

Risk Identification of Robotic Systems through the Application of System-Theoretic Process Analysis

BENSACI Chaima ^{(1)*}, ZENNIR Youcef ⁽²⁾, Marry Ann Lundteigen ⁽³⁾

^{(1), (2)} Institute of Applied Sciences and Techniques, 20 Août 1955 University, Skikda, Algeria

⁽³⁾ Norwegian University of Science and Technology, Trondheim, Norway

*ch.bensaci@univ-skikda.dz

Abstract: Autonomous multi-mobile robots are becoming increasingly prevalent in various applications, ranging from industrial automation to healthcare and logistics. While these robots offer enhanced efficiency and productivity, their operation introduces many safety challenges. In this paper, the application of System-Theoretic Process Analysis (STPA) is proposed as a systematic approach to identify and mitigate risks associated with the main features of autonomous multi-mobile robots. This approach is illustrated using a case study concerning a transportation task of hazardous products within a robotic analysis laboratory. Through a structured analysis process, STPA enables the identification of unsafe control actions, the establishment of safety constraints also the generation of safety requirements. The ultimate goal is to improve the autonomous attribute of mobile robots, so on ensuring their operational safety in high-risk environments.

Keywords: Risk identification, STPA, Autonomous Robotic systems, Unsafe control actions, Safety requirements.

1. INTRODUCTION

Due to the continuous development of industrialization and the challenges faced by workers in handling specific demanding tasks, there is a growing trend in industrial facilities, especially within the context of Industry 4.0, to adopt highly automated and complex systems, such as multi-mobile systems. This complexity serves as an efficiency factor, given these systems' ability to perform complex functions that optimize time, cost, and energy requirements. However, this complexity also introduces risks. Therefore, effective risk management and prioritizing safety become indispensable in these environments. Several researchers have considered safety as a significant challenge in collaborative and autonomous systems [1–6]. In this paper, we present a framework for identifying risks through the application of System Theoretic Process Analysis. This methodology is demonstrated through a case study focused on the transportation of hazardous materials within a robotic analysis laboratory designed for chemical analysis. This laboratory is equipped with analysis machines, multi-robots, and various hazardous chemicals, all in an environment where humans are present. The objectives of this paper are to emphasize the diverse risks associated with the key features of autonomous multi-mobile robots, establish essential safety

constraints, and address unsafe control actions by formulating safety requirements. The purposes of this paper are to highlight the set of unsafe control actions associated with the main features of autonomous multi-mobile robots; to establish the needed safety constraints also to generate safety requirements in order to improve the autonomous attribute of mobile robots.

2. DESCRIPTION OF STAMP/STPAMETHODOLOGY

The STPA method is a hazard analysis and identification approach based on an accident causality model denominated as STAMP. In advance of presenting the STPA analysis, it is imperative to describe the STAMP model as follows.

A. STAMP model

Systems theory has introduced an accident causality model known as STAMP (an acronym for "System-Theoretic Accident Model and Processes"), which is considered a philosophical and intellectual basis of systems engineering [7–8]. The STAMP model enhances the traditional causality model by extending its scope beyond a linear chain of directly connected failure events or component failures. It incorporates more complex processes and recognizes hazardous interactions among system components. The STAMP model relies on

three fundamental concepts: the hierarchical control architecture, process model, and safety constraints. In this model, systems are seen as interconnected components in a bidirectional relationship, working together to maintain a state of dynamic equilibrium. Safety in STAMP is viewed as a dynamic control issue rather than a failure prevention problem. In other words, The International Conference on Petrochemistry and Energy Transition (ICPET23.), November 21-23 2023 the focus has shifted from preventing failures to imposing constraints on the system's behavior [9].

B. STPA method

The STPA method (acronym for "System-Theoretic Process Analysis") is one of the systematic approaches to hazard identification that depends on the STAMP causality model. Its objective is to develop a new analysis strategy that overcomes the limitations of traditional hazard analysis by identifying a broader set of hazard scenarios and causal factors [10]. Recently, STPA analysis has been widely used due to its ability to analyze many types of automated systems. These include driving systems [10], air transportation systems [11], including robotic systems [12]. It is also used in autonomous systems such as autonomous vehicles [13] and autonomous ships [14–15]. The STPA analysis is conducted through four main steps. The methodology for this analysis is depicted in Fig 1.

