Safety Guided Design Analysis in Multi-purposed Japanese Unmanned Transfer Vehicle

by

Ryo Ujiie

M.S., Geophysics, Tohoku University, 2009
B.S., Geophysics, Tohoku University, 2007

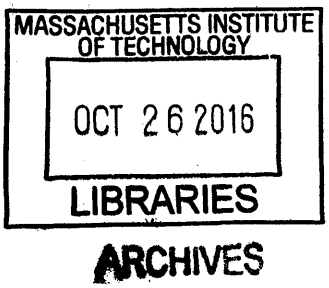
Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

September 2016



Signature of Author: Signature redacted

Ryo Ujiie
System Design and Management Program
August 5, 2016

Certified by: Signature redacted

Nancy Leveson
Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Signature redacted

Warren Seering
Weber-Shaughness Professor of Mechanical Engineering

[Page intentionally left blank]

Safety Guided Design Analysis in Multi-purposed Japanese Unmanned Transfer Vehicle

by

Ryo Ujiie

Submitted to the System Design and Management Program
on May 8, 2016 in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

As with other critical systems, space systems are also getting larger and more complex. Although Japan Aerospace Exploration Agency (JAXA) has designed various spacecraft and had not experienced any serious accident for more than 10 years, loss of an astronomical satellite finally happened in 2016 even though the development process was not drastically different from the past. The accident implies that the complexity of space systems can no longer be managed by the traditional safety analysis. Furthermore, in huge system developments, the fluidity of design is rapidly lost as the development proceeds. Thus, creating a safer system design in the early development phase that is capable of handling various undesirable scenarios will significantly contribute to the success of huge and complex system development.

The goal of this thesis is to establish the way to design a safer system in the context of modern huge and complex systems and demonstrate its effectiveness in an actual JAXA future transfer vehicle design. As a solution, in this thesis a new accident model called System Theoretic Accident Model and Process (STAMP) is used. The safety analysis methods based on STAMP were invented to handle the characteristics of modern complex systems. Furthermore, detailed designs are not required in the analysis. Therefore, the issues of modern complex systems are expected to be solved by the system theoretic safety design methods.

In this thesis, two types of system analysis were conducted based on STAMP: concept design analysis in the target system and incident analysis in a similar previous system. While any detailed specification was not available, various unsafe off-nominal system behaviors were derived from the concept design, and it was refined. Remarkably, off-nominal behaviors due to a new design policy being applied in the system were successfully described. Furthermore, various design flaws involving human-automation interactions were also found, which usually tends to be discussed in the later development phase. The result indicates the proposed system theoretic safety design approaches can be successfully interwoven with the early stage of development process, and systems can be fundamentally refined from a safety perspective to prevent future serious losses.

Thesis Supervisor: Nancy Leveson
Title: Professor of Aeronautics and Astronautics

[Page intentionally left blank]

ACKNOWLEDGEMENTS

First of all, I must most appreciate my advisor Prof. Nancy Leveson. She always guided me in the right directions in this research and inspired me by useful and concrete academic advice. She was always willing to educate me as a system thinker. Without her support, I would never complete this thesis and not deeply improve my insights about system thinking and system safety.

I am also deeply grateful to Dr. John Thomas. He gave me great insights to improve my research idea, and advised me to sophisticate my thesis. I learned a lot from him.

Thanks are also due to my company, Japan Aerospace Exploration Agency. It sponsored me to join the system design and management program, and my thesis is definitely based on the experience as a space engineer in the agency.

Finally, I thank my wife Natsuki and my son Keita. I could not lively enjoy the life in MIT without you.

Ryo Ujiie
Cambridge, Massachusetts
August 2016

[Page intentionally left blank]

Contents

Chapter 1. Introduction

As the needs from stakeholders has been growing and diversifying, the scale of social systems like space system has kept increasing. Because of this continuous expansion of system scale, the complexity has also rapidly grown as new technology is introduced. While the enhanced functionality benefits the stakeholders, the complexity sometimes leads to accidents (losses), such as loss of life or loss of property.

Especially in space systems, safety has been considered as one of the most important system characteristics to prevent such accidents. Even though the engineers spent tremendous effort on designing t safety into the systems and used accumulated design experience, unfortunately serious accidents can still happen. Japan Aerospace Exploration Agency (JAXA), for example, had not experienced any loss of spacecraft for more than 10 years, but in 2016 they completely lost an astronomical earth orbiting satellite on orbit [1]. This accident implies losses can happen even if there is no technological leap from an engineering perspective and the engineers have adequate development experience. In other words, the causes of accident in complex modern systems cannot be completely eliminated by traditional engineering approaches.

In complex modern systems, moreover, the relationship between systems and operators is no longer as it once was. Humans were able to understand comprehensively the behaviors of a traditional electro-mechanical system due to the simple and linear relationships among components, which enabled operators to predict the result of each failure and operate the systems safely even in abnormal situations. However, the current software-intensive systems are stretching the limits of operators' comprehensibility because software can assign various special behaviors to a general purpose component [2]. Although JAXA is one of the few space agencies that has contributed to human space it might be able to doom future human space systems and lose its international credibility based on the past successful contributions, if it does not understand this new trend of modern human supervisory systems and instead stick to its existing engineering approach.

The purpose of this study is to research a new engineering approach to realize safety in modern complex systems and demonstrate its effectiveness through applying the approach to JAXA's next generation human space system. Especially, the human and automation design is focused from system design perspective. This approach uses a system's theoretic approach to human and automation design. The detailed motivation of this study is stated in section 1.1, and then the concrete research objectives are defined in section 1.2.

1.1 Motivation

JAXA has conducted the system design of most Japanese spacecraft including satellites, rockets, and human space systems. As with other critical systems, the space systems are getting larger and more complex. While the agency has succeeded in a large number of spacecraft developments and operations, the engineers have made tremendous efforts to lead the systems to this success. However, the complexity of next generation spacecraft will be no longer controllable by such brute-force effort, and therefore their engineering approach has to be improved to keep succeeding in even more complex future spacecraft development.

The H-II Transfer Vehicle (HTV) is a Japanese unmanned supply cargo spacecraft to the International Space Station (ISS) [3], which has been successfully operated 5 times from 2009 to 2015. In 2015, JAXA announced the development of a next generation transfer vehicle called HTV-X that will tentatively be launched in 2021 [4]. The design heritage of the HTV will be utilized in the HTV-X, but its system architecture will be drastically changed because of the following two reasons: multi-missions and new safety design policy. The HTV-X will for sure be assigned three missions: ISS resupply mission, orbital experimentation mission, and future earth to moon transfer technology demonstration mission. The ISS resupply mission is exactly the same as the existing HTV's mission, although the cost restriction is more severe. In the orbital experimentation mission, the HTV-X will provide an opportunity for new space technology experimentation in Earth orbit. Before it re-enters the atmosphere after departing from the ISS, some experimentation will be executed using the vehicle's resources. The final mission is to demonstrate

key technology for a lunar transfer vehicle by designing the HTV-X so it can be extended to the future vehicle. In addition to this multi-mission, the new safety design policy called resilient design policy will be adopted in the HTV-X. While the multi-missions are driven by top-down decisions, this policy has risen from engineers' bottom up desire. Throughout the existing HTV operations, the operators had been suffering from inflexible and inefficient automation behaviors under off-nominal conditions. To make the system more robust against failures, they are introducing the resilient policy which is expected to make the system more adaptive to failures.

Integrating these top-down and bottom-up development directions into one system is a completely new challenge for the agency, which will surely make the HTV-X system development more difficult than ever. Because the multi-missions will introduce more stakeholders, more requirements, and more discrepancies, the new safety design policy will require a brand new architecture and operations. In addition, the vehicle is required to be safe enough as an ISS related space system while satisfying the cost limits. It is clear that the engineers cannot deal with the difficulty by just applying the existing design approach. Therefore, a novel system design approach to guide this complicated system development is required for the HTV-X project and JAXA, which will also be able to contribute to the success of similar huge and complex systems in other industries.

1.2 Research Objectives

Although JAXA has adequately designed their space systems using the current engineering approach, it should be improved to maintain the same success in their future more complex spacecraft like the HTV-X. Even if the future spacecraft is a highly complex system, some engineers will still believe that the system can somehow be developed and operated as planned based on rich space system development experiences. If the system is always in well-known nominal conditions, it would be possible. However, most undesirable situations happen under off-nominal conditions, and controlling those unexpected off-nominal cases is the

biggest challenge in huge and complex systems.

Moreover, as a nature of system development, the flexibility of system design tends to be rapidly lost as the design phase proceeds. Therefore, the direction of this thesis is to research the engineering approach to identify hazardous off-nominal situations in huge and complex system and design the control to prevent them in the early development phase.

As mentioned above, the HTV-X automation will be more complex than ever and human operators cannot deal with some off-nominal scenarios as they have done in the existing systems. Therefore, to create requirements to guide human operators and maximize their safety control capability will also be the biggest challenge in this thesis.

To make this statement more concrete, the following two research objectives are defined. The first research objective is to identify hazardous scenarios from the concept design of the HTV-X and create requirements and constraints to control the identified hazardous scenarios. In the HTV-X system, interconnected requirements and scenarios originating from multi-missions will be implemented into a single spacecraft. In addition, the resilient design policy introduces a lot of coupling among system elements to adapt to various unexpected conditions. These characteristics can be a source of unexpected system behaviors, which deteriorates the controllability of the system. Therefore, considering multi-purposed spacecraft characteristics and the resilient design approach to identify possible undesirable off-nominal scenarios is the important first step to maintain the safety of the HTV-X. To prevent the undesirable off-nominal scenarios as the next step, some requirements and constraints for the system have to be defined without contradicting the mission purposes and design policy. In the HTV-X, moreover, it can be a central concern to define requirements about how human operators supervise and intervene in this complex automation system.

The second objective is to analyze the actual operation experience in the existing HTV from a system level

point of view and effectively utilize the results in the HTV-X system design. In the HTV-X system development, a lot of heritage from the HTV will be utilized, but the intent is mainly to reuse the design for cost reduction. Although no serious accident has never happened in HTV operations, the operators and engineers actually suffered a few undesirable incidents. Surprisingly, one of the incidents is clearly related to the interaction between human operator and computer system, which is also a central concern in the HTV-X. Without eliminating the systemic causes for those incidents, similar or worse unexpected events could happen again in the HTV-X and, in the worst case, seriously damage the system. Moreover, in this incident analysis, the outcome should be system-level design recommendations, which is useful even in the HTV-X system design. While the HTV and HTV-X have a lot of commonality at the system design level, each specific component design can be different. Therefore, it will be the most important direction in this analysis to identify the design issue as the whole system from the actual incident and create useful design recommendation for the HTV-X.

Chapter 2. System Theoretic Safety Analysis

In order to accomplish more sophisticated missions in space, the functionality of space systems has been extended. On the one hand, in space systems, any causes of accidents have to be eliminated before launch, because it is impossible to stop the systems, return them to earth, fix their faults, and then re-launch the systems. Obviously, the target system of this thesis, the HTV-X, is also in this situation, and moreover the other social factors (e.g. cost reduction pressure) strongly influence the development.

Obviously, the context of system development has been dramatically changed, and it also has changed the nature of safety. However, many leading development organizations, including JAXA, still try to describe accidents in the traditional context, which never leads to effective solutions for modern complex systems. As mentioned in the research objectives, grasping modern complex systems like the HTV-X as a whole and guiding the safety design in the early development phase is the most critical factor to determine the success of the system. However, it can never be realized unless the traditional safety concept is replaced by a new system theoretic one. Section 2.1 explains the reason why the traditional approach is no longer effective in modern complex systems, and in the section 2.2 an alternative solution, a system theoretic approach, is described.

2.1 Limitation of Traditional Safety Analysis

In traditional electro-mechanical systems, accidents typically come down to individual component failures. Thus, the traditional analysis techniques, such as Fault Tree Analysis (FTA)[5] and Failure Mode, Effect, and Criticality Analysis (FMECA)[6], focus on analyzing the impact of each component failure on the entire system. This approach successfully prevented accidents in traditional systems. However, these traditional safety approaches were designed for analyzing the traditional electro-mechanical systems of 1960s and 1970s, and in the analysis it is assumed that accidents never happen without failure.

On the other hand, in modern complex systems, the safety of the systems can never be achieved simply by preventing failures; for example, the Mars Polar Lander incident showed that an accident can occur from interactions among components even if no individual element has failed [7]. The most persuasive scenario of this accident is that the control software recognized the noise from a sensor as the Mars surface landing signal, and therefore stopped the deceleration thrusting (used to achieve a soft landing) before actually landing and the spacecraft crashed on the planet surface. In this accident scenario, there was no component failure, and the software worked as designed and required. In other words, the accident was caused by the interaction among components and wrong system and software requirements. As this accident indicated, software has changed the nature of accidents. At the same time, any modern system can never be realized without software. Thus, engineers should understand the limitation of the traditional safety approach and design their systems using a new safety analysis approach that is applicable for modern software-intensive systems.

In modern complex systems, the role of operators is also quite different from the traditional systems. In the traditional systems, the operators were expected to perform as a single component inside the whole system loop, and consequently their role was simple and narrow. On the other hand, the role of the operators in modern complex system is changed to supervise the whole system, make a proper judgement based on the monitored data, and provide an adequate instruction to guide the whole system behavior in the right direction. Indeed, in the operation of the HTV, a serious incident occurred because of a lack of coordination between ISS crew, the ground station (GS) crews, and the automation [8]. Fortunately, this case did not result in an accident, but it was definitely an unexpected event. This incident is discussed in chapter 5 in detail. In the current complex systems, it is desired to adequately design the coordination between human operators and automation, while just analyzing each responsibility like the traditional approach is no longer enough.

What is behind the discrepancy between the traditional safety analysis and current complex system

accidents? Prof. Leveson explained it in her lecture by the differences between safety and reliability as shown in Figure 1. The figure clearly shows that unsafe but not unreliable hazardous scenarios can occur, while the traditional safety analysis can cover only the hazardous scenarios involving failures. Obviously, this unsafe but not unreliable scenario is the cause of typical modern accident like the Mars Polar Lander accident. Thus, the new safety analysis for the modern complex system should be required to be capable to handle this unsafe but not unreliable scenarios including the component interaction and the human and automation coordination.

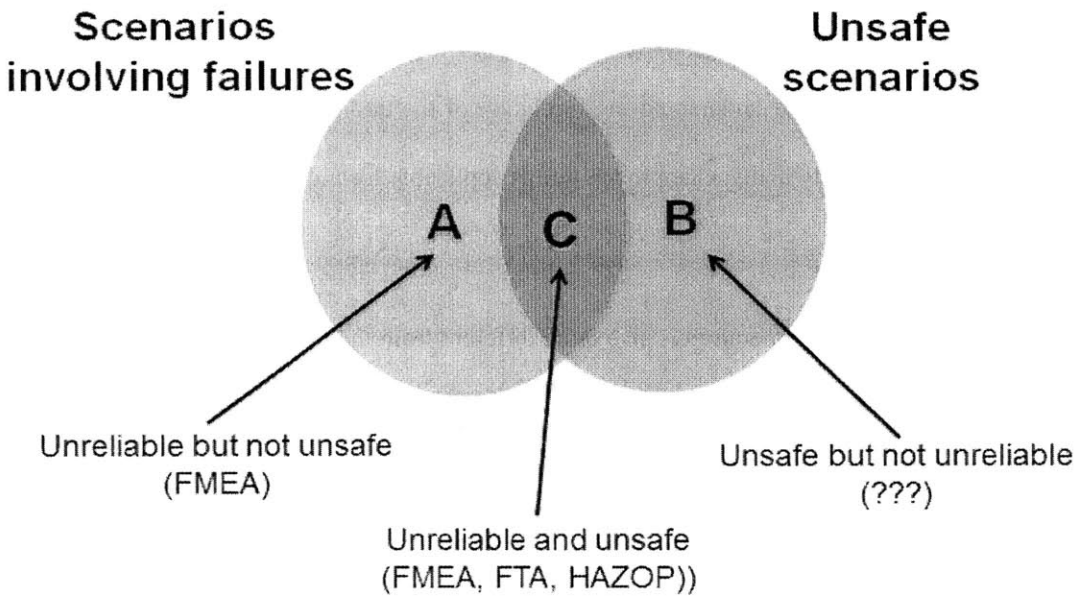


Figure 1: Difference and Overlapping between Safety and Reliability from Prof. Leveson's Lecture Notes

In order to efficiently find the unsafe but not unreliable scenarios and implement the countermeasures into the systems, the interaction and coordination among system elements should be adequately described and improved. However, this system level interaction and coordination tends to be designed in the early development phase, and a tremendous cost has to be spent if modifying the design in the later phase (see Figure 2). It cannot be definitely achieved by the traditional safety analysis methods to design the interaction

and coordination from safety perspective in the early development phase, because those methods assume the existence of detailed component design and in order to analyze the reliability of each component. Therefore, to efficiently design the system level safety countermeasures before the fluidity of system design is lost, the new safety analysis should be also applicable for the early development phase in which the detailed component design is still not available but the interaction and coordination can be flexibly changed.

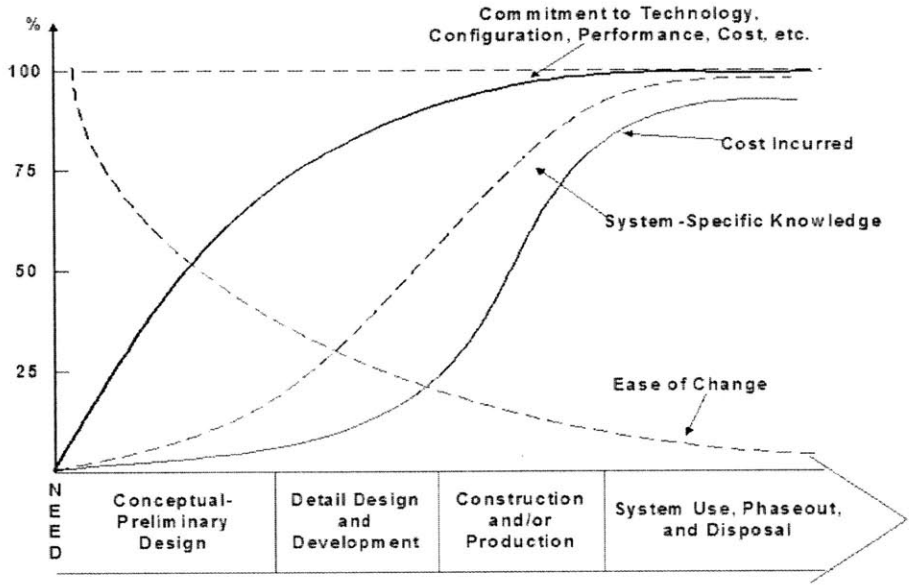


Figure 2: Cost Commitments and the Project Lifecycle [5]

2.2 New Accident Causality Model based on Systems Thinking

System-Theoretic Accident Model and Processes (STAMP) is a new accident model proposed by Prof. Leveson [2] [9]. In STAMP, an accident is defined as a control problem, while in the traditional approach an accident is seen as a result of component failures. The goal of STAMP is to make controls safe as a whole system. Because in complex modern systems hazardous controls are induced from lack of enforcement of safety constraints in the design and operation, the main focus of STAMP is to impose safety constraints on a system as preventing the hazardous controls.

The concept of STAMP is underpinned by systems theory. In the theory, there are several important principles to adequately describe the characteristics of modern complex systems. The first principle is that emergent system properties like safety are supposed to arise from the interactions among components. In the traditional system view, the emergent properties are assumed to be independently decomposed into subsystems. Take FTA as example. In FTA, safety is assumed to be always accomplished if each separated component works without any failure. This idea could be reasonable if only physical aspect of systems is discussed. However, like the Mars Polar Lander accident, the accidents in modern complex systems can be driven by the interaction among components even if any failure does not happen. Therefore, in modern complex systems, the emergent properties including safety should be described based on the interactions among components. .

To analyze the interactions and properly impose safety constraints on a target system, furthermore, the interactions are represented as a control structure made up of feedback control loops. Figure 3 shows a standard control loop diagram. A control loop is composed of controller, controlled process, control, and feedback. Each controller has specific goals and, in order to accomplish the goals, influences controlled processes by controls. To guide a controlled process to a goal state, a controller observes feedbacks from the controlled process and selects an adequate control. Moreover, controls can work on system through a hierarchy. Figure 4 shows an example of hierarchical control structure. In modern complex systems, various socio-technical factors are associated with actual system operation. For example, in the accident of an astronomical satellite of JAXA called "Hitomi", the direct causes were an inadequate software parameter design, an incorrect attitude estimation algorithm design, and a wrong parameter input before the launch. Although these causes directly generated high speed satellite rotation and consequently the satellite was broken, in the accident report, the other management and development process flaws were also pointed out [10]. Because the Hitomi project team focused on satisfying demanding observation requests from some science communities, most of the project reviews and meetings was spent for the science instrument

developments and science observation operations. As a result, the attitude control was designed as quickly stabilizing the attitude to maximize the observation time and the preparation for the initial critical operation phase was less prioritized. Originally, the purpose of a project team is to manage a whole system development as balancing various requirement and ensure the success of the spacecraft project. However, the project team was wrongly biased to the science mission side and lacked the system perspective, which resulted in the not robust attitude control design and careless wrong parameter input. Behind these flaws, a cultural factor also significantly influenced the accident. The Hitomi satellite was one of the science projects conducted by Institute of Space and Astronautical Science (ISAS) which is a research organization inside JAXA. Traditionally, in ISAS most of the project members has been selected from science researchers. Furthermore, they also hold an academic post like professor and have to spend their resources on education. While this tradition has contributed to great science outcomes from ISAS, it led to lack of organizational supervision for system safety.. Obviously, various inadequate controls can be found in the development process, project management and organizational control as well as the physical system design. Those inadequate controls are expected to be described by a hierarchical control structure like Figure 3. Therefore, in order to do a deep dive into accidents in modern complex systems and enforce effective countermeasures for the future systems, it also should be analyzed how engineering process and organizational controls can hierarchically have impact on a physical system.

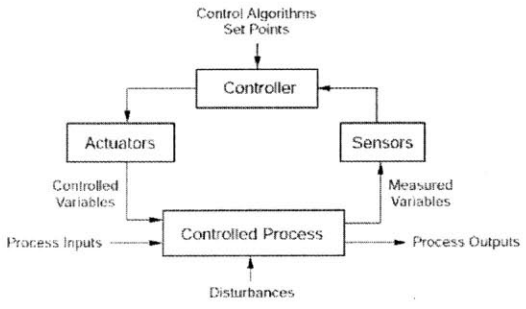


Figure 3: Standard Control Loop [2]

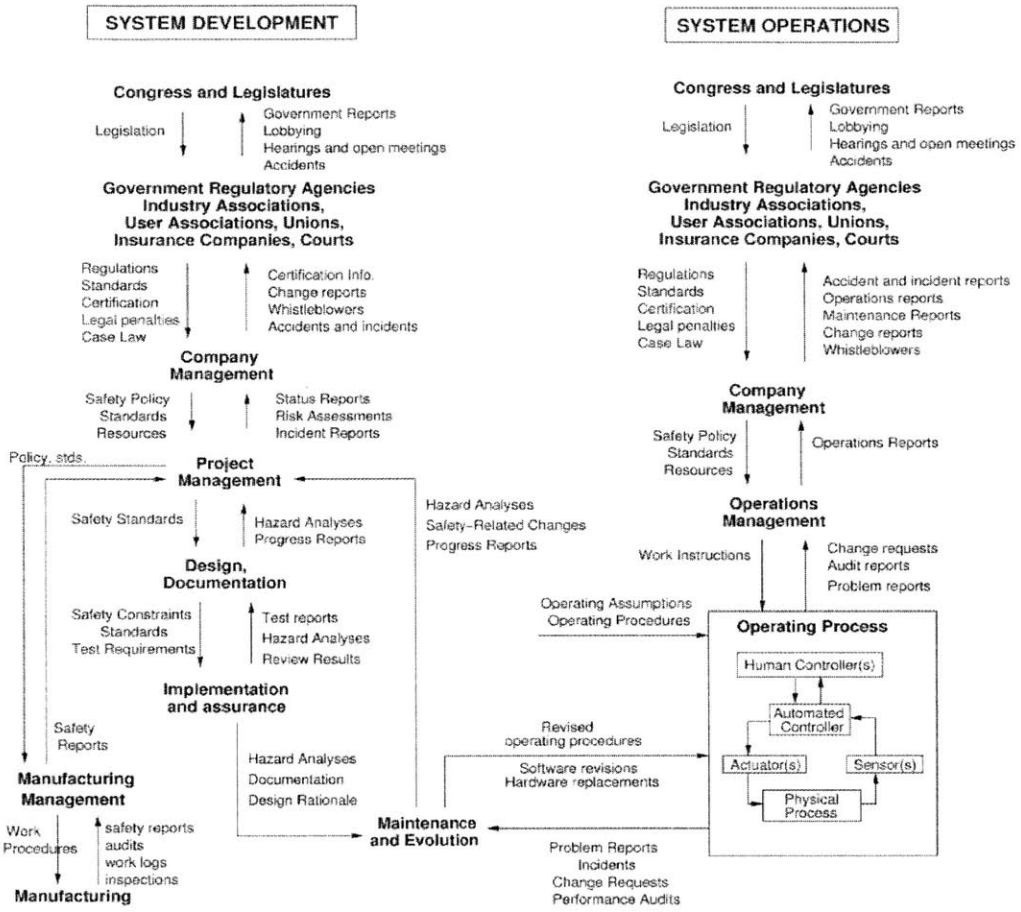


Figure 4: An Example of a Hierarchy of a Socio-Techncial Control Structure [2]

To consider why hazardous control happens in the control loop, process model plays an important role in system theory. Each controller has a process model which represents the controller's understanding about the following factors: the current state of the controlled process, the goal state of the controlled process, and the ways to change the state of the controlled process. Based on the process model, as shown in Figure 5, the controller updates the assumed current state through feedbacks and decides which control action should be provided to change it to the goal state. The advantage of process model is enabling the analyst to describe software and human behaviors. In software, parameter variables equal to the process model. Therefore, examining flaws of the process model results in analyzing the impact of inappropriate parameter setting. For humans, the process model can be seen as a mental model. Because this mental model is linked with the

control loops, human mental flaws can be analyzed in context of controls as a whole system. These features of the process model are surely helpful in analyzing software intensive systems and human supervisory systems.

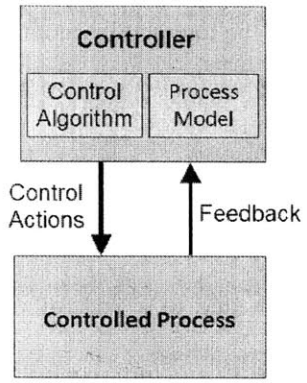


Figure 5: Role of Process Model from Prof. Leveson's Lecture Note

As introduced at the beginning of this section, in systems theory, accidents occur due to inadequate safety constraint enforcements such as a missing feedback, an inadequate control action, a component failure, uncontrolled disturbances, and so on. In STAMP, to guide engineers to find essential safety constraints in system-theoretic context, four types of unsafe control actions which potentially cause hazards are defined as follows:

- A control action required for safety is not provided or is not followed
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action is provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long

By applying these patterns, engineers can analyze if a control action can be hazardous in each potential unsafe pattern, and discuss how safety constraints should be enforced in the control structure to prevent the unsafe control actions.

Because STAMP has several advantages to handle modern complex systems as discussed above, it can be a solution to overcome the limitation of traditional safety analysis and lead the systems to safety. While some modern accidents like the Mars Polar Lander case cannot be described by only component failures, in STAMP the accidents can be discussed based on the interactions among components, and finally effective safety constraints to control the interactions as a whole system can be proposed. In addition, because behaviors of human and software can be logically translated into process models, oriented inadequate controls conducted by software or human operators can be properly analyzed in the model, which can be never accomplished by the traditional approach due to a lack of understanding software and human characteristics. Furthermore, in hierarchical control structure, control responsibility for each stakeholder related to a system can be discussed. As a result of discussion, new roles will be assigned to the stakeholders in order to enforce safety constraints on various organizational levels. Another advantage is that STAMP can be utilized to refine early system designs from safety perspective, because it is based on general systems theory and systems engineering. While STAMP is a concept model based on system theory, a specific purpose analysis method can be defined based on the concept. In section 2.2.1, several concrete methods based on STAMP are introduced.

2.2.1 Methods for System Theoretic Safety Analysis

The STAMP related methods and the possible targets of the analysis are summarized in Figure 6. There are totally four well-structured safety analysis methods for modern complex systems: System Theoretic Process Analysis (STPA), Causal Analysis based on STAMP (CAST), Systems-Theoretic Early Concept Analysis (STECA), and STPA-Sec. STPA is a hazard analysis method based on STAMP, and CAST is an accident investigation method. STECA and STPA-sec are relatively new methodologies. STECA is invented by Dr. Fleming and it is specialized for the analysis of Concept of Operation (ConOps) [11]. According to general system engineering process, ConOps is the first specification defined in the process. Thus, refining ConOps by

STECA can result in efficiently implementing system-theoretical constraints into modern complex systems. In current socio-technical systems, security is strongly associated with safety. STPA-Sec invented by Dr. Young is aimed for system-theoretical security analysis. While the basic idea is the same as STPA, hazards are replaced by security vulnerability in STPA-Sec. In the following paragraphs, the brief description of STPA and CAST are given, although the detailed analysis procedures are described in Prof. Leveson's book with concrete examples [2].

