SAFETY GUIDED DESIGN OF CREW RETURN VEHICLE IN CONCEPT DESIGN PHASE USING STAMP/STPA

Haruka Nakao[(1)] , Masa Katahira[(2)], Yuko Miyamoto[(2)], Nancy Leveson[(3)]

,

[(1)]Japan Manned Space Systems Corporation, Urban Bldg., 1-1-26, Kawaguchi, Tsuchiura, Ibaraki 300-0033, Japan
Email: nakao.haruka@jamss.co.jp,
[(2)]Japan Aerospace Exploration Agency, 2-1-1 Sengen, Tsukuba-shi, Ibaraki 305-8505, Japan
Email: miyamoto.yuko@jaxa.jp, katahira.masafumi@jaxa.jp,
[(3)]Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139-4307, USA
Email: leveson@mit.edu

ABSTRACT

In the concept development and design phase of a new space system, such as a Crew Vehicle, designers tend to focus on how to implement new technology. Designers also consider the difficulty of using the new technology and trade off several system design candidates. Then they choose an optimal design from the candidates.

Safety should be a key aspect driving optimal concept design. However, in past concept design activities, safety analysis such as FTA has not used to drive the design because such analysis techniques focus on component failure and component failure cannot be considered in the concept design phase.

The solution to these problems is to apply a new hazard analysis technique, called STAMP/STPA. STAMP/STPA defines safety as a control problem rather than a failure problem and identifies hazardous scenarios and their causes. Defining control flow is the essential in concept design phase. Therefore STAMP/STPA could be a useful tool to assess the safety of system candidates and to be part of the rationale for choosing a design as the baseline of the system.

In this paper, we explain our case study of safety guided concept design using STPA, the new hazard analysis technique, and model-based specification technique on Crew Return Vehicle design and evaluate benefits of using STAMP/STPA in concept development phase.

1. INTRODUCTION

Japan Aerospace Exploration Agency (JAXA) develops various types of space systems such as satellites, rockets, and manned systems including the International Space Station (ISS). Needless to say, safety is one of the essential characteristics to be achieved for these space systems. A hazard analysis is one of the most important elements in developing safe space systems. During system design, component failure based analyses, such as FTA and FMEA, are commonly used as hazard analysis methods. However, it is difficult to identify hazard causes that are not related to component failures using FTA/FMEA, which can lead to inadequate investigation for hazards.

Although JAXA has not experienced any critical accidents caused by factors other than component failures so far, JAXA is considering introducing a new hazard analysis methodology, called STAMP/STPA, to avoid future accidents. STAMP/STPA focuses on control problems, not component failures, and it is able to identify hazards that arise due to unsafe and unintended interactions among the system components without component failures.

JAXA is also considering to use STPA in very early mission or system design to support safety design of a system. To design system safe, it is important to perform system design and safety design in parallel and optimize functional design and safety design from the beginning of development.

In the early study and mission design phase, engineers design many different systems to find out optimal system design. Safety analysis provides safety related risk information of each design candidate which has to be considered in design trade-off. In this phase there are no concrete system configuration items nor system components that mean it is difficult to apply traditional fault based safety analysis like FTA. SPTA is focus on control problems that occur in system and it can analyze control related hazards based on function design of the system without tangible system components. Then the analysis results are organized as safety constraints or

requirements that indicate hazard related items to be eliminated or controlled in further system design.
As a pilot case study, we perform safety analysis using STPA in parallel with mission design and provide feedback between them iteratively as a trial of safety guided design.

2. RESEACH OVERVIEW

2.1. Early Study of Crew return Vehicle

JAXA has started early study of a manned space vehicle to obtain technical capabilities that are able to develop and operate a manned space vehicle. The vehicle is a visiting vehicle launched by the H-IIB rocket to carry crews and necessary components to the ISS and return to the earth. Figure 1 depicts operation overview of the Crew return Vehicle (CV). We are involved in a working group of Control System of the CV, which is one the most important target technology area. The objective of this WG is to design optimal vehicle control system and to establish a design methodology which is suitable for designing safety critical and human-centric complex system. One of the most difficult topics of the WG is to realize human-centric space system that provides seamless control between system and human and establish design method. The CV system needs to have many high autonomous functions considering appropriate autonomy level and control authority. For this purpose we start study of safety guided system design using STPA to enhance safety and optimization of control system design of the CV.

