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

Chaima Bensaci, Youcef Zennir, Denis Pomorski

A Comparative Study of STPA Hierarchical Structures in Risk Analysis:

The case of a Complex Multi-Robot Mobile System

Chaima BENSACI
Université 20 Août 1955 Skikda
LGCES Laboratory
Skikda, Algeria
ch.bensaci@univ-skikda.dz

Youcef ZENNIR
Université 20 Août 1955 Skikda
Automatic Laboratory of Skikda
Skikda, Algeria
y.zennir@univ-skikda.dz

Denis POMORSKI
Université de Lille
CRIStAL Laboratory – UMR9189
Lille, France
denis.pomorski@univ-lille1.fr

***Abstract*— Autonomous multi-robot systems are among the most complex systems to 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 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 those control architectures according to their properties, 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; Multi-Robot Mobile System; Control Architectures

I. INTRODUCTION

The use of 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...) in contact with or close to the human. All these factors would increase the control system complexity, especially when it becomes autonomous control. Therefore, before including those robots in such environments, we need to do a thorough analytical study of all potential risk scenarios likely to be created and their causal factors. Our study will be conducted on eleven mobile robots collaborating 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 three kinds of architectures (centralized, hierarchical and modified hierarchical) using a new, more powerful and rigorous analysis method called STPA.

II. STPA HAZARD ANALYSIS

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) [1]. In addition to the basic notions of systems theory, the STAMP analysis based on three concepts [2]:

- 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 [3].

A. 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 the STAMP causality model. The analysis is performed on the functional control structure of the system.

Once the control structure created, the first step of the STPA analysis is to identify potentially dangerous control actions, which typically consist in:

- 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;
- or 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 objective of the STPA analysis is the same as any hazard analysis: it is to create a set of potentially hazardous scenarios [4].

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

The STPA analysis has the same goals as the old methods like FTA, FMEA and HAZOP. It consists in creating a set of hazardous scenarios. 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.

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 [1;3;5-6].

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].

III. Initial Classification of Control Architectures

There are different types of architectures to model the control of complex systems. We present in the table below three architectures with their advantages and disadvantages.

TABLE I. Advantages and disadvantages of the three control architectures [4]

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 (ie 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.

The architecture giving the minimum of constraints presents a low danger. The architecture giving the maximum of constraints presents a serious danger (high danger). Finally, the intermediate state between these two extremes presents a medium danger.

TABLE II. CLASSIFICATION TABLE OF CONTROL ARCHITECTURES DEPENDING ON THE NUMBER OF CONSTRAINTS

Architecture type	***Centralized architecture***	***Hierarchical architecture***	***Modified hierarchical architecture***
Classification depending on the number of constraints	High	High	Medium

IV. APPLICATION OF STPA METHOD

Our system composed of eleven mobile robots transports dangerous chemicals into a chemical analysis lab as shown in Figure 1.

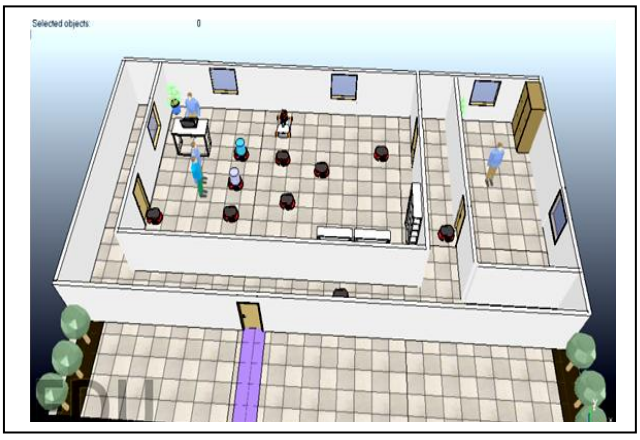

Fig. 1. Stage consisting of eleven mobile robots working in a chemical analysis lab.

In order to apply the STPA method on our system, we should follow the steps shown in the organizational chart of Figure 2 [14-16].

