ALGERIAN JOURNAL OF SIGNALS AND SYSTEMS (AJSS)

A New Approach to System Safety of human-multi-robot mobile system control with STPA and FTA

Chaima BENSACI [(1)*], Youcef ZENNIR[(2)], Denis POMORSKI[(3)]
[(1)] University 20 Août 1955 of Skikda, LGCES Laboratory Skikda, Algeria
[(2)] University 20 Août 1955 of Skikda, Automatic Laboratory Skikda, Algeria
[(3)] University of Lille 1, CRIStAL Laboratory– UMR 9189 Lille, France
[*]ch.bensaci@univ-skikda.dz

Abstract: Autonomous Mobile multi-robots are among the most complex systems in their control. Especially when those robots navigate in hazardous and dynamic environments such as chemical analysis laboratories which include dangerous and harmful products (poisonous, flammable, explosive ...). This study deals the safety problem in a robotic analysis laboratory and investigates the possibility to use those autonomous multi-robots in such environments with the presence of human workers without serious hazards. We used a systems-theoretic hazard analysis technique (STPA) in addition to fault tree analysis to identify the potential safety hazard scenarios, their causal factors and we conclude by a set of recommendations.

Keywords: Hazard Analysis, STPA, FTA, Collaborative multi-mobile robots.

1. INTRODUCTION

The use of mobile robots in high-risk factories and laboratories is one of the biggest challenges facing today's researchers. This environment requires a lot of precision in robots control and the respect of safety measures to prevent the occurrence of major disasters. Our study will be conducted on a robotic laboratory for chemical analysis where multi-mobile robots navigate autonomously, collaborating together in order to move dangerous chemicals (toxic, explosive, flammable…). This complex environment contains also analysis machines and working humans. The paper presents hazard analysis study applicable for multi-robots system navigate in a chemical laboratory using a combination of two risk analysis methods System-Theoretic Process Analysis (STPA) which is used recently to analyze Hazards of High complex systems in [1-7], and Fault tree analysis (FTA) in order to clarify the expected Hazard scenarios. It begins with a small introduction and STPA hazard analysis presentation. Then, STPA / FTA application in addition to their results are presented. Finally, recommendation and concluding remarks are closing the paper.

2. LABORATORY ENVIRONMENT DESCRIPTION

Our study made on a complex system composed of collaborative autonomous multi-mobile robots with differential wheels. Their main task is to transport dangerous chemicals (toxic, flammable, explosive..) within a chemical analysis laboratory as the figure 1 show.

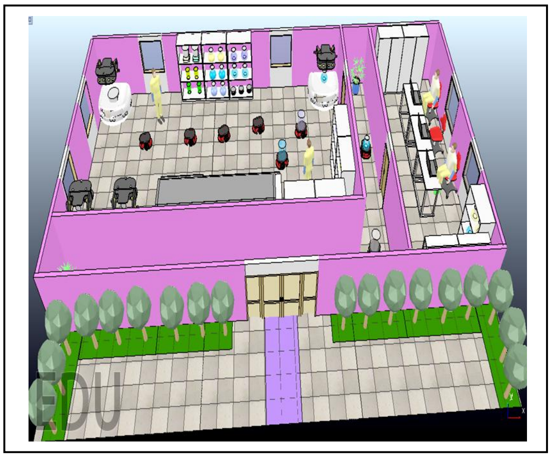

Fig. 1 Scenario of collaborative mobile robots work in chemical analysis laboratory.

3. SYSTEM -THEORETIC PROCESS ANALYSIS (STPA)

System-Theoretic Process Analysis (STPA) is a hazard identification and analysis technique based on STAMP causality model (System-Theoretic Accident Model and Processes). The STAMP based on three important concepts [8-10]:

- Safety constraints ;
- A hierarchical safety control structure ;
- Process models.

In STAMP, systems are interrelated components maintained in a state of dynamic equilibrium by feedback control loops. The interactions among 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 [11, 13].

STPA is a risk analysis method that specifically investigates risks generated by functional interaction between control units present in a system as well as risks caused by component failures. Safety is handled as an emergent system property in STPA; that is, it arises only when the various components of the system interact with one another [12,14, 15].