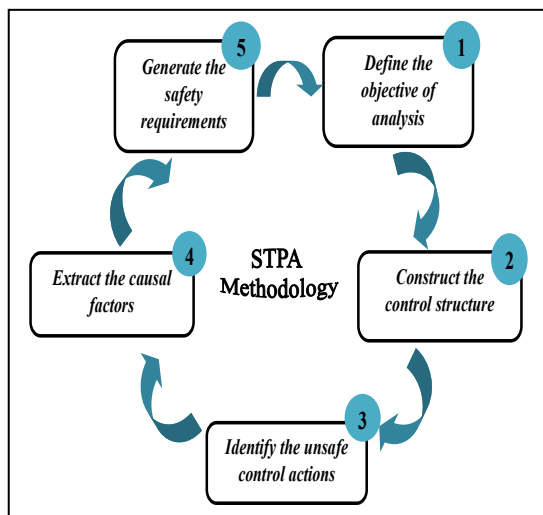


Fig. 1 STPA methodology.

The first step in any analysis method involves defining its objective, primarily by identifying the types of losses, accidents, and high-level hazards in the system under study. The aim in

this step is to define the system to be analyzed and its boundaries.

The second step involves constructing a model of the system, called the hierarchical control structure. This control structure represents functional relationships and interactions between controllers and their controlled processes by modeling the system as a collection of feedback control loops. The control structure usually starts at a very abstract level and is refined iteratively to capture more details about the system.

The third step is analyzing the control actions extracted from the control structure to assess how they might result in the losses defined in the first step. Control actions are analyzed using predefined guide words by checking [9]:

- If a control action is "provided", it may cause hazard.
- If a control action or measure necessary to prevent a hazard is "not provided".
- If a control action "is sent with imprecise timing", too early or too late, it can cause danger.
- If apply a control action for a long time or lose it too soon then it can produce a danger.

These unsafe control actions are used to create system requirements and constraints. The fourth step extracts the causal factors for which unsafe control could occur at the system level. Scenarios are created to explain:

1. How incorrect feedback, inadequate requirements, design errors, component failures, and other factors can lead to unsafe control actions, and ultimately lead to losses.
2. How safe control actions may be provided but not followed or executed correctly, resulting in a loss.

3. Application of STPA to the studied system

This section consists of developing a risk identification of a robotic analysis laboratory using the STPA method.

In particular, this case study aims to investigate risk scenarios produced during the operational phase of robotic systems.

Initially, before beginning any risk analysis process, it is recommended to provide a description of the system under study and its operational context.

A. Case study: Robotic analysis laboratory

The overall studied system is a complex industrial system. This complexity may be associated with its functionalities and tasks to be performed, as well as with its dimensions.

It is mainly composed of mobile wheeled robots collaborating to transport hazardous products, including toxic, flammable, and explosive substances. This process occurs within an analytical laboratory and involves the presence of both analytical machines and human workers. The laboratory has several rooms, including a large analysis room, chemical storage rooms, a battery charging room, and a room for presenting analysis results. These robots navigating together between the various rooms in a permanent way, as illustrated in Fig 2. A laboratory model has been developed using the V-Rep simulator.

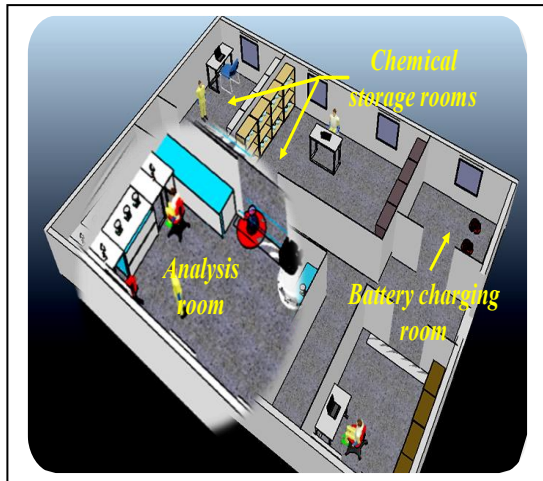


Fig. 2 Robotic analysis laboratory [16].

B. STPA Application

In this section, System Theoretic Process Analysis has been performed to identify the set of unsafe control actions, along with their causal factors, within the main features of autonomous multi-controller systems. These features include collision avoidance, motion control and coordination.

Step 1: define the system boundaries

In this step we have to identify the different losses, accidents, hazards and safety constraints.

• **Losses:**

- L1-Health Impacts: Health issues and injuries to laboratory personnel or nearby individuals resulting from exposure to hazardous products.
- L2-material Damage: Damage to physical assets in the laboratory, including analysis machines, mobile robots and chemical products, due to accidents or the transportation hazardous products.
- L3-Environmental Contamination:

Contamination of the laboratory environment, nearby areas due to chemical spills or accidents.