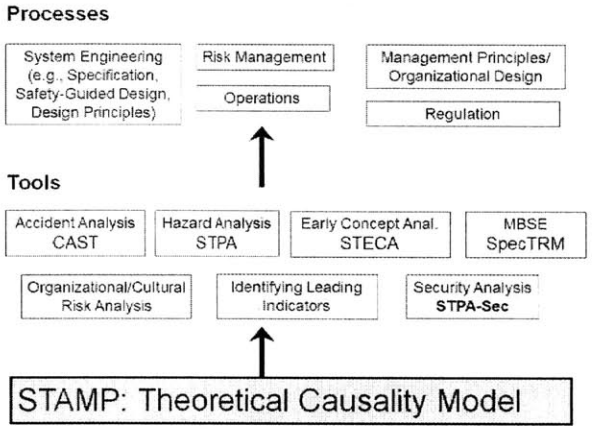


Figure 6: STAMP Related Tools from Prof. Leveson's Lecture Note

STPA is a hazard analysis method based on system theory. Although FTA might be the most common hazard analysis method especially in aerospace domain, STPA can not only replace it but also give more sophisticated insights to grasp modern complex system's behaviors. Basically, STPA is composed of two analysis steps. Of course, before starting the analysis, the accidents and hazards of a target system should be identified and then its control structure should be also created to describe what kinds of control action and feedback already exist inside the system. After that, the analysis is conducted by the following steps:

(1) Identify the potential unsafe control actions that could lead to a hazard by applying the four unsafe control patterns defined in STAMP

(2) Determine how each unsafe control action identified in step 1 could occur

In the first step, the four unsafe control patterns defined in STAMP are applied for each control action in order to evaluate if each unsafe pattern leads to the predefined hazard(s). Based on the identified unsafe control actions in the first step, how each unsafe control action happen is described in the second step. In this step, the control loop shown in Figure 7 helps the analysis. The control loop is composed of controller, controlled process, actuator, and sensor, and each element is connected as organizing a loop. Because various guide words to identify causal factors are given in the loop as shown in Figure 7, the scenarios causing unsafe control actions can be logically created, once a unsafe control action is applied for the loop. After these two step analysis, to implement countermeasures against the identified causal scenarios, safety constraints are discussed. Because concrete hazardous scenarios already exist, it is not a difficult task to come up with the effective safety constraints to prevent the scenarios. The constraints can be the modification of control structure such as adding new controls and feedbacks or refining the process model. Therefore, the result of STPA can directly improve system design from system safety perspective.

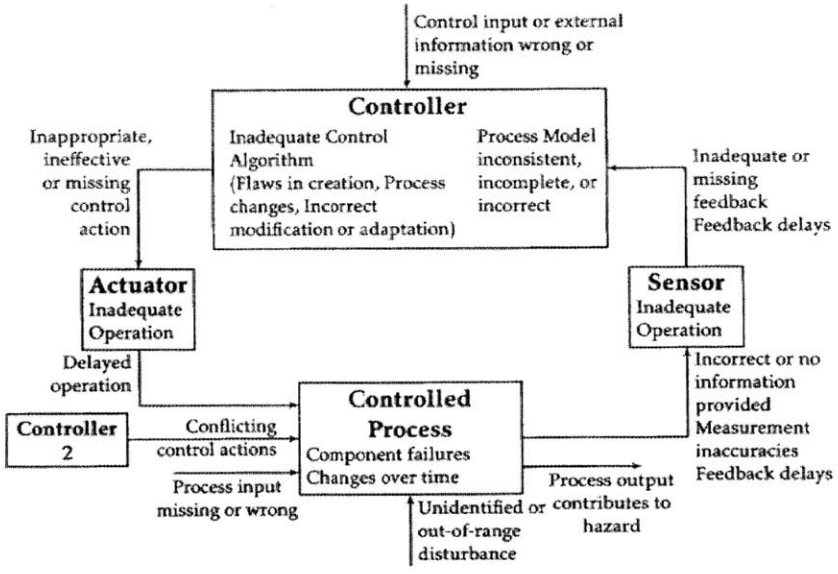


Figure 7: Control Loop with Causal Factor

Although STPA is a relatively new method comparing with the other traditional methods, its effectiveness has been already demonstrated in various domains including aerospace [12]. As one of the most important unique characteristics of STPA, it can be applied in early system design development, while FTA requires detailed component designs for the analysis. It means that system designs can be refined from safety perspective when it is still flexible. Due to this characteristic, the cost to implement safety features into systems can be drastically reduced, as well as essentially enforcing safety constraints on systems.

To analyze an actual accident based on the system theory, CAST can be utilized. In traditional accident analysis, only direct physical causes are investigated, and the final outcome tends to be the simple root cause which is valid to stop an only specific sequence of events or the reason to blame someone. On the one hand, CAST provides the framework to identify the most critical systemic factors and refine a system design as enforcing safety constraints to eliminate the factors as a whole system. The basic analysis steps are defined as follows:

(1) Identify violated system hazard and safety constraints

(2) Construct Safety Control Structure as it was designed to work

(3) Determine if each component fulfilled its responsibilities or provided inadequate control

(4) Examine coordination and communication

(5) Create design recommendation

In the first and second steps, fundamental accident information and system design are examined. The control structure should focus on not only physical process but also higher level controls as shown in Figure 4. After describing the target system by a control structure, how some components inside the system did not fulfill the assigned responsibility are analyzed. Through this analysis, consequently what kind of unsafe control actions were provided in the accident is also clarified. As a next step, to analyze why the responsibility was

not fulfilled and the unsafe control actions were provided, the coordination and communication among controllers are investigated. In this step, lack of control and missing feedback to cause the accident scenario are examined. Finally, based on the examination, design refinement is proposed. The design recommendation should not point out a specific factor in physical process as a result of CAST. Instead, more various design factors at various system levels should be suggested to make the system safer.

Chapter 3. Japanese Unmanned Transfer Vehicle

JAXA is one of a few space agencies that have contributed to international human space exploration, and one of the most valuable contributions is the ISS resupply service by unmanned transfer vehicle, the HTV. The construction of the ISS started from 1988, and the first resident crews arrived at the ISS in 2000. After that, there have been always 2 to 6 crews in the ISS, which means resupply from the ground has been essential to maintain the ISS operation. From 2009, the HTV has been in charge of this essential resupply task, and more than 25 tons of goods have already been supplied to the ISS.

Needless to say, the HTV system has been required to satisfy the highest level of safety, because it is also a human space system. National Aeronautics and Space Administration (NASA) as well as JAXA had carefully checked the design of the HTV, and finally the approval to approach and dock with the ISS was given. Moreover, in every operation, the Ground Station (GS) crew of the HTV has spent tremendous effort on the operation with the ISS crew to realize the safe flight and maintain the safety of the ISS. Although safety is an important concern in all of space systems, especially in the ISS related systems like the HTV it is the most important topic in the system development.

On the one hand, JAXA plans to replace the HTV with a new advanced vehicle called HTV-X, to realize more efficient resupply [13]. While the new vehicle is planned to be launched in 2021, the ISS operation plan after 2024 is still ambiguous, because NASA plans to move out from the ISS by 2024 and concentrate on deep space human exploration [14]. Therefore, the HTV-X is expected to be utilized for the Low Earth Orbit (LEO) experimentation platform and technology demonstration for the future vehicle contributing to the next human exploration mission like lunar space station in addition to the original resupply mission. Obviously, in the HTV-X system development, due to this complicated situation, JAXA will be required to handle a level of complexity they have never experienced, while maintaining the same level of safety as the HTV.

In this thesis research, the HTV-X is selected as the target system, because the safety design is definitely the biggest issue and the results from this study can directly contribute to the actual space system development. Moreover, the academic outcome can surely contribute to the similar types of complex system including the critical interaction between human operator and computer system. Because the basic design of the HTV-X is proceeding from the existing HTV, first of all, the HTV is described in the section 3.1. After that, the description of the HTV-X is given in the section 3.2.

3.1 Existing Transfer Vehicle

The HTV is an unmanned cargo transfer spacecraft aimed at delivering supply goods to the ISS (see Figure 8). The first HTV was launched in 2009 as the third unmanned vehicle to the ISS followed by the Progress of Russian Federal Space Agency (Roscosmos) and the Automated Transfer Vehicle (ATV) of European Space Agency (ESA) [15]. The vehicle has two types of cargo: pressurized cargo and unpressurized cargo, and the total loading capacity is 6,000 kg [3]. The uniqueness of the HTV is the rendezvous flight and berthing technologies. The vehicle autonomously approaches to the ISS and stays at a point 10 m below. After that, the vehicle is captured by the robotic arm of the ISS, called the Space Station Remote Manipulator System (SSRMS), and finally docks with the ISS. This rendezvous flight and robotic arm docking were brand new operations that had never been performed before the HTV. After the success of the HTV, these technologies were transferred to the Dragon Spacecraft [16]. By 2015, JAXA has successfully launched and operated five HTVs and plan to develop four more vehicles by 2019 [17].

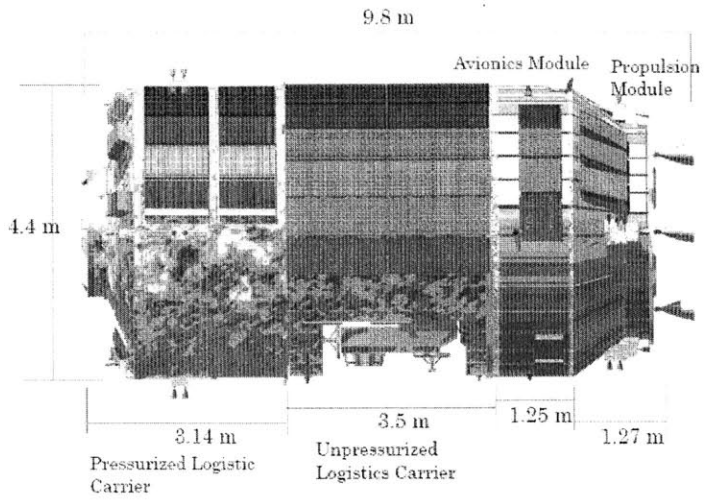


Figure 8: Physical Overview of the HTV [3]

3.1.1 Operation Phases

The operation of the HTV is mainly composed of five phases: launch phase, rendezvous phase, proximity operation phase, docked operation phase, and departure and reentry phase [3]. The overview of the operation is shown in Figure 9. The vehicle is launched by H-II B rocket from the Tanegashima Space Center and inserted at an altitude of about 300 km. Then, the vehicle starts to establish the rendezvous flight with the ISS and finally reaches a point 5 km behind the ISS called the Approach Initiation (AI) point and maintains that distance. After that, the vehicle moves to 500 m below the ISS, which is called the R-bar Insertion (RI) point , with the high accurate Relative Global Pointing Service (RGPS) navigation, and successively switches to the Rendezvous Sensor (RVS) navigation to gradually rise up to 10 m below point by a feedback control algorithm. Finally, the vehicle is captured by the SSRMS and docked with the ISS. After the astronauts in the ISS, called the ISS crew, unload the transferred goods and load the daily trash from the ISS, the vehicle is undocked by the arm and flies away from the ISS. At the end of the operation, the vehicle enters the earth atmosphere and it is finally burned out by the air drag.

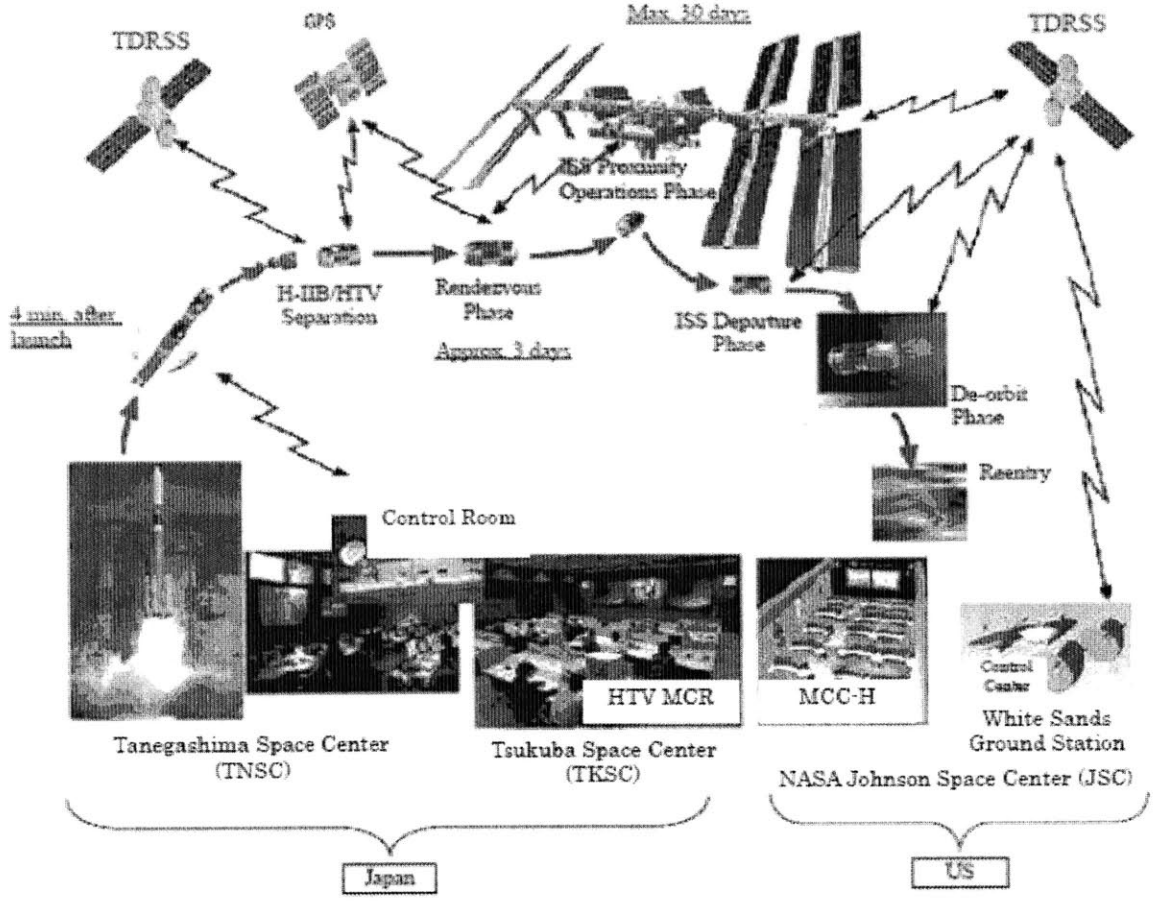


Figure 9: Operation Overview of the HTV [3]

The detailed maneuver plan of the HTV is also shown in Figure 10 [18]. Before reaching the AI point, the vehicle conducts a lot of orbit control maneuvers including some large burn thrusting. Between the AI and RI points, the vehicle executes three relatively small maneuvers called AI, RI', and RI maneuvers. After arriving at the RI point, the vehicle automatically starts feedback control for position and velocity to gradually approach the ISS. In the departure and reentry phase, several small maneuvers are executed, and finally three large deorbit maneuvers (DOM1, DOM2, and DOM3) are conducted to make the vehicle enter the earth atmosphere as planned.

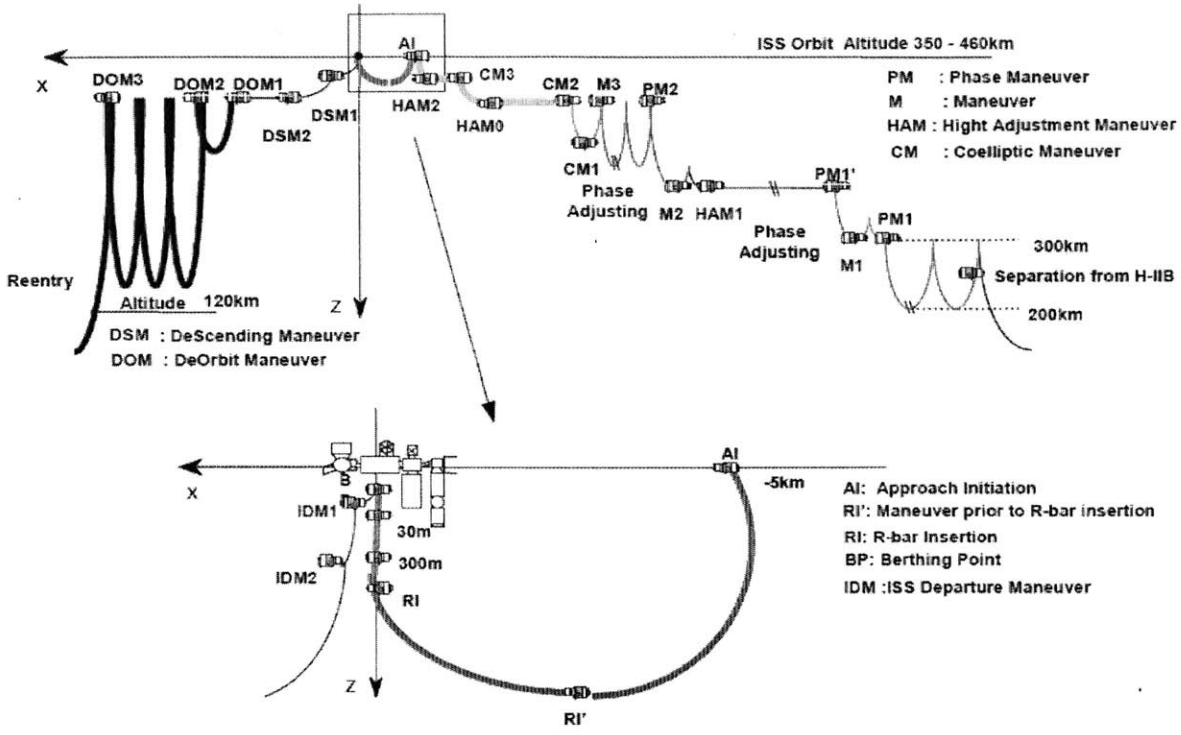


Figure 10: Maneuver Plan of the HTV [14]

3.1.2 System Characteristics

The vehicle is composed of five main modules: Pressurized Logistics Carrier (PLC), Unpressurized Logistics Carrier (ULC), Exposed Pallet (EP), Avionics Module, and Propulsion Module (see Figure 11) [3]. However, because the flight functionality of the HTV is realized by only the avionics module and propulsion module, in this thesis these two flight control related modules are explained in detail.

The avionics module is further decomposed into four subsystems: Communications, Data Handling, Electrical Power, and Guidance Navigation & Control (GNC) subsystems. The communication between the HTV and the ground or the ISS is established by the Communication subsystem that is supported by NASA's Tracking and Data Relay Satellite (TDRS). The Data Handling subsystem relays the commands received from the ground or ISS to each component and collects the telemetry data to be sent. The Electric Power

subsystem generates power by solar array panels, stores it in batteries, and distributes it to each component. Finally, the GNC subsystem, a core subsystem for the autonomous flight, consists of Space Integrated GPS & Instruments (SIGI), Rendezvous Sensors (RVS), Earth Sensor Assembly (ESA), Guidance and Control Computer (GCC), Abort Control Unit (ACU), and Valve Drive Electronics (VDE) are shown in Figure 12 [18]. Once the HTV is on orbit, this subsystem autonomously acquires the navigation information by using the SIGI and ESA and calculates the control amount based on the predefined flight plan. The ACU is a special computer component aimed only to maintain the safety for the ISS, and its only function is to make an abort operation which makes the vehicle fly away from the ISS, while the GCC has other various functions as well as the abort function. Because each component of the subsystems has is redundant, the ACU is activated only when more than 2 failures happens in the GCC. The VDE is an electric component to convert the control amount calculated by the GCC or ACU to electric signal, and finally the signal is the input for the propulsion module.

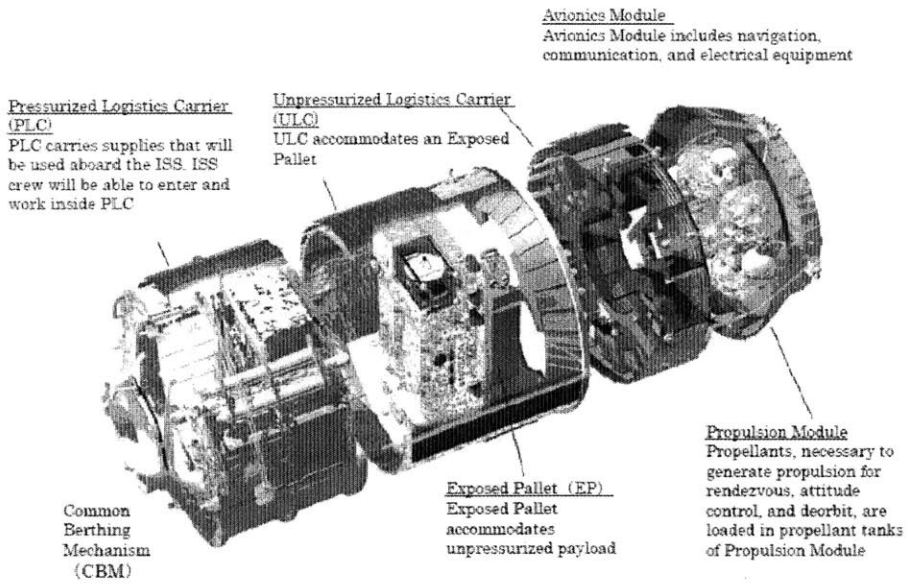


Figure 11: Module Configuration of the HTV[3]

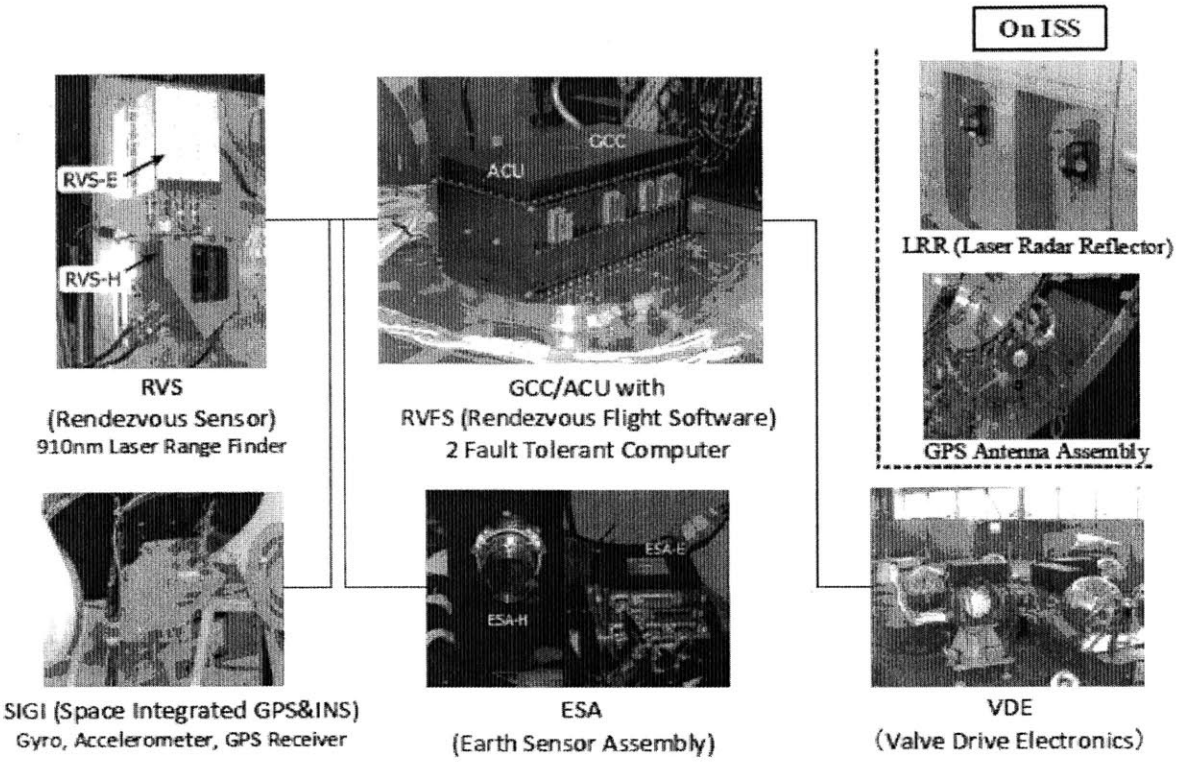


Figure 12: HTV GNC subsystem configuration [14]

Following the input signal from the avionics module, the propulsion module generates physical thrusting force by Main Engine (ME) thrusters of which propel force is 500 N and Reaction Control System (RCS) thrusters with 110 N (see Figure 13). In total, four ME thruster and twenty four RCS thrusters are included, but half of them are backup. Likewise, two of four chemical propellant tanks are also redundant ones. Generally, twelve RCS thrusters are used for the attitude control and small maneuver in the proximity and departure phases, and the large maneuvers conducted in the rendezvous and reentry phases are realized by two ME thrusters. Although the abort maneuver is generally made by the RCS thrusters because the required thrusting force is relatively small, the ME thrusters also can be in charge when the RCS thrusters are no longer available or the ACU conducts the abort.

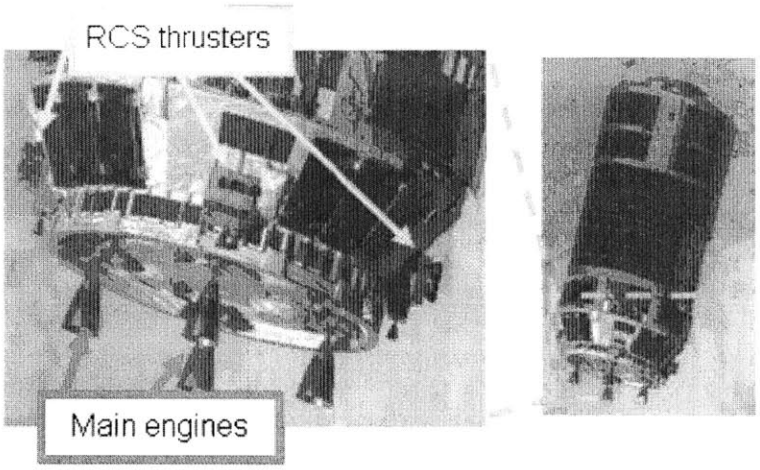


Figure 13: RCS thrusters and Main Engines of the existing HTV

Moreover, the HTV automation has an unique Fault Detection, Isolation, and Recovery (FDIR) function called "Safety Net" [18]. Through the whole approach operation, the vehicle has to avoid violating two safety areas: Approach Ellipsoid (AE) and Keep Out Sphere (KOS) (see Figure 14). During the rendezvous phase, the HTV is expected not to violate the AE of which the dimension is 4 km x 2 km x 2 km ellipsoid, centered at the center of the ISS mass, with the long axis along the ISS moving direction. Furthermore, during the proximity and departure phases, the KOS, which is a sphere with a radius of 200 m, is applied as the inviolable area. However, the vehicle cannot reach the SSRMS capture point without entering the KSO. Therefore, as shown in Figure 15, the vehicle is permitted to enter the KOS only through the predefined narrow 10 degree corn shaped corridor. To keep this safety area constraints, the FDIR always predicts the future vehicle trajectory by propagating the current position and velocity, and autonomously triggers a Collision Avoidance Maneuver (CAM) when the anticipated trajectory is largely deviated from the planned orbit. If the predicted trajectory interferes with the safety areas, the automation selects the abort maneuver as the CAM. On the other hand, the vehicle goes into free drift mode if there is no risk of violation but the orbit is just deviated.

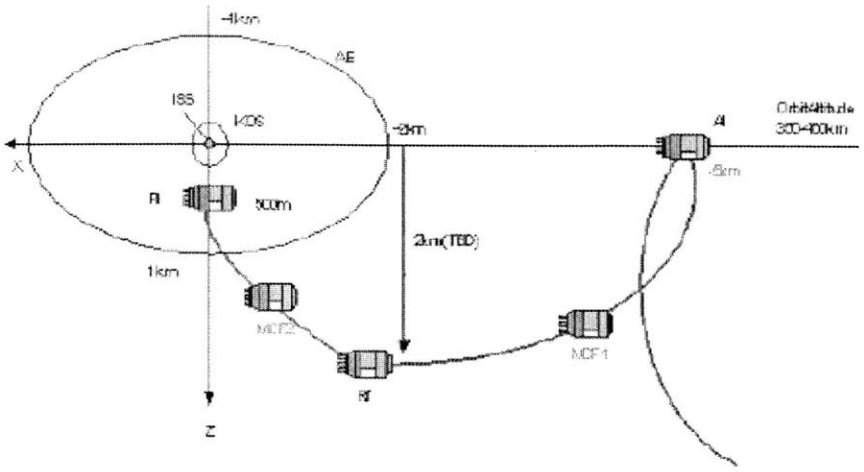


Figure 14: Overview of the AE and KOS [14]

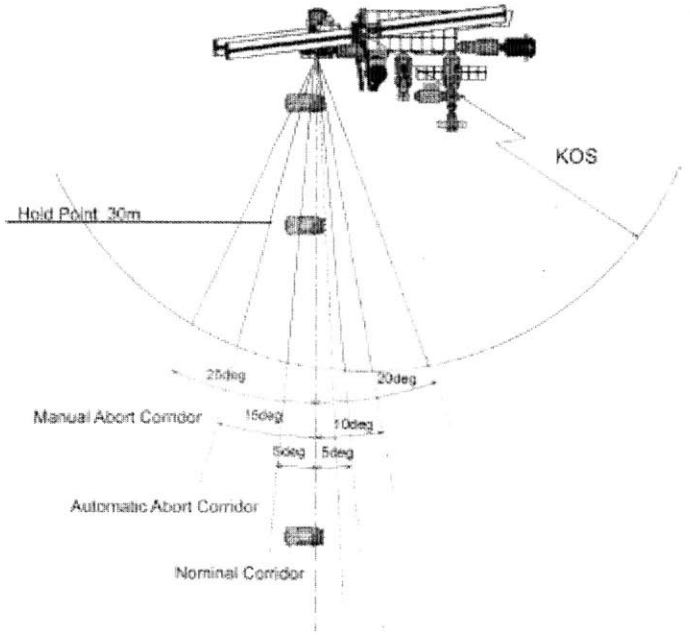


Figure 15: Permitted Approaching Corridor inside the KOS [14]

3.2 New Transfer Vehicle

In 2015, the development of the next generation transfer vehicle was permitted and the vehicle was temporarily named HTV-X [13]. The concept image of the HTV-X is shown in Figure 16. While the existing HTV has succeeded in the ISS resupply mission, two fundamental problems have emerged from the operations.

