24th ABCM International Congress of Mechanical Engineering
December 3-8, 2017, Curitiba, PR, Brazil

COBEM-2017-0375
APPLICATION OF A SYSTEMIC HAZARD ANALYSIS TO LAUNCH AND RESCUE OPERATION OF A MICROGRAVITY SUBORBITAL SPACE VEHICLE

Jonas Bianchini Fulindi
Instituto Tecnológico de Aeronáutica – ITA, São José dos Campos – SP, 12228-900
fulindi@ita.br

Rogério Pirk
Instituto de Aeronáutica e Espaço – IAE, São José dos Campos – SP, 12228-904
rogeriorp@iae.cta.br

Luís Eduardo V. Loures da Costa
Instituto Tecnológico de Aeronáutica – ITA, São José dos Campos – SP, 12228-900
loures@ita.br

Abstract. *This paper aims to present the application of a new systems approach on hazard analysis, called system-theoretic process analysis (STPA) for the launch and rescue operation of the SARA (acronym for atmospheric reentry satellite). In contrast with traditional methods used in the advanced stages of projects that focus on the likelihood of failures occurrence, STPA treats safety as a control problem rather than a failure problem. As a result, the application of this hazard analysis guides the safety-driven design of the launch and rescue operation allowing the anticipation of the safety requirements and design constraints in the early stages of the conception of the SARA launch and rescue operation.*

Keywords: *Hazard Analysis, Safety, STPA, Launch Campaign, Systems Engineering*

1. INTRODUCTION

Since 1954, Institute of Aeronautics and Space (IAE) has been devoting efforts in building a solid knowledge in rockets and launchers development. Among the many issues concerning the rocketry field, the hazardous features of these space systems must be considered, mainly due to the high energy released during rocket motors operations. In this framework, one can state that safety is an essential property to be achieved, which is a consequence of the reduction of hazards and the effectiveness improvement of systems operations. Hazard analysis is one of the most important tools to develop safe space systems and traditional component failure based analyses as FMEA (Failure Mode and Effects Analysis), FMECA (Failure Mode, Effects and Criticality Analysis) and FTA (Fault Tree Analysis) are usually applied. However, the drawback imposed for the application of such traditional methods in space systems is the difficulty in identifying the system related hazard causes, since these techniques treat safety as component failure problem. In light of this, it was created a new hazard analysis technique, based on systems theory rather than reliability theory, called STPA (System-Theoretic Process Analysis), based on the STAMP – A New Accident Causality Model (Leveson 2004a, Leveson 2004b, Leveson 2012), in which safety is treated as a control problem, in opposite with the traditional component failure based techniques.

According to Leveson (2012), potential causes of accidents can be eliminated or controlled before occurring damage by (a) identifying the potential for inadequate control of the system that could lead to hazards and (b) determining how each potentially hazardous control action could occur. Such that, important questions as how the causes of accidents and hazardous control actions could be potentially unsafe, must be considered before planning launch operations. The management and planning of launch campaign operations is a challenging task, once many activities, multi-disciplinary teams and organizations are usually involved. The main objectives of the launch and rescue operations must always be kept and the activities plan to successfully accomplish the safety goals represent a significant effort to be implemented and monitored by managers and safety engineers. In addition, it is necessary to achieve requirements as schedule, cost and operability, which impact the campaign as a whole.

In this paper, STPA is applied to the VS40M/SARA launch and rescue operation, where hazard analysis and causal factors are previously identified in order to well define the launch activities during countdown to H0 (time for the VS40M ignition) as well as the SARA tracking and rescue activities. In summary, through the application of STPA for the VS40M/SARA launch and rescue operation, possible hazardous scenarios that can lead to accidents can be assessed in the very early stages of the operations development and, as consequence, potential problems can be anticipated. As a result, impacts due those problems in the advanced stages of the launch mission can be avoided.

2. STAMP/STPA

To think safety in a new and systemic way, it is necessary to understand that large-scale engineered systems are more than a collection of technological artifacts. They are a reflection of the structure, management, procedures and culture of the organization that created them (Leveson, 2008). Then, to understand the cause of an accident can occur it is necessary to examine these factors for engineering safer systems (Leveson, 2004a).