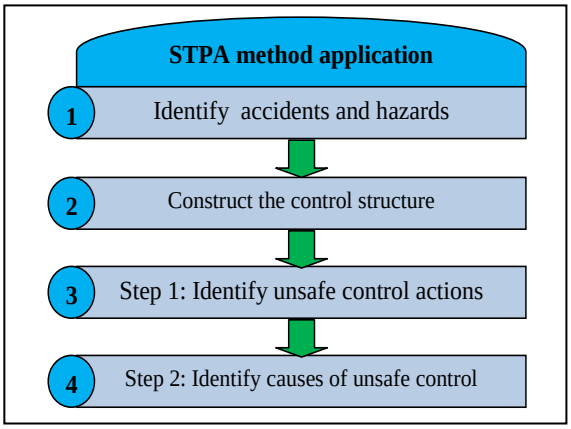

Fig. 2. Organizational chart of the STPA analysis.

In order to apply the STPA analysis on our system, the system accidents likely to occur and its hazards must be identified [17-18]:

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

2- The hazards of the system:
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.

After the hazard identification, a control structure must be selected. Consider the high-level (simple) control structure:

1. For one robot: Figure 3 shows the high-level control architecture for one robot with two differential wheels.

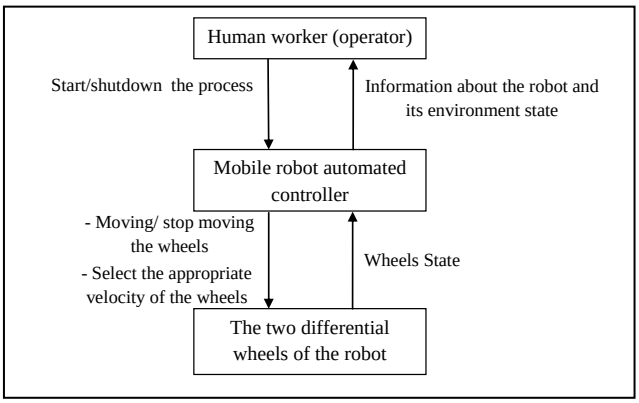

Fig. 3. The high-level control architecture for one robot with two differential wheels.

2. For several robots: There are several architectures to coordinate the control of this multi-robot system. We propose three architectures analysed in this paper [5;7]:

   - *The Centralized architecture:* Figure 4 shows the centralized control architecture.

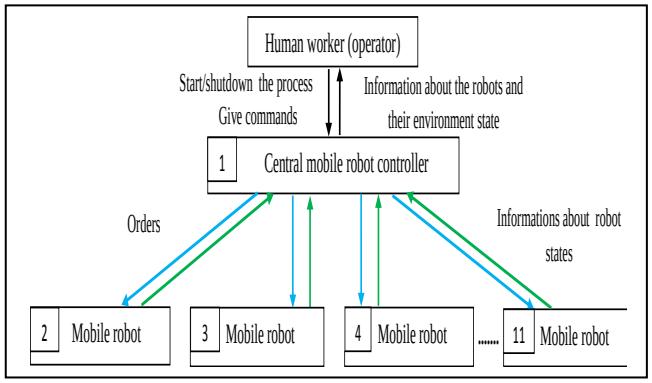

Fig. 4. The Centralized architecture of our system (the blue color refers to orders and the green color refers to feedback).

   - *The hierarchical architecture:* Figure 5 shows the hierarchical control architecture.

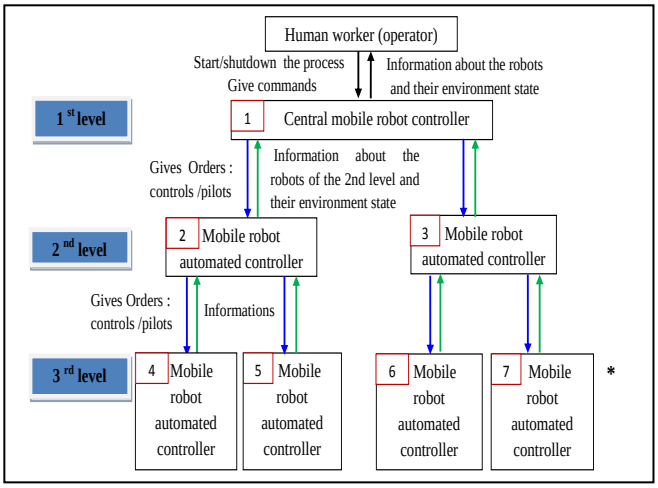

Fig. 5. The hierarchical architecture of our system (the blue color refers to orders and the green color refers to feedback).