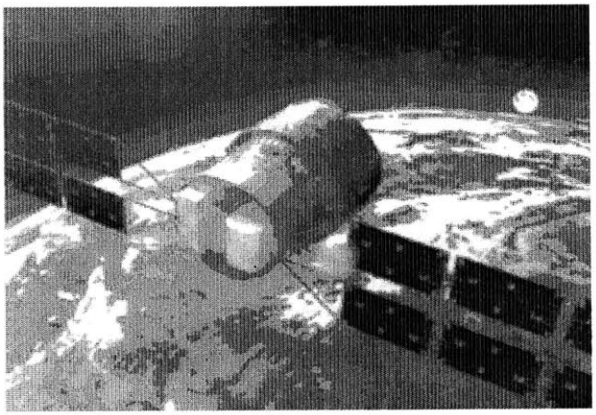


Figure 16: Concept Image of the HTV-X

The first problem is the cost. Although the total cost of the HTV is not extremely expensive comparing to the other existing unmanned transfer vehicles, JAXA has spent almost 67 billion yen on the development of the first HTV and 14 billion yen on vehicle manufacturing. Because of an economic recession in Japan, the whole national space development budget has been gradually decreased. The budget for the ISS resupply mission is not exempted.

The second problem is the operability. With every mission success, the GS crews of the HTV exert a tremendous effort for every operation due to the inflexible and inefficient vehicle behavior. For example, because each component has a redundant one, even a single trivial failure always triggers switching to the redundant component. This switching causes a transient behavior in the system, which finally leads to a suspension of the operation. Because the existing HTV system is conservatively designed, it could sensitively react to the small deviation caused by the transient behavior. The HTV-X is expected to realize

more smooth operation by accepting those trivial changes, which will surely reduce the burden of the GS crews.

Originally, the mission of the HTV-X was to supply goods to the ISS with lower cost and more efficient operation. However, to fully utilize the Japanese space resources and maximize the opportunity to make the Japanese space technology advance, the other two new missions are also additionally defined: to provide a flying technology experimentation platform on LEO and to demonstrate key technology for future moon transfer vehicles.

In the orbital experimentation mission, the HTV-X will provide an opportunity for new space technology experimentation on LEO before the vehicle re-enters the atmosphere and after departing from the ISS. Although it is still unclear what kind of experimentation will be performed, the experimentation of a new space propulsion technology called Electrodynamic Tether (EDT) in the HTV-6 is a good example [19]. Because of the geo-magnetic field, electromotive force is naturally induced on the conductive tether. Due to this electromotive force, by releasing the electrons from one edge of the tether and capturing them at the other edge, electric current also passes through the tether, which finally induces the Lorentz force as the propelent force of the EDT (see Figure 17). This technology is expected to be utilized in future space debris removal missions, because debris will be automatically deaccelerated by the Lorentz force without using any propellant only if the EDT is attached to the debris. In the HTV-6 flight, the EDT technology demonstration is planned on the vehicle. Like this demonstration, the HTV-X is also expected to provide the technology experimentation opportunities for various Japanese space technologists. While the LEO experimentation mission is derived from domestic demand, the technology demonstration for the future lunar transfer vehicle is driven by the international space exploration trend. In 2015, NASA officially announced they plan to move out from the ISS by 2024 and is committed to human exploring in the deeper space like the vicinity of the Moon [14]. Now the launch of the first HTV-X is schedule on 2021, and the

second and third vehicles will have been launched by 2023. Therefore, it should be reasonable to make the HTV-X development a heritage for the future mission.

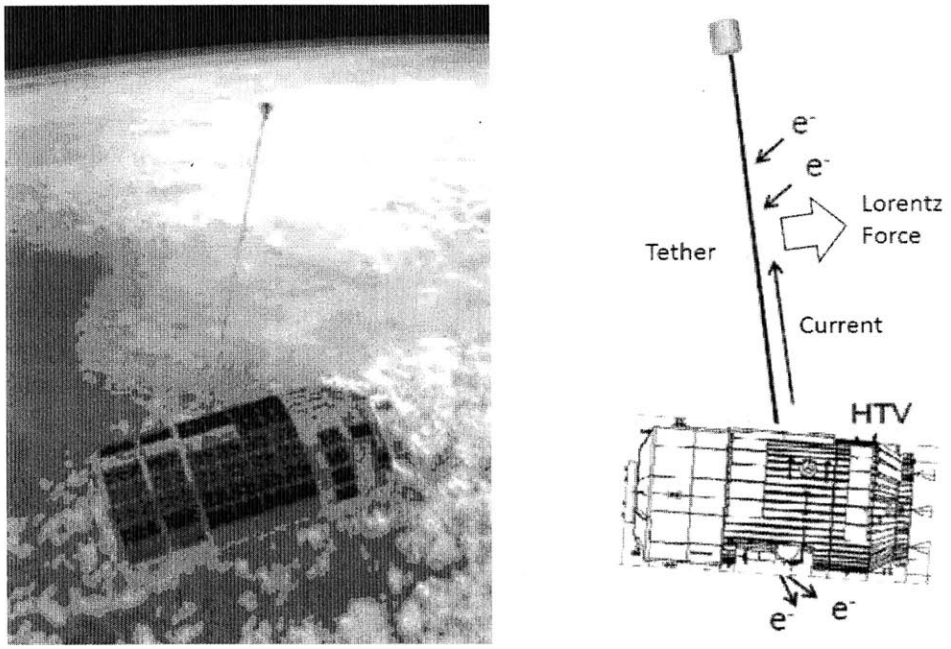


Figure 17: Overview of the Electrodynamic Tether Experimentation on the HTV

3.2.1 Operation Phases

In the ISS resupply mission, JAXA plans to conduct almost the same flight plan as the existing HTV. The maneuver plan will be the exact same, although the duration of the berthing at the ISS will be longer. The only change in the plan is inserting the LEO experimentation before the reentry. The operation overview of the HTV-X is shown in Figure 18.

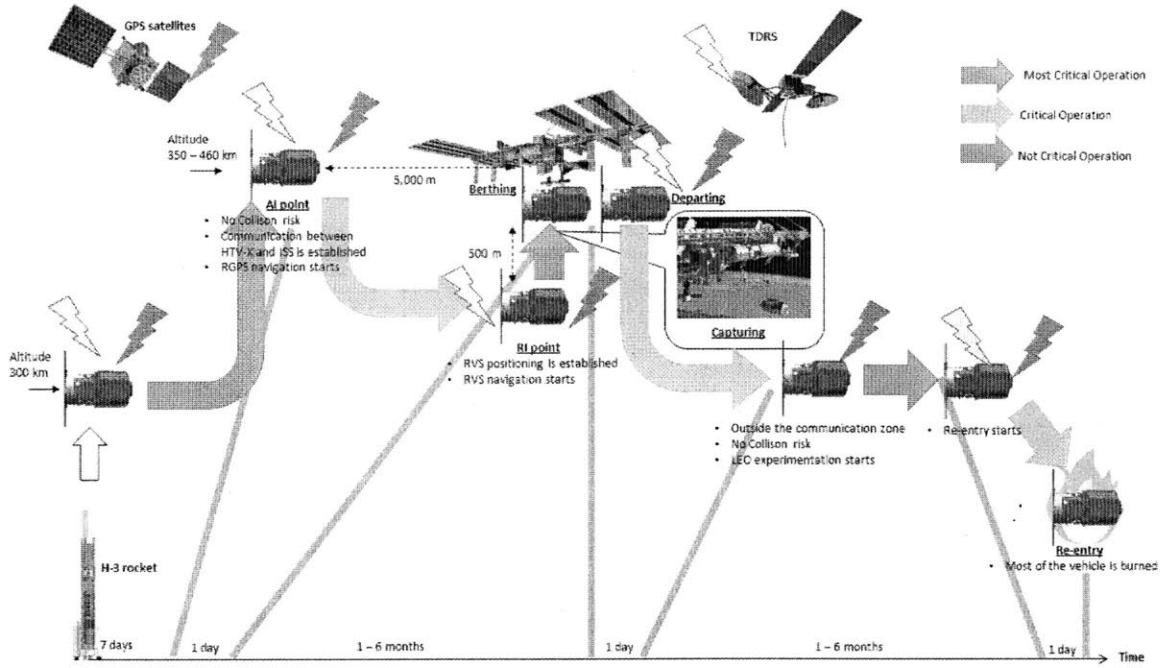


Figure 18: Operation Overview of the HTV-X

3.2.2 System Characteristics

While the development experience of the existing HTV can be utilized in the HTV-X development, various new requirements will be added. Although the System Requirement Review (SRR) has not been finished yet, some architectural studies for the HTV-X have been conducted and a few system architectural characteristics have already been specified.

The most significant change from the existing HTV is to integrate the Avionics Module and Propulsion Module into one module called the Service Module (see Figure 19). Moreover, through this integration, some of the system design will be simplified. For example, the RCS thrusters are aggregated into the Service Module, while in the HTV design the thrusters are distributed around the vehicle body. Although the control algorithm has to be largely modified, the piping from the propellant tanks to the thrusters will be shorter due to this simplification, which results in a cost reduction.

The other simplification is the solar array wing. In the existing HTV, the vehicle body is covered with the solar panel to steadily generate electric power without being influenced by the vehicle attitude. While the power generation of a solar array wing is strongly constrained by the attitude, the cost is expected to be decreased because of the solar panel aggregation. Beside of these two cost reductions, the most significant reduction will be accomplished by removing the ME thrusters. Of course, it requires the engineers to design a new control algorithm to fly with the same orbit without the ME thrusters, but the manufacturing cost will be tremendously reduced. Including the other configuration changes (e.g. the battery configuration simplification and sensor configuration change), JAXA plans to halve the manufacturing cost per vehicle from the existing HTV.

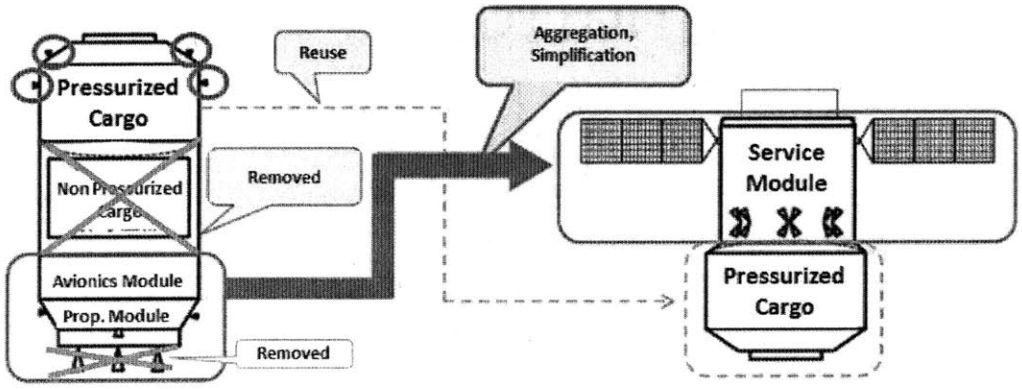


Figure 19: System Configuration Change from the HTV to the HTV-X

While the cost reduction can be realized by the simplification, the biggest issue is how to control the vehicle dynamics without the ME thrusters. In the HTV-X vehicle there will be only the RCS thrusters, but the same large burn maneuver will be required as with the existing HTV flight. To fully utilize the onboard resources and accomplish the orbit control requirements with less resources, JAXA plans to replace the redundant design policy bya new one called the resilient design policy [20]. Due to this new design policy, in the HTV-X propulsion system, there will not be any backup thruster, and therefore all of the 24 RCS thrusters will be always activated during the operation.

Figure 20 shows the difference in making a small maneuver, large maneuver, and rotation between the HTV and HTV-X. Each thruster of the HTV-X has a specific position and cant angle, while in the HTV there are two thruster having the same angle at the same position on the vehicle because of the redundancy. Moreover, the cant angle is neither vertical nor horizontal against the body axis of the vehicle. This characteristic makes it possible to control the vehicle without the ME thrusters. When making a small maneuver, as shown in the top panel of Figure 20, the existing HTV fires the two thrusters directed against the maneuver direction. In the HTV-X, four RCS thrusters will be used to make the same small maneuver. Although each thruster has a specific cant angle, the other forces except for the maneuver direction cancel each other among the four thrusters, and finally the vehicle can fly straight by the maneuver. However, the cancellation means that propellant is uselessly consumed.

Similarly, all of the RCS thrusters will be used for large maneuvers in the HTV-X, while the existing HTV just fires the two ME thrusters (see the middle panel of Figure 20). Of course, in this maneuvering, the same cancel mechanism works to generate one directional force and the useless propellant consumption also occurs. While causing the useless propellant consumption, the cant angle can be advantageous when considering the attitude control too. As shown in the bottom panel of Figure 20, the thrusters used in the attitude control are also used in the above translational maneuvering, because each thruster can generate various directional force. In the existing HTV, on the other hand, the different thrusters are utilized in the attitude control. It means few specialized thrusters are always used in a specific control in the existing HTV. However, in the HTV-X, each thruster can contribute to more varied control. Therefore, the same level control as the HTV can be realized without the ME thrusters in the HTV-X, of course, although the propellant consumption will be more.

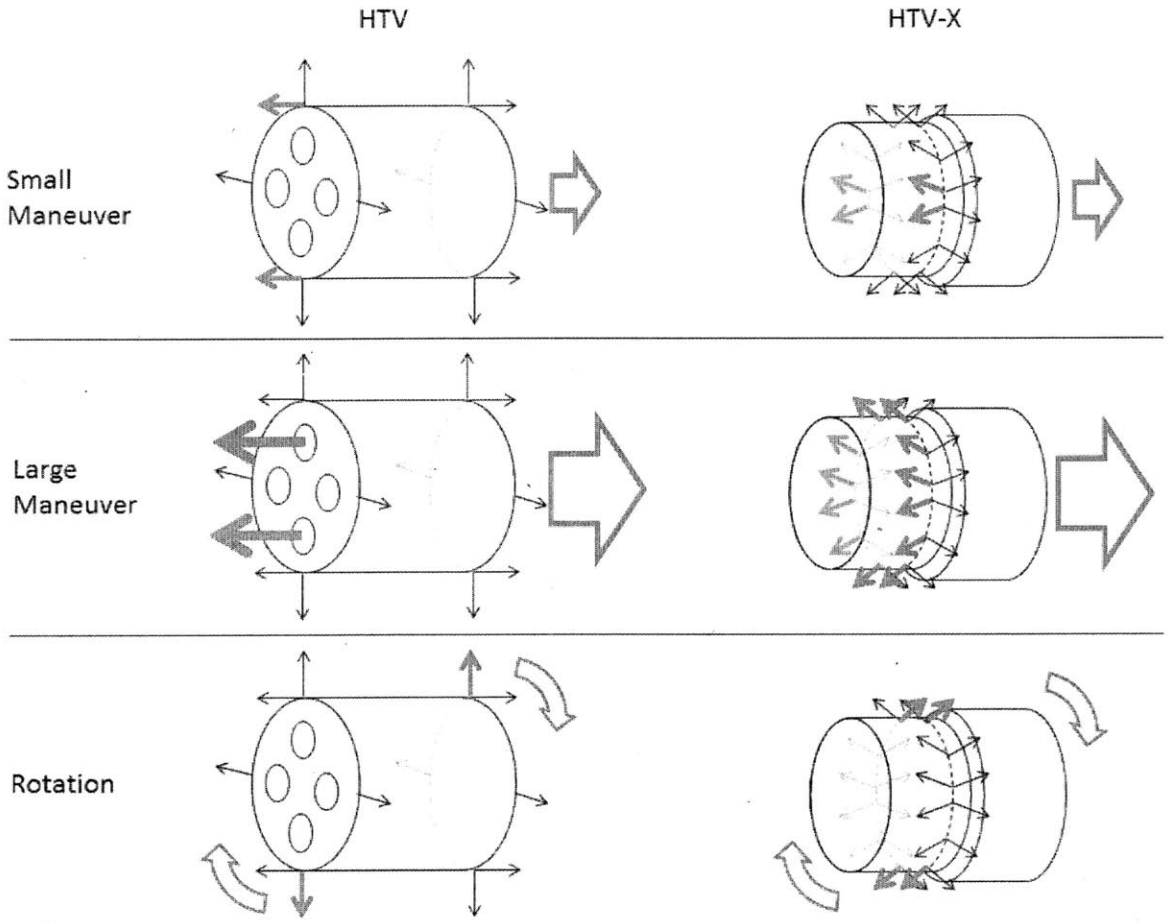


Figure 20: Comparison of Maneuver and Rotation between the HTV and HTV-X

Moreover, this resilient design policy can contribute to more effectively accomplish the required robustness level. When a thruster failure happens in the exiting HTV, the thruster is immediately switched to the redundant one, because the loss of even one of the twelve thrusters results in the collapse of the vehicle attitude control. That means that in the worst case the nominal control can be terminated by only two RCS thruster failures, and the vehicle has to make an abort by the ME thrusters. On the other hand, the HTV-X propulsion system is expected to be more robust against the thruster failure. When a thruster failure happens, the other thruster can compensate the loss of the thrusting force as shown in Figure 21, because one RCS thruster can be utilized in various orbit and attitude controls due to its cant angle. The thruster used for the

compensation is not the best choice to realize a required control, which means less maneuver performance but more propellant consumption, but the attitude of the vehicle can be stabilized by the compensation and somehow keep operating a planned maneuver with lower performance. Theoretically, the HTV-X vehicle can maintain the nominal attitude control even if more than two RCS failures happen, and only if at least eight symmetrical thrusters with respect to the center of the gravity survive, the six degrees of freedom (6DoF) control can be somehow realized.

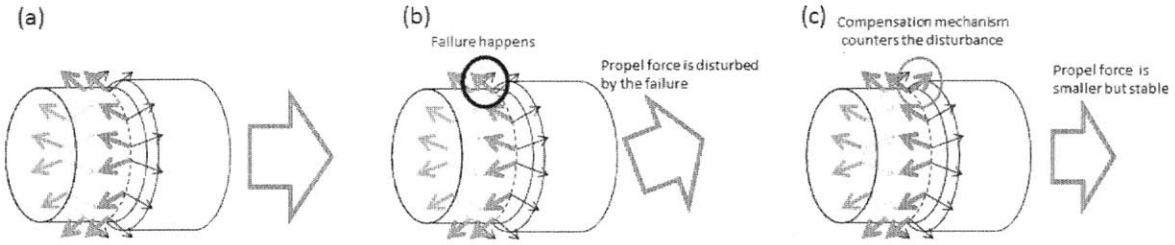


Figure 21: Compensation Mechanism of the HTV-X propulsion system

Because of this robustness of the resilient design policy, the operability of the HTV-X is also anticipated to be improved as well as the cost. For example, when a thruster failure happens, the vehicle can autonomously counter the disturbance from the failed thruster and keep executing the command from the ground. The advantage of this autonomous behavior is not only to keep operating under more than two failures, but also not to require any activation and switching. In the existing HTV, the redundant thruster is required to be suddenly activated when a failure happens and take over the task. During the five HTV operations, this discrete behavior often unexpectedly made the vehicle unstable and finally led to the suspension of the operation. However, the discrete and unstable switching will never happen in the HTV-X, and this will contribute to reducing the operation effort and the mental pressure of the operators preparing for unexpected behaviors.

Moreover, this resilient design can be also regarded as one of the key technology for the future lunar transfer vehicle. For example, if the future lunar station is located at the Earth Moon Lagrangian 2 point (EML2), it

is almost impossible to define an appropriate abort point around the station because of the potential gravitational instability. In other words, the abort in the future lunar transfer vehicle mission means completely giving up the mission, while in the current ISS supply mission the HTV can try again after aborting. Therefore, the future lunar vehicle is expected to somehow maintain the safety for the station without aborting and continuing to approach the station. In this context, obviously the resilient design will show better performance to successfully accomplish the mission.

3.2.3 Problem to be solved

While the resilient design is expected to benefit the cost and robustness of the HTV-X, it will also cause an issue that has never emerged in JAXA's space systems. In the existing HTV, the control performance is always constant even after thruster failure, because the exact same redundant thruster replaces the failed one. When there is no component to be switched from the failed one, the HTV cannot maintain the performance and it suddenly drops (see the left panel of Figure 22). In the resilient design, on the other hand, the performance will be gradually degraded by each failure (see the right panel of Figure 22). From a safety perspective, this control performance is critical, and it is mandatory during the operation to always maintain the performance required in the abort maneuver. In the existing HTV, the performance level required for safety can be assumed to be the same as the nominal control performance level. In other words, the abort cannot be executed, when there is no redundant thruster to be switched and another failure happens. Therefore, the number of failures can be the criterion to judge if the abort should be executed.

In the HTV-X, on the other hand, the abort cannot be executed when the control performance is below the required abort performance. However, it is definitely one of the most difficult tasks to predict how much performance will be degraded by the next failure. One of the possible solutions is to apply the same criterion as the existing HTV, the number of failures, and design the vehicle to maintain the safety performance level or more even if two failures happen. If this countermeasure is adopted, the resources cannot be fully utilized,

but it can give the operators a clear criterion.

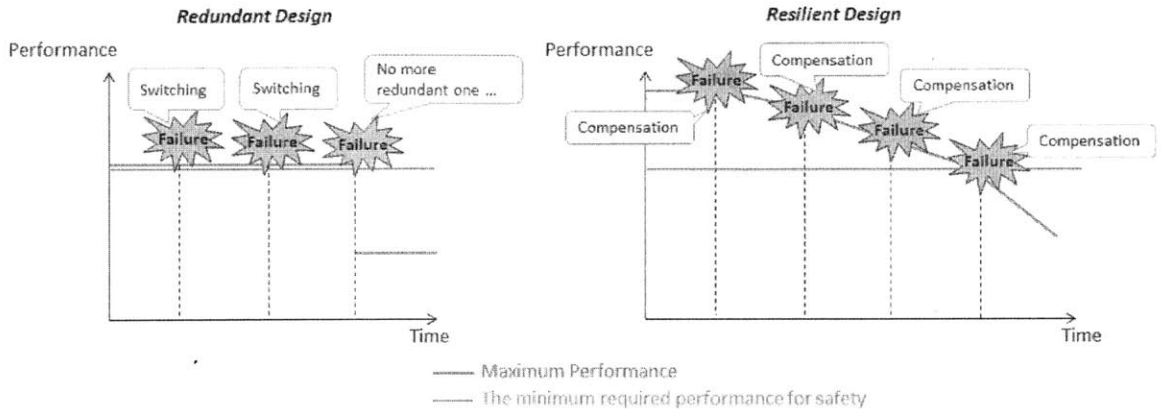


Figure 22: System Performance Variation against Failure in Redundant Design (left) and Resilient Design (right)

However, it should be also extremely difficult in the HTV-X to count the number of failures with certainty. In the existing HTV, the number of failure is increased when the redundant component is activated. However, this approach is not applicable in the HTV-X, because each failure is just controlled as a disturbance and any switching never happens. Therefore, the operators have to give up the clear and quite simple indicator of the failure, the activation of the redundant components, and conduct more complex judgement based on more careful and various performance parameter observation.

In addition, the resilient design also causes another problem because of the compensation mechanism. As introduced above, the more inefficient thruster will be utilized in the compensation. Therefore, the longer the vehicle tries to keep operating with the inefficient thruster configuration, the more propellant is consumed.

Figure 23 shows the result of the simulation about how much the total thruster firing time between the AI and RI can increase when one thruster close failure happens during the AI maneuver. The close failure means that the failed thruster never fires after once being failed. The timing of failure is also modulated from 10 sec before the center time of the AI maneuver to 10 sec after. As shown in the figure, while most

of failures increase the firing time by less than 30 per cent, some failure cases reach more than 75 per cent extra propellant consumption, and the worst case indicates that the vehicle spends almost twice the original consumption.

This simulation result shows that the propellant could be unexpectedly decreased and it could seriously damage the flight plan even if the vehicle looks like it is somehow continuously operating with acceptable control performance. If the propellant runs out, of course, the vehicle will not be able to be controlled at all. This phenomena is similar to the decompensation defined by Hollnagel et al [21]. This decompensation in the HTV-X should be carefully monitored and the human operator will be expected to take an appropriate action to avoid the critical situation.

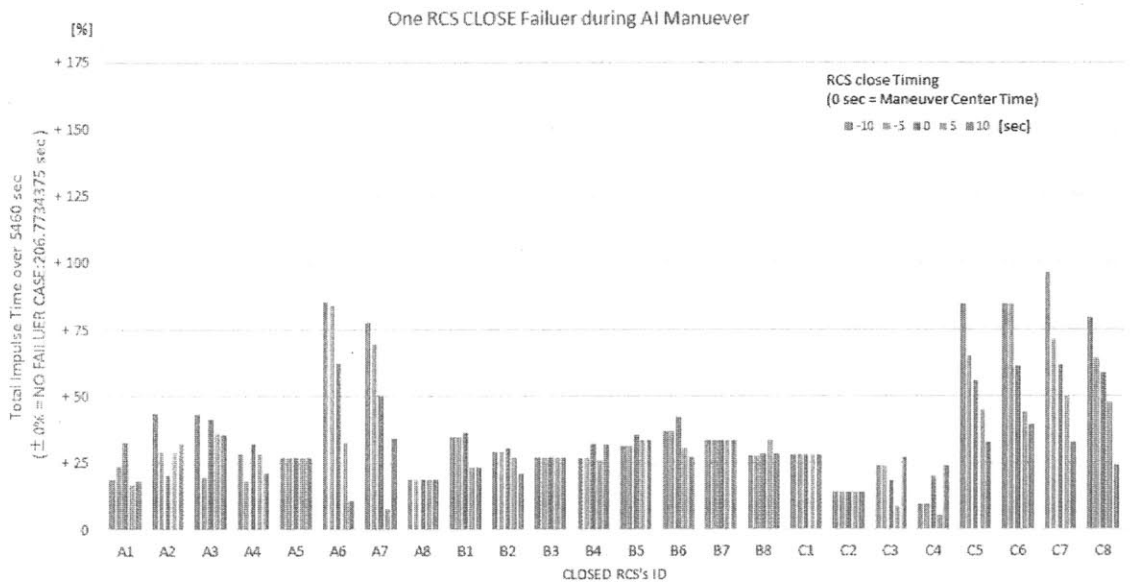


Figure 23: Impulse Time Change by one RCS Thruster Close Failure during AI maneuver

In short, the role of the human operators will be quite different in the HTV-X, although the mission concept and flight plan are the exact same as the existing HTV. The operators will be required to supervise more carefully the system performance, judge what actually happens inside the system while considering various parameters, and finally determine the adequate next action to guide the system to a successful state. Without

understanding these important changes in the relationship between human operator and computer system, any progress in the operability cannot be expected and rather a serious accident damaging the reputation of JAXA might even occur.

Chapter 4. Using STPA in New Vehicle Concept Design

In modern complex systems, implementing safety features in the later design phase is more difficult, because the design flexibility is rapidly lost as the design phase proceeds and consequently design change in the later phase is more expensive. Therefore, designing safety in the early phase is quite important for the success of developments. As discussed in section 2.3, the early system safety design can be effectively realized by STPA, while the traditional methods are only available in the later design phase.

In the HTV-X system development, the engineers need to newly create the system concept design, although the existing HTV specification is available. Therefore, applying STPA in the concept design will significantly contribute to leading the HTV-X project to success. Fortunately, the design is still fluid because even the System Requirement Review (SRR) has not been finished yet. Thus, it is feasible to feedback the result of concept design analysis by STPA into the actual HTV-X system design.

As introduced in section 3.2, the HTV-X project has unique missions and stakeholder needs which are different from the existing HTV. To satisfy these new project characteristics, the new design policy called resilient design policy is introduced. This new policy will differentiate the concept design of the HTV-X from the existing HTV even in the same ISS resupply mission. Therefore, one of the key in the analysis is if the characteristics of the resilient design can be described by STPA and the analysis successfully guide the improved concept design.

On the other hand, because again even the SRR has not been finished yet, any specification document about the HTV-X system had not existed yet. Of course, the existing HTV design documents are available, which can be utilized as useful references to create the HTV-X concept design. Because of the differences between the existing HTV and HTV-X systems, however, the only highest level system concept can be partially picked up from the existing HTV specification and customized for the HTV-X system. Therefore, STPA is

expected to effectively guide this concept design creation process from safety perspective.

Fortunately, this concept design generation by STPA has been already demonstrated in an automotive system by Thomas et al 2015 [22]. In the previous study, a generic Shift-By-Wire concept design is iteratively refined from safety perspective based on a system-theoretic model based approach. . This iterative design refinement process will be also advantageous in the HTV-X design analysis, because the initial HTV-X system design can be once roughly created based on the existing HTV and the basic HTV-X system concept and then it can be matured by this process.