The analysis with STPA is divided into two main steps:

Once the control structure is created, the first step of the STPA analysis is to identify potentially dangerous control actions using the four following keywords:

- **Provide** a control action that leads to a danger ;
- **Not provide** a control measure necessary to prevent a hazard ;
- **Provide** control action **too early or too late or out of sequence** ;
- **Continue** a control action **too long or stop it too early**.

The second step is to examine the system's control loops (using a structured and guided process) to identify the causal factors of unsafe control actions [11, 16]. The STPA has the same goals as traditional analysis methods like FTA, FMEA, HAZOP ... which is to create a set of hazardous scenarios, but STPA includes a broader set of potential scenarios, including those in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components. Most risk and vulnerability analysis techniques like HAZOP, FMEA, FTA...focus on physical failures rather than dysfunctional (unsafe or insecure) behavior, broader social and organizational factors. Therefore, STPA is a risk analysis technique based on systems theory rather than reliability theory. Therefore, in STPA Analysis 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 and advertising causes must also be controlled [8, 10, 16].

4. APPLICATION AND RESULTS

Application of STPA and FTA

In order to apply the STPA method on our system, we should follow the steps shown in the figure 2.

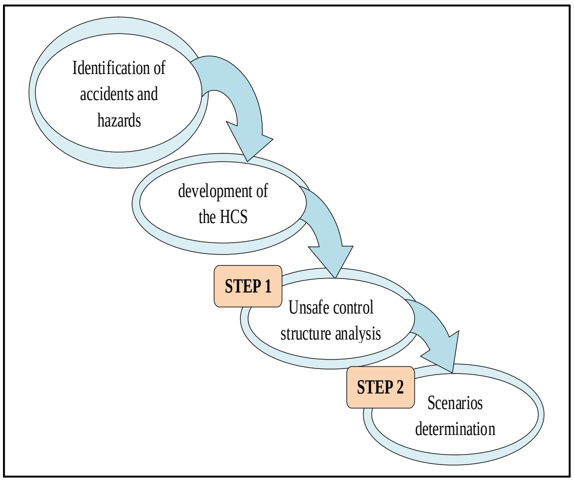
Identification of accidents and hazards
development of the HCS
STEP 1
Unsafe control structure analysis
STEP 2
Scenarios determination

Fig. 2 STPA methodology

To get started with the application of STPA on a system, the hierarchical control structure (HCS) must be developed.

A. The hierarchical control structure (HCS) :

The system to be analyzed first needs to be described as a hierarchical control structure using a simple set of modeling rules, this can make the system more obvious. All HCSs composed of 4 main concepts : Controlling units, control actions , feedback and controlled process. The figure (3) show the HCS of our system. The most important thing here is to provide a safly autonomous control of the wheels motion and their speeds in order to have a collision-free smooth multi-robot movement, which is done perfectly in collaboration between the robotics team of the laboratory. Therefore the STPA first step would be to analyse the system control structure and to identify the wrong behaviours that can produce from unsafe control actions then in STPA second step, we would determine the hazard scenarios and identify the causal factors of each unsafe control action or unwanted process reaction. Finally , we will organise the scenarios identified in a tree with the same principle as the fault tree analysis FTA.

