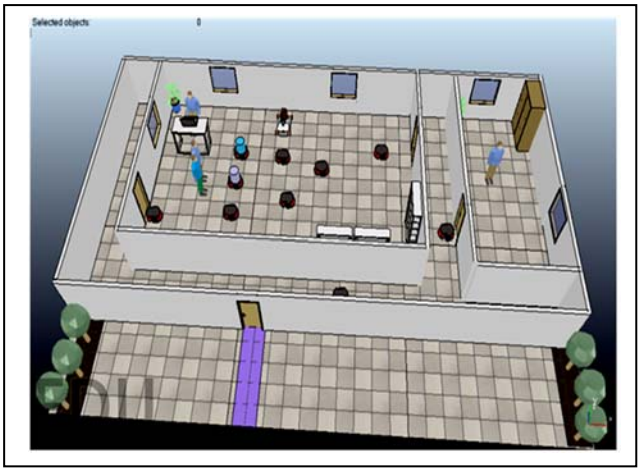


Fig. 2. Representation of a robotic chemical analysis laboratory.

3.1 Development of the hierarchical control structures using STAMP modeling

In this step, different control structures diagrams are established depending on STAMP modeling to determine interrelationships and interactions between the various system components. Actions or commands that a controller takes/sends to a controlled process and the response or feedback that the controller receives from the controlled process should be identified. It is also important to describe environmental disturbances that may affect the system and its operation.

3.2 For one robot

Figures 3 and 4 shows the high-level and a more detailed fully autonomous control structure for a differential mobile wheeled robot respectively; in which the operator launches the process and identifies the robot task or the target. The robot controller merges the sensors data, calculates feasible paths, chooses the optimal path to its mission and control the motion of the wheels.

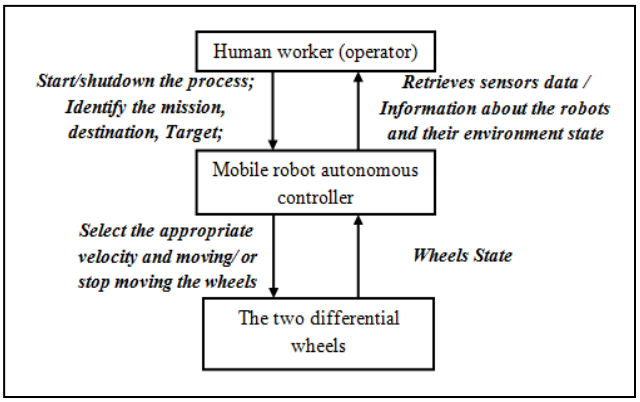


Fig. 3. The high-level control structure for one differential mobile wheeled robot.

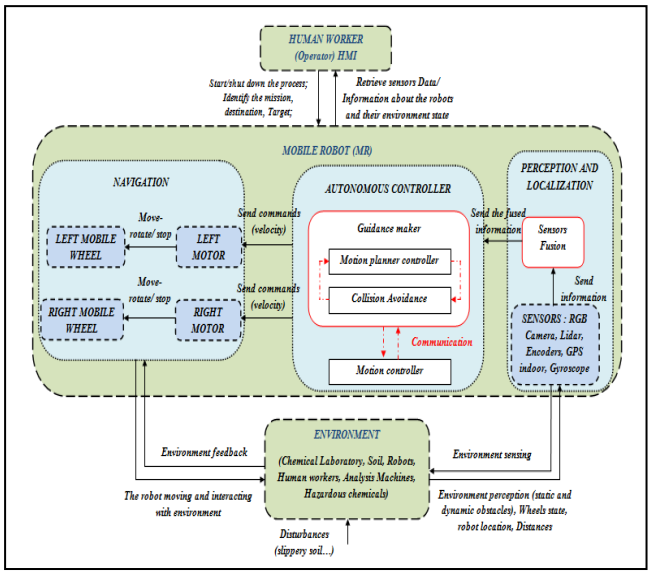


Fig. 4. The detailed control architecture for one robot with two differential wheels.

3.3 For a multi-robot system

There are several steering architectures. We can use them to coordinate the control of a multi-robot system and organize its tasks. [13;28;29]. Among them three architectures are analysed in this paper:

- *The Centralized architecture:* Figure 5 shows the centralized control architecture. In this structure, a control unit controls all the other robots and has decision-making power; it maintains the overall information of all the activities of our multi-robot system. This unit manages, processes events in real time, synchronizes and coordinates all tasks. The centralized structure is proposed by a limited number of researchers.