The purpose of this analysis is to demonstrate the effectiveness of the safety guided concept design analysis based on STPA by actually creating the concept design of the HTV-X. First of all, in section 4.1, the scope for the analysis is defined, and then the concept design generation methodology is described in section 4.2. After that, the actual application result in the HTV-X is introduced in detail in section 4.3. Finally, the discussion and conclusion about this analysis is given in section 4.4.

4.1 Analysis Scope

As introduced in section 3.2.1, the operation of the HTV-X consists of six phases. Here the proximity operation phase is focused in this analysis, because it is the most critical and complex operation. In the proximity phase, once the vehicle departs from the AI point, the onboard automation basically conducts all of the controls without any command from the ground until the vehicle reaches at the 10 m below point from the ISS, while in the other phases all maneuvers except for the autonomous abort are triggered by the commands.

Moreover, in this autonomous approaching operation, the collision with the ISS is more concerned than the other phases, because the vehicle autonomously penetrates the KOS through the permitted corridor and

approach to the ISS until the 10m below. While this critical operation is basically conducted by the automation, the human operators are expected to adequately intervene the autonomous operation. From human operator perspective, their role during the proximity operation phase is really different from the other phases. In the proximity operation, the operators are expected to supervise and guide the autonomous approaching operation, while they can almost fully control the vehicle behaviors by the manual commands in the other phases. Therefore, in order to effectively contribute to the successful HTV-X system development, the human supervisory system design in the proximity operation will be a good scope of this early safety design analysis.

Because the final approaching orbit of the existing HTV was already agreed between NASA and JAXA, the same orbit will be applied for the HTV-X operation, which means that the nominal maneuver plan in the proximity phase will not be different between the HTV and HTV-X. Thus, in this study the nominal operation scenario for the HTV-X is defined based on a fundamental system specification document of the existing HTV called mission press kit [3]. In the scenario, before starting the proximity operation, all of the vehicle health check has been finished, and the RGPS navigation has been also established. Between the AI and RI points, four maneuvers are executed in total: Approach Initiation maneuver (AI maneuver), the first Mid-Course maneuver (MC1 maneuver), the maneuver prior to R-bar insertion (RI' maneuver), and the second Mid-Course maneuver (MC2 maneuver). The AI and RI' maneuvers are relatively large thrusting maneuvers to drastically change the flying trajectory, while the MC1 and MC2 maneuvers are small thrusting maneuvers aimed for precisely adjusting the orbit after those two large maneuvers. After reaching at the RI point, the vehicle navigation is switched from the RGPS to the RVS, which triggers off the feedback position control to gradually approach to the 10 m below point from the ISS called hold point. These operation steps are described in detail in time series as follows;

(1) After NASA GS confirms the ISS status and the duty time of ISS crew, it finally gives the final approach

permission to JAXA GS

(2) JAXA GS issues the approach initiation command by which the autonomous successive approaching maneuvers are started.

(3) The vehicle automation calculates the control amount for each maneuver based on the predefined approaching orbit and current RGPS data.

(4) The vehicle executes the AI maneuver with the calculated maneuver plan.

(5) After the AI maneuver, the vehicle automation updates the maneuver plan based on the RGPS data.

(6) The vehicle executes the MC1 maneuver with the updated maneuver plan.

(7) After the MC1 maneuver, the vehicle automation updates the maneuver plan based on the RGPS data.

(8) The vehicle executes the RI' maneuver based on the updated maneuver plan.

(9) After the RI' maneuver, the vehicle automation updates the maneuver plan based on the RGPS data.

(10) The vehicle executes the MC2 maneuver based on the updated maneuver plan

(11) The vehicle reaches at the RI point.

(12) When a reflected laser from the ISS is captured by the RVS at the RI point, the vehicle automation switches the navigation data source from the RGPS to the RVS, and subsequently starts to vertically rise up to the hold point by the feedback control

(13) The vehicle finally reaches at the hold point and stays there.

In this operation sequence, there are three types of human operators: NASA GS, JAXA GS (GS crew), and ISS (ISS crew). However, the NASA GS does not provide any control for the vehicle, and just give the permission to the JAXA GS before starting the approaching maneuvers. Although the GS and ISS crews

also seem not to actively intervene the automation behaviors in the nominal scenario, indeed they can issue a few commands to suspend the operation or make the vehicle quit approaching to the ISS. The abort command which can be issued by either of them makes the vehicle execute the abort maneuver and consequently fly back to the AI point. The hold command is also available for both crews, and it makes the vehicle stay and keep the current distance from the ISS during the R-bar approach. Although the abort maneuver is one of Collision Avoidance Maneuvers (CAM), there is another CAM called passive CAM. The passive CAM command is provided by the only GS crew, and when receiving the command the vehicle just stops executing maneuvers and drift as maintaining the nominal attitude. The passive CAM is used when the current orbit does not violate the KOS but the vehicle is under an off-nominal condition. By using these commands, the GS and ISS crews guide the vehicle to safe states.

In addition, the vehicle automation can also autonomously conduct the abort maneuver by the Safety Net function. When the KOS violation is detected, the automation immediately executes the maneuver without any command. Moreover, another full autonomous control is the attitude control. Because each RCS thruster is fixed on the vehicle body with a specific direction, the direction of maneuvers is always influenced by the vehicle attitude. Therefore, the vehicle always has to maintain a nominal attitude to finish each maneuver as expected, because each maneuver calculation premises the nominal attitude. These two full autonomous controls also work in parallel with the above human operators' control to keep the system safe.

Although a part of the concept design of the HTV-X is already clear due to the existing HTV design as discussed above, the resilient design policy will introduce completely new behaviors under off-nominal conditions which has never been seen in the existing HTV. As discussed in section 3.2.2, when a thruster failure occurs, the vehicle keeps operating with degraded control performance due to the compensation mechanism, while typical switching to a redundant component happens in the existing HTV. To adapt the system to this new off-nominal behavior, the intervention by the ISS and GS crews will be also drastically

changed as well as the autonomous control. Even if any new control is not added to those human controllers, their judgement process will be significantly different at least, because some of the system indicators which were useful in the existing HTV (e.g. switching to the redundant RCS thrusters) are no longer available in the HTV-X. Consequently, this new design policy will lead to a quite different system design. However, no one has clarified how the system design should be changed. Therefore, it will significantly contribute to the actual HTV-X development to safely integrate the unique off-nominal behaviors into the concept design by STPA.

4.2 Concept Design Generation based on STPA

To create the concept designs for modern complex systems from safety perspective, STPA is the best methodology. Because detailed design is not mandatory in the analysis, STPA is applicable even in concept designs. Moreover, a concept design can be described by a control structure and it can be directly refined by finding missing elements in the control loops through identifying unsafe control actions and essential safety constraints. Therefore, applying STPA for the concept design analysis of the HTV-X is a reasonable solution to integrate safety into the system from the beginning of the development. Fortunately, a previous study has already demonstrated a concrete method to utilize STPA in concept design analysis and the steps to analyze the system design based on STPA are already defined as follows [22];

(1) Define system accidents and hazards

(2) Create initial control structure

(3) Identify initial unsafe control actions

(4) Derive safety constraints from unsafe control actions, and use the safety constraints to revise the control structure and design

(5) Identify high-level causal scenarios, and identify controls to eliminate or mitigate the high-level

scenarios

(6) Formalize the unsafe control actions to identify any missing or conflicting UCAs and constraints, resolve the identified conflicts, and revise the safety constraints

(7) For scenarios not already controlled, identify more detailed causes by incorporating additional design detail, and provide controls for the new causal factors identified

The first and second steps are the fundamental tasks to understand a system and start safety analysis. In the third step, unsafe control actions are identified by the four potential unsafe control patterns defined in the general STPA framework. Subsequently, safety constraints are derived from the identified unsafe controls. Through considering how the constraints can be realized in the system, potential critical design decisions are elicited. The following questions can support this elicitation process:

- Does the initial control structure allow the controller to monitor the conditions in the constraints?
- Do additional control actions need to be added to achieve or enforce the constraints?
- Are there other controllers that may interfere with or violate the constraints?

By applying these questions, the initial control structure can be revised based on the safety constraints. After that, causal scenarios are identified as assuming the cases violating the constraints. Based on the scenarios, the system design can be again improved by applying the following questions:

- How does the controller determine the information referenced in the scenarios?
- Are additional controls needed to prevent identified flaws?
- Are new controllers or new functionalities needed?
- Do new constraints need to be defined?

The answers for these questions can guide system engineers to introduce new system elements to prevent the scenarios. Although the initial system design has been already modified based on each UCA, the design can be further improved by analyzing the interactions among the UCAs. In the next step, the context table developed by Dr. Thomas is applied to analyze the interactions [23] . In the context table, the possible combinations of control execution conditions are holistically surveyed. From the combinations, missing control execution conditions emerge, and it is investigated if each control action can be hazardous under each missing condition. Moreover, by using the context table, it is also possible to identify conflicted unsafe control actions. For example, if two unsafe control actions simultaneously happens under an identical condition but fundamentally conflict against each other like providing a control action and not providing the same one, the safety constraints derived from them would lead to an inconsistent system design, which would potentially doom the system to the accidents. To prevent such situations, the safety constraints should be revised as eliminating the conflicts. Finally, based on these missing unsafe control action identification and control action confliction, more refined system design recommendation will be proposed.

In general system engineering process, system designs are getting more detailed through an iterative design cycle. The integrated approach to system concept design and hazard analysis also enables engineers to gradually refine the concept design from safety perspective. Although the concept design of the HTV-X still includes some ambiguity especially in integrating the resilient characteristics into the off-nominal vehicle behaviors, this safety guided system design approach can lead to a sophisticated concept design through the design refinement process.

4.3 HTV-X Concept Design Analysis

To create the safer HTV-X system design that is capable of handling the off-nominal behaviors derived from the resilient design policy, the concept design was refined based on the safety guided design process introduced in section 4.2. Although the initial design was not so different from the existing HTV (see section

4.3.1 and 4.3.2), the unique system characteristics emerged due to the new design policy after analyzing its off-nominal behaviors based on STPA (see section 4.3.3, 4.3.4, and 4.3.5). Finally, the concept design was sophisticated as it can safely handle the new system features and successfully complete the operation (see section 4.3.6). The detailed results are shown in the following sections.

4.3.1 System Accidents and Hazards

As the first step of the safety guided design process, the system accidents and hazards are identified. For the HTV-X system during the proximity phase, the following simple two accidents were defined:

- [A-1] Collision with the ISS
- [A-2] Loss of the resupply mission

The first accident is set to maintain the safety for the ISS. This accident should be most concerned in the HTV-X project, because the accident can result in not only loss of the only space habitation station for human being but also loss of the ISS crews. Although the first accident should be more critical for the HTV-X operation, the second accident, loss of the resupply mission, is also a tremendous loss. If the opportunity to transport the goods to the ISS is completely lost, it would be recognized as the serious failure of the HTV-X project among the stakeholders, which will finally damage the credit of JAXA from the ISS community. Subsequently, the hazards leading these two accidents were defined as follows:

- [H-1] The vehicle's orbit violates the KOS
- [H-2] The vehicle is deviated from the planned orbit
- [H-3] The vehicle is under uncontrollable state
- [H-4] The vehicle keeps approaching when the ISS cannot accept the approaching operation

The H-1 and H-2 are the hazards related to the physical vehicle orbit. The KOS is the most critical safety

zone to avoid the collision risk with the ISS, and it is mandated for all of the ISS related vehicles not to violate the zone except through a pre-permitted corridor. Moreover, even when the HTV-X vehicle orbit does not violate the KOS, the only predefined flight orbit is permitted as an approaching route to the ISS. It means the vehicle has to quit approaching to the ISS if the vehicle orbit is deviated from the predefined route. Basically, the orbit deviation can be recover by the abort maneuver unless the deviation is so large, and the vehicle can restart the approaching maneuvers from the AI point. However, it costs the operators additional effort. If the deviation is so large and the orbit is totally unexpected, a lot of propellant would be consumed for the recovery and in the worst case the recovery operation might be terminated. In addition to these vehicle orbit dynamics related hazards, if the vehicle unexpectedly falls into a mechanically uncontrollable state (e.g. loss of power, and loss of propulsion), it could cause both accidents. While the vehicle health status is a critical factor for the safe operation, similarly, the condition of the ISS is also important to avoid the accidents. If the vehicle keeps approaching when the ISS is not ready for the approach, the vehicle might have to give up the mission or might even enter the collision course. For the HTV-X systems, to prevent these hazards will be top priority for safety in the proximity operation phase.

4.3.2 Initial Control Structure

The second step is to create the initial control structure to describe fundamental system elements in the HTV-X system. Figure 24 shows the control structure for the proximity phase. As shown in the control structure, there are four subsystems: NASA GS, JAXA GS, ISS, and vehicle, and three controllers: GS crew, ISS crew, and vehicle automation provide 8 control actions in total. The control actions are listed in Table 1. At the beginning of the operation, the GS crew provides the approach initiation command to start the nominal approaching maneuvers. After receiving the command, the vehicle automation provides the nominal maneuvers for the vehicle dynamics based on the maneuver plan, and the vehicle flies to the RI point. When capturing the reflected laser from the ISS, the vehicle automation autonomously starts the R-

bar approaching control, and the vehicle gradually approaches to the ISS. Therefore, in the nominal scenario, the ISS and GS crew do not provide any control action except for the approach initiation provided at the very beginning of this sequence.

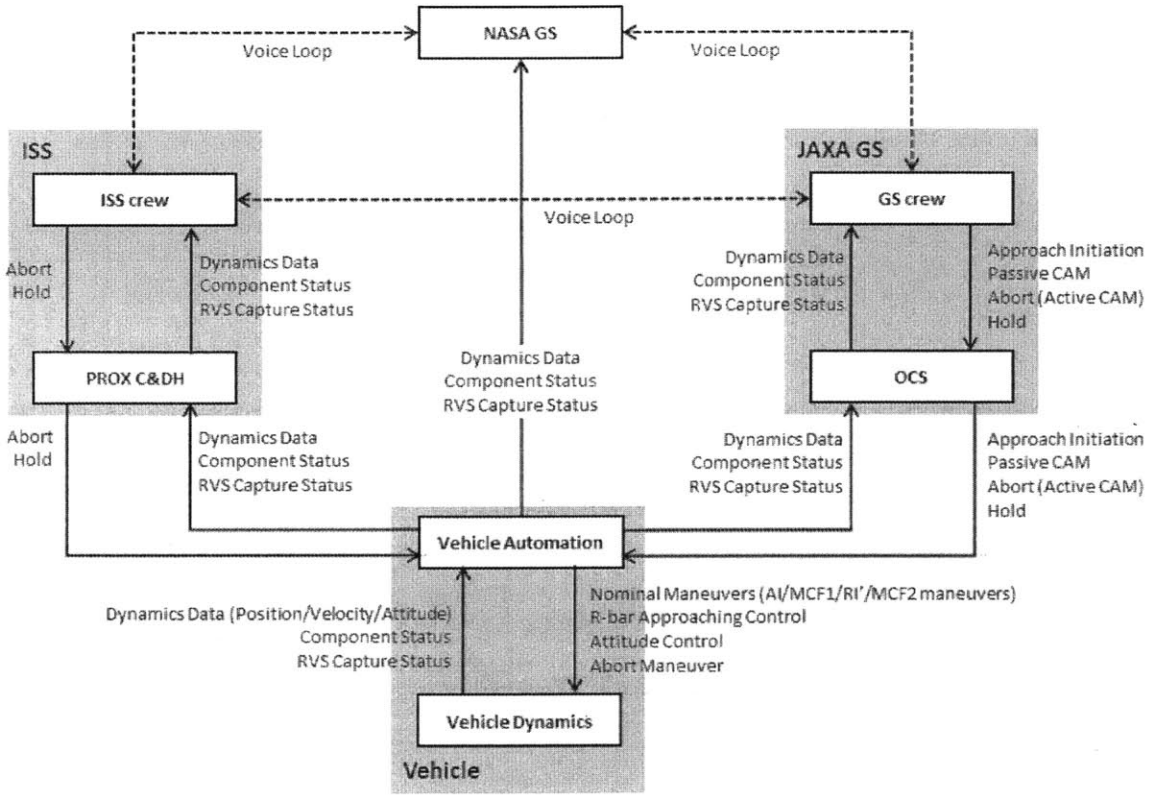


Figure 24: Control Structure Diagram for the Final Approaching Phase

Table 1: Control Action List

#	Control Action	Description
1	Approach Initiation	Initiate the successive nominal maneuvers (AI, MC1, RI', MC2)
2	Passive CAM	Make the vehicle drift as maintaining its attitude
3	Abort	Make the vehicle execute the abort maneuver
4	Hold	Make the vehicle maintain the current distance from the ISS
5	Nominal Maneuvers	Execute the nominal maneuvers (AI, MC1, RI', MC2)
6	R-bar Approaching Control	Execute the feedback control to gradually approach to the ISS
7	Attitude Control	Maintain the vehicle nominal attitude
8	Abort Maneuver	Execute the abort maneuver

On the other hand, to handle off-nominal situations, the human controllers are expected to properly use three types of control actions: abort, hold, and passive CAM. While both GS and ISS crews can issue the abort and hold commands, the passive CAM command can be provided by the only GS crew. The abort command is literally the command to make the vehicle execute the abort maneuver. The hold command is only available in the R-bar approaching operation. When the command is provided the vehicle automation once suspends the approaching control and then maintains the current distance from the ISS by the feedback control. When the passive CAM command is provided, the vehicle automation immediately stops the nominal maneuvers and starts free drift as maintaining the nominal attitude.

In addition to these three control actions, the vehicle automation can also provide the abort maneuver without receiving the abort command. When the automation detects the KOS violation, it autonomously provides the control action to avoid the collision with the ISS. Moreover, during the proximity operation, of course, the vehicle automation always provides the attitude control to maintain the nominal attitude.

For the feedbacks against the control actions, the dynamics data, component status, and RVS capture status are available. The dynamics data represents the physical vehicle's position, velocity and attitude. The component status shows each component's condition inside the vehicle. If a failure happens, it can be identified from the component status data. Because the laser capture is an important control transition signal, it is monitored by the RVS capture status. These data are delivered to all system elements including the NASA GS from the vehicle dynamics.

4.3.3 Initial Unsafe Control Actions

Based on the system hazards and control actions, the unsafe control actions which can lead the system to the hazards were identified by applying the four off-nominal patterns. To smoothly identify the unsafe control actions, in this study the execution conditions for each control action were also analyzed. Take the nominal maneuvers provided by the vehicle automation as example. The condition table for the nominal

maneuvers is shown in Table 2. The table format follows the formalism used in SpecTRM-RL (Specification Tools and Requirements Methodology - Requirement Language) [24], because it can guide a rigorous condition definition and the definition is intuitive for engineers. Obviously, one of the execution conditions for the nominal maneuvers is that the approach initiation command has been already provided before the nominal maneuvers start. Moreover, the vehicle orbit should not be deviated from the planned orbit, and the vehicle attitude should be also nominal. Since the vehicle has to suspend the nominal maneuvers and perform the abort maneuver if any critical failure happens, the vehicle component status should not indicate any failure before the maneuvers. Similarly, the ISS status should be ready for the approaching and docking. Considering the off-nominal behaviors, the passive CAM and abort maneuver have to be prioritized more than the nominal maneuvers, because any additional maneuver during the passive CAM or abort maneuver can lead to the KOS violation. Therefore, the nominal maneuvers should be prohibited when the vehicle is executing the passive CAM or abort maneuver. Due to the resilient design policy, as discussed section 3.2.3, the vehicle control performance is no longer stable. If it is less than the performance required for the nominal maneuvers, the vehicle would not complete the maneuvers, and furthermore would go to an unexpected state once initiating the maneuvers with the degraded performance. Therefore, the control performance should be more than the required performance before the nominal maneuvers are initiated.

Table 2: Condition Table for the Nominal Maneuvers

Approach Initiation is Provided	T
Vehicle Orbit = Deviated	F
Vehicle Attitude = Nominal	T
Vehicle Component Status = Ready	T
ISS Status = Ready	T
Vehicle Mode = CAM	F
Control Performance > Nominal	T

The execution conditions for the other control actions were also respectively analyzed as with the nominal maneuvers. However, note that it should be quite difficult to identify the complete conditions in this step. Generally, it is impossible to create the complete design at the beginning of system design. Instead, the design including the condition tables should be iteratively refined through the design process. Therefore, in this step, the execution conditions should be independently identified for each control action, and the completeness should be discussed later in the context table analysis.

Finally, based on the first version condition tables, each control action was analyzed by the four potential unsafe patterns. As a result, 40 unsafe control actions were identified in total from the initial HTV-X concept design. Table 3 shows the result of the analysis about the nominal maneuvers. As shown in the table, when the maneuvers are not provided, it is expected not to cause any hazard. Indeed, if the nominal maneuvers are not provided when the vehicle is at the AI point, the vehicle will stay there. Even if one of the maneuvers is suddenly cancelled after the vehicle initiates the successive maneuvers, the vehicle automation will conduct the abort maneuver when the orbit violates the KOS. Therefore, not providing the nominal maneuvers cannot cause any hazard.

On the other hand, the other three providing patterns can cause the hazards. When all of the condition is satisfied, of course, proving the nominal maneuvers can never be hazardous. However it can be hazardous if one of the conditions is not satisfied. Therefore, the unsafe control actions were identified by considering when each condition is not satisfied. In the first case (UCA-5.1), the vehicle can violate the KOS or fly to an unexpected orbit if the nominal maneuvers are provided when the orbit is deviated from the planned orbit. Although the MC1 and MC2 might be able to recover the deviation, the vehicle cannot keep following the planned trajectory if the deviation is large. Potentially, it can result in the situation that the vehicle automation forcefully tries to keep executing the nominal maneuvers but cannot adequately update the maneuver plan due to the large orbit deviation. Finally, it will cause H-1 or H-2 hazard. Because the nominal

attitude is premised in any maneuver calculation, the nominal maneuvers under an off-nominal attitude can lead an unexpected trajectory and cause H-1 or H-2 as defined in UCA-5.2. In the third unsafe case (UCA-5.3), providing the nominal maneuvers when the vehicle is executing the CAM (abort or passive CAM) can cause H-1, H-2 or H-3. Because the CAM is executed when there is a risk in the operation, it can retrieve the risk and endanger the safety for the ISS. Moreover, as shown in UCA-5.4, the vehicle can be in an uncontrolled state if the maneuvers is provided when the vehicle component status indicates an abnormality, because the vehicle behavior cannot be predicted after executing the maneuver under the abnormal condition. As discussed in section 3.2, in the resilient design, the control performance is no longer stable, and it can be degraded by the vehicle condition. Therefore, the nominal maneuvers can potentially be executed with the degraded control performance which is less than the required level to complete the maneuvers. Finally it can lead to H-1, H-2, or H-3 as indicated by UCA-5.5. The UCA-5.6 is related to the order of commands. After the GS crew clears various status checks to confirm the vehicle healthiness, the approach initiation command is provided. Thus, before receiving the approach initiation or so long after it is provided, the nominal maneuvers can be inadequate against the surrounding conditions because the permission is ignored or no longer effective. In addition, too long maneuver execution (UCA-5.7) can also happen when the control performance is degraded in the HTV-X. When the vehicle control does not work as expected, the compensation mechanism autonomously tries to recover the control. This compensation mechanism can lead to applying the maneuvers longer and consequently consuming more propellant. If the compensation is too much, a damage can be caused in the thruster firing too long or too much propellant consumption can cause loss of propulsion. In these unexpected conditions, of course, the vehicle will go to an uncontrolled state. This unsafe control action never happen in the existing HTV, because the compensation mechanism is not designed in the existing vehicle. That is to say, the unique off-nominal behavior of the resilient design was successfully described by the STPA framework.

The same analysis result for the other control actions is shown table A-1 in appendix A.

Table 3: Unsafe Control Action Table for the Nominal Maneuvers

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
Nominal Maneuvers	The vehicle stay at the AI point Or -> No.10	UCA-5.1: Providing the nominal maneuver when the vehicle orbit is deviated or violates the KOS can cause H-1, or H-2 UCA-5.2: Providing the nominal maneuver when the attitude is not nominal can cause H-1, or H-2 UCA-5.3: Providing the nominal maneuver when the vehicle is executing abort or passive CAM can cause H-1 or H-2 UCA-5.4: Providing the nominal maneuver when the vehicle status is not ready can cause H-1, H-2, or H-3 UCA-5.5: Providing the nominal maneuver when the control performance is less than the AI maneuver performance can cause H-1, H-2, or H-3	UCA-5.6: Providing the nominal maneuvers when the ISS is not ready (= before the approach initiation is not provided) can cause H-4	UCA-5.7: Applying the nominal maneuvers too long can cause H-3

4.3.4 Initial Safety Constraint and Causal Scenario

As a next step, the safety constraints to prevent the identified unsafe control actions are defined. By translating the 40 unsafe control actions identified in section 4.3.3, in total, 21 safety constraints were defined in the HTV-X concept designs. To simplify the constraints, 10 of 21 constraints were described as enforcing to prevent multiple UCAs, although the other eleven constraints are derived by just rephrasing a single UCA. For example, the UCA-5.7: Applying the nominal maneuvers too long can cause H-3 is an unique unsafe control action in the resilient design, and the other several controls also can be applied too long or too short like UCA-5.7. Therefore, to prevent such undesirable control execution with wrong duration, the following safety constraint should be defined: each control must be executed within an acceptable thrusting range. The other safety constraints are shown in table A-2 in appendix A.

Furthermore, the control structure is revised based on the safety constraints. Take "each control must be executed within an acceptable thrusting range" as example. The acceptable thrusting range is still not clear, because any detailed design has not existed yet. Although the range should be clearly defined in the later development phase, an additional information should be monitored at least to estimate the current thrusting amount. In reality, it is quite difficult under weightless environment to directly monitor how much propellant is consumed in the vehicle propellant tank. On the other hand, it is possible to count the firing time of each thruster and indirectly estimate the amount. The estimation cannot be super accurate, but can be utilized in judging the over propellant consumption. Therefore, from this discussion, the thruster firing time was added on the feedbacks from the vehicle dynamics to vehicle automation as a new system element.

Likewise, the other constraints were also analyzed (see table A-3 in appendix A) and nine new elements were added in total on the control structure as listed on Table 4. Figure 25 shows the updated control structure. As discussed above, the thruster firing time is introduced as a new feedback from the vehicle automation. Moreover, the other important new feature proposed by this analysis is that the OCS / PROX C&DH

provides new feedbacks to the GS crew / ISS crew based on the existing raw data from the vehicle. For example, the attitude anomaly and KOS violation warming were added as new feedbacks. These feedbacks can be easily calculated from the dynamics data, and the dynamics data had existed before the analysis. However, is the dynamic data itself what the human operators really want to know to guide the vehicle? The critical information for the operators is definitely whether the attitude is off-nominal or nominal, and the orbit violates the KOS or not. In order for the computer system to effectively support the human operators, rather than just providing the raw data, the feedback to the operators should make them easily aware of the critical changes in the system like the attitude and orbit anomalies. As described in this discussion, considering how to enforce the safety constraints as a whole system consequently led to those important human - automation interaction designs.