According to Leveson (2012), “the most widely used existing hazard analysis techniques were developed fifty years ago and have serious limitations in their applicability to today´s more complex, software-intensive, sociotechnical systems”. The causes of the accidents are changing and are not based just on the individual components, but in the relationship between components (Leveson, 2004a). This new way of understanding the causes of the accidents, including the human behavior, the new technologies growing faster than the techniques to tackle the problems that arise from the use of those technologies, the interconnected and integrated digital systems, and the decision-making processes are some causal factors that lead to losses.

A new model that can guide a systemic hazard analysis and encompasses these problems is called Systems-Theoretic Accident Model and Processes (STAMP). In STAMP the theories of systems and control are incorporated and the accidents are considered as complex processes that involve the entire sociotechnical system. In this model, systems are viewed as interrelated components in a dynamic state of equilibrium by feedback control loops. Therefore, systems are not treated as static but as dynamic processes that react and change, according to the environment. As a result, this model changes the focus that is usually only in components, but an overview on the understanding of the system behavior as a whole and all the interactions among the entities of the system that can contribute to the losses. Thus, accidents are the result of flawed processes involving interactions among many elements in a system as operators, organizational structures, physical system components and the environment in which the errors occurs (Leveson, 2012).

In systems theory, systems are viewed as hierarchical structures (Checkland, 1981) and each level imposes constraints on the level below it. In STAMP, the constraints or lack of constraints at a higher level control the lower-level behavioral processes. In the hierarchical structure, inadequate control may result from inadequate safety control commands, missing constraints, commands not executed adequately or inadequate feedback to the constraints enforcement in the lower levels (Leveson, 2012). The impacts of the decision at each level in the hierarchy must be evaluated. The feedback between levels is used to communicate how successfully the results of the decision are being performed. Systems theory provides the foundation for the safety development of the whole system, even it is composed of many different components. The objective is to integrate all components into the most safe and effective to achieve the mission objectives, according to all set of conditions that the system is designed to operate.

According to STAMP, instead of preventing component failures it is created a safety control structure that enforces behavioral safety constraints. This safety control structure may be useful to understand how to design the controls at each level of the system hierarchy. As mentioned above, the higher levels in the safety control structure enforce the safety constraints that control the behavior of the lower levels to avoid accidents. This is done through the control actions, that is, the imposition of the safety constraints to control the behavior of the controlled process in the hierarchy of the system. Therefore, in STAMP the control is related to the imposition of the safety constraints.

Safety is an emergent property that arises from the interactions among the system components. The emergent properties are controlled by the enforcement of the constraints on the interactions among the components. Safety becomes a control problem where the goal of the control is to enforce the safety constraints.

Accordingly the control point of view, in STAMP, the accident can be understood by determining how ineffective was the control. Such a way, the focus on preventing components failures is changed to a new way of thinking that considers the design and implementation of effective control actions that enforce safety constraints into the system. Based on the control theory, four conditions are required to control a process (Leveson, 2012).

- The safety constraint: enforced by the controller in the hierarchical safety control structure;
- The action condition: implemented in the downward control channels;
- The observability condition: embodied in the upward feedback channels;
- The process model condition: any controller – human or automated – needs a model of the process being controlled.

Figure 1 illustrates a general feedback control loop.

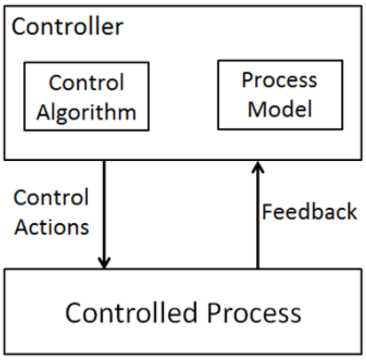

Figure 1. A feedback control loop (adapted from Leveson (2012))

The controller could be human or automated. The process model contains the model of the controlled process (controller´s understanding of the states and behavior of the controlled process). Control actions are the downward arrow that represents the controller actions to control the process. Feedback is the upward arrow that represents the information on the process behavior observed by the controller. Accidents may occur when the process model conflicts with the controlled process feedback, it means, the process changed its state and the controller could not control or perceived the actual process state. Independently whether the control is human or automated, the model of the controlled process must contain the same type of information as the system variables and states that the process can assume (the current and the changed values). This process model is updated by the feedback and is issued to determine what the control actions are needed (see Fig. 1).