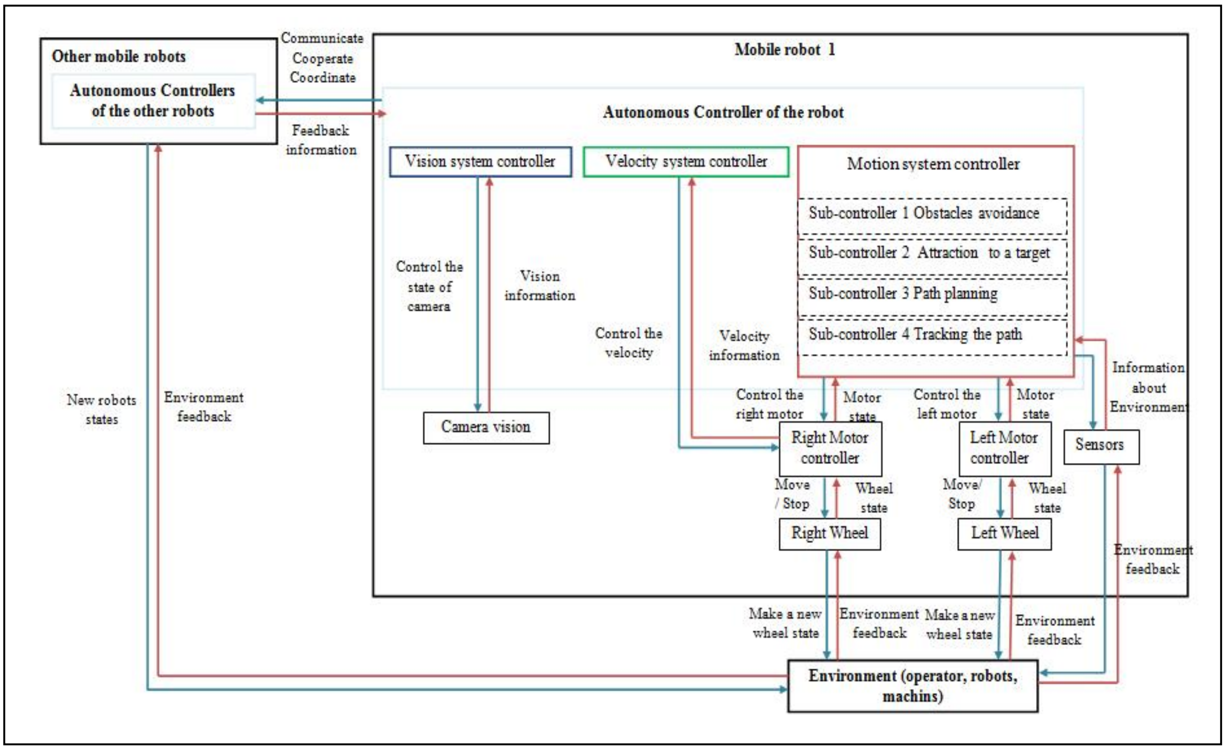

Fig. 3 The hierarchical control architecture of multi-mobile robots system.

The results of STPA analysis are aggregated in table I and table II.

The table I shows the set of unsafe control actions (UCAs) and their causal factors whereas the Hazard identification of each UCA, their probable accidents and losses are collected in table II.

Table 1 STPA Hazard analysis Table

Unsafe control actions (UCAs)	**Number of UCA**	**Causal factors (Scenarios)**
The robot **does not** avoid a dynamic or static obstacle (like other robots loaded by chemicals, workers, analysis machines, wall ...)	UCA1	- 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. - Failure of communication components (robot receiver). - Inadequate control algorithm of the robot. - Inadequate control parameters. - Memory card saturation of the robot. - Motors failure. - Wheels lock up - Conflicting control action from actuator.
The controller **issues** a false order	UCA2	
Command **stopped too soon or applied too long**	UCA3	
The controller **does not choose** the appropriate velocity for the robots (very high)	UCA4	
The controller **provides** an order after a delay time	UCA5	- Receive a large range of feedback information from robots in the same time. - Memory card saturation of the robot. - Program blockage of the robot. - Feedback delays.
The controller **changes** the velocity value in an incorrect time	UCA6	

TABLE 2 IDENTIFICATION OF HAZARDS ,ACCIDENTS AND LOSSES FOR EACH UCA.

UCAs	Hazards	Probable Accidents	losses
UCA1	- Robots violate the safer distance between them. - Robots enter Dangerous area. - Chemicals spill.	- Collision of robots loaded with chemicals. - Collision between robot and human worker. - Robot loaded with chemicals crash to wall or falling down. - Chemical spill on the worker. - Mixing of incompatible chemicals. - Fire broke out in the laboratory. - An explosion might be occurred in the laboratory.	- Workers killed or become injured - Installation, machines and robots damaged - Loss of chemicals - Reduced production - Environment contaminated - Toxic effects of chemicals spill, fire smoke, toxic gases, vapors and dust.
UCA2	- Robot enters uncontrolled state or unsafe attitude.		
UCA3	- Robot enters uncontrolled state or unsafe attitude.		
UCA4	- Robot enters dangerous state.		
UCA5	- The robot can not respond quickly in hazardous situations (when there are obstacles).		
UCA6	- Robot enters unsafe attitude.		

Through STPA analysis results shown in the table 2, it’s clear to us the emergence of a set of unwanted events. We selected the most dangerous of them (explosion, Fire, worker killed or become injured) to reflect more deeply over the possible causes of these hazards using the fault tree analysis FTA.