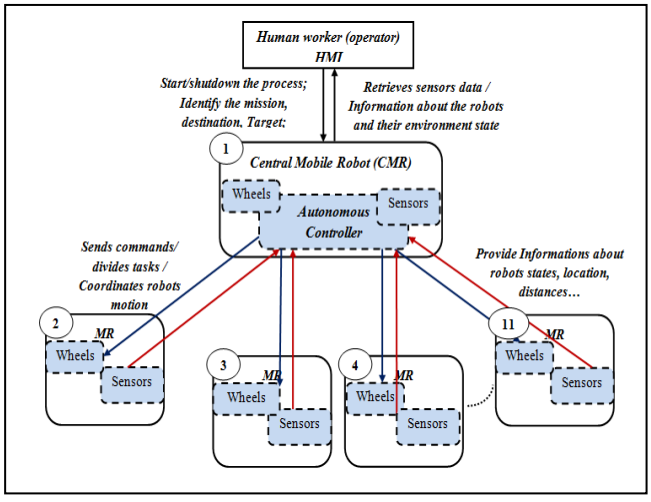


Fig. 5. The Centralized architecture of our system (the blue color refers to orders and the red color refers to feedback).

- *The hierarchical architecture:* Figure 6 represents the hierarchical control architecture. Where 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 [29]. In this type of architecture, management decisions are made by the high level leader, which must necessarily have all the information necessary to make decisions allowing good overall performance.

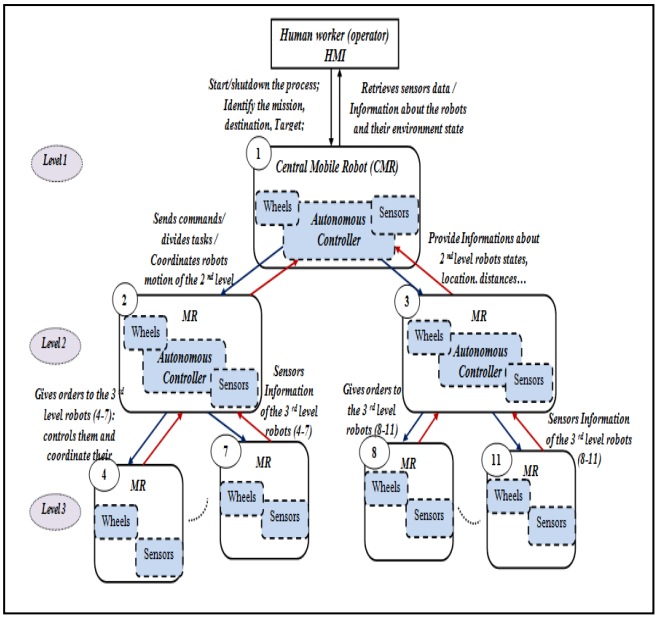


Fig. 6. The hierarchical architecture of our system (the blue color refers to orders and the red color refers to feedback).

- *The Modified hierarchical architecture:* Figure 7 represents the modified hierarchical control architecture. There is another form of hierarchical architecture where robots at the same level can coordinate with each other and communicate. This type of architecture is called a modified hierarchical architecture.

Extended version from EECS 2018

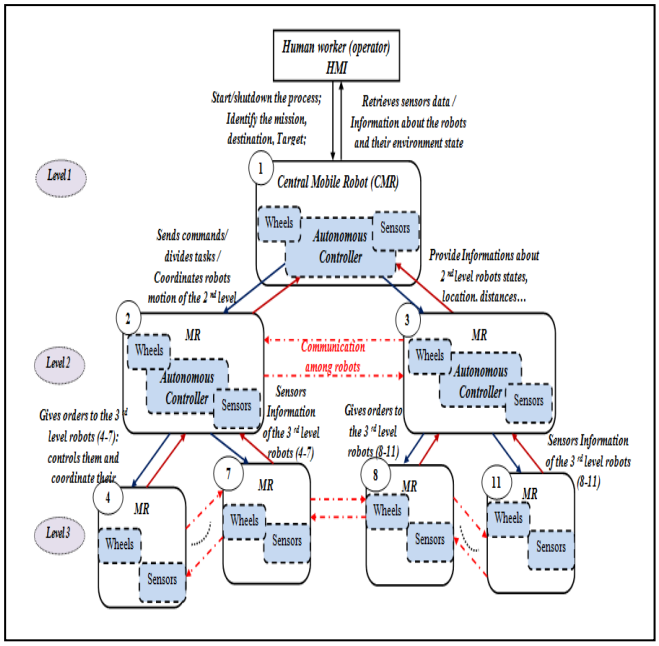


Fig. 7. The modified hierarchical architecture of our system.