According to Leveson (2012) accidents occur if "particularly component interaction accidents and accidents involving complex digital technology or human error, when the process model used by the controller (automated or human) does not match the process". Process model and feedback of the human mental model play an important role in understanding why accidents occur and why humans provide inadequate controls. In the hierarchical control structure, controlled process is required in all levels. Conflicts between process models of the designers and operators can impact the whole system development. Human controllers may update their mental models of the system according it evolves through the time. For the mental models updating it is necessary to provide feedback and include the operator in the system design, it allows the operator to optimize their control over the system to be operated. Hence, the feedback must communicate through each level of the hierarchical safety control structure.

In STPA, accidents in complex systems are caused by inadequate enforcement of constraints on unsafe interactions among elements of the system. It is not only caused by component failure, but considering interactions and impacts on human errors in the design phase, erroneous control actions by humans, automated components or software. It also includes system and software design errors and human decision making through design and operations of the system (Leveson, 2004a).

3. SARA LAUNCH AND RESCUE OPERATION

The SARA project encompasses the development of a spacecraft designated to perform microgravity experiments. The so called SARA Sub-orbital is developed by Institute of Aeronautics and Space (IAE) and will be launched by a two stages sounding vehicle VS-40M (also developed by IAE) from Alcântara Lauch Center (CLA), in the state of Maranhão, Brazil. The first qualification flight designed for the SARA Sub-orbital comprehends a flight mission, in which 150 Kg of scientific experiments will be carried on-board up to an altitude of 300 Km. As a recoverable module, the SARA atmospheric re-entry flight is previewed as well as its rescue (done by search and rescue teams) from the sea in a ray of 100 Km from CLA. The mission architecture to accomplish the SARA Sub-orbital launch and rescue operation is described in Fig. 2.

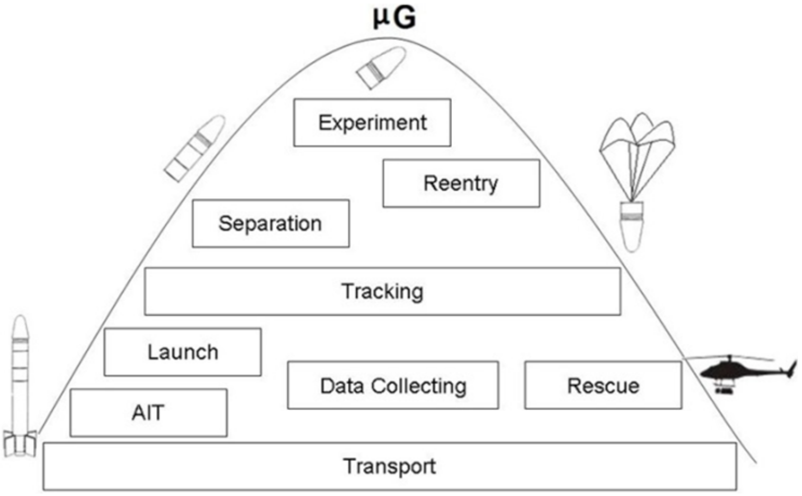

Figure 2. SARA flight mission (AIT is assembly, integration and tests)

As seen in Fig. 2, many tasks must be performed for a successful mission achievement. A launch campaign conception considers from the necessary manpower to fulfill the technical activities and modules transportations up to the safety and security operations, flight trajectory tracking and spacecraft rescue tasks. It is important to highlight that all the activities previewed must take into account possible hazards, since the nature of these tasks is highly hazardous and personal safety is the most important item to be considered. An overview of the most significant tasks conceived to successfully achieve the launch and rescue of the SARA Sub-orbital is described below:

- Sounding vehicle VS-40M and payload SARA are transported to CLA;
- AIT are performed on the vehicle VS-40M;
- AIT are performed on the payload SARA;
- AIT are performed on the VS-40M/SARA at launch pad;
- Sounding vehicle VS-40M and SARA communication tests (control bench, CLA telemetry and ground station tracking);
- Clearing the space area to launch VS-40M/SARA (patrol aircrafts, authorities);
- Sounding the climate conditions (weather balloons);
- Authorization from flight safety and security to lift off;
- Sounding vehicle VS-40M lift off;
- VS-40M 1st stage separation;
- SARA separation;
- VS-40M/SARA tracking (CLA telemetry and ground station tracking);
- SARA performs microgravity experiments;
- SARA reentry;
- SARA open parachutes command;
- Rescue teams in action (boats, helicopters and aircrafts);
- SARA is recovered from the sea and transported to CLA.