The fault tree analysis that we used in this paper is different than the traditional fault tree analysis, it does not represents only the faults and failure; it includes more other causes. We aggregate in this tree the causes from all the control hierarchy (from regulations to the final process) and inappropriate behaviors of workers and robots in addition to faults. A set of hazard scenarios represented in the trees shown in figures 4, 5 and 6.

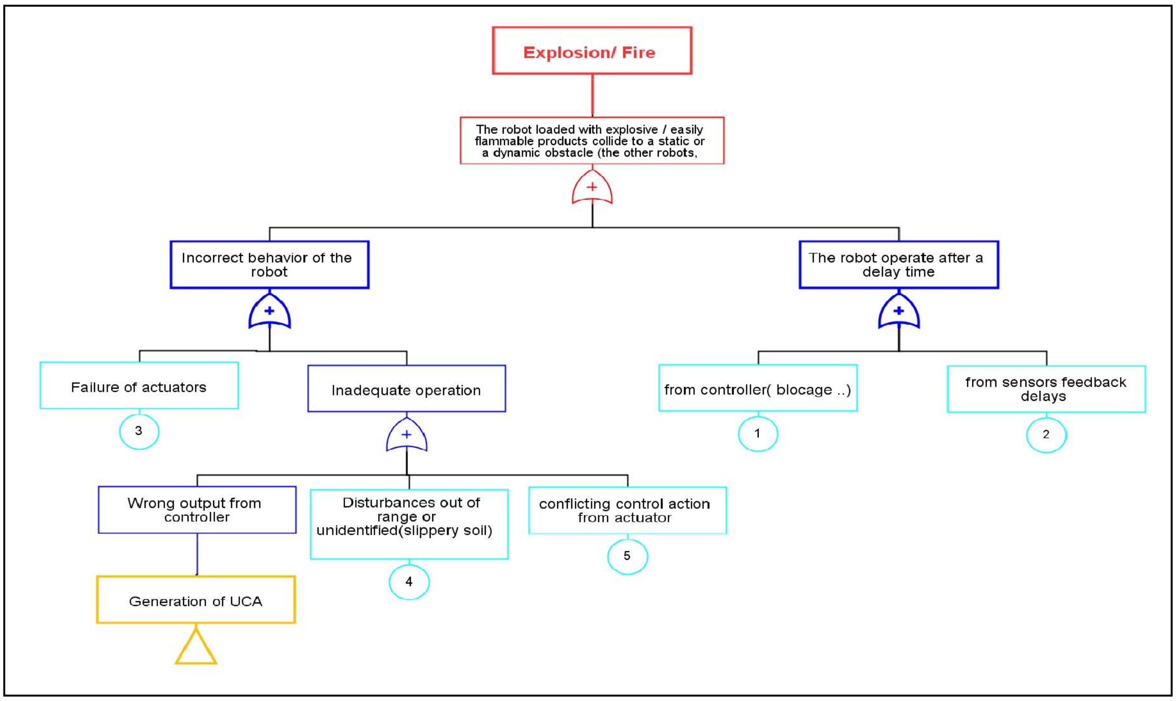
Explosion/ Fire
The robot loaded with explosive / easily flammable products collide to a static or a dynamic obstacle (the other robots,
+
Incorrect behavior of the robot
+
The robot operate after a delay time
+
Failure of actuators
3
Inadequate operation
+
from controller(blocage ..)
1
from sensors feedback delays
2
Wrong output from controller
Disturbances out of range or unidentified(slippery soil)
4
conflicting control action from actuator
5
Generation of UCA

Fig. 4 Tree represents scenarios of Explosion/ Fire hazards part 1.