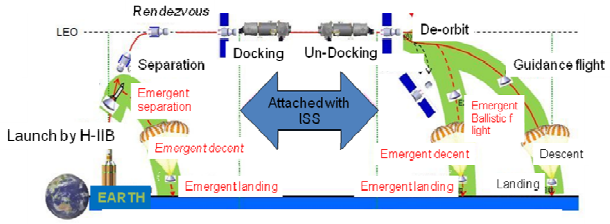

Figure 1. Operation overview of the Crew return Vehicle

2.2. STAMP/STPA

Current hazard analysis techniques start from a completed design and assume that accidents are caused by component failures. Because the primary cause of accidents in the old systems was component failure, the hazard analysis techniques and safety design techniques focused on identifying critical components and either preventing their failure (increasing component integrity) or providing redundancy to mitigate the effects of their failure.

There are several limitations of these approaches. One of the major problems is that most common hazard analysis techniques such as FTA or FMEA, work on an existing design. Therefore, much of the effort goes into proving that existing designs are safe rather than building designs that are safe from the beginning. But system designs have become so complex that waiting until a design is mature enough to perform a safety analysis on it is impractical. The only practical and cost-effective safe design approach in these systems is to design safety in from the beginning. In safety-driven design, the information needed by the designers to make good decisions is provided to them before they create the design and the analyses are performed in parallel with the design process rather than after it. Because software errors and flawed human decision making do not involve random failures, hazard analysis techniques that only identify such failures will not be effective for them. A new approach to hazard analysis is required, which in turn must rest on an expanded model of accident causality.

Against this background, Leveson developed a new accident model called STAMP (Systems-Theoretic Accident Model and Processes), which has been described in detail elsewhere [2]. The rest of this section describes a new hazard analysis technique, based on STAMP, which is called STPA (STAMP-Based Process Analysis) [3]. An important advantage of this technique is that it can be used to drive the earliest design decisions and then proceed in parallel with ensuring design decisions and design refinement.

In STPA, the system is viewed as a collection of interacting loops of control. The assessment begins with identifying hazards for the system and translating them into top-level system safety constraints. Next, a basic control structure is defined. A control structure diagram depicts the components of the system and the paths of control and feedback. Using the control structure diagram as a guide for conducting the analysis, each control action is assessed for potential contribution to hazards. Identified inadequate control actions are used to refine system safety constraints. Finally, the analyst determines how the potentially hazardous control actions could occur. If the controls in place are inadequate, recommendations should be developed for additional mitigations.

3. CASE STUDY ON SYSTEM CONCEPT DESIGN PHASE of CREW RETURN VEHICLE

3.1. System Overview

We are conducting a case study of safety guided concept design of CV using STPA. One of the important advantages of STPA is that it can identify hazardous scenarios or their causal factors with regard to interaction between controller and controlled process.
In this section we explain a scope and conditions to perform STPA at first.

CV is a capsule type re-entry module. Figure.2 shows the reference model of CV. As Figure 1 shows, the CV is launched by Japanese rocket and rendezvous with ISS and dock to ISS. After departure from ISS, CV performs de-orbit maneuver and detaches the re-entry capsule before arriving reentry point. Then the capsule return to the earth.

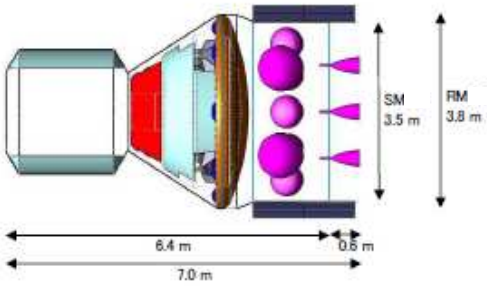

Figure 2. Reference model of CV

In this CV study, we focused on de-orbit flight phase, from completion of un-dock to passing through re-entry point. Figure 3 shows de-orbit flight phase.

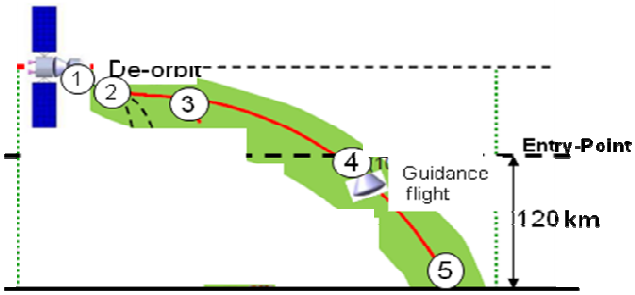

Figure.3 De-orbit flight phase

Figure 4 shows the state chart of de-orbit phase. The state chart shows nominal sequence of de-orbit procedure. Last two gray colored states that are “4.Guidance flight” and “5.Landing” are out of scope of this analysis.