4 Hazards Analysis and accident identification with Bowtie analysis method

4.1 Hazard analysis using Bowtie method

We use the BowTieXP software to develop our Bowtie models. The Bowtie represented in Figures 8, 9, 10 include risk scenarios of bad control for each architecture. We identify causes that could lead to hazard and their effects. The center of the Bowtie is the 'Top Event' which is losing control by the leader.

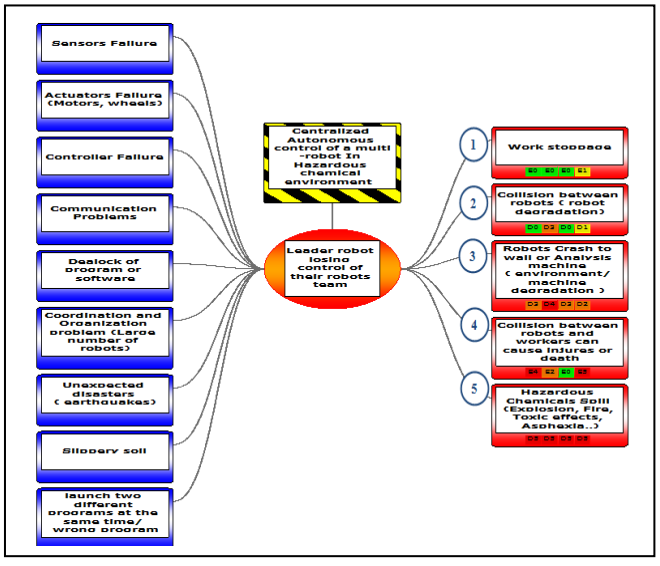


Fig. 8. Application of the Bowtie method using BowTieXP software for the centralized architecture.

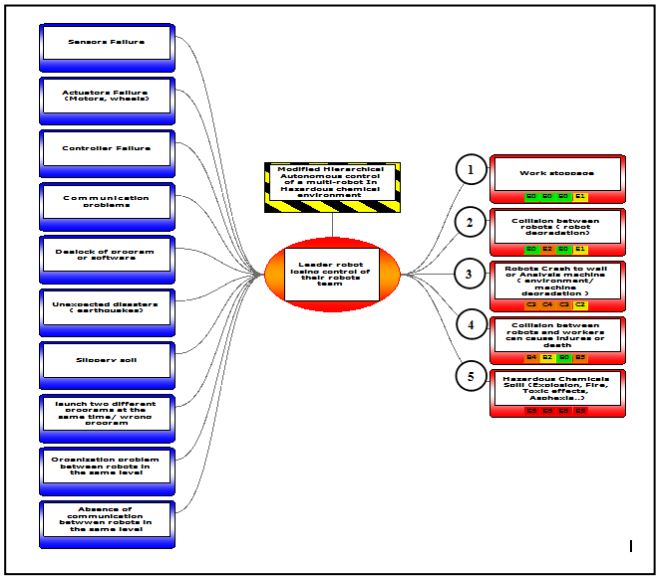


Fig. 9. Application of the Bowtie method using BowTieXP software for the hierarchical architecture.

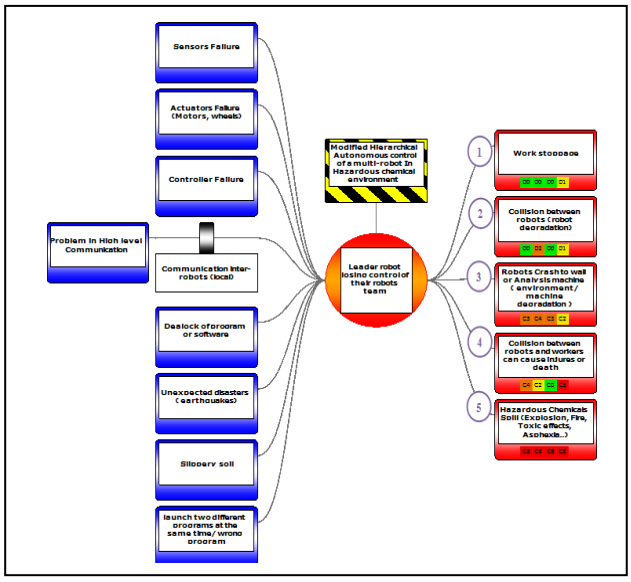


Fig. 10. Application of the Bowtie method using BowTieXP software for the modified hierarchical architecture.