* It depends on the location of the robots from 8 to 11.

   - *The Modified hierarchical architecture:* Figure 6 shows the modified hierarchical control architecture.

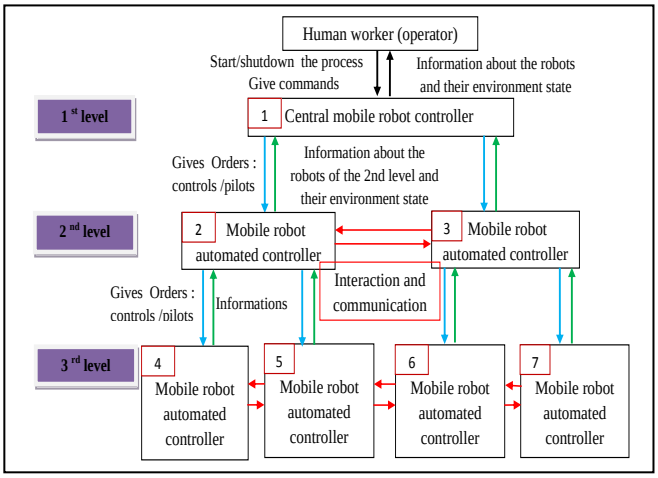

Fig. 6. The modified hierarchical architecture of our system (the blue color refers to orders, the red color refers to communication between robots and the green color refers to feedback).

V. RESULTS

The STPA hazard analysis allow us to detect all hazardous scenarios that can cause if there is any problem in a control action (provided, not provided, provided in an incorrect timing, stopped too soon or applied too long).

To evaluate the hazard scenarios, we have classified each hazard in a severity order (classification relating to the robots situation and their environment). From the results of the STPA analysis shown in table 3, we note that not all scenarios lead to a hazard. The centralized architecture represents seven hazard scenarios; four of them are classified as a high-level of severity. The hierarchical

architecture represents six hazard scenarios; three of them are classified as a high-level of severity. The modified hierarchical architecture represents six hazard scenarios; one of them are classified as a high-level of severity. It means that our initial classification is true. According to this table, we conclude that the centralized architecture is the most dangerous architecture with four serious hazards from seven hazard scenarios.

TABLE III. HAZARD ANALYSIS TABLE FOR THE STPA APPROACH

Architecture	Control actions	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 to avoid a dynamic or static obstacle (other robots loaded by chemicals or not, workers, analysis machine...)	H1	Yes
	The master controller issues a false order	H2	Yes
	The master controller provides an order after a delay time (especially when the master controller controls a large number of robots)	H3	Yes
	The master controller gives a command to the false robot	H4	Yes
	Command stopped too soon or applied too long	H5	Yes
	The master controller does not choose the appropriate velocity for the robots	H6	Yes
	The master controller changes the velocity value in an incorrect time	H7	Yes
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 by chemicals or not, workers, analysis machine...)	H8	Yes
	The master controller gives a false order	H9	Yes
	The master controller provides an order after a delay time	H10	Yes
	Command stopped too soon or applied too long	H11	Yes
	The master controller does not choose the appropriate velocity for the robots	H12	Yes
	The master controller changes the velocity value in an incorrect time	H13	Yes
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...)	H14	Yes
	The master controller gives a false order	H15	Yes
	The master controller provides an order after a delay time	H16	Yes
	Command stopped too soon or applied too long	H17	Yes
	The master controller does not choose the appropriate velocity for the robots	H18	Yes
	The master controller changes the velocity value in an incorrect time	H19	Yes

This last table 4 shows the possible causes that can lead to the hazard scenarios obtained.