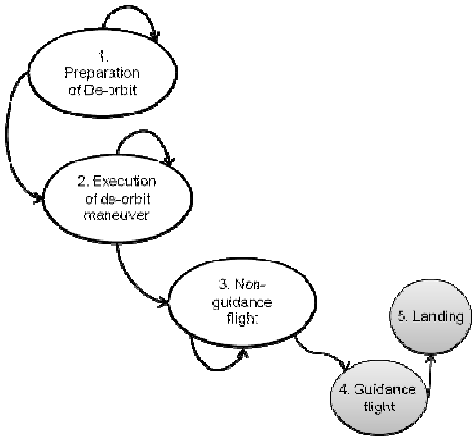

Figure 4. State chart of de-orbit flight phase

In table 1, we defined states that are “1.Preparation of De-orbit”, “Execution of de-orbit maneuver” and “3.Non-guidance flight”.

Table 1. Definition of States

1. Preparation of De-orbit Maneuver Process on this state : **Maneuver preparation** Activation and Health check of H/W component that is used for De-orbit Maneuver. For example activation of engines. Expected event on this state : **Maneuver start** State of CV System transit to De-orbit Maneuver Execution. Triggering condition : Maneuver preparations shown below is completed. ● CV time become planned Maneuver time. ● Health check of H/W components is successful. ● Confirmation of dispersion of touch down point is successful. Next state : 2. Execution of De-orbit maneuver
2. De-orbit Maneuver Execution Process on this state : **Maneuver execution** -Inject engines until predefined generation of predefined ΔV. -Maintain maneuver attitude. Expected event on this state : **Maneuver end** State of CV System transit to Descent without Lifting Guidance.

Triggering condition :
Pre-defined delta-V is generated.

Next state : 3. Non-guidance flight

3. Non-guidance flight
Process on this state :
Descent without guidance
-Perform attitude control
-Health check for Lifting Guidance flight
Expected event on this state :
Guidance start
State of CV System transit to Lifting Guided flight
Triggering condition :
Dynamic pressure by atmosphere is greater than TBD [MPa]

Next state : 4. Guidance flight

3.2. System-Level Hazards

During this de-orbit phase, one of the most catastrophic accident is a fail of de-orbit maneuver. It is not only a result in damage of the CV itself, but could also lead to loss of crews and the vehicle. In this study, we focused on the De-orbit maneuver fail such as over burn or under burn as a system hazard.

3.3. Hazard analysis using STAMP/STPA

As a preparation of STPA, we defined a control structure of CV system. Figure 5 shows a top level-control structure diagram for the CV system. There are 5 major parts: CV (CV crew and CV system), ISS, NASA ground station, JAXA ground station, and Tracking and Data Relay Satellite (TDRS) as data relay communication. Connecting lines between those parts show control actions, information, and acknowledgments (feedback) between each part. There is also a voice loop connection between the ISS crew, NASA ground station and JAXA ground station.

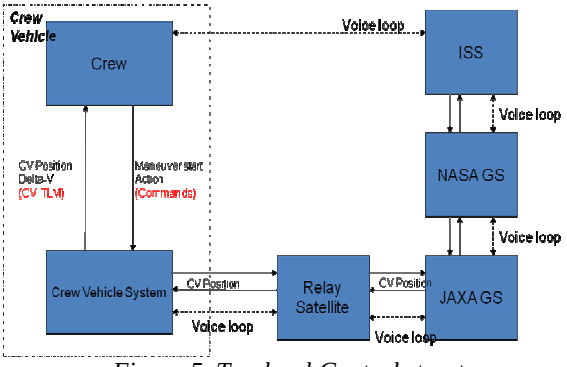

Figure 5. Top level Control structure

3.4. STPA Step.1 and Step.2

i. STPA Step.1 Identification of Hazardous control behaviours

The first step in STPA is to assess the safety controls provided in the system design to determine the potential for inadequate control, leading to hazard. The assessment of the hazard controls uses the fact that control actions can be hazardous in four ways [3].

1. A control action required for safety is not provided or is not followed.
2. An unsafe control action is provided that leads to a hazard.
3. A potentially safe control action is provided too late, too early, or out of sequence.
4. A safe control action is stopped too soon (for a continuous or non-discrete control action)

For convenience, a table can be used to record the results of this part of the analysis like Table 2.

Table 2. Identifying Hazardous System Behaviour

Control Action	Not Given or Not followed	Given incorrectly	Wrong timing or order	Stopped too soon
Maneuver start	Katahira, M.,			
Guidance start				
Etc...	---	---	---	---

To be analyzed.

ii. SPTA Step.2 Determining How Unsafe Control Actions Could Occur

Performing the first step of STPA provides the safety requirements, which may be sufficient for CV system. A second step can be performed, however, to identify the scenarios leading to the hazardous control actions that violate the safety constraints.