- L4-Operational Disruption: Disruption of laboratory operations, resulting in delays and financial losses.

- L5-Reputational damage: Damage to the Laboratory’s reputation and the trust in robot operations, affecting collaborations and funding opportunities.

• **Accidents and hazards:**

In environments where hazardous materials and robotic operations are present, collisions rank among the most common accidents. These collisions may occur between robots, between robots and other objects (e.g., walls and machinery) or between robots and human workers. They can lead to subsequent accidents, including human injuries, chemical spills, toxic exposure, fires, explosions, and environmental contamination.

With regard to the hazards and safety constraints, they are identified in table 1.

Table 1 System-level hazards and safety constraints

System-level hazards	Safety constraints
H1- Unsafe human-robot interactions (L1, L3, L4, L5).	Sc1- Providing proper training to human operators and workers who interact with or supervise the robots.
H2- The robots violate the safe distance between them (L2, L3, L4, L5).	Sc2- Robots must respect safety policies and must not exceed the minimum separation distance.
H3- The robot does not maintain a safe distance from other static objects (L2, L3, L4, L5).	Sc3- Providing robots with emergency stop mechanisms, either in the form of buttons or procedures, to quickly stop operations in the event of a safety issue.
H4- The robot deviates from its intended behaviour (L1, L2, L3, L4, L5).	Sc4- Enforcing speed limits to ensure that robots move at a safe and controlled state.

Step 2: Constructing the hierarchical control structure (HCS)

The hierarchical control structure of the system has presented in Fig 3. The figure provides a clear depiction of the different interactions among the various components of the system (Controllers and Controlled process). Control actions from the

robot's controllers, feedbacks affect the system operation has been and environmental disturbances that may illustrate.

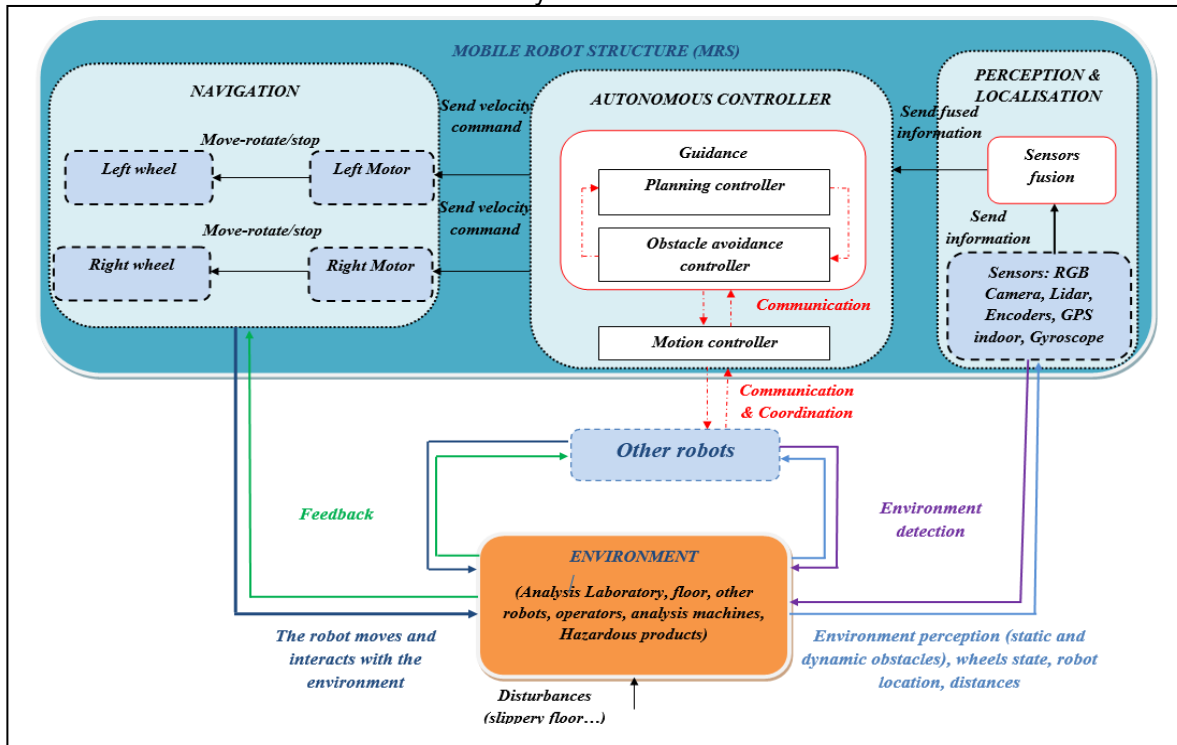


Fig.3 The hierarchical control structure of the system.