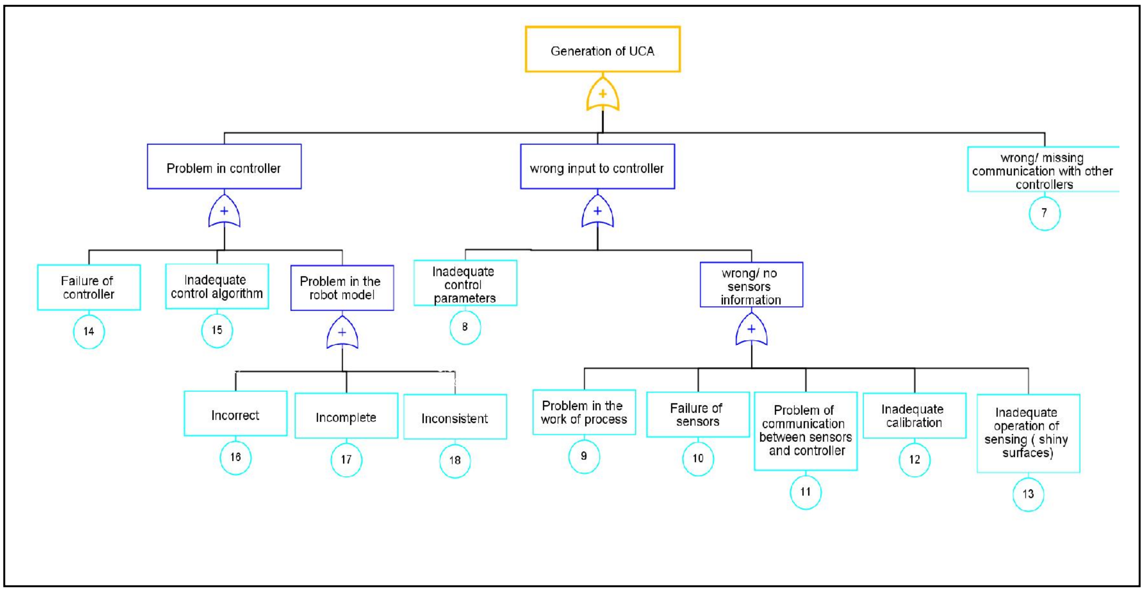
Generation of UCA
+
Problem in controller
wrong input to controller
wrong/ missing communication with other controllers
7
+
+
Failure of controller
14
Inadequate control algorithm
15
Problem in the robot model
+
Inadequate control parameters
8
wrong/ no sensors information
+
Incorrect
16
Incomplete
17
Inconsistent
18
Problem in the work of process
9
Failure of sensors
10
Problem of communication between sensors and controller
11
Inadequate calibration
12
Inadequate operation of sensing (shiny surfaces)
13

Fig. 5 Tree represents scenarios of Explosion/ Fire hazards part 2.

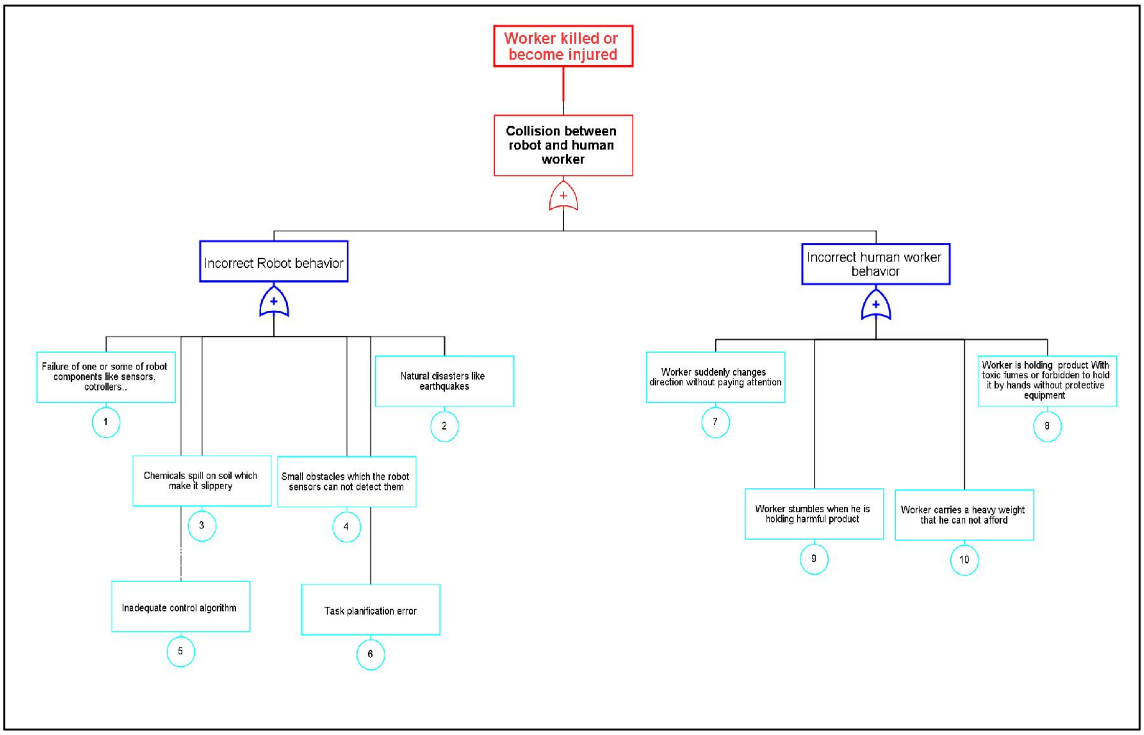
Worker killed or become injured
Collision between robot and human worker
+
Incorrect Robot behavior
+
Incorrect human worker behavior
+
Failure of one or some of robot components like sensors, cotrollers..
1
Natural disasters like earthquakes
2
Chemicals spill on soil which make it slippery
3
Small obstacles which the robot sensors can not detect them
4
Inadequate control algorithm
5
Task planification error
6
Worker suddenly changes direction without paying attention
7
Worker is holding product With toxic fumes or forbidden to hold it by hands without protective equipment
8
Worker stumbles when he is holding harmful product
9
Worker carries a heavy weight that he can not afford
10