4.2 Initial classification of consequences for the health and safety of persons, environment, the establishment reputation and the safety of the assets

The criticality assessment is done based on four levels : safety of persons, assets, establishment reputation and the environment respect according to the risk matrices defined in BowTieXP software; by the combination of the occurrence probabilities of

consequences and their severity. The following figures show the risk classification according to these levels.

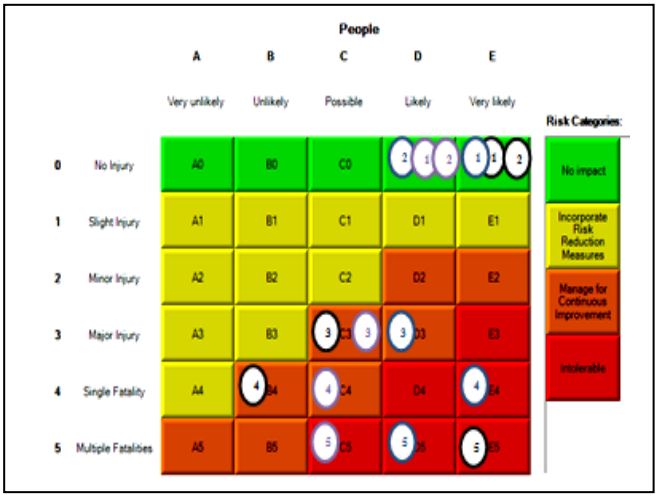


Fig. 11. Health and safety of persons.

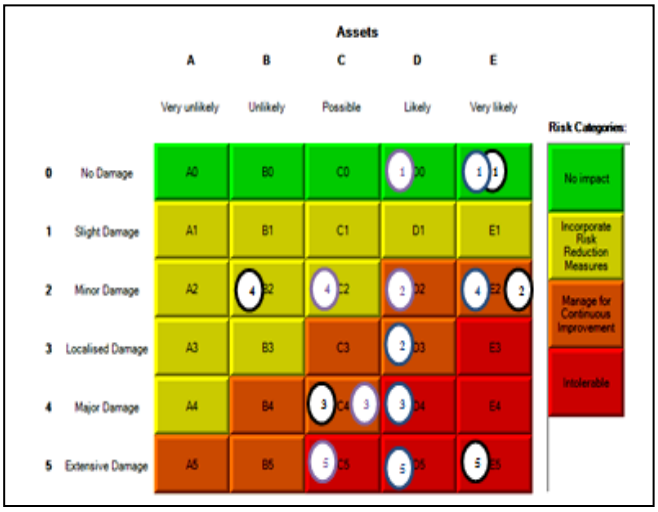


Fig. 12. Safety of assets.

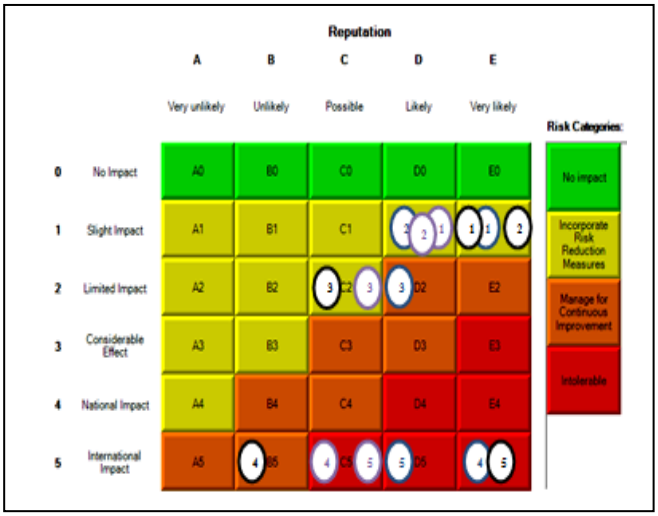


Fig. 13. The Establishment reputation.