Table 4: Control Structure Revision List in the First Iteration

#	Revised Control Structure	Related Constraints
1	"Attitude Anomaly" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	SC-1
2	"Vehicle Mode" should be added on the feedback from the vehicle automation to GS/ISS crew through the OCS/PROX C&DH	SC-2
3	"Vehicle Status Anomaly" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	SC-3
4	"Thruster Firing Time" should be added on the feedback from the vehicle dynamics to the vehicle automation	SC-4, 9, 10
5	"Thruster Firing Time" should be added on the feedback from the vehicle automation to the OCS and PROX C&DH	SC-4
6	"Control performance" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	SC-4
7	"KOS Violation Warning" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	SC-5
8	"Orbit Deviation Warning" should be added on the feedback from the OCS to GS crew	SC-11
9	"ISS Status" should be added on the voice loop between the ISS and GS crew	SC-13

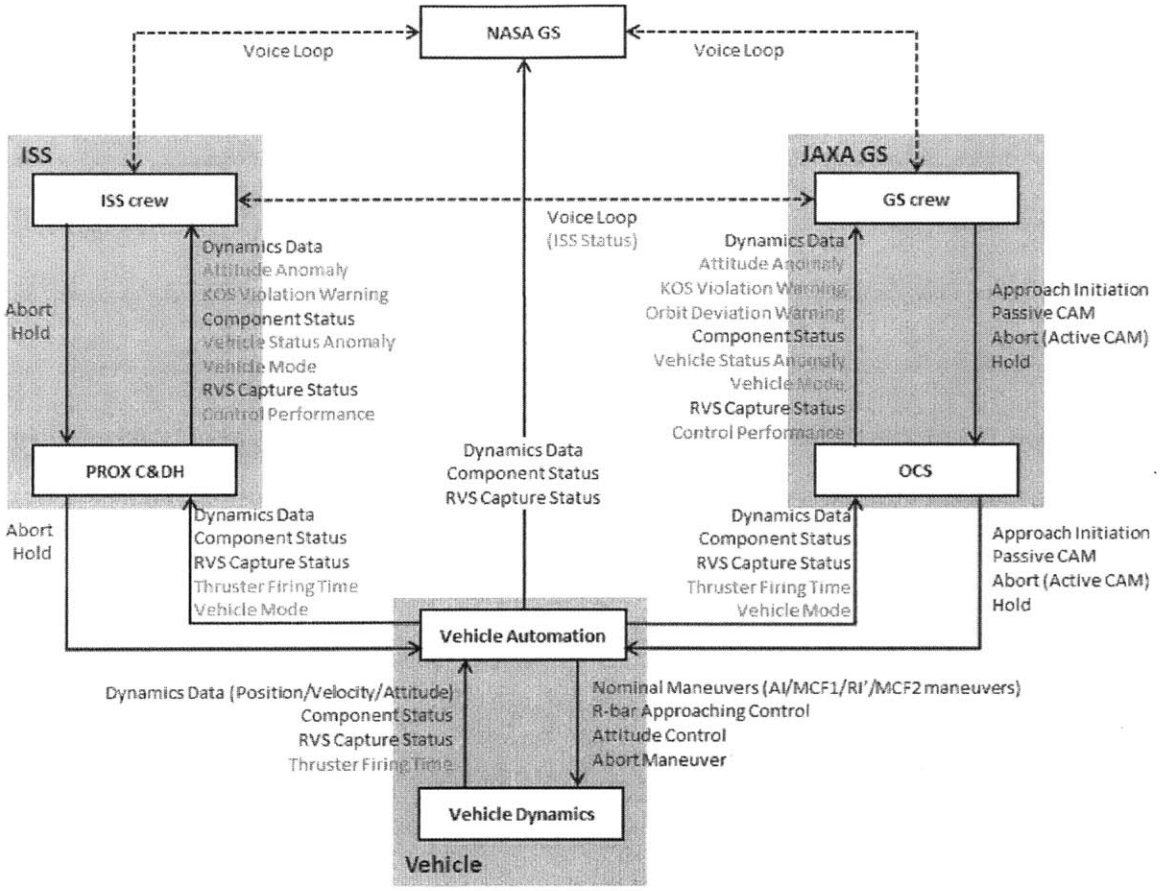


Figure 25: Revised Control Structure Diagram by the First Iteration

Subsequently, the causal scenarios were derived from each safety constraint. This causal scenario analysis was guided by the control loop diagram. Take the same constraint, SC-10: Each control must be provided within an acceptable thrusting range, again as example. Figure 26 shows the control loop diagram to identify the causal scenarios violating SC-10. Although 9 causal scenarios were identified in total, two following scenarios are focused here;

- Because the vehicle automation incorrectly believes that each control should not be stopped until it is completed, the control is provided over the acceptable thrusting range
- Because the thruster firing time range is wrong, the control is provided over the actual range

The first scenario indicates an incorrect algorithm implementation in the vehicle automation. This scenario can be prevented by implementing a function to count the thrusting time and stop the control if the thrusting time is over the acceptable thrusting range. However, what could happen if the threshold is wrong? The second scenario represents this case. Obviously, the threshold is a critical controller input for this control loop, and if this input parameter is incorrectly given to the vehicle automation, the automation could incorrectly apply the control too long. While the algorithm and threshold are recognized as important design elements, the problem is how to prevent these undesirable scenarios. Of course, the effort to verify and validate the threshold and algorithm will be mandatory. However, there is a limitation of this effort especially in huge and complex systems. Moreover, similar inadequate algorithm and parameter setting can be hazardous in the other cases. Therefore, these scenarios should be prevented by not only the automation design but also human operators. For example, if the GS crew monitors each control result which can be evaluated by the firing time and dynamics data, it can judge whether the control is successfully completed within the acceptable time range. If the control is not finished when the firing time already overs the range, the GS crew can issue the command to stop the maneuver like the passive CAM. These scenarios and design recommendation are summarized in Table 5. Likewise, the causal scenarios, and design recommendations for the other safety constraints are shown in figure A-1 and table A-4 in appendix A.

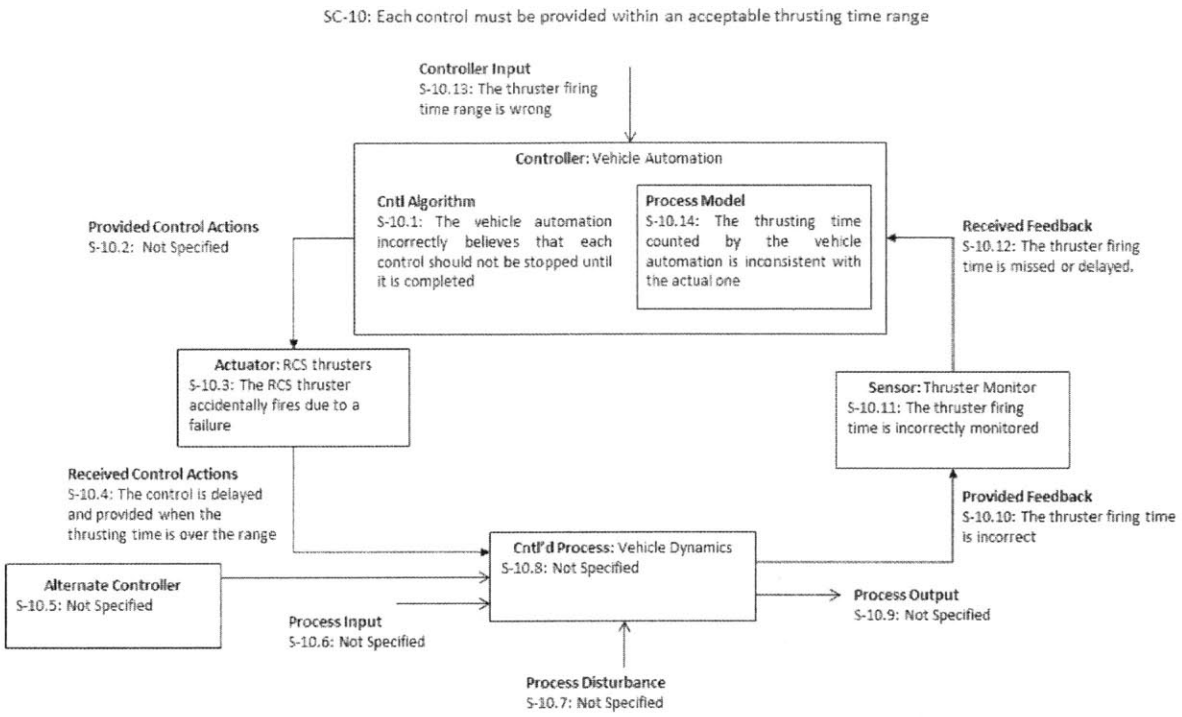


Figure 26: Control Loop Diagram for SC-10

Table 5: Sample Causal Scenarios and Design Recommendation for SC-10

Safety Constraint	Causal Scenarios	Design Recommendation
SC-10: Each control must be provided within an acceptable thrusting range	**S-10.1:** Because the vehicle automation incorrectly believes that each control should not be stopped until it is completed, the control is provided over the acceptable thrusting range **S-10.13**: Because the thruster firing time range is wrong, the control is provided over the actual range Etc.	The vehicle automation shall count the thruster firing time. If the firing time is over the acceptable firing time range, the vehicle automation shall autonomously stop thrusting. The GS crew shall monitor each control result (thrusting time & dynamics data) and judge if the control is completed within the acceptable time range. If not, the GS crew shall issue the command to stop the maneuver.

4.3.5 Refining Unsafe Control Scenario and Adding Design Detail

While the design recommendations derived from the initial unsafe control actions should be reflected to the system design, additional unsafe control actions can be identified in the next step. This analysis helps the engineers to realize of the system designs which have not been discussed during the previous design analysis cycle. In the previous analysis, the execution conditions for each control action had been already identified, and the conditions are composed of the following eight elements: ISS Status, Vehicle Orbit, Vehicle Attitude, Vehicle Status, Vehicle Mode, Control Performance, RVS Capture, and Control Duration. The context table can be defined based on these elements as shown in Table 6 and Table A-5 in appendix A. From this context table, four additional unsafe control actions were identified by considering a few missing control execution conditions in the previous analysis. Moreover, the conflictions among safety constraints were found in three controls.

One of four additional unsafe control actions is shown in Table 6. In this additional unsafe control action case, the nominal maneuvers are provided when the RVS is activated (see UCA-5.8 in Table 6). In the initial unsafe control action analysis, this RVS capture status was ignored when considering the control execution conditions for the nominal maneuvers, because the RVS capture status is implicitly expected not to be "ON" before the vehicle reaches at the RI point. This implicit design assumption indicates that the laser reflection only comes from the reflector attached on the bottom of the ISS. However, in reality the RVS could be accidentally activated due to the sensor noise like the Mars Polar Lander accident introduced in section 2.1. In the current design, it is not sure what could happens if the RVS is activated before reaching at the RI point. If this unexpected scenario is not found until the end of the development, in the worst case, the navigation data source for the nominal maneuver can be incorrectly switched to the RVS from the RGPS, although the RVS cannot produce any appropriate dynamics data. This totally inappropriate behaviors will cause an unstable maneuver based on the wrong navigation data, and it finally leads the vehicle to an

unknown state.

The same navigation data source confusion could happen in the other two vehicle maneuvers: the R-bar approaching control and abort maneuver (see UCA-6.8 and 8.7 in table A-5 in appendix A). If the RVS capture status is "On" but the vehicle orbit data indicates that the vehicle is outside the RVS navigation range, it would be dangerous to rely on the RVS data because of the inconsistency between the capture status and vehicle orbit. These three cases has not been considered at all in the initial unsafe control action analysis, and it definitely points out the vulnerability of the navigation transition from the RGPS to RVS. The complete context table and the other additional unsafe control actions are shown in Table A-5 in appendix A.

Table 6: Context Table for the Nominal Maneuvers

#	Control Action	ISS Status	Vehicle Orbit	Vehicle Attitude	Vehicle Mode	Vehicle Status	Cntrl Perf.	RVS Capture	Cntrl Duration	Not Providing Causes Hazards	Providing Causes Hazards	
19	Nominal Maneuvers	*	Deviated / KOS	*	*	*	*	*	*	No	Yes	UCA-5.1
20		*	*	Off-Nominal	*	*	*	*	*	No	Yes	UCA-5.2
21		*	*	*	CAM	*	*	*	*	No	Yes	UCA-5.3
22		*	*	*	*	Not Ready	*	*	*	No	Yes	UCA-5.4
23		*	*	*	*	*	< AI	*	*	No	Yes	UCA-5.5
24		Not Ready	*	*	*	*	*	*	*	No	Yes	UCA-5.6
25		*	*	*	*	*	*	*	Too long	No	Yes	UCA-5.7
26		*	*	*	*	*	*	ON	*	No	Yes	New UCA-5.8

* denotes conditions that do not matter for a given row

To successfully complete the navigation transition between the RVS and RGPS, an additional safety constraint should be required as follows: "each maneuver must be provided based on the valid navigation data source." The next question is how to realize this constraint as a system design. First of all, the RVS should be prohibited until the vehicle reaches at the RI point and the reflected laser is actually captured. In addition, the automation should also check if the vehicle position is inside the RVS range as well as the capture status is activated. If the inconsistency between the position and status is detected, the vehicle automation should autonomously switch again the navigation source from the RVS to RGPS and perform the abort maneuver. Furthermore, the GS crew should also have an authority to manually change the navigation data source, because the human operator can finally correct the automation judgement from a whole system perspective.

Another benefit of the context table is the conflict identification among UCAs. Table 7 shows the confliction about the abort maneuver. As described in UCA-8.2, when the vehicle orbit violates the KOS, the vehicle must execute the abort maneuver. However, if the control performance is less than the abort maneuver performance, the maneuver must not be executed because the control will be unstable and unexpected. Therefore, if the KOS violation happens when the current performance is less than the abort maneuver performance, both providing and not providing cases would cause hazards.

Table 7: Conflicts between the UCAs for the Abort Maneuvers

	<= Conflict =>	
UCA	[UCA-8.2] Not Providing the abort maneuver when the KOS is violated can causes H-1	[UCA-8.4] Providing the abort maneuver when the control performance is less than the abort performance can cause H-1, H-2, or H-3.
Safety Constraint	[SC-21] The abort maneuver must be provided when the orbit violates the KOS	[SC-9] Each control must be provided only when the current control performance satisfies the required performance for the control

How can this conflict be avoided? Although the other solution might be able to be proposed, there are two possible ways to update the safety constraints to resolve this conflict. The first one is to constrain the vehicle to perform the abort before the performance is less than the abort maneuver performance. This idea is derived from the existing HTV design. In the existing HTV, the vehicle always checks the component status and autonomously conducts the abort maneuver before the vehicle cannot perform the abort maneuver due to component failures. This design is reasonable in the existing HTV, because the system is based on a simple redundant design and the performance of the existing HTV can be predicted by counting the number of failure (see Figure 22). However, taking the exact same approach in the HTV-X will be quite difficult. In the existing HTV, a thruster failure immediately results in the attitude anomaly, which enables the automation to count the number of failures and switch the whole thruster system to redundant one. On the other hand, in the resilient thruster design of the HTV-X, although a thruster failure also disturbs the attitude, the disturbance is immediately controlled. In addition, the automation cannot precisely know how many failures cause the disturbance. Therefore, even if the HTV-X vehicle also has the same control capability to execute the abort maneuver under any 2 failure conditions as the existing HTV, it will be hard for the automation to judge the abort timing.

An alternative design idea is to engage the human operator in this critical judgement. Because of human's excellent capability of understanding data trends, the human operators might be able to recognize the performance variation and make an appropriate judgement for the abort timing. To realize this operation, as the second safety constraint, the GS crew is constrained to reconfigure the RCS thrusters when the performance is less than the abort performance. As discussed in section 3.3, if 8 of 24 thrusters are available, the vehicle can perform the abort maneuver. Therefore, only if the GS crew selects available eight thrusters and deactivates the other ones, the KOS violation would be able to be avoided by this operation. This thruster reconfiguration was added to the control structure as a new control action, to somehow recover the control performance to maintain the safety for the ISS.

However, for the human operators to judge the abort execution, a certain amount of time will be spent, because generally human processing is not so fast as computer. Furthermore, the performance can be further degraded and be less than the abort performance during they are judging it. Therefore, in order to keep the time for the GS crew to find the available thrusters, the vehicle should be designed as the control performance is gradually degraded, because it can be quite difficult to make the successful reconfiguration if the performance suddenly drops by a few failure. The updated safety constraint, detailed causal scenario, and new design recommendation are summarized in Table 8.

Figure 27 shows the revised control structure through the second design refinement process. In the second iteration, as discussed above, two new control actions were added: sensor reconfiguration and thruster reconfiguration. Because the resilient design leads to more complex system behaviors than the existing HTV, it is infeasible to deal with the behaviors by only the automation. Therefore, to guide the system to safety, these new human interventions will be essential in the HTV-X operation.

Table 8: Updated Safety Constraint, Causal Scenario, and Design Recommendation for the Confliction between UCA-8.2 and 8.4

Refined Safety Constraint	Detailed Causal Scenario	New Design Recommendation
[Revised SC-9] Thruster reconfiguration must be provided when the current performance is less than the required maneuver performance	The vehicle automation provides the abort maneuver when the KOS violation is detected. However, the control performance is already less than the abort performance due to some thruster failures, and therefore the abort is imperfect, which leads the vehicle to an unexpected orbit. Etc	Each RCS thruster's control duty shall be reconfigured by command The reconfiguration command shall be acceptable during any control, and after the reconfiguration the control immediately restarts. The control performance shall not drop under the abort performance by a single failure

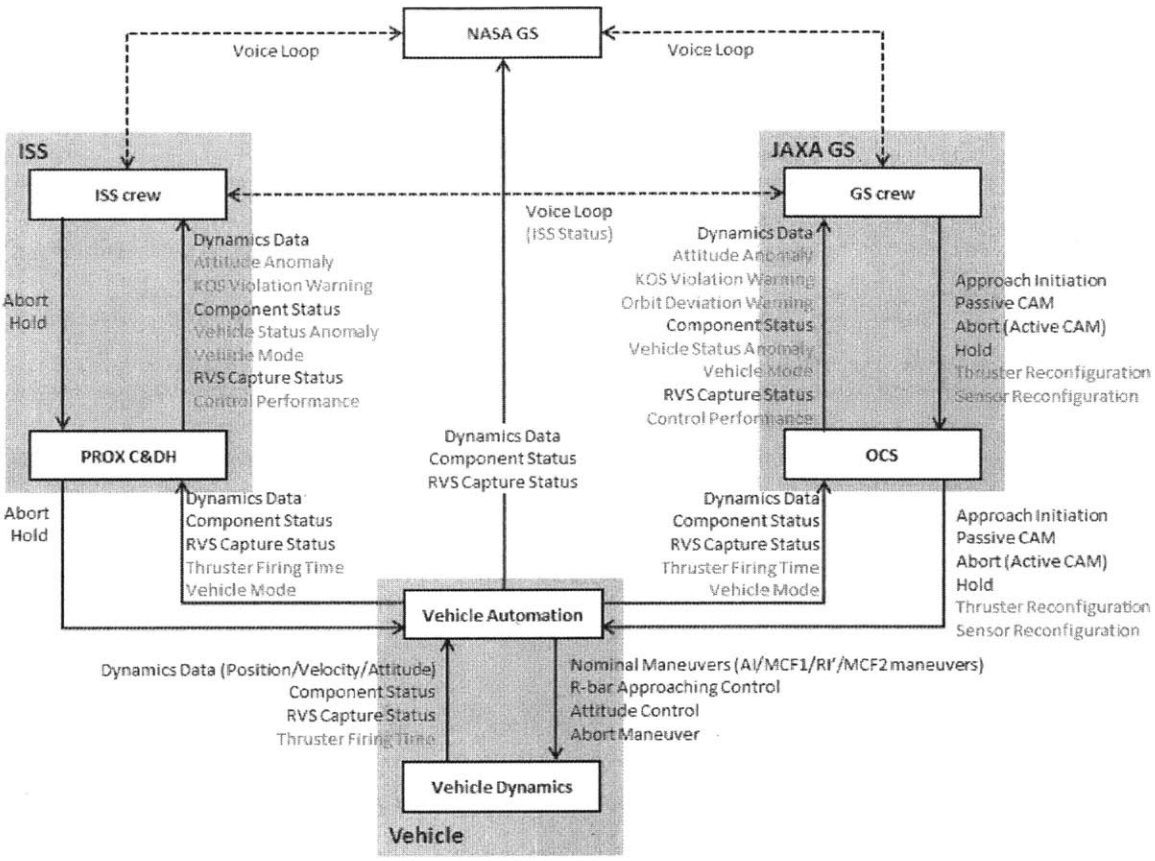


Figure 27: Revised Control Structure Diagram for the Final Approaching Phase

4.4 Conclusion of STPA application

Various design recommendations have been successfully generated from the safety guided design process. Although any safety analysis has never been applied in the concept design of JAXA's spacecraft, this result indicates that STPA can help the engineers in creating the safer HTV-X system design from the early development phase. Furthermore, because the approach is quite systematic, this outcome can be reproduced in the other general complex systems. The technical conclusion for the HTV-X system is given in section 4.4.1 and the academic conclusion about the effectiveness and applicability for the general systems is discussed in section 4.4.2 in detail.

4.4.1 Technical Conclusion

One of the most important outcomes from this analysis is that concrete but still system level designs were successfully derived from just ten fundamental control actions in the early concept design of the HTV-X. By applying the four unsafe control patterns, 45 unsafe control actions were identified in total and then 22 system level safety constraints were also defined. Although there is not any formal specification, various concrete causal scenarios violating the constraints were also created from the control loop analysis. Finally, a lot of useful design recommendations were proposed based on the scenarios. During actual design tradeoff discussion, to convince various stakeholders, concrete and logical backgrounds are required for each design recommendation. All of the design recommendations from STPA is not only supported by systems theory but also traced to concrete scenarios and fundamental system controls. Moreover, the recommendations covers a wide range of system behaviors. Therefore, this analysis results will deserve actual concept design candidates.

As another important result, although the resilient design is still conceptual, its characteristics were successfully described from safety perspective. In the HTV-X development, the central concern of the engineers will be how to implement the resilient design policy into an actual system without any critical flaw. While the design policy can significantly contribute to the cost reduction and smooth operation, it can also cause unexpected off-nominal behaviors which never happen in the existing HTV system. Therefore, it will be definitely beneficial if the engineers find various unsafe control actions and causal scenarios related to the resilient design policy. Indeed, 18 of 45 unsafe control actions (UCA- 1.2, 1.5, 2.3, 3.2, 3.3, 4.2, 4.5, 5.2, 5.5, 5.7, 6.2, 6.5, 6.7, 7.2, 7.3, 8.3, 8.4, 8.5, and 8.6) identified in this analysis are caused due to the resilient design. Furthermore, the causal scenarios and design recommendations related to the policy were already derived from those unsafe control actions. These outputs will surely contribute to understanding the risk of the new design policy at the very beginning of the development, and provide support to the design

discussion about the resilient system.

Furthermore, it is also a significant outcome that new feedbacks and control actions to prevent specific causal scenarios were added to the basic control structure. The thruster firing time and control performance do not exist in the existing HTV system, but in the HTV-X system these are definitely essential for the human operators to adequately understand the vehicle state. The thruster reconfiguration is the new control to guide the autonomous compensation mechanism to complete the maneuvers without imposing too much burden on the vehicle. Although the control amount calculation and control execution are still conducted by the automation, the GS crew can assist the automation in successfully completing the maneuvers under off-nominal conditions. This cooperative operation also has never been observed in the existing HTV, but it is essential to lead the more complex new vehicle to safe states in any situation.

From the context table, the unsafe control actions that had been missed in the first cycle were identified with a systematic way. During the concept design phase, engineers tend to rely on unstructured creativity because of a high degree of freedom in design space and, therefore, conflicts among control execution conditions and lack of consideration about the conditions can easily happen. Indeed, the RVS capture status had not been considered in the nominal maneuver execution conditions in the first cycle, even though it can cause the navigation data source confusion in the control. Furthermore, the conflict about the abort maneuver in a specific condition was also missed in the first analysis. While the conditions are getting more detailed in the later development phase, it will be more difficult to find and eliminate these system design pitfalls, because the system is decomposed into several subsystems and the viewpoint as a whole system tends to be lost. Therefore, to reduce the design rework as well as critical operation risk, it is quite important to identify the hard-to-find unsafe controls in the early design phase and find a solution for each control as a whole system.

4.4.2 Academic Conclusion

This analysis demonstrated that the integrated approach to system design and hazard analysis can effectively

work in concept design creation and consequently guide the design to be more robust against off-nominal behaviors. Generally, every design recommendation has to be always appropriate with respect to the design maturity level. If the recommendation is too detailed, it will be declined in order to maintain the design trade space for the later phase. On the one hand, too general recommendations not based on any specific target system characteristic will be never accepted. In this safety guided design approach, because the causal scenarios were induced from the basic system level controls, each design recommendation generated from the scenarios can be traced back to the basic controls. Therefore, the result of the analysis will be always acceptable even in the concept design phase as long as a proper control structure and control actions are defined based on the original system design at the very first step of the analysis.

In addition, while the analysis process is based on the basic system information, the system design can be improved as the system can deal with various off-nominal situations. As discussed in the previous section, the design recommendations to prevent various unsafe control actions were actually proposed through the analysis. It indicates the process successfully helps the analysist in holistically identifying undesirable system behaviors and systematically proposing the countermeasures to avoid them.

As another important feature of this approach, the interaction between the automation and human operators can be designed from the whole system perspective. In the HTV-X concept design analysis, by deeply diving into the causal scenarios based on the control loop diagram, the causes why the human operators can miss important system indicators were analyzed and finally countermeasures were also defined. For example, although the vehicle status is important information from the operators' perspective, the critical information for their decision making will be if the status indicates an anomaly or not. Therefore, the ground systems should notify them of the anomaly rather than simply display the status. It is also one of the important advantages of STPA to enable the analysts to think what the operator should really know to safely control the system.

Moreover, the cooperative controls between the automation and human operators were proposed in the design recommendations. When considering some recommendations, it was quite difficult to prevent the causal scenarios by only improving the vehicle design. For example, if the vehicle mode expected by the automation is inconsistent with the actual mode, can the automation detect the inconsistency by itself? Although it might be possible, the design of the vehicle will be surely quite complicated and redundant. In this analysis, the intervention from the human operators was naturally guided by the analysis process, because the existence of the human controllers is clearly impressed by the control structure at the beginning of the analysis. Furthermore, the process guidance promotes thinking about the needs of additional controls to prevent the causal scenario. Especially in the early stage of system design, to re-consider the functionality allocation among the automation and human operators is quite important, because changing the allocation in the later stage will endanger the development as well as result in rework. Thus, it has an important meaning for utilizing the integrated design approach in the early development phase that the allocation can be successfully improved from safety perspective.

Chapter 5. Using CAST in Existing Vehicle's Incident Analysis

In new system development, creating a successful system design from the early development phase (e.g. the concept design development using STPA) significantly contributes to the success of the mission. However, it is also quite important to analyze the past actual accidents in similar systems and propose design recommendations to prevent future accidents having the same characteristics. For example, in 2003 JAXA experienced a serious rocket accident that the rocket had to be intentionally destroyed by command [25]. After this accident, some rocket parts submerged at the sea bottom were salvaged to investigate the cause of the accident. Due to this tremendous effort, JAXA has succeeded successfully in rocket launch operations more than 30 times in a row after the accident. Similarly, to learning from past undesirable operations in the existing HTV will surely contribute to the success of the future HTV-X system.

Fortunately, no serious accident has never happened in HTV operations. Despite the successes of the missions and the lack of critical failures, there have still been a few undesirable incidents. In this study, the HTV-3 abort incident is the focus, and CAST is applied for the incident analysis. Because system-level design recommendations based on an actual accident or incident can be derived from CAST analysis, the result of the analysis can be immediately fed back to the system design of HTV-X.

In addition, the incident is strongly related to the human and automation interaction. In this incident, the uncoordinated behavior between human operator and automation could be observed. If systemic viewpoint is lacked in the incident analysis, the result of the analysis will just conclude human mis-operation. However, this simple conclusion is not useful at all for modern complex systems. To avoid the useless design recommendation and utilize the incident for the future system, it should be essential to analyze the incident from system theoretic perspective and identify system control issues using CAST.

While this incident looks like a good example of human - automation design issue, the intent of the analysis

is not to blame any operator. Instead of thoughtlessly determining who should be blamed, this discussion will focus on which system design should be modified in order to create proactive and useful recommendations for the HTV-X system design. First of all, the detail of the incident is described in section 5.1, and then, in order to holistically analyze the human mental behavior from engineering viewpoint, a new human controller model is introduced in section 5.2. After that, the result of the CAST analysis for this incident is explained in section 5.3, and finally the evaluation of this analysis is given in section 5.4.

5.1 Incident in HTV-3

In 2012, HTV-3 autonomously executed an abort thrusting immediately after being released from the ISS by a robotic arm, called the SSRMS [26]. The HTV-3 was expected to gradually lower the altitude like the HTV-1 and 2, but indeed the vehicle rapidly escaped from the ISS (see Figure 28) and reached at the AI point. Although the HTV-3 safely completed the abort by its large 500 N thrusters, called ME, the abort was undesirable because chemical substance jets by the large thrusting can contaminate the ISS external equipment like solar panels.

Figure 28: Snapshot from the Video Monitor of HTV-3 aborting

After the incident, the cause was investigated in detail, and finally the unexpected friction between the grapple fixture of the vehicle and the SSRMS was identified as the root cause [8]. This cause was the origin

of the incident, but because completely eliminating the friction is impossible, the effective countermeasure should have been detecting the unexpected vehicle velocity imposed by the friction (or even other causes) and selecting an alternative acceptable operation scenario. Indeed, the vehicle automation could successfully detect the wrong velocity and conduct the ME abort to ensure the safety of the ISS. However, this vehicle behavior was not totally predicted by the ISS and GS crews, which indicates that they did not notice the wrong velocity at all. If they noticed the off-nominal situation, they would manually issue the abort command and the vehicle would conduct a smaller abort, which did not cause any chemical contamination risk to the ISS. Therefore, this undesirable incident could be also avoided if the operator's awareness was more enhanced by the system design.

In order to show the details of this incident, the detailed sequence of events are described in section 5.1.1. Moreover, the impact of this incident is discussed in section 5.1.2, and finally section 5.1.2 provides the investigated direct causes of the incident and what was originally expected as a desirable scenario.

5.1.1 Sequence of Event

The HTV-3 was launched from Tanegashima Space Center on UTC 02:06, July 21, 2012 and successfully docked with the ISS on UTC 15:22, July 28 [27]. Although the Guidance and Control Computer (GCC), which is a main onboard computer system to guide, navigate, and control the vehicle, was switched to a redundant one during this operation, it was an acceptable hardware failure event and did not influence the flight plan.

After unloading the supply goods and loading the trash from the ISS, the hatch door of the vehicle was closed at UTC 13:59, September 11, and the vehicle was undocked from the ISS by the SSRMS at UTC 11:50 on 12th. The ISS Crew controlled the robot arm and located the vehicle at the releasing point, and finally the vehicle was released from the arm at UTC 15:50. After almost one minute, the ISS Crew activated the vehicle's autonomous control to stabilize the attitude. Until this operation, everything had seemed to

work as planned, and all of the operators believed that they could successfully lower the altitude of the vehicle as they had for HTV-1 and 2. However, at UTC 15:55 the automation detected a Safety Net Violation and executed the large thrusting abort maneuver by the ACU unit. Because of this maneuver, the vehicle unexpectedly flew to the AI point [28].

Due to this unexpected abort maneuver, some recovery operations to return to the planned reentry orbit were required. In total, four additional maneuvers were executed and finally the first Deorbit Orbit Maneuver (DOM1), which was originally planned for September 12, was conducted on 14th. After that, the HTV-3 successfully finished the rest of mission, safely entered the earth atmosphere, and finally burned up as it was designed to do.