4. STPA APPLICATION ON VS40M/SARA LAUNCH AND RESCUE OPERATION

The example provided in this paper is the application of STPA on the launch and rescue operation of the SARA space vehicle. STPA analysis starts defining the high-level possible accidents and the hazards leading to accidents.

A long experience devoted on activities in space field has shown that the most painful and critical high-level accidents that severely affect space projects are:

(A1): People injured or killed by vehicle/payload;
(A2): Mission loss;
(A3): Economic loss.

As consequence, the VS40M/SARA associated high-level hazards that can drive to the previously identified possible accidents are also identified as:

(H1): SARA unable to achieve the specified altitude;
(H2): SARA unable to perform experiments;
(H3): SARA unable to land on the sea;
(H4): SARA unable to be rescued.

In high-level of abstraction, the interaction entities that represent the system and its relationships for a launch and rescue operation are depicted in the Fig. 3 as the high-level control structure.

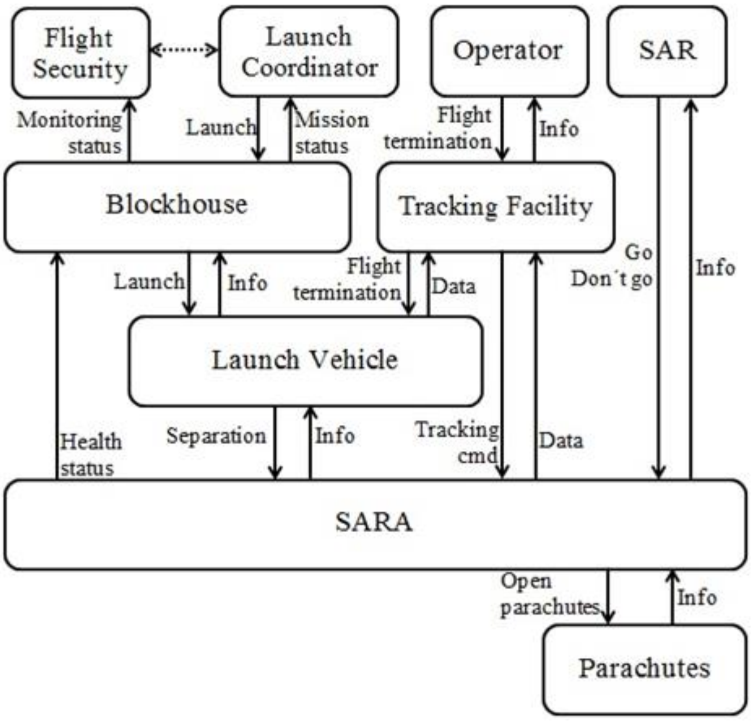

Figure 3. Control structure of the VS-40M/SARA launch and rescue operation (SAR is search and rescue teams and down arrows are control actions, up arrows are feedbacks and bidirectional dotted arrow is communication)

The control structure is a very important tool, used to allow the communication of the team involved in the whole system development, in this case, for the whole launch and rescue operation. Furthermore, the systems engineering team must be aware of the impacts on the system, if a control action is unsafe. From the control structure, a table with the control actions to avoid the hazards and, consequently, accidents can be defined. Table 1 describes the conditions in which a control action can be unsafe. Notice in the referred table that for the control actions identified in the Fig. 3 (down arrows), four categories of unsafe actions are represented in the Table 1 and, as consequence, alternatives for a safer design can be created. Furthermore, for each of those control actions it is possible to understand the relationship among the interaction elements and the constraints that can be enforced to keep a safe control action, as presented by (Leveson, 2012).