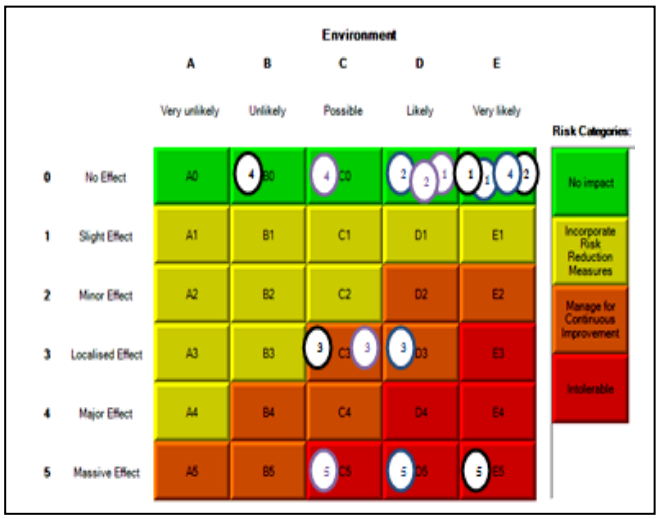


Fig. 14. Classification of consequences impact in environment.

These risk matrices contain four risk categories: No impact (green color), incorporate risk reduction measures (yellow color), manage for continuous improvement (orange color), intolerable (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 Bowtie risk classification and for each architecture, the high risk levelreached the intolerable risk column(with different degrees of criticality). The modified hierarchical architecture is the one contains a low criticality degree (C5) in the intolerable risk zone.

TABLE 2. CLASSIFICATION TABLE OF CONTROL ARCHITECTURES DEPENDING ON EFFECTS CRITICALITY

Architecture type	***Centralized architecture***	***Hierarchical architecture***	***Modified hierarchical architecture***
Classification of high risk level depending on effects criticality	High (E5)	High (E5)	High (C5)

5 STPA Hazard Analysis Application

In order to apply the STPA method on our system [30-32], we should follow the two steps shown in the organizational chart of Figure 1.

- In step 1, we have to identify unsafe control actions using the guidewords or identify hazard. Table 3 gathers the possible hazards.

- In step 2, we identify causes of unsafe control using the control loop. Table 4 gathers the possible causes of hazards obtained.

Before starting with STPA analysis application on our system, the system accidents likely to occur and its hazards must be identified [33]. These accidents and hazards have beendefined from Bowtie results:

1- The system accidents:
A1- Collision of robots loaded with chemicals or collision between robot and human (Human worker die or become injured).
A2- Collision between robots (two or more).
A3- Robot crashes to wall or falls down.

2- The system hazards:
H1- A robot enters in a prohibited area / Dangerous chemicals spill.
H2- A robot does not meet the safety distance between them.
H3- A robot enters in an uncontrolled state or unsafe attitude.
H4- The untimely stoppage of production.

5.1 Identification of hazard scenarios by STPA

The STPA hazard analysis allows us to detect all hazardous scenarios that can cause if any control action (provided, not provided, provided in an incorrect timing, stopped too soon or applied too long). Corresponding hazard scenarios and their causal factors can be found in table 3 and table 4.

To evaluate the hazard scenarios, we have classified each hazard in a criticality order (classification relating to the robots situation and their environment). From the results of the STPA analysis shown in table 3, we note that:

- The centralized architecture represents 16 hazard scenarios; 12 of them are classified as intolerable risk scenarios. The hierarchical architecture represents 14 hazard scenarios; 7 of them are classified as intolerable risk scenarios. The modified hierarchical architecture represents 11 hazard scenarios; 3 of them are classified as intolerable risk scenarios. According to this table, we conclude that the centralized architecture is the most dangerous architecture followed by the hierarchical architecture.
- The modified hierarchical architecture has outperformed the other architectures, due to two main characterized properties: the first is the multi-level control and the second is the inter-robots communication in the same level, so that the master can freed from the huge pressure of incoming information.