5.1.2 Negative Impact from the Incident

While the GS crews unexpectedly spent a huge effort on planning and executing this recovery operation, the most negative impact of this unexpected abort was the risk of chemical contamination to the ISS by the large thrusting maneuver.

As shown in Figure 13, the existing HTV vehicle is equipped with two kinds of thrusters: RCS thruster and ME thruster. The RCS thrusters are mainly used for the attitude control and relatively small orbital maneuvers, while the ME thrusters are used in only large maneuvers like fundamental orbital changes in the distant rendezvous phase and deorbiting maneuvers inn the deorbit and reentry phase. The propellant force of the RCS thruster is 110 N and in total 24 RCS thrusters are symmetrically allocated around the vehicle body. The propellant force of the ME thruster is 500 [N], and there are only four ME thruster in the vehicle, which are attached on one edge of the vehicle (see Figure 13). In the final approach phase, every approaching maneuver is planned to be conducted by only the RCS thrusters. However, the abort maneuver is off-nominal operation and can be executed by either theRCS or the ME thrusters. This choice depends on the vehicle configuration when the safety net violation is detected (see section 5.1.3). These two aborts have the same

purpose but the behavior and performance are different.

In the RCS abort, the thrusting quantity is small and controlled by the feedback control algorithm, and the attitude is also accurately maintained by the RCS thrusters. In the ME abort, the attitude control is unavailable, and moreover, to surely fly away from the ISS under an emergency situation (e.g. any RCS is unavailable), the ME abort is executed by prefixed simple and conservative time cutoff control. It indicates that the thrusting quantity can be more than needed. The comparison between the RCS abort and ME abort is summarized in Table 9. Because the large and inaccurate ME abort maneuver was conducted in the vicinity of the ISS, the risk of the chemical contamination emerged.

After this incident, JAXA had to work on a huge number of numerical simulations for the evaluation of the contamination, in order to respond to criticism from the other ISS partners. Fortunately, they could finally prove any serious contamination was not caused by the abort. However, it should be considered that this incident would have been able to damage the trusted relationship among JAXA and the ISS community as well as to deteriorate the operability of the ISS by the chemical contamination.

Table 9: Comparison between RCS and ME abort

	RCS abort	ME abort
Output	Small (RCS 110 N)	Large (Main Engine 500N)
Propulsion Accuracy	Accurate (delta V cutoff control)	Inaccurate (Timer control)
Attitude Accuracy	Accurate (PD control)	Inaccurate (No Control)

5.1.3 Direct Causes and Desirable Scenarios

In this incident, the vehicle automation detected the safety net violation and automatically decided to conduct the abort. The violation occurred because the predicted vehicle position for 300 sec later violated the safety zone of the ISS [18], which means the wrong initial velocity was imposed on the vehicle [28]. After the incident, the cause of this wrong initial velocity was investigated and JAXA concluded it was caused by an unexpected friction between the robot arm and vehicle's grappling fixture [8]. They also pointed out that the friction might have happened even in the HTV-1 and 2, although both of the vehicles carried out the deorbit operation without any unexpected event. It is still controversial why the friction strongly influenced only the HTV-3. One possible explanation is that the uncertainty of the center of gravity of the vehicle might influence the robot arm operation. Before departing from the ISS, a certain amount of trash is loaded into the vehicle, and this loading process can create the uncertainty. However, because the ISS Crew cannot precisely load the trash under the extreme environment in the ISS, this uncertainty is inevitable. As for other possible explanations, a manufacturing error of the fixture and/or the robot arm operation error might also be considered. However, any explanation is still only a guess.

One of the important facts for this incident is that an alternative scenario is that the wrong velocity existed but it was not executed. When the vehicle drifted out from the planned orbit before activating the automation control, the GS or ISS crews were expected to manually send the abort command. Even before activating the automation, the vehicle can react to the command and execute the abort. In order to judge the orbit violation, of course, the vehicle's position and velocity are displayed on the monitors for the GS and ISS crews. Figure 29 shows an example of the monitoring environment for the ISS crew. Generally, the position and velocity information is displayed on the right hand side panel as text data. Likewise, almost the same information is also monitored by the GS crews. Moreover, the voice communication loop between the ISS and ground station is always established during the departure phase. If the GS or ISS crews have detected

the wrong velocity and manually sent the abort command, the RCS abort would have been selected instead of the ME abort, and the risk of the chemical contamination would not have emerged because of the accuracy of the RCS abort.

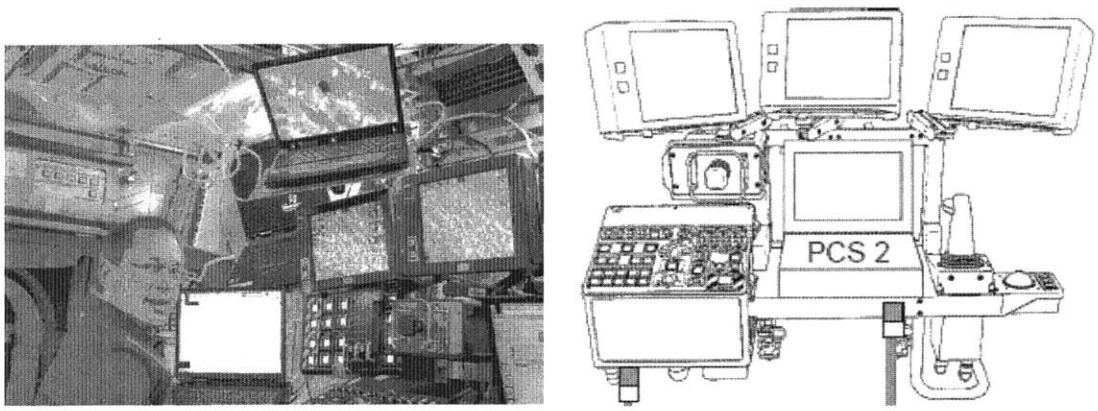


Figure 29: HTV monitoring environment for the ISS Crew

To surely maintain the safety of the ISS, even if the GS or ISS crew misses the orbit violation, the automation is designed to detect it and execute the abort without any command after the vehicle is once activated. Indeed, in this incident case, this automation design worked and avoided the collision course. In addition, if the GCC failure had not happened during the approaching operation, the automation would have surely selected the RCS abort by itself. In other words, the GCC failure also influenced this incident.

The top panel of Figure 30 shows the transition of vehicle's propulsion system configuration caused by the safety net violation under no failure condition. If there is no failure in the three GCC computers, the most probable computation result can be determined by the majority rule. Thus, when the safety net violation is detected by this computer configuration, the automation presumes that the detection is reliable and the violation is caused by the other component. So, the automation decides to switch the Input Output Controller (IOC) to the redundant one and conduct the RCS abort. On the other hand, when there is one GCC failure, the majority rule no longer works because there are only two available computers. If the violation occurs under this condition, the automation cannot determine if the violation was caused by the computational error

or some other factor. In this case, therefore, the vehicle control authority is transferred from the GCC to the ACU, which has only the simple functionality to perform the abort with the ME thruster (see the bottom panel of Figure 30). In fact, this transition happened in this incident due to the one GCC failure.

Although the friction and the GCC failure wrongly influenced this incident, the manual abort command by the GS or ISS crews was the desirable action. Figure 31 summarizes the scenarios explained above. While the friction and the GCC failure are reliability issues, obviously the lack of the manual command can be regarded as a system design issue. Again, this analysis should focus on s why the GS and ISS crews missed the wrong velocity and did not send the abort command, rather than who made a mistake. The main focus of this analysis is to clarify which system designs lead to the undesirable scenario and how it can be improved in the whole system.

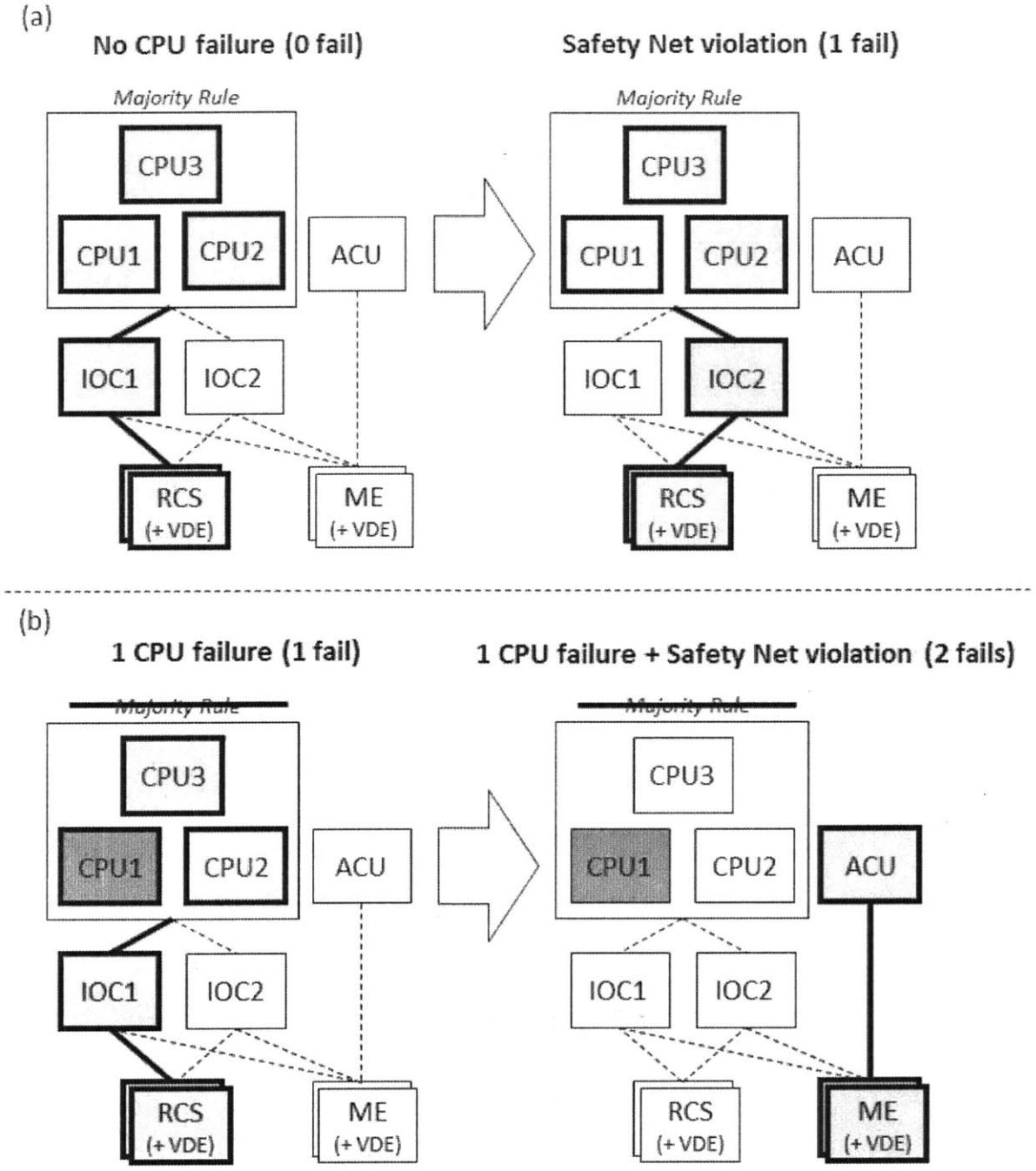


Figure 30: HTV Guidance & Control Computer and Propulsion Configuration change by the Safety Net Violation under no failure (top panel) and one GCC failure (bottom panel)

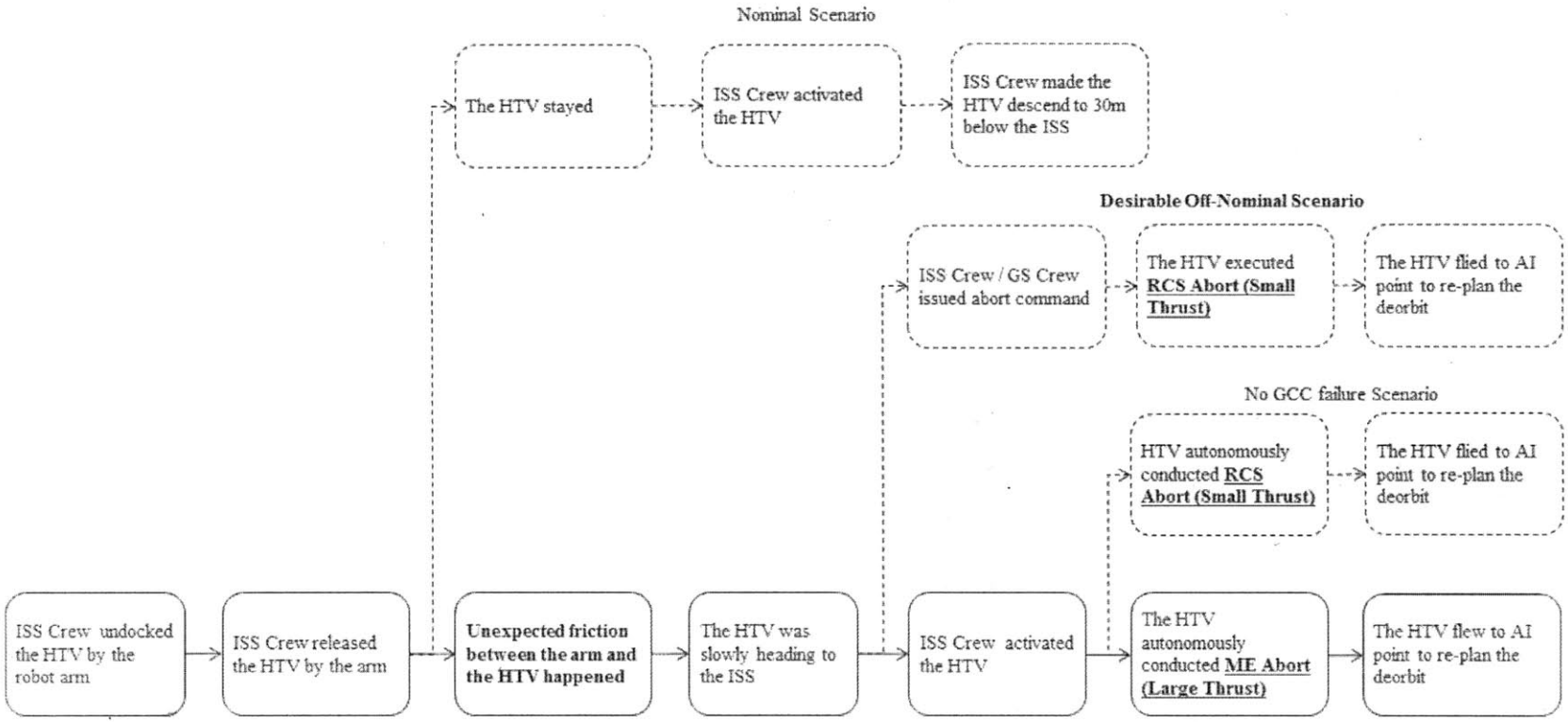


Figure 31: Comparison among the actual sequence of events in the incident, nominal scenario, desirable manual abort scenario, and no GCC failure abort scenario

5.2 New Human Controller Model

As discussed in the previous section, deeply investigating the human and automation interaction should be a core part of this incident analysis. To deep-dive into the interaction, the new human controller model invented by France and Thomas is introduced. In the control loop of the STAMP model, the controller part is generic and can be applied for both humans and automation. In order to more specifically focus on human controller behavior, France and Thomas extended the controller model. This new human controller model is not aimed for perfectly describing human mental behavior, but the purpose is to reinforce the system theoretic analysis approach by adding new human specific behaviors from engineering viewpoint.

The new human controller model is shown in Figure 32. The model is mainly composed of three elements: PM Update, Process Model, and Devise Control Actions. In this model, the human controller is assumed to handle the input information through these three mental steps, and the consequence of a flaw in this process is, of course, always an unsafe control action. Each element has a different role to determine and execute a control action in the control loop, and therefore the various unsafe scenarios can be acquired by assuming a flaw in each one.

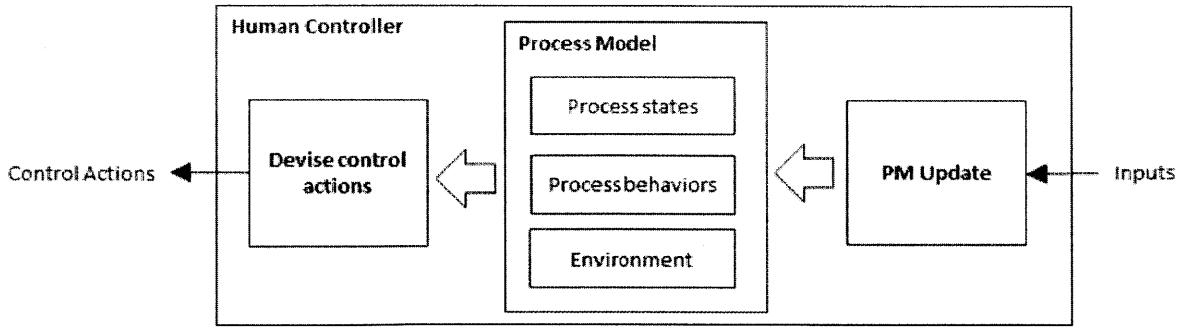


Figure 32: New Human Controller Model

The Process Model (PM) variables are the variables to describe and differentiate the system states [29]. The PM update is the process to catch the information from the sensor and update the PM variables based on the information. Naturally, updating the PM variables inside the human controller means updating the system

state anticipated by the human controller. In other words, a flaw in this updating process rcan result in an inconsistency between the assumed system state and the actual state, which finally leads to providing an unsafe control action.

The second element describes the parts of th dynamic system process model inside the human controller. This element is decomposed again into three sub-elements; Process State, Process Behavior, and Environment. In each of these three sub-elements, a different type of system understanding flaw inside human operator can be described.

The Process State is the mental linkage between the PM variables and system states. Even if correctly updating the PM variables, the human operator could wrongly translate the variables into a specific system state and finally provide an inadequate control action against the actual system state.

In the Process Behavior, understanding about system behavior is stored. After successfully identifying the system state, the operator should know how the system behaves in the state. If they misunderstood the behavior and their expected behavior was different from the actual one, they could take an inadequate action which results in the hazardous state.

Moreover, even if the expected and actual behaviors were consistent, the operator could not guide the system to the safe direction unless they could correctly understand the environment around the system. For example, when the behavior is inappropriate against the current environmental condition, the operator is generally expected to provide a control to guide the system to a desirable state and behavior. However, if they did not properly identify the environmental condition, they could think the behavior is appropriate and not take any action.

The third element is related to human operator's control action selection. Operators use the process model plus other information they may have to identify the appropriate control action to provide. This part of the

model is the decision-making process. For example, in the HTV departure operation case, the ISS and GS crews would never issue the abort command even though they noticed the orbit violation, if they just wanted to avoid the abort and planning of the off-nominal deorbit sequence from the AI point. Thus, this element represents the human decision-making process using the process model information. The process model may be correct but the human decision making based on that information may be incorrect.

The third element is related to human operator's control action selection. Operators use the process model plus other information they may have to identify the appropriate control action to provide. This part of the model is the decision-making process. For example, in the HTV departure operation case, the ISS and GS crews would never issue the abort command even though they noticed the orbit violation, if they just wanted to avoid the abort and planning of the off-nominal deorbit sequence from the AI point. Thus, this element represents the human decision-making process using the process model information. The process model may be correct but the human decision making based on that information may be incorrect.

Finally, the general procedure to use this new human controller model is given as follows

(1) Identify Unsafe Control Actions

(2) Identify PM variables

(3) Identify inadequate Process Model Updates

(4) Identify Process Model Flaws

(5) Identify unsafe Control Action Selections

As mentioned at the beginning of this section, it is assumed that the automated controller model in the control loop is replaced by this human controller model when a human is the controller. Thus, the UCAs and PM variables should be identified like the general STAMP related methodologies before applying this

model. Based on those UCAs and PM variables, the human mental flaw analysis can be conducted and the unsafe scenarios based on the human - automation interaction flaws can be derived.

5.3 Applying CAST for the Incident

To analyze the HTV-3 incident from the system theoretic perspective and gain the design recommendations for the HTV-X system, the CAST is done. The detailed result of each step is shown in the following sections.

5.3.1 Violated System Hazard and Safety Constraints

First of all, the violated hazard and safety constraint in this incident is identified. In Table 10, the accidents, hazards, and safety constraints during the departure phase are listed. In total, there are 3 accidents and 6 hazards. For each accident, the severity level can be specified; "Collision with the ISS" and "Damage to the SSRMS" are severer accidents than "Contamination to the ISS." Fortunately, any accident happened in the HTV-3 operation, but obviously the following hazard and safety constraint were violated;

- [H-3.1] The vehicle performs a large thrusting near the ISS
- [SC-3.1] HTV system shall select the small thrusting abort if possible

In this context, the HTV system includes all of human operators and automation. Indeed, in the HTV-3 incident, the ME abort was conducted just 10 m below from the ISS, and the ISS Crew and GS Crew did not send the abort command manually.

Table 10: Hazard and Safety Constraint List

#	Accident	Severity	Hazard	Safety Constraint
1	[A-1] Collision with the ISS	High	[H-1.1] the vehicle performs unplanned maneuver into the KOS	[SC-1.1] HTV system shall avoid to make the vehicle enter the KOS except for the planned orbit.
2			[H-1.2] the vehicle is out of the corridor within the KOS.	[SC-1.2] HTV system shall maintain the vehicle's position inside the corridor when it is inside the KOS.
3			[H-1.3] the vehicle drifts to the ISS with uncontrolled state.	[SC-1.3] ISS Crew shall activate the vehicle after T[s] drift out.
4	[A-2] Damage to the SSRMS	High	[H-2.1] the vehicle is activated when it is grappled by the SSRMS	[SC-2.1] ISS Crew shall not activate the vehicle when it is grappled by the SSRMS
5			[H-2.2] the vehicle is not deactivated when ISS Crew starts to grapple or release it by the SSRMS	[SC-2.2] ISS Crew shall deactivate the vehicle before they starts to grapple or release it by the SSRMS
6	[A-3] Contamination to the ISS	Low	[H-3.1] the vehicle performs a large thrusting near the ISS	[SC-3.1] HTV system shall select the small thrusting abort if possible

5.3.2 Safety Control Structure

During the departure phase, three controllers are engaged in controlling the vehicle. The ISS crew manipulates the robot arm and releases the vehicle from the ISS. After releasing, the ISS and GS crews monitor the state of the vehicle by the video image and the status telemetry data from the automation. If the release is successfully completed, the ISS crew issues Free Drift ARM command to activate the automation's attitude control. When receiving the command, the automation starts to automatically stabilize the attitude. After several status data are checked, the vehicle starts to gradually lower its altitude by the

Retreat command from the ISS crew. For redundancy, the GS crews can also issue the same commands. Moreover, the voice loop communication between the ISS and GS crews is always established. When detecting an anomaly in the vehicle, the ISS and GS crews can issue the Abort command. In this case, the ISS and GS crews are not expected to independently judge and issue the Abort command. They can communicate with each other as long as the voice loop is established, and make a decision. Because the same information is displayed on both monitors, if either of them detect the anomaly, it would be shared through the voice loop and finally the ISS crew would issue the Abort command. Moreover, after the activation, the vehicle automation can also autonomously execute the abort maneuver when detecting the safety net violation. These control loops are summarized in Figure 33.

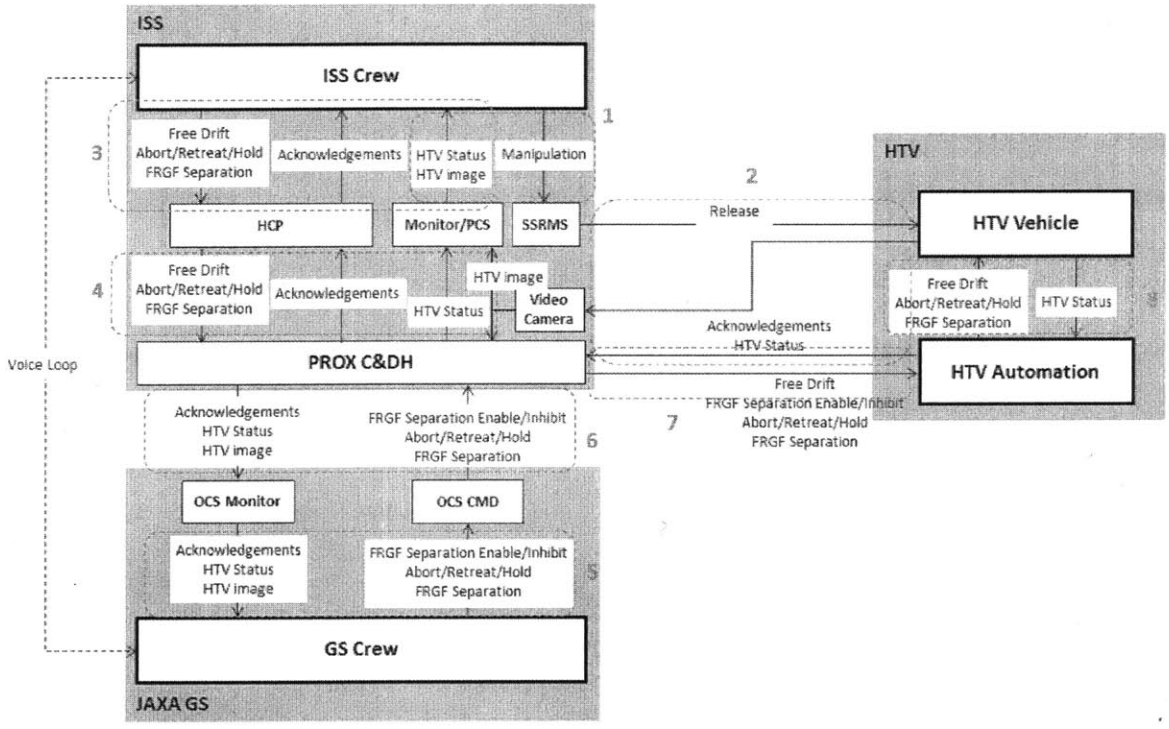


Figure 33: Safety Control Structure for HTV departure operation

5.3.3 Expected Safety Responsibility and Executed Unsafe Control Action

From the safety control structure shown in Figure 33, eight control loops can be identified. In each control loop, the safety responsibility that was originally expected in the system design was investigated, and the actual control action executed in the incident was also identified. In this analysis, No.1, 2, 3, 5, and 8 are the focus, while No.4, 6, and 7 are not analyzed because these three loops just follow their upper control loops without any judgment and furthermore any hardware failure happened in these loops. The result of analysis is shown in Table 11.

First of all, as a result of investigation, the quality of robot arm manipulation by the ISS crew was expected to be fair in the incident (Loop No.1). If the quality was quite worse than the HTV-1 and 2, the GS or ISS crews could have noticed it. Indeed, the Rendezvous Sensor (RVS) attached on the vehicle successfully captured the laser reflection from the ISS and started the measurement of position, which indicated the release position of the vehicle was not extremely deviated.

As discussed above, one of the direct causes of this incident is the unexpected friction between the robot arm and the vehicle. Therefore, in the Loop No.2, an inadequate control action ("Impose an unexpected force on the vehicle by the unexpected friction") is identified. However, any process flaw cannot be specified in this loop, because it is almost impossible to eliminate any friction or perfectly control the friction by the existing ISS robot arm. Of course, it should be possible to attach a new sensor on the SSRMS and to feed back the reaction from the grappled object. However, the functional extension of the robot arm would be extremely expensive, because any ISS equipment must be operated under extreme conditions and the extension construction of the ISS facility also requires much time and special tools. Thus, to change the physical design of the SSRMS would be an infeasible solution.

Instead, the variation of position and velocity caused by the robot arm operation should be monitored and the abort command should be issued when the violated orbit is recognized in the loop No.3 or No.5. The

reason why the ISS and GS crews were not aware the violation was investigated, and an interesting biased recognition about the robot arm operation was identified. This incident was discussed with Prof. Hoffman, who is a former NASA astronaut, and he pointed out that in the robot arm operation generally the operators pay attention to the attitude disturbance caused by the arm. Behind this operation direction, there is an experience based common understanding that the velocity and position disturbance rarely happens in the robot arm operation, while the attitude disturbance is easily caused. In the HTV-3 incident case, it can be assumed that this biased understanding created the mental model flaw of the ISS and GS crews, which distracted both operators' attention to the orbit violation.

Table 11: Safety Responsibility and Inadequate Control Action for each loop

Loop	Safety Responsibilities	Inadequate Control Action	Context in which Decision Made	Process or Mental Model Flaws
1	Ensure the vehicle is moved to the release point and released without significant disturbance	This control was adequate	N.A.	N.A.
2	Ensure the given control is successfully converted to physical robot arm manipulation	Impose an unexpected force on the vehicle by the unexpected friction	Unexpected friction between the robot hand and grappling fixture	Nothing (It's almost impossible to perfectly prevent any unexpected friction)
3	**Execute the abort if the vehicle is heading to a hazardous state.**	**the abort command was not provided**	**Was not aware the vehicle was drifting to the ISS**	**The attitude of the cargo is easily disturbed by the robot arm, but the orbit disturbance by the arm is unusual**
5	**Execute the abort if the vehicle is heading to a hazardous state**	**the abort command was not provided**	**Was not aware the vehicle was drifting to the ISS**	**The attitude of the cargo is easily disturbed by the robot arm, but the orbit disturbance by the arm is unusual**
8	Execute the abort if a hazardous condition is recognized	This control was adequate (To keep the other higher level safety constraints, the ME abort was autonomously executed)	Before the departure phase, the first GCC hardware failure had happened. After the automation control was activated by the retreat command, the automation immediately recognized the orbit violation as the second failure and selected the ME abort	N.A.