An example with five control actions for the VS-40M/SARA launch and rescue operation is provided in Table 1. For those control actions it was possible to identify eighteen unsafe control actions, which are labeled as UCA1 to UCA18. Notice that each UCA is related to the high-level hazards (H1, H2, H3, H4) leading to the high-level accidents (A1, A2, A3).

Table 1. Table of UCA´s for the VS-40M/SARA launch and rescue operation.

Control Actions	**Unsafe Control Actions**			
	Not Providing Causes Hazard	**Providing Causes Hazard**	**Incorrect Time/Order Causes Hazard**	**Stopped too Soon or Applied too long Causes Hazard**
Launch	UCA1 Launch command not provided when the vehicle is ready to lift off and all set in the launch pad (H2)	UCA2 Launch command provided when vehicle is not ready to lift off (H2) UCA3 Launch command is provided when wind conditions are not OK (H1)	UCA4 Launch command provided out of the specified sequence during countdown (H1)	N/A

Separation	UCA5 Separation command not provided when the first stage has already finished all propellant burning (H1, H2, H3)		UCA6 Separation command provided out of the specified sequence (H1, H2, H3)	UCA7 Separation command applied too long, when vehicle losses the tracking visibility (H1, H2, H3)
Flight termination	UCA8 Flight termination command not provided when vehicle is out of the defined trajectory (H1, H2, H3) UCA9 Flight termination command not provided when vehicle is unstable (H1)	UCA10 Flight termination command provided when vehicle is at the launch pad (H2)	UCA11 Flight termination command provided too early when vehicle is just few meters of altitude (H1, H2) UCA12 Flight termination command provided too late when vehicle is out of the range (H1)	N/A
Open parachutes	UCA13 Open parachutes command not provided when SARA reentry (H3)		UCA14 Open parachutes command provided too early or provided too late when SARA is not in the specified altitude (H3)	N/A
Go/Don´t go		UCA15 Go command provided when the SARA position on the ocean is not known (H3) UCA16 Go command provided when the SARA is on the ocean but the rescue helicopter is not fueled enough (H4)	UCA17 Go command provided too early when SARA is in the reentry phase before impacts in the ocean (H3) UCA18 Don´t go command provided too late after the rescue helicopter started the search and rescue phase (H4)	N/A

In order to better understand the unsafe control actions described in Table 1, a brief example showing how a control action can be unsafe is presented. The constraints, unsafe control actions, related hazards and accidents derived from STPA are also described next:

Control action “launch”:

The flight security authorizes the launch of the VS-40M/SARA, after checking all technical procedures previously programmed in the launch countdown. This command can be unsafe if the control action is provided when the wind conditions are not in the limits established for recovering the SARA spacecraft. This unsafe control action appears in the Table 1 as UCA3 and the hazard associated is (H1) that consequently may lead to accident (A2). This unsafe control action (UCA3) can cause the loss of the payload (A2), since the launch with wind velocities above 12 m/s could extrapolate the established rescue zones in the sea and, as a consequence, one of the requirements of the mission would not be achieved.

Control action “flight termination”:

Another example to depict an unsafe control action and a related constraint derived from the analysis of the Table 1 is herein provided for the flight termination. This command, usually issued by the flight control authority, is issued from the ground station when the vehicle is in an anomalous flight or the vehicle is out of the defined trajectory the flight must be terminate. If this command is not provided (UCA8) it leads to hazards (H1), (H2) and (H3) that could lead to the accidents (A1), (A2) and (A3). A constraint to avoid the unsafe control action UCA8 could be a product design constraint. If the only way to terminate the flight is remotely from the ground station, so doing this analysis based on the information provided in Table 1 in the early stages of the development, a trade off study can be done to assess the feasibility to design an automated flight termination system, considering the limit zone plans and trajectories.

In the conceptual phases for the VS-40M/SARA launch and rescue operation, the control structure (Fig 3) and the identification of the unsafe control actions (Table 1) drives the development in high-level of abstraction and leads the manager of the project to focus in the early assessment of the safety issues that could appear in the late stages of the launch operation, when all hardware are physically interconnected and the changes are costly. As consequence, safety requirements are anticipated, which is a different approach in comparison with traditional systems development, when safety is not thought too early in the development phases (Fleming, 2015).