TABLE 3. HAZARD ANALYSIS TABLE FOR THE STPA APPROACH

Architecture	Scenarios	Hazard N°	Hazard
The centralized architecture	The initial command provided (or not provided) by the operator to the master robot	**No**	
	The master controller does not issue the command to one of the robots or more to avoid a dynamic or static obstacle (other robots loaded with chemicals or not, workers, analysis machine...)	**Yes**	**H1**
	The master controller provides high velocity to robots in slippery soil	**Yes**	**H2**
	The master controller doesn't provide commands (velocity) in front of static obstacle	**Yes**	**H3**
	The master controller issues a false order	**Yes**	**H4**
	The master controller provides an order after a delay time (especially when the master controller controls a large number of robots)	**Yes**	**H5**
	Sensors information provided wrong or too late	**Yes**	**H6**
	A huge number of sensors information provided to the master robot	**Yes**	**H7**
	One of the two motors doesn't rotate the robot wheel	**Yes**	**H8**
	The master controller gives a command to the wrong robot	**Yes**	**H9**
	Command stopped too soon or applied too long	**Yes**	**H10**
	The master controller does not choose the appropriate velocity for the robots	**Yes**	**H11**

	The master controller changes the velocity value in an incorrect time	**Yes**	**H12**
	Robot internship communication doesn't provided among controllers	**Yes**	**H13**
	Communication doesn't provided between slave robots and the master	**Yes**	**H14**
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (empty robots)	**Yes**	**H15**
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (robots loaded with chemicals)	**Yes**	**H16**
The hierarchical architecture	The initial command provided (or not provided) by the operator to the master robot	**No**	
	The master controller does not give the order to one of the robots of the second level to avoid a dynamic/ static obstacle (other robots loaded with chemicals or not, workers, analysis machine...)	**Yes**	**H17**
	The master controller provides high velocity to robots in slippery soil	**Yes**	**H18**
	Robot internship communication doesn't provided among controllers	**Yes**	**H19**
	The master controller gives a false order	**Yes**	**H20**
	Sensors information provided wrong or too late	**Yes**	**H21**
	A huge number of sensors information provided to the master robot	**Yes**	**H22**
	The master controller provides an order after a delay time	**Yes**	**H23**
	Communication doesn't provided between slave robots and the master	**Yes**	**H24**
	One of the two motors doesn't rotate the robot wheel	**Yes**	**H25**
	Command stopped too soon or applied too long	**Yes**	**H26**
	The master controller does not choose the appropriate velocity for the robots	**Yes**	**H27**
	The master controller changes the velocity value in an incorrect time	**Yes**	**H28**
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (case of empty robots)	**Yes**	**H29**
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (case of robots loaded with chemicals or not)	**Yes**	**H30**
The modified hierarchical architecture	The initial command provided (or not provided) by the operator to the master robot	**No**	
	The master controller does not give the order to one of the robots of the second level to avoid a dynamic/static obstacle (other robots loaded by chemicals or not, workers, analysis machine...)	**Yes**	**H31**
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (case of empty robots)	**Yes**	**H32**
	Sensors information provided wrong or too late	**Yes**	**H33**
	Robot internship communication doesn't provided among controllers	**Yes**	**H34**
	A huge number of sensors information provided to the master robot	**No**	
	One of the two motors doesn't rotate the robot wheel	**Yes**	**H35**
	Communication doesn't provided between slave robots and the master	**No**	
	The operator identifies two different missions (destinations) or launches two different programs to the master robot in the same time (case of robots loaded with chemicals or not)	**Yes**	**H36**
	The master controller provides an order after a delay time	**Yes**	**H37**
	The master controller provides high velocity to robots in slippery soil	**Yes**	**H38**
	Command stopped too soon or applied too long	**Yes**	**H39**
	The master controller does not choose the appropriate velocity for the robots	**Yes**	**H40**
	The master controller changes the velocity value in an incorrect time	**Yes**	**H41**

Extended version from EECS 2018

TABLE 4. CAUSAL FACTORS OF HAZARD TABLE

Hazard N°	Possible causal factors
H1,H3, H4, H6, H7, H10, H11, H13, H14, H17, H19, H20, H22, H24,H26, H27, H31, H34, H39, H40	- Wrong/ no sensing of the distances between obstacles and the robot or the position of obstacles (small obstacles, shining surfaces, measurement inaccuracies). - Sensors failure / inappropriate calibration. - Communication components failure for the slave robot (slave robot receiver). - Inadequate control algorithm of the master robot (requirement not implemented correctly in software). - The master robot sent the command to a bad robot address. - Memory card saturation.
H5, H6, H11, H12, H21, H33, H23, H27, H28, H37, H40, H41	- A large number of robots controlled by one master robot. - Receive a large range of feedback information from slave robots in the same time. - Program blockage of the master robot. - Feedback delays.
H9	- The master robot sent the command to a bad robot address. - Error filling initial data by operator.
H31, H37, H39, H40, H41	- Missing /wrong communication between slave robots in the same level.
H8, H25, H35	- Motors failure, wrong command, low battery
H2, H18,H38	- Chemicals spill or water on the soil
H15, H16, H29, H30, H32, H36	- Human lose focus, Extreme tiredness…