Table 2 Unsafe control actions and causal factors identification

CONTROL ACTION	GUIDE-WORD	UNSAFE CONTROL ACTION	SYSTEM LEVEL-HAZARD	CAUSAL FACTORS
AVOID OBSTACLE	PROVIDED	<i>The action provided to avoid obstacles is inaccurate. (Turn right or Turn left, Stop)</i>	H1,H2,H3	- Failure of detecting sensors - Inadequate calibration - Failure of controller
	NOT PROVIDED	<i>The controller don't provide any action to avoid obstacle during the robot motion</i>	H1,H2,H3	- Failure of detecting sensors - controller failure - Inadequate control algorithm
	PROVIDED TOO EARLY OR TOO LATE	<i>The obstacle-avoidance action is delayed in its execution</i>	H1,H2,H3	- Delayed data from sensors - Actuator blockage
	STOPPED TOO SOON, APPLIED TOO LONG	<i>The obstacle-avoidance action stopped prematurely during robot's task</i>	H1,H2,H3	- Ineffective collision avoidance algorithm (lacking robustness) - Controller failure, failure of detecting sensors - Inadequate calibration of sensors.
CONTROL THE MOTION	PROVIDED	<i>The controller provides imprecise motion control</i>	H4	- Inadequate control algorithm - Failure of sensors, actuators - Inadequate calibration of sensors. - Receiving sensor data with a delay - Inadequate data fusion.
	NOT PROVIDED	<i>The controller does not provide the correct control action</i>	H4	- Inadequate control algorithm. - Failure of a motion controller. - Failure of position sensors. - Insufficient sensor fusion - Inadequate calibration of sensors. - Actuator failure (wheel locking).
	STOPPED TOO SOON, APPLIED TOO LONG	<i>The motion control is interrupted</i>	H4	- Interruption in sensor information - Lack of power (due to battery failure or discharge) - Failure of controllers, sensors or actuators
	PROVIDED	<i>Inadequate coordination exists among robot controllers</i>	H2	- Inadequate communication - Weak wireless connectivity
	NOT PROVIDED	<i>Coordination is not provided among</i>	H2	- No connection between robots.

COORDINATE BETWEEN CONTROLLERS		<i>robots</i>		- <i>Failure of communication components.</i>
	PROVIDED TOO EARLY OR TOO LATE	<i>Delayed coordination among robots</i>	H2	- <i>Low network throughput.</i> - <i>High data volume.</i> - <i>Power outage.</i>
	STOPPED TOO SOON, APPLIED TOO LONG	<i>Interrupted coordination among robots</i>	H2	- <i>Lock of communication software</i> - <i>Communication system failure</i> - <i>The amount of information received exceeds the processor's capacity</i> - <i>Reduced network throughput</i> - <i>Network Interruption</i>

Step 3: Identification of unsafe control actions

The set of unsafe control actions and their causal factors has been identified in table 2. In this identification process, three main features are considered: collision avoidance, motion control and coordination.

Step 4: Safety requirements generation

In order to improve the autonomous features of robot's controllers, the suggested safety requirements are presented in table 3.

Table 3 Proposing safety requirements

Control action	Safety requirements
<i>Avoid obstacle</i>	<ul style="list-style-type: none"> - The robot is required to maintain a minimum safe distance between the robot and other obstacle to prevent any physical contact. - Implement safety interlocks on robotic equipment to stop or slow down operations when unsafe conditions are detected. -The robot is required to maintain specific safety distances from both static and dynamic obstacles in order to avoid any form of collision. - Install both a contact sensor and an emergency shutdown system that activates in the event of any contact with the robot.
<i>Control the motion</i>	<ul style="list-style-type: none"> - Use of sensor redundancy (multi-sensor system) in order to reduce the failure risk. - Choose the best filter to increase motion accuracy. - Implement fault tolerant approach.
<i>Coordinate between controllers</i>	<ul style="list-style-type: none"> -Use of multi-layered software, such as ROS. -Use of powerful programming tools. -Employ robust communication protocols. -Add a centralized planning unit that can distribute tasks and coordinate activities among the robot controllers. -Implement a hierarchical control architecture where there is a higher-level controller overseeing and coordinating the actions of individual robot controllers.

4. Results and discussion

The application of STPA is conducted for three main features in autonomous controllers: collision avoidance, Motion control and coordination. The aim was to improve the control/command aspect in autonomous multi mobile robots during their transportation tasks. The outcome of this study highlights a set of safety requirements that designers address to improve the control structure of autonomous robots.