After doing the analysis above, the next step in the STPA is the identification of the causal factors that can lead to the accidents. Through the next example it is possible to create the hazardous scenarios for each unsafe control action identified in the Table 1. As a second step of STPA, potential causes for the unsafe control actions are identified through the causal scenarios. Figure 4 illustrates the basic high level causal factors used to perform the causal scenarios analysis.

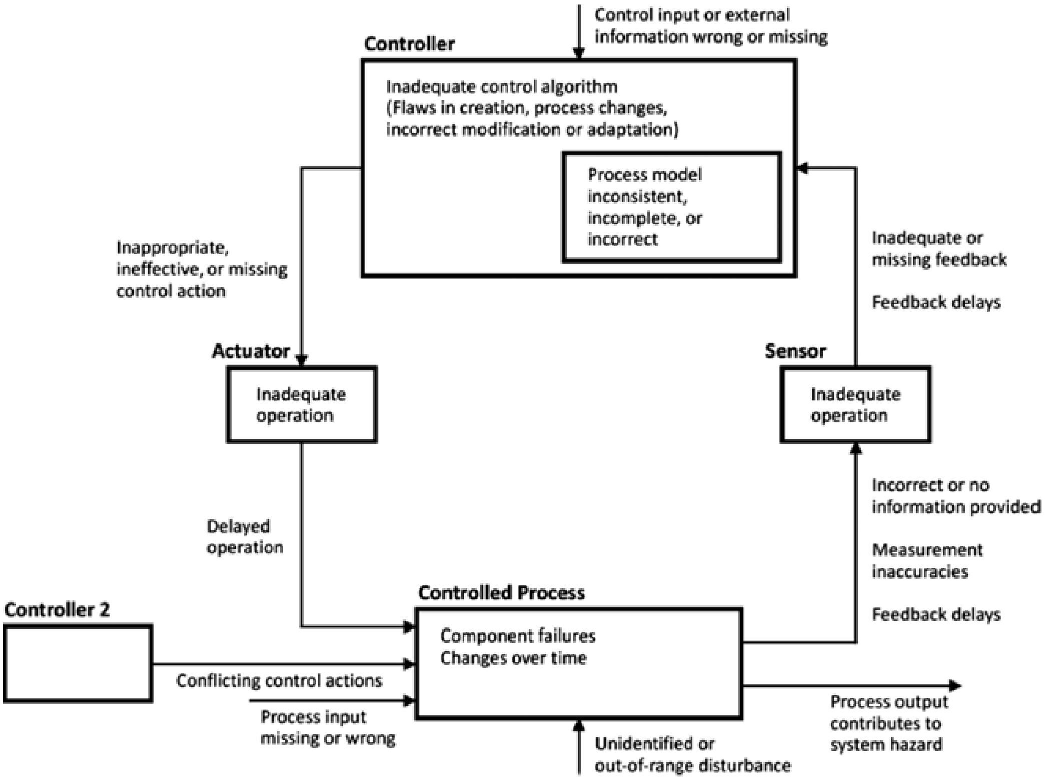
Control input or external information wrong or missing
Controller
Inadequate control algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
Process model inconsistent, incomplete, or incorrect
Inappropriate, ineffective, or missing control action
Inadequate or missing feedback
Feedback delays
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Delayed operation
Controller 2
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 4. Generic causal loop for the identification of the causal factors (Leveson, 2012)

Each of the unsafe control actions from Table 1 can be used to identify causal scenarios that explain how the hazards might occur. For the purposes of this paper, only one unsafe control action (UCA1) will be analyzed in more detail to identify causal scenarios.

The possible scenarios for the UCA1 that can lead to accidents include:

UCA1: Launch command not provided when the vehicle is ready to lift off and all set in the launch pad (H2).