Starting with each hazardous control action identified in Step 1, the analysis in Step 2 involves identifying how it could happen. To gather information about how the hazard could occur, the parts of the control loop for each of the hazardous control actions identified in Step 1 are examined to determine if they could cause or contribute to it. Once the potential causes are identified, design controls and mitigation measures can be designed if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design. Figure 6 shows example of Step 2 STPA analysis on CV.

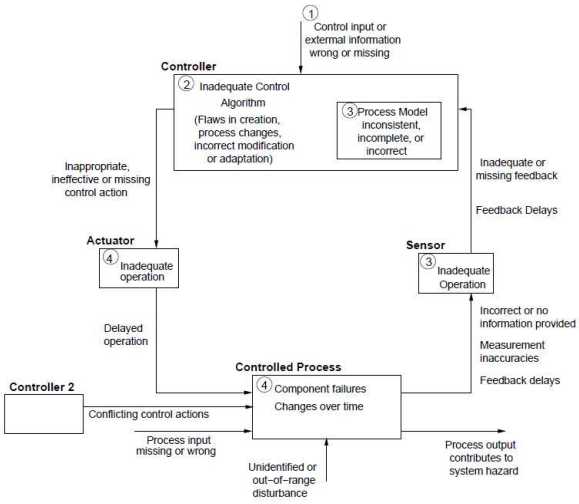

Figure 6. The causal factors to be considered to create scenarios in Step 2
(It is to be analyzed on CV case)

3.5. Safety guided design process

Figure 7 shows our idea of safety guided design process. We are trying to apply the safety guided design to CV. Safety guided design process is compared to JAXA's traditional Safety analysis process in Figure 7. As Figure 7 shows, in JAXA's traditional safety analysis process, JAXA identifies system hazards in Preliminary Hazard Analysis. On the other hand, the control structure of space system and functions are designed in the design process. The control structure is refined based on identified system hazards.

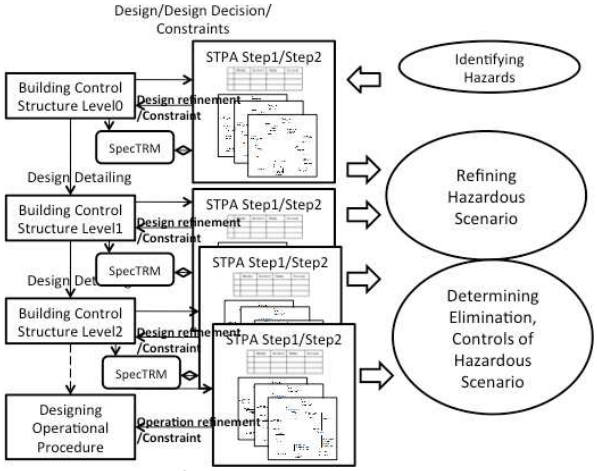

Figure 7 Safety guided design process with STPA and SpecTRM analysis

STPA is used for identification of hazardous control behaviour and their causal factors. In addition to that, SpecTRM analysis [4] is used for checking the existence of concrete hazardous conditions in the design. Using the results of STPA and SpecTRM analysis, we investigate how to eliminate or how to control the hazards and causal factors. The safety constraints against the causal factors are used as "Guide" for Design detailing such as adding design controls and mitigation measures in next control structure level i.e. From Control Structure Level 0 to Control Structure Level 1. In such way the design is refined. This refinement using STPA and SpecTRM analysis is repeated in the safety guided design process.
In this CV case study, we are studying how to apply this safety guided design process from the concept design phase.

4. SUMMARY AND FUTURE WORK

Since we are now in early study phase, there is no concrete system configuration nor architecture. Therefore we defined states of de-orbit phase using state chart. Currently we are performing STPA Step1 and Step2 analysis. After we identify hazardous control behaviours and causal factors, we will investigate safety constraint, design control or mitigation together with system design team of CV. Based on the safety guided design process we defined, we will perform second iteration of hazard analysis on the refined system design.

5. ACKNOWLEDGMENTS

The authors would like to thank system design studying team, Dr. Ueno, Mr. Wakabayashi and Mr. Kawano of Manned spacecraft research working group of JAXA.

6. REFERENCES

1. Leveson, Nancy G., "A New Accident Model for Engineering Safer Systems," *Safety Science*, Vol. 42, No. 4, pp. 237-270, April 2004.
2. Leveson, Nancy G., "Software Challenges in Achieving Space Safety," *Journal of the British Interplanetary Society* (JBIS), Volume 62, 2009.
3. Leveson, Nancy G., "Engineering a Safer World", 2009.
4. Masa Katahira, Leveson, Nancy G., "Use of SpecTRM in Space Applications", 2001.