5.2 Recommendation:

After the application of the STPA and Bowtie methods, we conclude that:

- The modified hierarchical architecture is the architecture that has a minimum number of constraints compared to the two others (centralized and hierarchical). So it is the best architecture to control our multi-robot system.
- It must be ensured that the control equipment has a high reliability.
- The program must be validated.
- It should be also checked the integrity of the software and hardware.
- No changes of the program are allowed except by a trusted specialist.
- Based on the results obtained from the method of Bowtie, we conclude that this method does not show the difference between the different architecture. It considers the situation in general, regardless of the control structure. It does not focus on interactions among the different components, but we can combine it with STPA to make accidents and hazards identification easy.

6 Conclusion

In this paper, we have presented the hazard analysis STPA method and we have highlighted many differences between this approach and the other traditional analysis methods.

The most powerful point in the STPA analysis is that it takes into account a broader set of potential scenarios including those for which no failures occur, the problems arising due to unsafe and unintended interactions between the system components.

We have classified three types of control architectures that we can use in order to coordinate our multi-robot mobile system (centralized, hierarchical and modified hierarchical) according to their properties using Bowtie method. We have also analyzed those control architectures using STPA hazard analysis.

Bowtie analysis method considers the situation in general regard, whatever the control structure type, it does not focus on interactions among the different components, and however its combination with STPA analysis makes accidents and hazards identification easy.

According to the result of the analysis technique STPA, we have concluded the most dangerous control architecture (to avoid) is the centralized architecture. Properties that characterize this architecture make it more prone to accidents and hazards. The modified hierarchical architecture is the one that leads to a medium risk.

References:

[1] Homa, A., et al., "Systems-theoretic Safety Assessment of Robotic Telesurgical Systems", International Conference on Computer Safety, Reliability, and Security, SAFECOMP, 2015, pp.1-14.

[2] Kazanzides, P., "Safety Design for Medical Robots", Annual International Conference of the IEEE Engineering in Medicine and Biology Society, pp.7208–7211, 2009.

[3] Suwoong, L. and Yamada, Y., "Risk Assessment and Functional Safety Analysis to Design Safety Function of a Human-Cooperative Robot", Human Machine Interaction - Getting Closer , edited by M. Inaki. Intech, 2012.

[4] Bensaci, C., Zennir, Y., Pomorski, D., "Complex Safety Study of Intelligent Multi-Robot Navigation in a Risk's Environment", International Carnahan Conference on Security Technology, Madrid, Spain, 2017.

[5] Böhm, P. and Gruber, T., "A Novel HAZOP Study Approach in the RAMS Analysis of a Therapeutic Robot for Disabled Children", Computer Safety, Reliability, and Security, pp.15–27. Springer, 2010.

[6] Woodman, R., Winfield, A. F., Harper, C., and Fraser, M., "Building Safer Robots: Safety Driven Control", Internatioanl Journal of Robotics Research, 31(13), pp.1603–1626, 2012.

[7] Alexander, R., Herbert, N., and Kelly, T., "Deriving Safety Requirements for Autonomous Systems", SEAS DTC Technical Conference, 2009.

[8] Dogramadzi, S., Giannaccini, M. E., Harper, C., Sobhani, M., Woodman, R., and Choung, J., "Environmental Hazard Analysis – a Variant of Preliminary Hazard Analysis for Autonomous Mobile Robots", Journal of Intelligent & Robotic Systems, 76(1), pp.73–117, 2014.

[9] Guiochet, J., "Hazard Analysis of Human–Robot Interactions with HAZOP–UML", Safety Science, Elsevier, 2016, 84, pp.225-237.

[10] Leveson, N.G., "Engineering a Safer World: Systems Thinking Applied to Safety", Cambridge, MA: MIT Press, 2011, 555 pages.

[11] Alemzadeh, H., Chen, D., Lewis, A., Kalbarczyk, Z., and Iyer, R., "Systems-Theoretic Safety Assessment of Robotic Telesurgical System", 34th International Conference on Computer Safety, Reliability and Security, 2015.

[12] Jiahui Zou, "Systems-Theoretic Process Analysis (STPA) Applied to the Operation of Fully Autonomous Vessels, Reliability", master's thesis, Availability, Maintainability and Safety (RAMS), NTNU, Department of Mechanical and Industrial Engineering, 2018.