5.3.4 Coordination and Communication

As discussed in section 5.3.3, the most critical system control problem in the incident was that the abort command was not provided in the loop No.3 and No.5. The fundamental problem of this inadequate control is not that the ISS and GS crews did not issue the abort command. It is just a symptom of an inadequate system design. In other words, to improve the system design and prevent similar future accidents, it is essential to deep dive into the coordination among the human operator, the monitoring system, and the vehicle system.

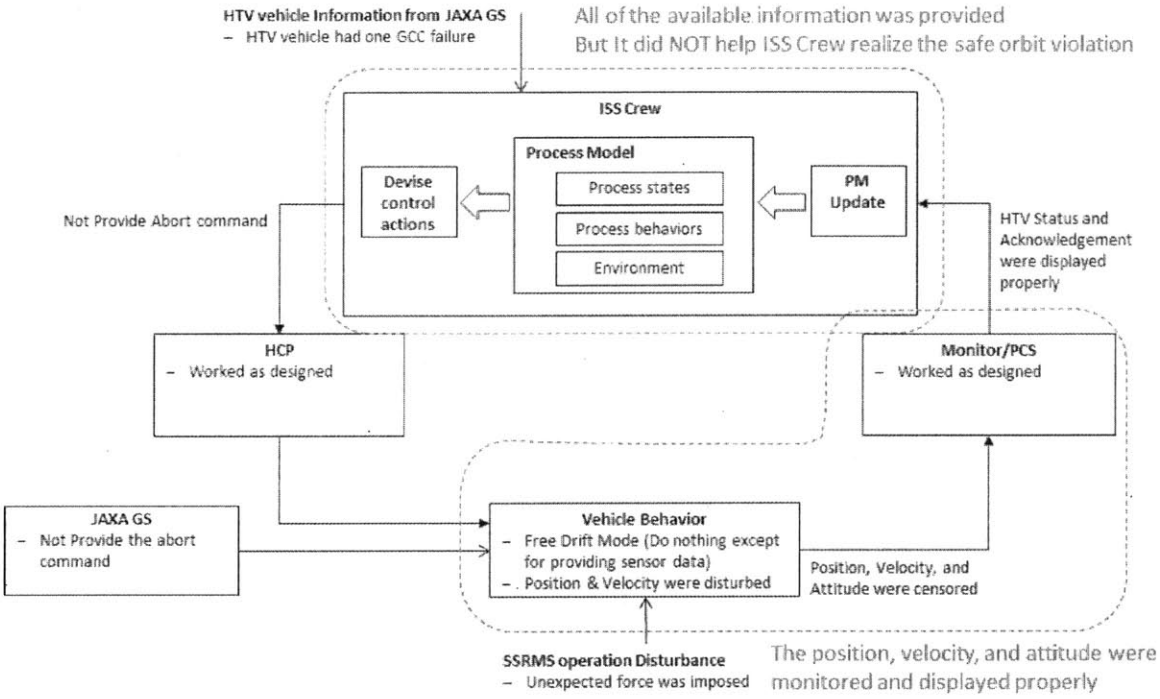


Figure 34: Control Loop for the ISS Crew Behavior in the incident

In order to analyze the coordination, first of all, the control loop diagrams for the loop No.3 and No.5 are created. Figure 34 shows the control loop diagram for the loop No.3. From this diagram, the following two important facts can be found.

- The position, velocity, and attitude of the vehicle were monitored and displayed as designed.
- The ISS and GS crews did not notice the violation although all of the required information was available.

The first point might not seem to be problematic, but it implies that the current design cannot help the human operator's awareness. As indicated in the second point, the operators did not pay attention to the violation even if everything worked as designed. Prof. Leveson pointed out in her lecture that engineers are always thinking about the "screen-in" design of the target system but operators control the system based on the "screen-out" information provided by the system (see Figure 35). This idea indicates that, in complex system, the human factors should be also integrated into the whole system design to maintain safe system operation. The first point exactly represents that the engineer of the HTV system only focused on the screen in, and the second fact definitely indicates that the operators failed in the operation because of the inadequate screen out design. This lack of the integrated system design should be the critical issue which led to the undesirable HTV-3 incident.

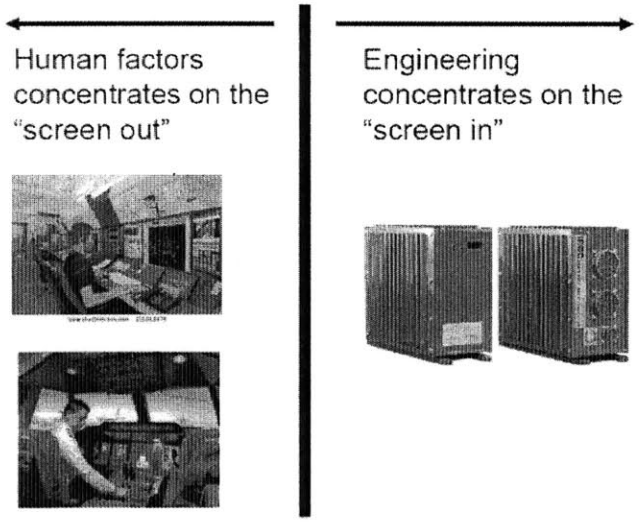


Figure 35: Concept between Screen out vs. Screen in from Prof. Leveson's lecture notes

To analyze how the human factors worked on this incident and improve the human – automation interaction as integrating the human factor into the whole system design, the new human controller model is applied for this incident analysis. This analysis is composed of the following 5 steps:

(1) Identify Unsafe Control Actions (UCAs)

First of all, the unsafe control action which caused the incident is identified. Obviously, the UCA in this incident is "the abort command was not provided when the orbit violation happened." Because the abort could be provided by not only the ISS crew but also GS crew, the UCA should be identified in both control loops.

(2) Identify Process Model (PM) variables

The PM variables represents the important system indicators for controllers to determine the control action. For the PM variables in this incident, the following three system states are identified.

- PM-1: Vehicle Orbit (Not Violated / Violated)
- PM-2: Vehicle Mode (Free Drift / Activated / Hold / Retreat / Abort)
- PM-3: Autonomous Abort Selection (RCS / ME)

The PM-1 represents the vehicle orbit dynamics and it is a critical judgement in this PM if the current orbit violates the safe area or not. The PM-2 is the vehicle mode which can be controlled by the ISS or GS crews, and the automation also can select only the Abort mode when the mode is not Free Drift. Finally, the PM-3 indicates which abort mode the automation selects. This variable is also important, because there would not have been any concern about the contamination if the automation had been able to select the RCS abort.

(3) Identify Inadequate Process Model Update

From this step, based on the new human controller model, it is discussed how the human operators misunderstood the system and wrongly executed the UCA. Firstly, the PM update flaws which can result in the UCA are investigated. For each PM, it is discussed how the update failure influences the whole control. Although possible unsafe scenarios can be also derived from PM-2, the scenario is not a realistic one. On the other hand, the scenarios based on PM-1 and 3 can successfully propose the system design flaws from the human and automation interaction perspective.

The first unsafe control scenario is caused by missing or misunderstanding the change of the PM-1. When the incident happened, the vehicle orbit data was displayed on the monitor as designed, which surely indicated the violation. One of the possible unsafe scenarios is that the ISS and GS crews missed the change or could not understand it meant the violation even if they noticed it, and then did not provide the abort command (see Figure 36). The question is why they missed the change or did not understand it, even though the orbit data was surely displayed. In the current monitor system, the orbit data is just displayed as normal text data, and any highlight (e.g. changing the color of the text) is not given on the monitor. This system characteristic implies that the engineer just designed the monitoring system to show the essential data set, while they had not contemplated how to grab the operator's attention to the critical data variation.

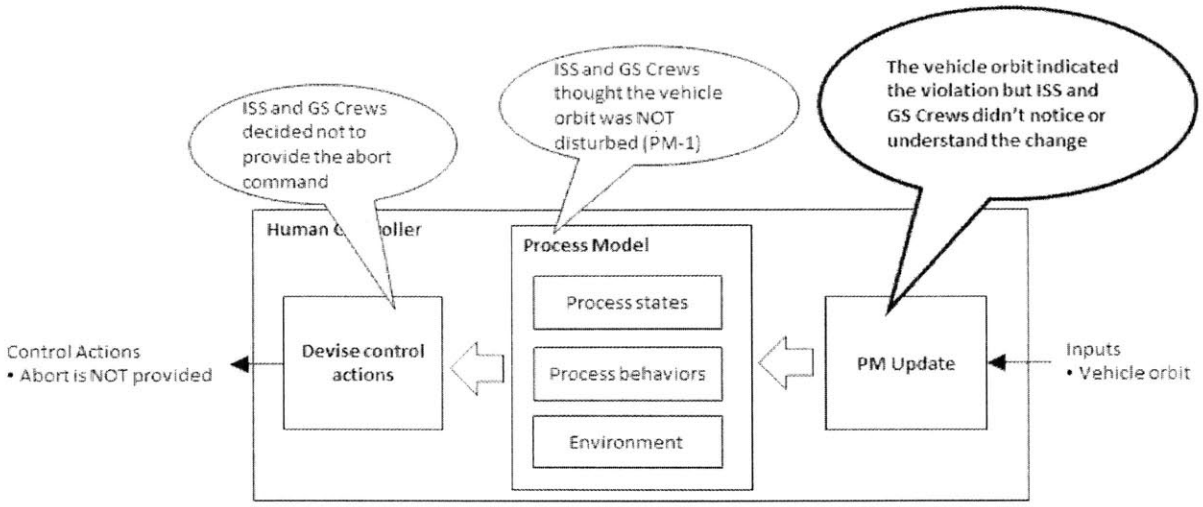


Figure 36: Unsafe Control Scenario cause by PM-1 update flaw

The vehicle mode, PM-2, confusion might be the potential unsafe scenario. Before receiving the retreat or abort command, the vehicle looks staying there even after it is activated, but indeed it can gradually drift out from there because the orbit control is not started yet. When receiving the hold command, on the one hand, the vehicle actually starts the orbit control and keep the current relative position from the ISS by feedback control mechanism. Therefore, if they had been confused with the vehicle mode and thought the vehicle was in the Hold mode, it would have been reasonable not to send the abort command because the position of the vehicle should be stabilized at 10 meter below point from the ISS in the Hold mode. However, this scenario is unrealistic, because the vehicle is in the Hold mode only when the ISS or GS crews issue the Hold command and the Hold command was not actually used in the HTV-3 departure operation. Moreover, issuing the Hold command after releasing the vehicle is not originally planned in the nominal scenario. Thus, it is hard to imagine they guessed the vehicle was in the Hold mode.

The other possible unsafe scenario caused by the PM update flaw is that the ISS and GS Crews forgot that the orbit violation immediately resulted in the ME abort because of one GCC failure and thought the vehicle could conduct the RCS maneuver when detecting the orbit violation. As a result, the manual

abort was not provided (see Figure 37). Of course, all of the vehicle failure status is always shared between the ISS and GS crews before undocking the vehicle from the ISS. However, it is suspicious that in the HTV-3 operation the ISS and GS crews kept the failure in mind during the robot arm operation, because the information was not displayed on the monitor. This failure information should be displayed on the monitor for the operators to be always aware of the failure, because it has a huge impact on the operation.

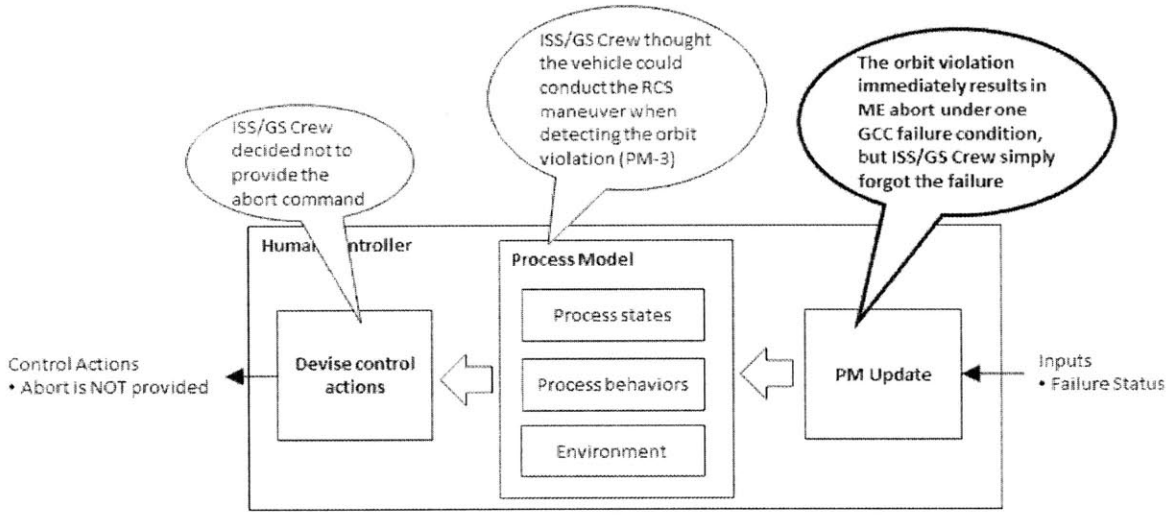


Figure 37: Unsafe Control Scenario caused by PM-3 update flaw

(4) Identify Process Model Flaws

The next step of the analysis is to identify process model flaw. The process model part is composed of three elements: Process States, Process Behaviors, and Environment. In this analysis, a mental flaw in each element is investigated in each PM variable processing, and if the flaw can lead to the UCA is determined. Again any useful scenario cannot be derived from PM-2 processing mental flow, but four probable unsafe control scenarios can be extracted from PM-1 and 3 related flows.

The first unsafe scenario can be defined due to the biased understanding about the SSRMS operation.

If the ISS/GS Crew had believed the vehicle orbit cannot be disturbed by the SSRMS, they would not care about the risk of the orbit violation immediate after the vehicle releasing operation and would miss the opportunity to detect the violation and issue the abort command even if recognizing the displayed orbit information (see Figure 38). As introduced in section 5.3.3, indeed, it had been generally believed that the attitude is easily disturbed by the robot arm but the orbit is rarely influenced. This inadequate belief is behind this unsafe control scenario. The direct countermeasure for this biased belief might be a training and education to fix the belief. However, a better system design solution would be to make the system annunciate the violation to help the human operator in being aware of it. Another similar unsafe scenario is that the ISS/GS Crew notices the orbit disturbance but does not did not think the disturbance is so server as to result in the abort (see Figure 39). In this scenario, it is suggested that the ISS and GS Crews cannot judge the orbit violation from the text data displayed on the monitor, because the violation judgement is based on the orbit propagation algorithm which cannot be calculated without a computer. Therefore, the text orbit data is not exactly what the operators should know, although it is displayed on the monitor. The operators should know if the current orbit violates the safety net or not, because it is the criterion for the abort, and therefore the computer system should calculate the orbit violation and display the result to help their decision making.

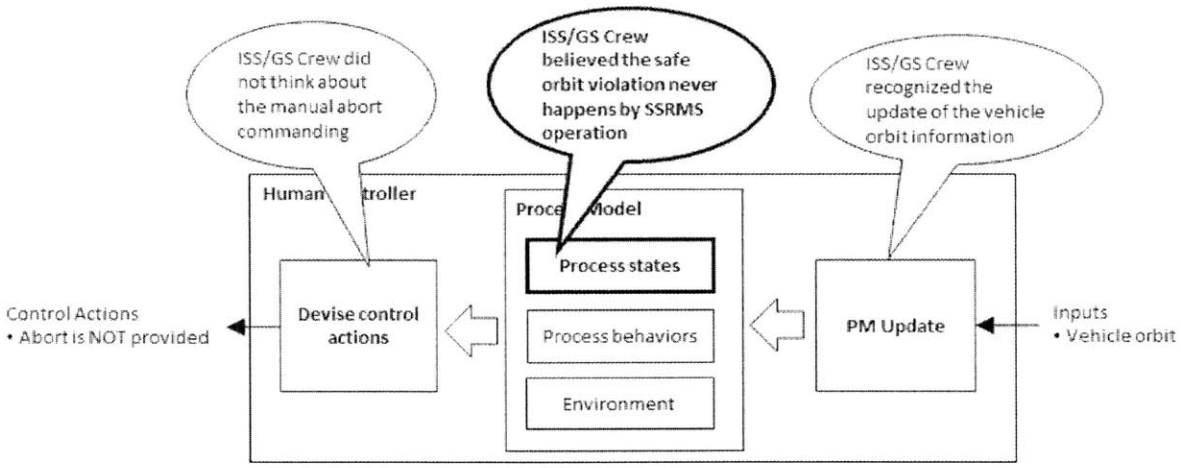


Figure 38: Unsafe Control Scenario caused by PM-1 Process State flaw

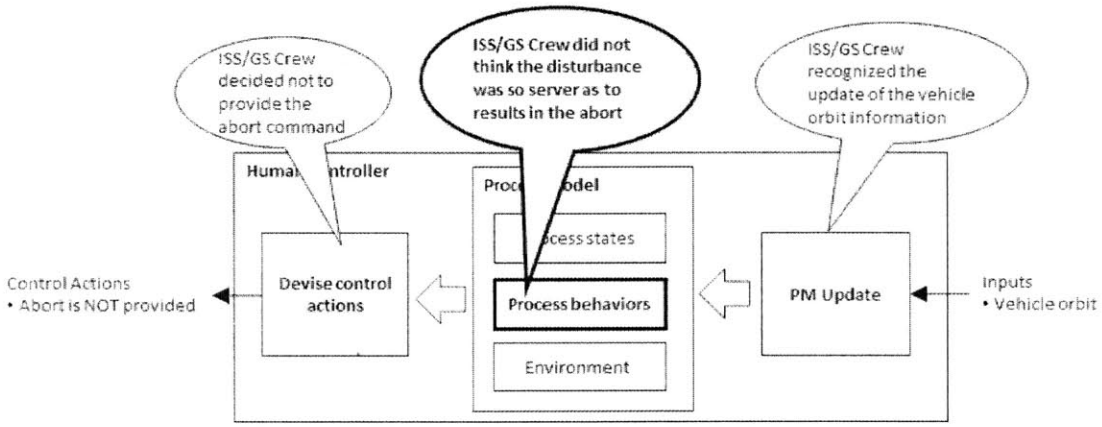


Figure 39: Unsafe Control Scenario caused by PM-1 Process Behavior flaw

The other two unsafe scenarios are related to the autonomous abort behavior. Because the GCC failure is an off-nominal condition, the ISS and GS Crews might not fully understand how it can affect the vehicle functionality. Basically, the existing HTV is a typical redundant system, which could give the operators the wrong impression that the system will work in the same way even when a failure occurs. This lack of system understanding could cause the situation that the ISS and GS Crews wrongly rely on the automation because they believe that the automation can execute the RCS abort like the no failure case (see Figure 40). Moreover, even if they know the GCC failure can change the functionality,

they might not decide to issue the abort command in that situation unless they know how the automation behavior can be changed.

In the incident case, if they knew the orbit violation immediately results in the ME abort under one GCC failure condition, they would carefully manipulate the robot arm and immediately issue the abort command when they noticed the orbit change (see Figure 41). In both scenarios, however, the human operators should not be criticized for the lack of understanding. Instead, it should be taken into account that they have to monitor a lot of data to supervise this complex system. To help them in avoiding the lack of understanding, , the critical component failures having an impact on the functionality should be clearly identified in advance, and the consequences of the failure and the expected manual operation should be shared before starting the operation. In addition, the automation should annunciate its decision to the human operators. Even in the current HTV design, the automation can access any sensor data before the activation. If the software is slightly modified, the automation can also judge the orbit violation even before the activation and annunciate what the automation will do after the activation. Once the ISS and GS Crews know the vulnerability caused by the component failure and the automation's behavior after the activation in advance, they would be able to carefully handle the operation and conduct the manual support before the automation judges everything.

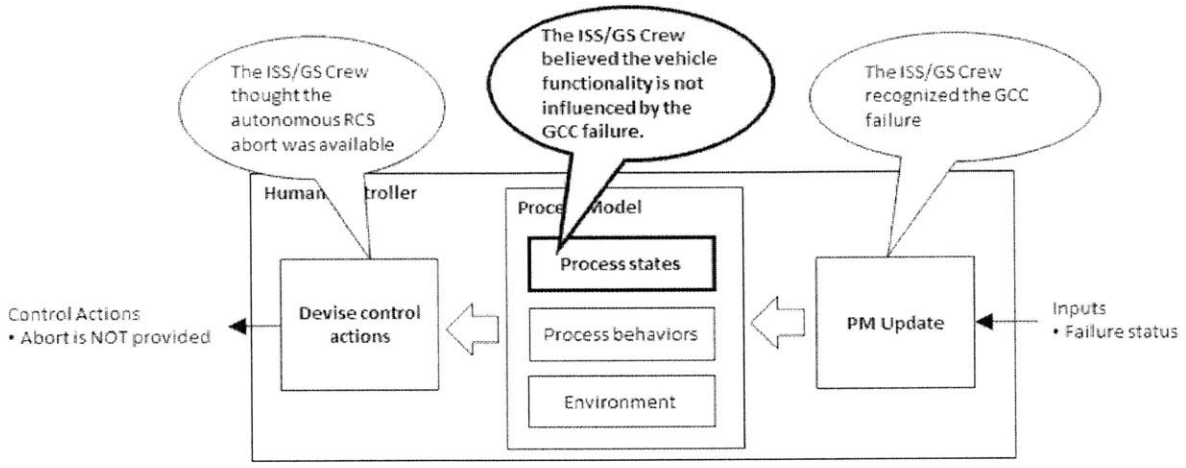


Figure 40: Unsafe Control Scenario caused by PM-3 Process State flaw

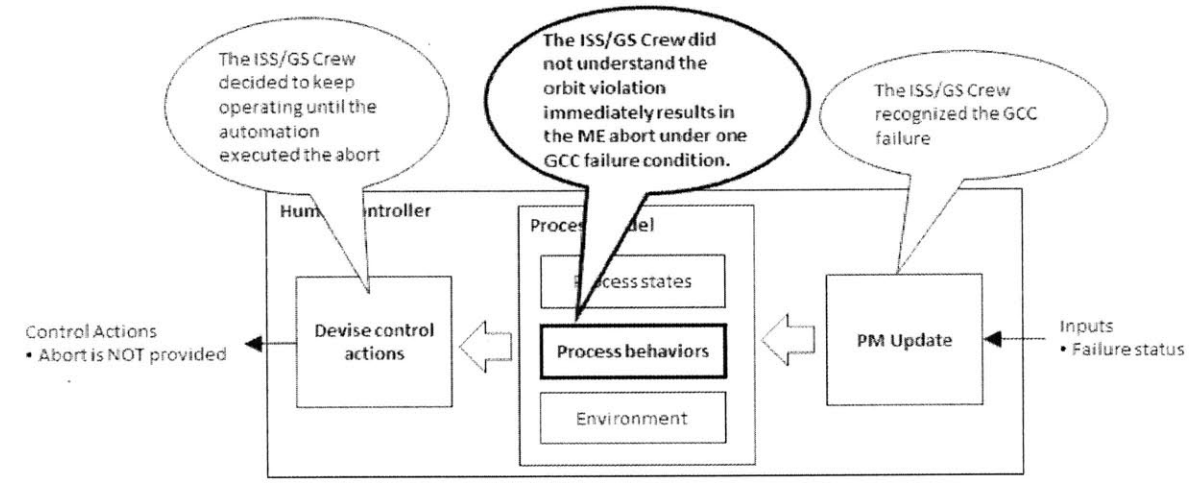


Figure 41: Unsafe Control Scenario caused by PM-3 Process Behavior flaw

(5) Identify Unsafe Decision (Control Action Selection)

Because the ISS and GS Crews are well trained, simple decision mistakes are not expected to happen. Potentially, the following two wrong action selections can be considered.

- The ISS/GS Crew did not know they can make the vehicle do the RCS abort by the manual abort command.

- The ISS/GS Crew did not want to interfere with the automation behavior by the manual abort command.

In both cases, the ISS and GS Crews would not issue the abort command even if the PM variables are adequately updated and the process model of the vehicle is consistent with the actual process. These two unsafe scenarios are theoretically possible, but unrealistic from the ISS program culture perspective. Indeed, the HTV is required to always accept and follow the commands from the ISS and GS Crews. This specification indicates the ISS and GS Crews are always more prioritized than the automation. Therefore, it is hard to assume the scenarios actually happens in the current system.

5.3.5 Design Recommendation

In the discussion in the previous section, a specific design recommendation has been identified from each unsafe scenario. There is no recommendation to impose new brute-force effort (e.g. carefully checking several data items) on the human operator, and rather all of the design recommendations focus on how the computer system can help the human operators. The unsafe scenarios and recommendations are summarized in Table 12. Moreover, the current designs are also listed to compare with the recommended designs.

As shown in the table, the recommended design is intended to support the human operators' decision making by providing the exact information that they need for the decision. The current system just provides the raw data for the decision and requires them to translate the data and guess the actual process state. For example, in the current design, the orbit data is displayed but the orbit violation judgement is not displayed, although it is critical from the operators' decision perspective if the orbit is violated or not. Moreover, the judgement function is already implemented in the vehicle software. In other words, the software to evaluate the orbit violation is already available. Because the orbit data is already available in the ISS and GS Crew's computer systems, it is surely possible to implement the orbit violation judgement function into both computer systems.

Why was this function not implemented in the computer systems? The cost should be quite low, because there is no extra algorithm development and no extra interface design. It is assumed that most of engineering effort was spent on the screen-in design of the system and little effort on the screen-out design. Because the operators of space systems are experts having a lot of knowledge about their systems, they can somehow safely operate the system in most cases. However, like this incident, under off-nominal situations, safe system operation is quite difficult for even such expert operators. Therefore, the recommendations from this analysis will be quite useful design guidelines for the future more complex vehicle design.

Table 12: Safety Responsibility and Inadequate Control Action for each loop

#	Unsafe Scenario	Design Recommendation	Current Design
1	The displayed orbit data indicated the violation, but ISS/GS Crew didn't notice or understand the change. Then, they did not think the abort command was required.	Critical parameter variation (e.g. orbit change) should be highlighted on the monitors	Provides data only. no variation detection, no highlight
2	The orbit violation immediately results in ME abort under one GCC failure condition, but ISS/GS Crew simply forgot the failure. Then, they did not consider to manually execute the RCS abort.	all of the information related to the operator's decisions (e.g. orbit violation, vehicle failure condition) should be displayed.	Simply fundamental data is displayed (e.g. vehicle position and velocity). Some complex information translation is needed for each decision.
3	The ISS/GS Crew believed the orbit violation never happens by the SSRMS. Then, they did not pay attention to the orbit data and missed the violation.	Each safety violation (e.g. safe orbit violation) should be checked and notified to human operators	No violation notification on the monitor. No violation checking function in the ISS and GS systems.
4	The ISS/GS Crew did not think the disturbance was so server as to results in the abort. Then, they did not think the abort command was required.	The system should check the safety violation threshold and annunciate it to the human operators when the violation is detected.	No violation notification on the monitor. No violation checking function in the ISS and GS systems, while the vehicle automation is checking the violation after the activation.
5	The ISS/GS Crew believed the vehicle functionality is not influenced by the GCC failure. Then, they did not think the abort command was safer than the autonomous abort under the GCC failure.	Every component failure which has impact on the system behavior should be identified and shared. This failure information should be displayed.	The critical failures are identified and shared. But it is not displayed on the ISS Crew's monitor.
6	The ISS/GS Crew did not understand the orbit violation immediately results in the ME abort under one GCC failure condition. Then, they decided to keep operating until the automation executed the abort	The vehicle automation should annunciate its future behavior in the Free Drift mode (before the activation).	No one knows the automation behavior before the activation.

5.4 Conclusion of CAST Application

The CAST analysis with the new human controller model suggests various unsafe scenarios and design recommendations. Obviously, these results have not occurred in the technical discussion inside JAXA and can be significantly useful input for the future HTV-X system design. In addition, this approach is not specialized for the HTV system, but should be applied for other human supervisory complex systems. The technical conclusion for the HTV system is given in section 5.4.1 and the academic conclusion about the effectiveness and applicability for the general systems is discussed in section 5.4.2 in detail.

5.4.1 Technical Conclusion

From this analysis, several missing links between displayed items and human operator decisions have been found. Although the displayed information should help the operators in understanding the system state, this result indicates that unfortunately the existing system design is different from the expected one. To solve this problem in the future vehicle development, the engineers should consider "What is critical information for the operators?" when they design the system. In other words, they need to think how to integrate the screen out and screen in designs and create safer interactions between human and computer system.

Another important result from this analysis is that the human operator should know what automation will do. In the incident case, for example, the ISS and GS Crew should have known that the automation tended to execute the ME abort before they sent the activation command. Although the previous study pointed out that the high level automation, which judges and executes everything without human operator's intervention, makes the system rather unstable [30], in space systems this idea cannot be always applied because the human operators cannot always supervise and control the spacecraft from the ground. Indeed, the current full autonomous abort is necessary in the other off-nominal situation to lead the system to safety. However, specifically in this analysis case, the notification before the activation is expected to help the ISS and GS Crews in understanding the system state. Therefore, it is important to analyze the required automation

behavior in each system control and lead to the optimal design by system-theoretic methodology (e.g. STPA) rather than just applying a uniform automation level for all of the automation designs.

