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

Article *in* Algerian Journal of Signals and Systems · June 2024

DOI: 10.51485/ajss.v9i2.217

3 authors:

Chaima Bensaci
Université 20 août 1955-Skikda
15 PUBLICATIONS **90** CITATIONS
SEE PROFILE

Zennir Youcef
Université 20 août 1955-Skikda
121 PUBLICATIONS **450** CITATIONS
SEE PROFILE

Mary Ann Lundteigen
Norwegian University of Science and Technology
119 PUBLICATIONS **1,275** CITATIONS
SEE PROFILE

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

threefundamental concepts: the hierarchical controlarchitecture, process model, and safety constraints. Inthis model, systems are seen as interconnectedcomponents in a bidirectional relationship, workingtogether to maintain a state of dynamic equilibrium.
Safety in STAMP is viewed as a dynamic control issuerather 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 toimposing constraints on the system's behavior [9].

B. STPA method

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

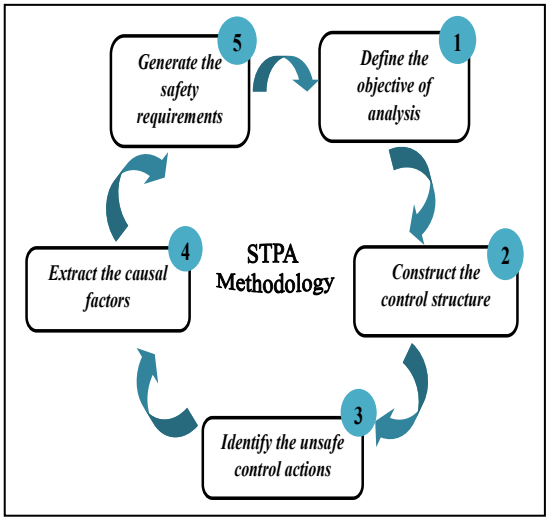

Fig. 1 STPA methodology.

The first step in any analysis method involves definingits objective, primarily by identifying the types of losses,accidents, and high-level hazards in the system understudy. 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. Thiscontrol structure represents functional relationships andinteractions between controllers and their controlled processes by modeling the system as a collection offeedback control loops. The control structure usuallystarts at a very abstract level and is refined iteratively tocapture more details about the system.
The third step is analyzing the control actions extracted from the control structure to assess how theymight result in the losses defined in the first step. Control actions are analyzed using predefined guide words bychecking [9]:
- If a control action is "provided", it may cause hazard.
- If a control action or measure necessary to prevent ahazard 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 ittoo soonthen it can produce a danger.
These unsafe control actions are used to create systemrequirements and constraints.
The fourth step extracts the causal factors for whichunsafe control could occur at the system level. Scenariosare created to explain:
1. How incorrect feedback, inadequate requirements,design errors, component failures, and other factors canlead to unsafe control actions, and ultimately lead tolosses.
2. How safe control actions may be provided but notfollowed or executed correctly, resulting in a loss.

3. Application of STPA to the studied system

This section consists of developing a risk identificationof a robotic analysis laboratory using the STPA method.
In particular, this case study aims to investigate riskscenarios produced during the operational phase ofrobotic systems.
Initially, before beginning any risk analysis process, it isrecommended to provide a description of the systemunder study and its operational context.

A. Case study: Robotic analysis laboratory

The overall studied system is a complex industrialsystem. This complexity may be associated with itsfunctionalities and tasks to be performed, as well as withits dimensions.

It is mainly composed of mobile wheeledrobots collaborating to transport hazardous products,including toxic, flammable, and explosive substances.
This process occurs within an analytical laboratory andinvolves the presence of both analytical machines andhuman workers. The laboratory has several rooms,including a large analysis room, chemical storage rooms, a battery charging room, and a room for presentinganalysis results. These robots navigating togetherbetween the various rooms in a permanent way, asillustrated in Fig 2. A laboratory model has beendeveloped using the V-Rep simulator.

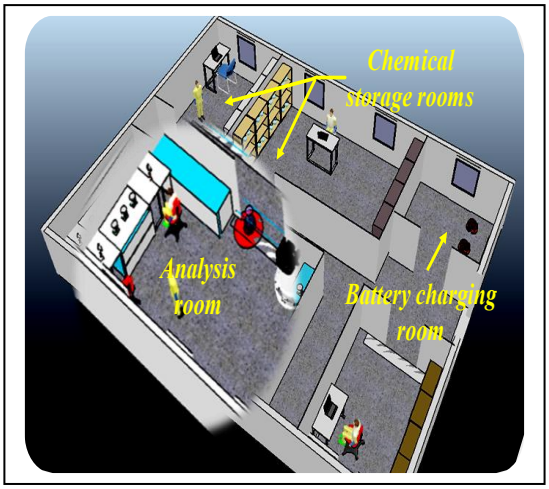

Fig. 2Robotic analysis laboratory [16].