[13] Zennir, Y., « Apprentissage par renforcement et systèmes distribués : application à l'apprentissage de la marche d'un robot hexapode », PhD thesis, INSA Lyon, 2004, 180 pages.

[14] Demesure, G., « Coordination et planification de systèmes multi-agents dans un environnement manufacturier », PhD thesis, Université de Valenciennes et du Hainaut-Cambresis, 2016.

[15] Dilts, D.M., Boyd, N.P., and Whorms, H.H., "The Evolution of Control Architectures for Automated Manufacturing Systems", J. Mfg. Sys., vol.10, no.1, pp.79-93, 1991.

[16] Kim, B.I., "Intelligent Agent Based Planning, Scheduling and Control: Warehouse Management Application", PhD thesis, Rensselaer Polytechnic Institute, Troy, New York, 2002.

[17] Pujo, P., Kieffer, J.P., « Concepts fondamentaux du pilotage des systèmes de production », dans « Fondements du pilotage des systèmes de production », Hermès, Lavoisier, 2002.

[18] Reaidy, P.J., « Etude et mise en œuvre d'une architecture d'agents en réseau dans les systèmes dynamiques situés : pilotage des systèmes de production complexes », PhD, Génie Industriel, université de Savoie, 2003.

[19] Takuto, I., et al., "Modeling and Hazard Analysis using STPA", IAASS Conference, Making Safety Matter, May 19-21, 2010, Huntsville, Alabama, USA SP-680 (September 2010), pp.1-11.

[20] Young, W., Leveson, N.G., "An Integrated Approach to Safety and Security based on

Extended version from EECS 2018

Systems Theory", Communications of the ACM, vol.57, no.2, February 2014, pp.31-35.
[21] Takuto, I., Leveson, N.G., John, P.T., Cody, H.F., Masafumi, K., Yuko M., Ryo, Ujiie H.N., and Nobuyuki H., "Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis", Journal of Spacecraft and Rockets, 2014, vol.51, no.2, pp.509–522.
[22] Li-Jeng, H., "A Quantitative Method for Dynamic Risk Prediction Using AHP and Grey Modeling: Case Study of a Mud-Flow Hazard", International Journal of Safety Science, 2017, vol.1, no.3, pp.61-73.
[23] Abdulkhaleq, A., Baumeister, M., Böhmert, H., and Wagner, S., "Missing no Interaction – Using STPA for Identifying Hazardous Interactions of Automated Driving Systems", International Journal of Safety Science, 2018, vol.2, no.1, pp.115-124.
[24] Rejzek M., Björnsdóttir S.H., and Krauss S.S., "Modelling Multiple Levels of Abstraction in Hierarchical Control Structures", International Journal of Safety Science, 2018, vol.2, no.1, pp.94-103.
[25] Adesina, A.A., et al., "Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management", Pharmaceutical Medicine, 2017, vol.31, no.4, pp.267-278.
[26] Pawlicki, T., et al., "Application of Systems and Control Theory based Hazard Analysis to Radiation Oncology", Medical Physics, 2016, vol.43, no.3, pp.1514-1530.
[27] Rejzek, M., "Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System", STAMP Workshop 2012, 2012: MIT, Boston.
[28] Reaidy, P.J., « Etude et mise en œuvre d'une architecture d'agents en réseau dans les systèmes dynamiques situés : pilotage des systèmes de production complexes », PhD, Ecole des Mines d'Alès / Université de Savoie Mont Blanc, 2003, 181 pages.
[29] Demesure, G., « Coordination et planification de systèmes multi-agents dans un environnement manufacturier », PhD thesis, Université de Valenciennes et du Hainaut-Cambresis, 2016.
[30] Rejzek, M., "Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System – a Review", 1st European STAMP Workshop, 2012: Braunschweig.
[31] Antoine, B., "Systems Theoretic Hazard Analysis (STPA) applied to the Risk Review of Complex Systems: an Example from the Medical Device Industry", Massachusetts Institute of Technology, 2013.
[32] Rejzek, M., "Use of STPA in Digital Instrumentation and Control Systems of Nuclear Power Plants", 2nd European STAMP Workshop, 2014: Stuttgart.
[33] Rejzek, M., Hilbes, C., and Krauss S.S., "Safety Driven Design with UML and STPA", STAMP Workshop 2015, 2015: MIT, Boston.

View publication stats