TABLE IV. CAUSAL FACTORS OF HAZARD TABLE

Hazard N°	Possible causal factors
H1, H2, H5, H6, H8, H9, H11, H12, H14, H15, H17, H18	- 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.
H3, H6, H7, H10, H12, H13, H16, H18, H19	- 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.
H4	- The master robot sent the command to a bad robot address. - Error filling initial data by operator.
H14, H15, H16, H17, H18, H19	- Missing /wrong communication between slave robots in the same level.

RECOMMANDATION:

After the application of the STPA method, 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.

VI. CONCLUSION

In this paper, we have presented the hazard analysis STPA method and we have highlighted many differences between this approach and the others 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. We have also analyzed those control architectures using STPA hazard analysis.

According to the result of the analysis technique STPA, we have concluded that our initial classification is correct and that the most dangerous control architecture (to avoid) is the centralized architecture.

The modified hierarchical architecture is the one that leads to a medium risk.

REFERENCES

[1] William Young and Nancy G. Leveson, “An Integrated Approach to Safety and Security based on Systems Theory”, ACM, vol. 57, no. 2. pp.31-35, february 2014.

[2] Nancy G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, Cambridge, MA: The MIT Press, 2012.

[3] Homa Alemzadeh et al., “Systems-theoretic Safety Assessment of Robotic Telesurgical Systems”, the International Conference on Computer Safety, Reliability, and Security (SAFECOMP), 2015.

[4] Takuto 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).

[5] Youcef Zennir, « Apprentissage par renforcement et systèmes distribués : application à l'apprentissage de la marche d'un robot hexapode », Phd thesis, INSA de Lyon, 2004, 186 p.

[6] Takuto Ishimatsu, Nancy G. Leveson, John P. Thomas, Cody H. Fleming, Masafumi Katahira, Yuko Miyamoto, Ryo Ujiie, Haruka Nakao, and Nobuyuki Hoshino, “Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis”, Journal of Spacecraft and Rockets 51, no. 2 (March 2014): 509–522.

[7] Reaidy J. Etude et mise en œuvre d’une Architecture d’Agents en Réseau dans les Systèmes Dynamiques Situés : Pilotage des Systèmes de Production Complexes. Thèse génie industrielle. Nîmes : LGI2P-site-EERIE_EMA, 2003, 181 p.

[8] Li-Jeng, Huang, " A Quantitative Method for Dynamic Risk Prediction Using AHP and Grey Modeling: Case Study of a Mud-Flow Hazard". International Journal of Safety Science Vol. 01, No. 03, (2017), pp.61-73.

[9] Asim Abdulkhaleq, Markus Baumeister, Hagen Böhmert, Stefan Wagner, " Missing no Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems", International Journal of Safety Science Vol. 02, No. 01, (2018), pp.115 - 124.

[10] Martin Rejzek1, Svana Helen Björnsdóttir, Sven Stefan Krauss, " Modelling Multiple Levels of Abstraction in Hierarchical Control Structures", International Journal of Safety Science, Vol.02, No.01, (2018), pp.94-103.

[11] Leveson, N.G., Engineering a safer world: Systems thinking applied to safety. 2012, Cambridge MA, USA: MIT Press.

[12] 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. 31(4): pp.267-278.

[13] Pawlicki, T., et al., Application of systems and control theory- based hazard analysis to radiation oncology. Medical physics, 2016. 43(3): pp.1514-1530.

[14] Rejzek, M., Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System, in STAMP Workshop 2012. 2012: MIT, Boston.

[15] Rejzek, M., Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System ... a Review, in 1st European STAMP Workshop. 2012: Braunschweig.

[16] Antoine, B., Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry. 2013, Massachusetts Institute of Technology.

[17] Rejzek, M., Use of STPA in digital instrumentation and control systems of nuclear power plants, in 2nd European STAMP Workshop. 2014: Stuttgart.

[18] Rejzek, M., C. Hilbes, and S.S. Krauss, Safety Driven Design with UML and STPA, in STAMP Workshop 2015. 2015: MIT, Boston.