5. Conclusion

In conclusion, the application of STPA (Systems-Theoretic Process Analysis) to the context of multi-robot transportation of hazardous products within an analysis laboratory setting proves to be a valuable approach. Through the case study presented, we have illustrated the control complexities involved in ensuring the safe and effective operation of autonomous multi-mobile robots in an environment containing risky chemicals and human presence. We have also proposed a set of safety requirements to resolve certain control and communication problems. One of the limitations of this approach is that STPA is still purely qualitative method. Therefore, it is necessary to find the best combination with another technique for an accurate assessment. In our future work, we intend to incorporate a thorough quantitative evaluation and then proceed to define the proposed safety requirements in more detail.

References

- [1] J. Guiochet, M. Machin, and H. Waeselynck, "Safety-critical advanced robots: A survey," *Robotics and Autonomous Systems*, vol. 94, pp. 43–52, Aug. 2017. <https://doi.org/10.1016/j.robot.2017.04.004>
- [2] Alexander, R. et al. (2009) 'Deriving safety requirements for autonomous systems', in 4th SEAS DTC Technical Conference.
- [3] R. Woodman, A.F.T. Winfield, C. Harper, and M. Fraser, "Building safer robots: Safety driven control," *International Journal of*

- Robotics Research, vol. 31, no. 13, pp. 1603–1626, 2012.
<https://doi.org/10.1177/0278364912459665>
- [4] Dogramadzi, S. et al. (2014) 'Environmental Hazard Analysis – aVariant of Preliminary Hazard Analysis for Autonomous Mobile Robots', *Journal of Intelligent and Robotic Systems: Theory and Applications*, 76(1), pp. 73–117.
- [5] Guiochet, J. (2016) 'Hazard analysis of human–robot interactions with HAZOP–UML', *Safety science*. Elsevier, 84, pp. 225–237.
- [6] Bensaci, C. et al. (2020) 'STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison' *Alexandria Engineering Journal*. Elsevier, 59(5), pp. 3799–3816., <https://doi.org/10.1007/s10846-013-0020-7>.
- [7] T. Ishimatsu et al., "Hazard analysis of complex spacecraft using systems-theoretic process analysis," *Journal of Spacecraft and Rockets*, vol. 51, no. 2, pp. 509–522, 2014. <https://doi.org/10.2514/1.A32449>
- [8] M. Rejzek, S. H. Björnsdóttir, and S. S. Krauss, "Modelling multiple levels of abstraction in hierarchical control structures," *International Journal of Safety Science*, vol. 2, no. 01, pp.94–103, 2018.
- [9] N.G. Leveson and J.P. Thomas, *STPA handbook*, Onlinedocument, vol. 3, 188 pages, March 2018.
- [10] A. Abdulkhaleq, M. Baumeister, H. Böhmert, and S. Wagner, "Missing no Interaction—Using STPA for Identifying Hazardous Interactions of Automated Driving Systems," *International Journal of Safety Science*, vol. 02, no. 01, pp.115–124, March 2018.
- [11] C. H. Fleming, M. Spencer, J. Thomas, N. Leveson, and C. Wilkinson, "Safety assurance in NextGen and complex transportation systems," *Safety science*, vol. 55, pp. 173–187, 2013. <https://doi.org/10.1016/j.ssci.2012.12.005>
- [12] H. Alemzadeh et al., "Systems-theoretic safety assessment of robotic telesurgical systems," *International conference on computer safety, reliability, and security*, pp.213–227, 2014. https://doi.org/10.1007/978-3-319-24255-2_16
- [13] K. Wróbel, J. Montewka, and P. Kujala, "Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels," *Reliability Engineering and System Safety*, vol. 178, pp. 209–224, 2018. <https://doi.org/10.1016/j.ress.2018.05.019>
- [14] O.A.V. Banda and S. Kannos, "Hazard Analysis Process for Autonomous Vessels," *Novia University of Applied Sciences*, 69 pages, 2017.
- [15] B. Rokseth, O. I. Haugen, and I.B. Utne, "Safety Verification for Autonomous Ships," *MATEC Web of Conferences*, vol.273, No. 02002, p. 15, 2019. <https://doi.org/10.1051/mateconf/201927302002>
- [16] C. BENSACI, Y. ZENNIR, D. POMORSKI et al. Collisionhazard modeling and analysis in a multi-mobile robots system transportation task with STPA and SPN. *Reliability Engineering & System Safety*, 2023, vol. 234, p. 109138.