Scenario: Launch coordinator receives indication that the vehicle is ready to lift off and everything is set in the launch pad, but the launch command is not provided. Possible causal factors could be:

a) Launch coordinator receives a high level order from a military authority cancelling or delaying the mission;

b) Launch coordinator believes the reported limited zone area is incorrect, causing a false positive indication that everything is ready

c) Launch coordinator receives indication that the vehicle and launch pad are ready, but also receives conflicting information about vehicle or launch path readiness (such as payload health monitoring)

d) Launch coordinator does not see or does not believe indications that the launch vehicle and pad are ready due to past experiences with failed launches or incorrect indications (assumes that something is going wrong)

e) There is an emergency or intrusion in the prohibited area, causing a launch delay or cancellation despite the vehicle and launch pad being ready

From the analyses for the UCA1 hazardous scenarios, it is possible to capture and derive constraints for the launch operation. For example, a constraint derived from those scenarios concern the aborting of the launch a few minutes/seconds before the lift-off. The launch countdown defines at H0 - 3 minutes the automatic countdown is turned on. In this mode, only the launch coordinator is allowed to abort the flight, considering that all teams are updating him about the tasks. In addition, at this point of the countdown, the electrical suppliers of the vehicle and payload are switched from the umbilical to the batteries mode. If any abort command is issued by the coordinator, the countdown stops and as consequence, the vehicle and payload heating increase due to the radiated heating caused by the telemetry transmitters. A constraint that cannot be violated is concerned to the allowed temperature in the vehicle and payload equipment after an abort command. It is not allowed to re-start the countdown before verifying if the temperatures in the vehicle and payload are appropriate and, besides, if the batteries are fully recharged. An alternative solution for this problem could be the use of a shield to cover the SARA, in order to keep the appropriate inner environmental temperature. Once again, there are different technological solutions to avoid this hazardous scenarios that may lead to accidents (A2 and A3), and the design solutions should be built by considering to those causal factors (inadequate feedback from the sensors and unidentified external interruptions during the countdown).

5. CONCLUSION

This paper presented an application of a new hazard analysis for the launch and rescue operation of a space vehicle conceived to perform technological experiments in microgravity environment.

High-level accidents and the hazards associated to those accidents were identified. Then, a control structure that represents the launch and rescue campaign and its interactions through control actions and feedbacks were designed to provide the elements of the operation (that is, the operation was considered as a system to be engineered).

The control structure aids the whole view of the system and its interactions allow allocating the safety constraints to control, mitigate or avoid the hazards that lead to accidents. This is possible looking at the unsafe control actions (Table 1), where an example is provided with five control actions captured from the control structure (Fig. 3). After the analysis on the unsafe control actions, three examples of causal scenarios that could lead to losses for those unsafe control actions were presented to illustrate how each potentially hazardous control action could occur.

Instead of looking at the systems separately, through STPA it is possible to analyze the interactions between human, hardware and software, which is a new way to think on the systems safety. The team involved in the launch and rescue operations can capture requirements from the analysis and trace them back to the accidents and hazards to accomplish the launch center procedures for safety.

When STPA is performed in the early stages of the launch and rescue operation, planning requirements from the problem domain are anticipated instead of the solution domain, when the engineers are defining the technology to be implemented. Many solutions or alternatives in how the operations should meet the safety standards are cheapest when identified early. Through STPA, safety requirements can be derived to accomplish the launch site regulations and to enhance procedures for the launch and rescue.

6. REFERENCES

Leveson, N., “A new accident model for engineering safer systems,” Saf Sci 42(4):237-270, 2004a.

Leveson, N., “A systems-theoretic approach to safety in software-intensive systems,” IEEE Transactions on Dependable and Secure Computing 1(1): 66-86, 2004b.

Leveson, N., “Engineering a safer world: systems thinking applied to safety,” 2012, Cambridge: MIT Press.

Leveson, N., “Technical and Managerial Factors in the NASA Challenger and Columbia Losses: Looking Forward to the Future,” In: Kleinman DL, Cloud-Hansen KA, Matta C, Handelsman J, editors. Controversies in Science and Technology Volume 2: From Climate to Chromosomes. New York: Mary Ann Liebert Press, 2008, p. 237-261.

Checkland, P., “Systems thinking, systems practice,” New York: John Wiley & Sons, 1981.

Fleming, C., H., “Safety-driven early concept analysis and development,” (PhD thesis). Cambridge: Massachusetts Institute of Technology, 2015.

7. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.