Fig. 6 Tree represents scenarios of worker killed or become injured hazards.

Analysis results

On the basis of the results obtained through the application of STPA / FTA analysis methods, it is concluded that the sources of danger in this type of Robotized laboratory may be of human, robotized or environmental origin (environmental disturbances). Both mobile systems (workers and robots) can be damaging if they bring inappropriate behaviors. These sources can be concluded in the following figure.

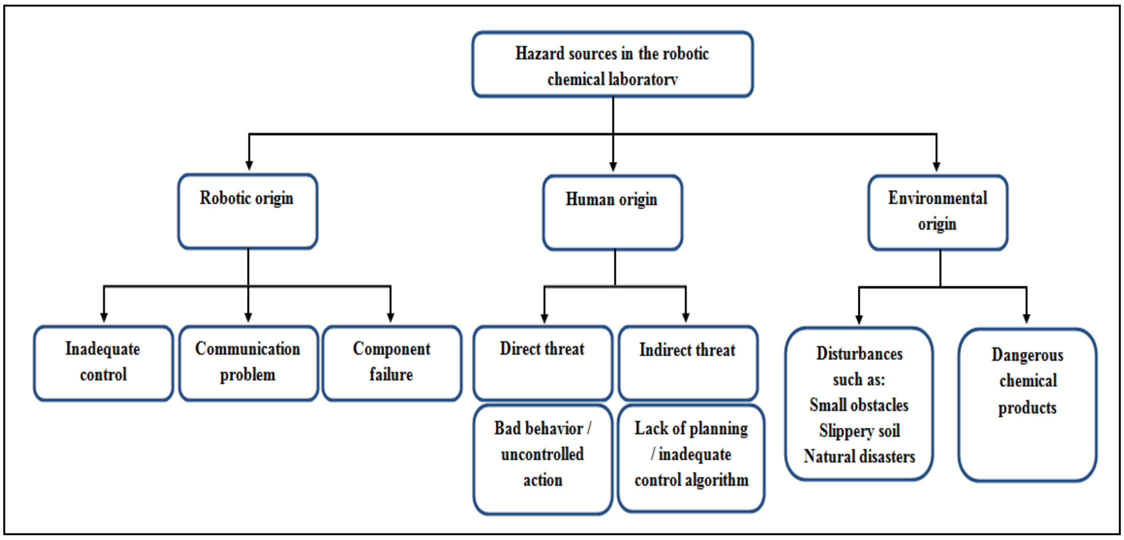
Hazard sources in the robotic chemical laboratory
Robotic origin
Human origin
Environmental origin
Inadequate control
Communication problem
Component failure
Direct threat
Indirect threat
Bad behavior / uncontrolled action
Lack of planning / inadequate control algorithm
Disturbances such as: Small obstacles Slippery soil Natural disasters
Dangerous chemical products

Fig. 7 Diagram shows hazard sources in the robotic chemical laboratory.