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 safetyconstraints

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 controlStructure (HCS)

The hierarchical control structure of the system haspresented in Fig 3.The figure provides a clear depiction of the differentinteractions among the various components of the system(Controllers and Controlled process). Control actionsfrom the

robot's controllers, feedbacks andenvironmental disturbances that may affect the systemoperation has been illustrated.

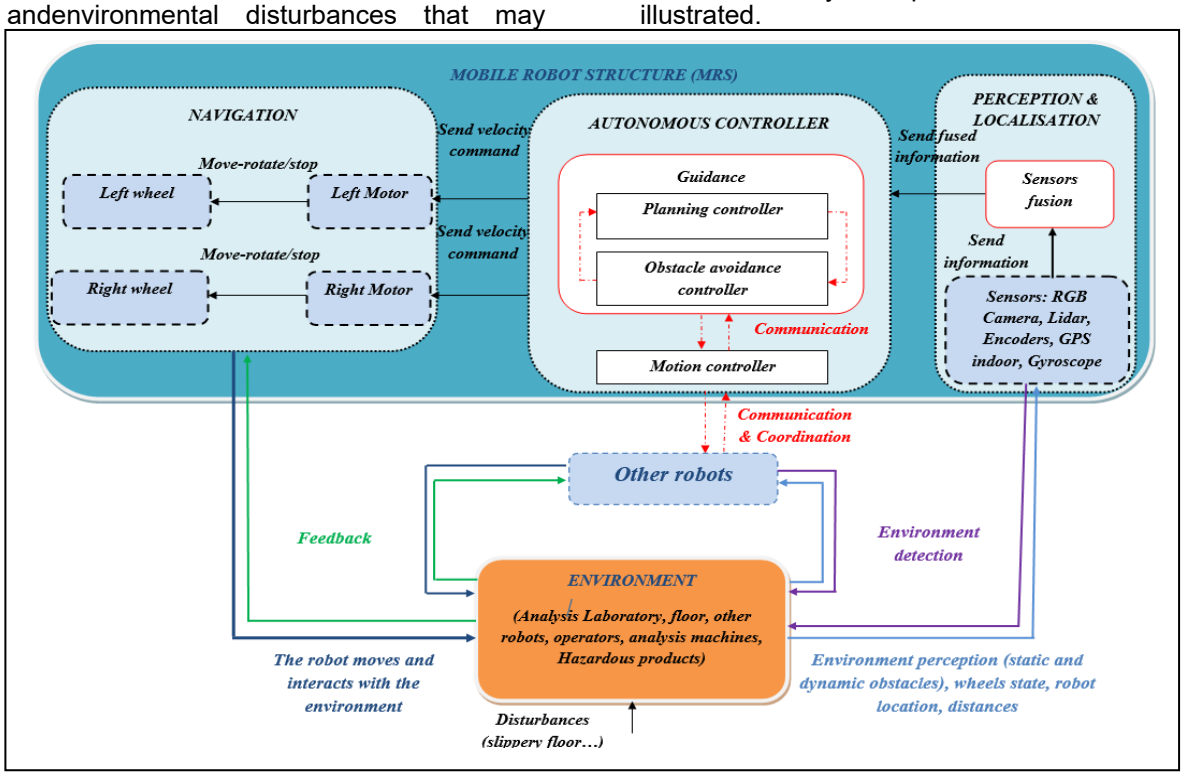

Fig.3 The hierarchical control structure of the system.

Table 2Unsafe control actions and causal factors identification

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

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

Step 3: Identification of unsafe control actions

The set of unsafe control actions and their causalfactors has been identified in table 2. In this identificationprocess, three main features are considered: collisionavoidance, 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*
Avoid obstacle	- 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.
Control the motion	- 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.
Coordinate between controllers	-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 ananalysis laboratory setting proves to be a valuable approach. Through the case study presented, we haveillustrated the control complexities involved inensuring the safe and effective operation ofautonomous multi-mobile robots in an environmentcontaining risky chemicals and human presence. Wehave also proposed a set of safety requirements toresolve certain control and communication problems.

One of the limitations of this approach is that STPAis still purely qualitative method. Therefore, it isnecessary to find the best combination with anothertechnique for an accurate assessment.

In our future work, we intend to incorporate athorough quantitative evaluation and then proceed todefine 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 Spacecraftand 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, "Modellingmultiple 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 IdentifyingHazardous 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 complextransportation 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 ofrobotic telesurgical systems," International conference oncomputer 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 thedevelopment of a system-theoretic model for safety assessmentof autonomous merchant vessels," Reliability Engineering andSystem 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 forAutonomous Vessels," Novia University of Applied Sciences,69 pages, 2017.

[15] B. Rokseth, O. I. Haugen, and I.B. Utne, "Safety Verificationfor Autonomous Ships," MATEC Web of Conferences, vol.273, No. 02002, p. 15, 2019. https://doi.org/10.1051/matecconf/201927302002

[16] C. BENSACI, Y. ZENNIR, D. POMORSKI et al. Collisionhazard modeling and analysis in a multi-mobile robots systemtransportation task with STPA and SPN. ReliabilityEngineering & System Safety, 2023, vol. 234, p. 109138.