Through the analysis results of hazards; we obtained the following recommendations:

- Ensure the good control of robots ;
- The right choice of control architecture ;
- Ensure good cooperation, communication and coordination between the robots ;
- Ensure the proper functioning of the robots ;
- The hygiene of the working environment ;
- The protective equipments is obligatory for each operator ;
- Enforcement of security constraints.

5. CONCLUSION

In this paper, we have analyzed the hazard within a robotic analysis laboratory where two kinds of mobile systems are presented (humans and robots); using STPA hazard analysis method in addition to FTA fault tree analysis. STPA analysis includes a set of potential scenarios including those in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components. Scenarios of hazards obtained by STPA may result from both unsafe control action and inadequate or incorrect execution. Most of problems in hierarchical architectures arise from unintended interactions between control system components and due to bad communication between other robots. According to the results of STPA and FTA we have concluded that of danger in this type of Robotized laboratory may be of human, robotized or environmental origin (environmental disturbances). This methodology can provide the same safety recommendations as other traditional techniques also considering other factors out of the scope of those techniques.

References

[1] M. Rejzek, N.G. Leveson, B. Antoine, C. Hilbes, M. Grossmann, D. Meer, “Evaluation of STPA in the safety analysis of the gantry 2 proton radiation therapy system”, Talk. In: 1st MIT STAMP Workshop. (April 17-19). Boston, USA: Massachusetts Institute of Technology.pp.1-22, 2012.

[2] A. Abdulkhaleq, M. Baumeister, H. Böhmert, S. Wagner, “Missing no interaction – using stpa for identifying hazardous interactions of automated driving systems”. International Journal of Safety Science, vol.2, no.1, pp.115-124, 2018.

[3] W. Krzysztof, M. Jakub, K. Pentti, “Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels”, Reliability Engineering & System Safety, ISSN: 0951-8320, Vol: 178,2018, Page: 209-224,2018.

[4] O. A. V. Banda, and S.Kannos, “Hazard analysis process for autonomous vessels”. 69, 2017.

[5] A. Plioutsias, and N. Karanikas, “Using STPA in the evaluation of fighter pilots training programs”. Procedia Engineering, *128*, 25–34, 2015.

[6] Y.Song, “Applying system-theoretic accident model and processes (STAMP) to hazard analysis”, 2012.

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

[8] W.Young, N.G.Leveson, “Inside risks an integrated approach to safety and security based on systems theory applying a more powerful new safety methodology to security risks, communications of the acm”, vol. 57, no. 2. pp.31-35, february 2014.

[9] N.G. Leveson,”STPA primer”, 2013.

[10] N.G.Leveson, “ Engineering a safer world: systems thinking applied to safety”, Cambridge, MA: The MIT Press, 2012.

[11] B. Rokseth, I. Bouwer Utne and J. Erik Vinnem, “A systems approach to risk analysis of maritime operations”, Norwegian University of Science and Technology (NTNU), Volume: 231 issue: 1, page(s): 53-68,2017.

[12] Ishimatsu, Takuto, N.G. Leveson, John P. Thomas, Cody H. Fleming, M. Katahira, Y. Miyamoto, R. Ujiie, H. Nakao, and N. Hoshino. “Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis”, Journal of Spacecraft and Rockets 51, no. 2 (March 2014): 509–522.

[13] H. Alemzadeh et al, “Systems-theoretic Safety Assessment of robotic telesurgical systems”, the International Conference on Computer Safety, Reliability, and Security (SAFECOMP), 2015.

[14] M. Rejzek,*S.* Björnsdóttir, *S. Krauss. “ Modelling multiple levels of abstraction in hierarchical control structures”.* Talk presented at: 5th European STAMP/STPA Workshop and Conference; 2017 September 13-15; Reykjavík, Iceland.

[15] M. Rejzek, C. Hilbes, “ Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants”, Nuclear Engineering and Design, Volume 331, 2018, Pages 125-135, ISSN 0029-5493,

[16] Ishimatsu et al. "Modeling and hazard analysis using STPA", Proceedings of the 4th IAASS Conference, Making Safety Matter, 19–21 May 2010, Huntsville, Alabama, USA SP-680 ,September 2010.