5.4.2 Academic Conclusion

In this analysis, the new human controller model was applied for CAST and the human-automation interaction issues could be deeply analyzed. The model can completely fit in the CAST analysis process, and the various and concrete mental flaw patterns can be derived. While existing approaches are composed of not structured process, just provide open brainstorming, or only create too specific design, recommendation, the result of this analysis holistically covered lack of situation awareness, misunderstanding of system behavior, and mis-selection of control action.

In addition, more importantly, system design recommendations can be guided without blaming operators. As mentioned at the beginning of this chapter, the intent of this analysis is not to find and blame human operators' incompetence. In modern complex system context, it does not make sense at all. Instead, the computer system should be designed to enhance the human operator's competence. This analysis did not only answer why the ISS and GS crews did that, but also successfully answered smart engineering solutions for the future vehicle system which do not rely on only the operators' effort. This characteristic is quite useful to design harmonized human – automation interaction in all of modern complex systems

Finally, this approach can be rigorously repeated for understanding accidents and making design recommendations. Once identifying inadequate control actions by human controllers based on the CAST process, the model can be smoothly applied and provide a lot of insights of the accidents from a system control perspective. The other existing models tend to only focus on human mental flow[13] [32], but in this new human mental controller model the controlled process model is in the human mental loop and the focus of this model is how human operators handle the process model. This characteristic is quite important to effectively use the human mental model in the control loop. Because this new model can be harmonized

with the system theoretic model like the control loop model in STPA and CAST, more systemic design approach for the human and automation interaction design can be established.

Chapter 6. Conclusion & Future Plan

The goal of this thesis is to establish the way to design safer systems in the early development phase as preventing hazardous off-nominal behaviors. In addition, because cooperative human - automation design is one of the biggest issues in modern huge and complex systems, the systems are expected to be designed as being capable of supporting human operators to guide a whole system to safety. According to the literature research as shown in chapter 2, the safety design approach based on STAMP is the only way to accomplish this goal. Therefore, to demonstrate the effectiveness, the approach was applied for the future space system in JAXA called HTV-X.

Generally, in the early design phase, two types of engineering effort can be done. One is to directly analyze concept design of the system and refine it. The other one is to elicit important lessons learned from similar past systems and reflect it to the current target system. Based on these two general directions, the following two research objectives for this thesis were defined.

- To identify hazardous scenarios from the concept design of the HTV-X and create requirements and constraints to control the identified hazardous scenarios
- To analyze the actual operation experience in the existing HTV from a system level point of view and effectively utilize the results in the HTV-X system design.

For the concept design analysis, the integrated approach to requirements development and STPA was applied as shown in chapter 4. Furthermore, in chapter 5, the most serious incident from the existing HTV was also analyzed by the system-theoretic accident analysis. While the range of these analyses is limited because the purpose is to demonstrate the effectiveness of those methodologies, the outcomes from the analyses cover various aspects of the system design including the safe human - automation interaction. In section 6.1, the results are summarized again and the remarkable contributions from the analyses are discussed. Finally, the

future work is given in section 6.2.

6.1 Contribution

Generally, a concept design is concurrently analyzed from various disciplinary perspectives, and finally the design is fixed. In this thesis, design recommendations for the concept design of the HTV-X were created from safety perspective. Therefore, some of the recommendations might not be acceptable due to the other design factors not considered in this research. However, to realize a safer system design, it is impossible not to accept the existence of unsafe control actions and causal scenarios. It means that the unsafe control actions and causal scenarios must be eliminated to maintain the system safety even if the recommendations are not acceptable. The significance of the system theoretic analysis is that each recommendation can be traced back to a basic system control through concrete scenarios. In addition, because there is a high affinity between the analysis and general systems engineering, it will be easy for system engineers to understand and discuss the results. Thus, the unacceptable recommendations can be discussed again and modified as being integrated into the system design based on the traced unsafe control actions and causal scenarios. As a result, each design recommendation will have enough high quality to be directly reflected into the actual system design or at least be seriously discussed by the future project team.

The variety of design recommendations is also one of the benefits that can never be gained in any other safety analysis. Generally, in any system analysis, the coverage of unsafe scenarios is quite important. In addition, because a new system architecture is introduced in the HTV-X system, the engineers' central concern of engineers is if they can thoroughly identify new hazardous behaviors induced from the new architecture as early as possible. While it is not a tough task to design essential functions to realize a nominal scenario, identifying holistically off-nominal scenarios and designing the countermeasures are quite difficult, because the designers need to think undesirable system behaviors beyond their original assumption about the system. In the safety guided design analysis based on STPA, a wide variety of off-nominal scenarios

were successfully identified based on the basic system design. Furthermore, the off-nominal scenarios included a lot of undesirable system behaviors induced from the resilient design policy. This result suggests the analysis can help engineers in identifying various unsafe system behaviors and designing new functions to guide the system to safety even if the system architecture is new and immature. Because the flexibility of system design is rapidly lost as the design phase proceeds, this early holistic system safety analysis will be beneficial from the viewpoint of cost as well as safety.

Another important outcome is that the interaction between the human operators and vehicle automation was well analyzed. Especially, in the concept design analysis it was discussed how the operators can guide the automation to safety under complex conditions, and in the incident analysis the way to promote the operator's awareness was discussed. In space systems, some autonomous controls are always essential due to the limitation of the communication between spacecraft and ground stations. The ground operators are required to supervise them and lead their systems to successful states. Therefore, designing the human – automation interaction is always one of the most important tasks in space system development. However, the discussion about the human and automation design tends to be left until the later development phase. Furthermore, some engineers even misunderstand a good interaction between human operator and automation can be realized by only user interface design. Indeed, in most of JAXA's system developments, the issues related to operations always arise after the system designs are almost fixed.

The reason why engineers cannot discuss the design from a whole system perspective in the early development phase is that no one can discuss how human operators guide automation under off-nominal situations unless the off-nominal scenarios are defined from human - automation interaction perspective. Because the traditional safety analysis focuses on physical system structure, the interaction can never be discussed. On the other hand, in the system theoretic safety analysis, it can be described in the control structure and control loop, and finally safer human - automation designs can be established. Therefore, the

analysis will significantly contribute to the successful HTV-X design as a whole system including the human operators and the automation, and show the new system design aspect that has never been discussed in the early system design phase in JAXA's spacecraft.

6.2 Future Work

In the concept design analysis based STPA, because a specific operation phase was the focus, all of the system functions could not be covered by this thesis. Therefore, the system behaviors in the other operation phases should be also analyzed in the future with the same approach. Especially, because the departure and reentry phases are also critical like the final approaching phase, these two phases should be the focus of the next analysis. In addition, although the LEO experimentation will not be a critical operation, it is the operation which has never been conducted in the existing HTV. Therefore, after the concept of the experimentation becomes clearer, this operation should be also analyzed from safety perspective by this method.

Furthermore, more formal analysis can be applied in the safety guided design process. For example, the context table analysis can be already seen as a semi-formal analysis. Therefore, the analysis can be relatively easily upgraded to a formal analysis. In this formal analysis, SpecTRM-RL [24] will support the formalization process and even automatically produce several important indications about the system behaviors under complex conditions that human analysts cannot find [23] [12].

For the incident analysis, the other incidents should be also examined. In this thesis, a specific incident was analyzed, and the ineffective human-automation design was pointed out. While the incident was the most serious one during the existing HTV operations, the other design improvements can be done based on the accident and incident analyses. In the actual operations of the existing HTV, a few operation problems arose

from almost each operation, which were always solved by the operators' effort. First of all, these incidents should be also analyzed from the system theoretic perspective. In addition, the incidents and accidents that happened in JAXA's space systems after the first HTV development should be investigated, because the organizational control and engineering process flaws can be described by CAST. For example, JAXA recently experienced an unexpected automatic launch sequence suspension in 2013 and a serious satellite accident in 2016 [33] [10]. Although these systems are not a human space system like the HTV-X, the outcomes from the CAST analysis for these two cases might be effective even in the HTV-X system development, because an identical organizational or engineering process problem might exist behind the incident and accident.

Finally, the most important next step for the future successful system developments is to interweave the system-theoretic analysis into system engineering process as a whole organization. Generally, engineers tend to rely on the methods that they used in the past developments unless the past systems did not fail. However, the complexity of systems keeps increasing and consequently new systems are largely different from the past. Moreover, the development cycle in space systems are quite longer than the other industries. For example, the existing HTV development was officially started in 1997, and after almost 20 years later the new transfer vehicle development is being started. Therefore, JAXA should appropriately accept the fact that the past engineering approach somehow worked effectively a few decades ago but now its validity is suspicious in modern complex systems. Instead of applying the past engineering methods for new systems, the system engineering process should be enhanced from system safety perspective based on STAMP and related methodologies.

Bibliography

[1] A. Witze, "Software error doomed Japanese Hitomi spacecraft : Nature News & Comment," *Nature*, vol. 553, 28-Apr-2016.

[2] N. Leveson, *Engineering a safer world: systems thinking applied to safety*. Cambridge, Mass. : MIT Press, c2011 (Norwood, Mass. : Books24x7.com [generator]), 2011.

[3] Japan Aerospace Exploration Agency, "HTV-1 Mission Press Kit." 2009.

[4] Japan Aerospace Exploration Agency, "Development Proposal for Next Generation Unmanned Transfer Vehicle, HTV-X (HTV-X(仮称)の開発案について)," 02-Jul-2015. [Online]. Available: http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu2/059/shiryo/__icsFiles/afieldfile/2015/07/16/1359656_5.pdf.

[5] W. F. Larsen, "Fault tree analysis," U.S. Army Picatinny Arsenal, Dover, Technical Report 4556, Jan. 1974.

[6] Department of Defense, "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," MIL-STD-1629A, Nov. 1980.

[7] S. B. Arden Albee, "Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions," *NASA STIRecon Tech. Rep. N*, p. 61967, 2000.

[8] "HTV-3 Abort Caused By Friction With Station Arm," *Aviation Week Network*, 2013. [Online]. Available: http://aviationweek.com/awin/htv-3-abort-caused-friction-station-arm. [Accessed: 20-Oct-2015].

[9] N. Leveson, "A new accident model for engineering safer systems," *Saf. Sci.*, vol. 42, no. 4, pp. 237–270, 2004.

[10] Japan Aerospace Exploration Agency, "Accident Report of the X-ray astronomical satellite ASTRO-H, Hitomi (X 線天文衛星 ASTRO-H 「ひとみ」異常事象調査報告書)," *JAXA official website*, 14-Jun-2016. [Online]. Available: http://www.jaxa.jp/press/2016/06/files/20160614_hitomi_01_j.pdf.

[11] C. H. Fleming, "Safety-driven Early Concept Analysis and Development," Massachusetts Institute of Technology, 2015.

[12] T. Ishimatsu, N. G. Leveson, J. P. Thomas, C. H. Fleming, M. Katahira, Y. Miyamoto, R. Ujiie, H. Nakao, and N. Hoshino, "Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis," *J. Spacecr. Rockets*, vol. 51, no. 2, pp. 509–522, Mar. 2014.

[13] "Proposal of Next Generation Unmanned Transfer Vehicle, HTV-X."

[14] E. Berger, "NASA official warns private sector: We're moving on from low-Earth orbit | Ars Technica," *arstechnica*, 07-Dec-2015.

[15] European Space Agency, "Automated Transfer Vehicle," EUC-ESA-FSH-003, 2007.

[16] SpaceX, "Dragon Spacecraft Fact Sheet." [Online]. Available: http://www.spacex.com/sites/spacex/files/pdf/DragonLabFactSheet.pdf.

[17] *Work Schedule of the Basic Plan for Japanese Space Policy*. 2015.

[18] S. Ueda, T. Kasai, and H. Uematsu, "HTV rendezvous technique and GN&C design evaluation based on 1st flight on-orbit operation result," in *Proceedings of the AIAA Guidance Navigation, and Control Conference*, 2010.

[19] Y. Ito and K. Inoue, "Status Report of the Electrodynamic Tether experimentation in the HTV-6 Flight (HTV 搭載導電性テザー実証実験の検討状況について)," 04-Sep-2013. [Online]. Available: http://www.jaxa.jp/press/2013/09/20130904_htv_j.pdf.

[20] H. Nomoto, S. Ueda, and R. Ujiie, "Risk Assessment based on Resilience Engineering for Adaptive GNC System," presented at the 30th International Symposium on Space Technology and Science, 2015.

[21] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience engineering : concepts and precepts*. Aldershot, England ; Burlington, VT : Ashgate, c2006., 2006.

[22] J. Thomas, J. Sgueglia, D. Suo, N. Leveson, M. Vernacchia, and P. Sundaram, "An Integrated Approach to Requirements Development and Hazard Analysis," 2015.

[23] J. Thomas, "Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis," Massachusetts Institute of Technology, 2013.

[24] N. Leveson, "Completeness in formal specification language design for process-control systems," in *Proceedings of the third workshop on Formal methods in software practice*, 2000, pp. 75–87.

[25] "H-IIA Launch Vehicle No.6 Why did the accident happen?," *JAXA official website*. [Online]. Available: http://global.jaxa.jp/article/special/h2a6/index_e.html.

[26] P. Harding, "Japan's HTV-3 aborts to depart the ISS following resupply mission | NASASpaceFlight.com," *NASA Spaceflight.com*, 12-Sep-2012. [Online]. Available: http://www.nasaspaceflight.com/2012/09/htv-3-aborts-iss-following-successful-resupply-mission/.

[27] "HTV-3:H-II Transfer Vehicle KOUNOTORI (HTV) - International Space Station - JAXA," *JAXA official website*. [Online]. Available: http://iss.jaxa.jp/en/htv/mission/htv-3/.

[28] Y. Koyari, "Report of HTV-3 depature and reentry operation results (宇宙ステーション補給機「こ

うのとり」3号機（HTV3）の分離・再突入結果について)," 11-Oct-2012. [Online]. Available: http://www.jaxa.jp/press/2012/10/20121011_kounotori3.pdf.

[29] N. G. Leveson, "Integrating Safety Information into the System," presented at the 21st International System Safety Conference, Ontario, Canada, 2003.

[30] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *Syst. Man Cybern. Part Syst. Hum. IEEE Trans. On*, vol. 30, no. 3, pp. 286–297, 2000.

[31] T. B. Sheridan, "Rumination on automation," *Annu. Rev. Control*, vol. 25, pp. 89–97, 2001.

[32] B. Brehmer, "The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control," in *Proceedings of the 10th international command and control research technology symposium*, 2005, pp. 365–368.

[33] "JAXA | Launch Cancellation of Epsilon-1 with SPRINT-A Onboard," *JAXA official website*. [Online]. Available: http://global.jaxa.jp/press/2013/08/20130827_epsilon_e.html.

Appendix A

In Appendix A, all of the detailed analysis results of chapter 4 is shown. Table A-1 is the full unsafe control action table including all unsafe control actions, and all of the safety constraints for the HTV-X system is shown in Table A-2. Table A-3 lists the first revised control structure elements based on the constraints. In Figure A-1, the control loop diagrams used in identifying the causal scenarios are shown, and TableA-4 lists the design recommendations derived from the scenarios. Finally, Table A-5 shows the complete context table used in the second analysis cycle.

Table A-1: Unsafe Control Action Table (1/3)

#	Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
1	**Approach Initiation** ISS Status = OK: T Vehicle Orbit = Deviated: F Vehicle Attitude = Nominal: T Vehicle Mode = CAM: F Vehicle Status = OK: T Control Performance > AI: T	(The vehicle keeps staying at the AI point)	**UCA-1.1**: Providing the approach initiation when the orbit is deviated can cause H-1, or H-2 **UCA-1.2**: Providing the approach initiation when the vehicle's attitude is not nominal can cause H-1, H-2, or H-3 **UCA-1.3**: Providing the approach initiation when the vehicle is executing the abort maneuver or passive CAM can cause H-1, or H-2 **UCA-1.4**: Providing the approach initiation when the vehicle is not ready can cause H-1, H-2, or H-3 **UCA-1.5**: Providing the approach initiation when the control performance is less than the AI maneuver performance can cause H-1, H-2, or H-3.	**UCA-1.6**: Providing the approach initiation when the ISS is not ready (= before the approach permission is not provided) can cause H-4	N.A.
2	**Passive CAM** Vehicle Orbit = KOS: F, F Vehicle Orbit = Deviated: T Vehicle Mode = CAM: F, F Vehicle Status = OK: F Control Performance > Attd Control: T, T	-> No.8	**UCA-2.1**: Providing the passive CAM when the orbit violates the KOS can cause H-1 **UCA-2.2**: Providing the passive CAM when the vehicle is executing the abort maneuver can cause H-1 **UCA-2.3**: Providing the approach initiation when the control performance is less than the attitude control performance can cause H-1, H-2, or H-3	-> No.8	N.A.
3	**Abort** ISS Status = OK: F Vehicle Orbit = KOS: T Vehicle Attitude = Nominal: T, T, T Vehicle Status = OK: F Control Performance > Abort: T, T, T	**UCA-3.1**: Not providing the abort when the ISS is not ready can cause H-4	**UCA-3.2**: Providing the abort when the control performance is less than the abort performance can cause H-1, H-2, or H-3 **UCA-3.3**: Providing the abort when the vehicle attitude is not nominal can cause H-1, H-2, or H-3	-> No.8	N.A.

Table A-1: Unsafe Control Action Table (2/3)

#	Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
4	**Hold** ISS Status = OK: F Vehicle Orbit = KOS: F Vehicle Orbit = Deviated: T Vehicle Attitude = Nominal: T T Vehicle Mode = CAM: F F Vehicle Status = OK: T T Control Performance > Hold: T T RVS Capture = ON: T T	(-> No.3, No.8)	**UCA-4.1**: Providing the hold when the orbit violates the KOS can cause H-1 **UCA-4.2**: Providing the hold when the vehicle attitude is not nominal can cause H-1, H-2, or H-3 **UCA-4.3**: Providing the hold when the vehicle is executing the abort maneuver or passive CAM can cause H-1, or H-2 **UCA-4.4**: Providing the hold when the vehicle status is not ready can cause H-1, H-2, or H-3 **UCA-4.5**: Providing the hold when the available maneuver performance is less than the hold performance can cause H-1, H-2, or H-3 **UCA-4.6**: Providing the hold when the laser reflection is not captured by the RVS can cause H-1 or H-2	-> No.8	N.A.
5	**Nominal Maneuvers** Approach Initiation is Provided: T Vehicle Orbit = Deviated: F Vehicle Attitude = Nominal: T Vehicle Mode = CAM: F Vehicle Status = Ready: T Control Performance > AI: T	The vehicleStay there or -> No.8	**UCA-5.1**: Providing the nominal maneuver when the vehicle orbit is deviated or violates the KOS can cause H-1, or H-2 **UCA-5.2**: Providing the nominal maneuver when the attitude is not nominal can cause H-1, H-2, or H-3 **UCA-5.3**: Providing the nominal maneuver when the vehicle is executing abort or passive CAM can cause H-1 or H-2 **UCA-5.4**: Providing the nominal maneuver when the vehicle status is not ready can cause H-1, H-2, or H-3 **UCA-5.5**: Providing the nominal maneuver when the control performance is less than the AI maneuver performance can cause H-1, H-2, or H-3	**UCA-5.6**: Providing the nominal maneuvers when the ISS is not ready (= before the approach initiation is not provided) can cause H-4	**UCA-5.7**: Applying the nominal maneuvers too long can cause H-3

Table A-1: Unsafe Control Action Table (3/3)

#	Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopping Too Soon /Applying Too Long Causes Hazard
6	**R-bar Approaching Control** Vehicle Orbit = KOS: F Vehicle Attitude = Nominal: T Vehicle Mode = CAM: F Vehicle Status = OK: T Control Performance > R-bar: T RVS Capture = ON: T	-> No.8	**UCA-6.1**: Providing the R-bar approaching control when the orbit violates the KOS can cause H-1 **UCA-6.2**: Providing the R-bar approaching control when the vehicle attitude is not nominal can cause H-1 or H-2 **UCA-6.3**: Providing the R-bar approaching control when the vehicle is executing the abort maneuver or passive CAM can H-1, or H-2 **UCA-6.4**: Provides the R-bar approaching control when the vehicle status is not ready can cause H-1, H-2, or H-3 **UCA-6.5**: Providing the R-bar approaching control when the control performance is less than the R-bar approaching control performance can cause H-1, H-2, or H-3 **UCA-6.6**: Providing the R-bar approaching control when the laser reflection is not captured by the RVS can cause H-1 or H-2	-> No.8	**UCA-6.7**: Applying the R-bar approaching control too long can cause H-3
7	**Attitude Control** Control Performance > Attitude Control: T	**UCA-7.1**: Not providing the attitude control can cause H-1, H-2, or H-3	**UCA-7.2**: Providing the attitude control when the control performance is less than the attitude control performance can cause H-1, H-2, or H-3	-> No.8	**UCA-7.3**: Applying the attitude control too long can cause H-3
8	**Abort Maneuver** Abort is Provided: T Vehicle Orbit = KOS: T Control Performance > Abort: T T	**UCA-8.1**: Not providing the abort maneuver when the ISS is not ready (= the abort is provided by ISS or GS crew can cause H-4 **UCA-8.2**: Not Providing the abort maneuver when the KOS is violated can causes H-1	**UCA-8.3**: Providing the abort maneuver when the control performance is less than the abort performance can cause H-1, H-2, or H-3.	(The vehicle can autonomously execute abort without any command)	**UCA-8.4**: Stopping the abort maneuver too soon can cause H-1 or H-2 **UCA-8.5**: Applying the abort maneuver too long can cause H-2, or H-3.

Table A-2: Safety Constraint Table (1/2)

Safety Constraint		Related UCAs
SC-1: Any command except for the passive CAM must not be provided when the attitude is not nominal	**SC-1.1**: The approach initiation command must not be provided when the attitude is not nominal	UCA-1.2
	SC-1.2: The abort command must not be provided when the attitude is not nominal	UCA-3.2
	SC-1.3: The hold command must not be provided when the attitude is not nominal	UCA-4.2
SC-2: Any command except for the abort must not be provided when the vehicle is executing the abort maneuver or passive CAM	**SC-2.1**: Tne approach initiation command must not be provided when the vehicle is executing the abort maneuver or passive CAM	UCA-1.3
	SC-2.2: Tne passive CAM command must not be provided when the vehicle is executing the abort maneuver	UCA-2.2
	SC-2.3: Tne hold command must not be provided when the vehicle is executing the abort maneuver or passive CAM	UCA-4.3
SC-3: The approach initiation and hold command must not be when the vehicle status is not ready for the maneuvers	**SC-3.1**: The approach initiation command must not be provided when the vehicle status is not ready for the maneuvers	UCA-1.4
	SC-3.2: The hold command must be provided when the vehicle status is not ready for the control	UCA-4.4
SC-4: Each command must be prvided only when the current control performance satisfies the required performance for the command	**SC-4.1**: The approach initiation command must not be provided when the control performance is less than the AI maneuver performance	UCA-1.5
	SC-4.2: The passive CAM command must not be provided when the control performance is less than the attitude control performance	UCA-2.3
	SC-4.3: The abort command must not be provided when the control performance is less than the abort maneuver performance	UCA-3.3
	SC-4.4: The hold command must not be provided when the control performance is less than the hold control performance	UCA-4.5
SC-5: The passive CAM and hold command must not be provided when the orbit violates the KOS	**SC-5.1**: The passive CAM command must not be provided when the orbit violates the KOS	UCA-2.1
	SC-5.2: The hold command must not be provided when the orbit violates the KOS	UCA-4.1
SC-6: Any maneuver must not be provided when the attitude is not nominal	**SC-6.1**: The nominal maneuvers must not be provided when the attitude is not nominal	UCA-5.2
	SC-6.2: The R-bar approaching control must not be provided when the attitude is not nominal	UCA-6.2
	SC-6.3: The abort maneuver must not be provided when the attitude is not nominal	UCA-8.3
SC-7: Any maneuver except for the abort maneuver must not be provided when the vehicle is executing the abort maneuver or passive CAM	**SC-7.1**: The nominal maneuvers must not be provided when the vehicle is executing the abort maneuver or passive CAM	UCA-5.3
	SC-7.2: The R-bar approaching control must not be provided when the vehicle is executing the abort maneuver or passive CAM	UCA-6.3
SC-8: The nominal maneuvers and R-bar approaching control must not be provided when the vehicle status is not ready for the maneuvers	**SC-8.1**: The nominal maneuvers must not be provided when the vehicle status is not ready for the maneuvers	UCA-5.4
	SC-8.2: The R-bar approaching control must not be provided when the vehicle status is not ready for the maneuvers	UCA-6.4

Table A-2: Safety Constraint Table (2/2)

Safety Constraint		Related UCAs
SC-9: Each control must be provided only when the current control performance satisfies the required performance for the control	**SC-9.1**: The nominal maneuvers must not be provided when the control performance is less than the AI maneuver performance	UCA-5.5
	SC-9.2: The R-bar approaching control must not be provided when the control performance is less than the R-bar approaching control performance	UCA-6.5
	SC-9.3: The attitude control must not be provided when the control performance is less than the attitude control performance	UCA-7.2
	SC-9.4: The abort maneuver must not be provided when the control performance is less than the abort maneuver performance	UCA-8.4
SC-10: Each control must be provided within an acceptable thrusting range	**SC-10.1**: The nominal maneuvers must not be applied over an acceptable thrusting amount	UCA-5.7
	SC-10.2: The R-bar approaching control must not be applied over an acceptable thrusting amount	UCA-6.7
	SC-10.3: The R-bar approaching control must not be applied over an acceptable thrusting amount	UCA-6.7
	SC-10.4: The attitude control must not be applied over an acceptable thrusting amount	UCA-7.3
	SC-10.5: The abort maneuver must be provided within an acceptable thrusting amount range	UCA-8.5, 8.6
SC-11: The approach initiation command must not be provided when the orbit is deviated from the planned orbit		UCA-1.1
SC-12: The approach initiation command must not be provided before the approach permission is provided by NASA GS		UCA-1.6
SC-13: The abort command mush be provided when the ISS is not ready for the approaching		UCA-3.1
SC-14: The hold command must not be provided when the laser reflection is not captured by the RVS		UCA-4.6
SC-15: The nominal maneuvers must not be provided when the orbit is deviated from the planned orbit		UCA-5.1
SC-16: The nominal maneuvers must not be provided before receiving the approach initiation command		UCA-5.6
SC-17: The R-bar approaching control must not be provided when the orbit is violates the KOS		UCA-6.1
SC-18: The R-bar approaching control must not be provided when the laser reflection is not captured by the RVS		UCA-6.6
SC-19: The attitude control must be provided		UCA-7.1
SC-20: The abort maneuver must be provided when the abort command is provided		UCA-8.1
SC-21: The abort maneuver must be provided when the orbit violates the KOS		UCA-8.2

Table A-3: Control Structure Revision Analysis Table (1/2)

Safety Constraint	Does the initial control structure allow the controller to monitor the conditions in the constraints?	Do additional control actions need to be added to achieve or enforce the constraints?	Are there other controllers that may interfere with or violate the constraints?
SC-1: Any command except for the passive CAM must not be provided when the attitude is not nominal	"Attitude Anomaly" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	No	No
SC-2: Any command except for the abort must not be provided when the vehicle is executing the abort maneuver or passive CAM	"Vehicle Mode" should be added on the feedback from the vehicle automation to GS/ISS crew through the OCS/PROX C&DH	No	No
SC-3: The approach initiation and hold command must not be when the vehicle status is not ready for the maneuvers	"Vehicle Status Anomaly" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	No	No
SC-4: Each command must be prvided only when the current control performance satisfies the required performance for the command	"Thruster Firing Time" should be added on the feedback from the vehicle dynamics to the vehicle automation "Thruster Firing Time" should be added on the feedback from the vehicle automation to the OCS and PROX C&DH "Control Performance" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	No	No
SC-5: The passive CAM and hold command must not be provided when the orbit violates the KOS	"KOS Violation Warning" should be added on the feedback from the OCS/PROX C&DH to GS/ISS crew	No	No
SC-6: Any maneuver must not be provided when the attitude is not nominal	Yes	No	No
SC-7: Any maneuver except for the abort maneuver must not be provided when the vehicle is executing the abort maneuver or passive CAM	Yes	No	No
SC-8: The nominal maneuvers and R-bar approaching control must not be provided when the vehicle status is not ready for the maneuvers	Yes	No	No
SC-9: Each control must be provided only when the current control performance satisfies the required performance for the control	"Thruster Firing Time" should be added on the feedback from the vehicle dynamics to vehicle automation	No	No
SC-10: Each control must be provided within an acceptable thrusting range	"Thruster Firing Time" should be added on the feedback from the vehicle dynamics to vehicle automation	No	No
SC-11: The approach initiation command must not be provided when the orbit is deviated from the planned orbit	"Orbit Deviation Warning" should be added on the feedback from the OCS to GS crew	No	No

Table A-3: Control Structure Revision Analysis Table (2/2)

Safety Constraint	Does the initial control structure allow the controller to monitor the conditions in the constraints?	Do additional control actions need to be added to achieve or enforce the constraints?	Are there other controllers that may interfere with or violate the constraints?
SC-12: The approach initiation command must not be provided before the approach permission is provided by NASA GS	Yes	No	No
SC-13: The abort command mush be provided when the ISS is not ready for the approaching	"ISS Status" should be added on the voice loop between the ISS and GS crew	No	No
SC-14: The hold command must not be provided when the laser reflection is not captured by the RVS	Yes	No	No
SC-15: The nominal maneuvers must not be provided when the orbit is deviated from the planned orbit	Yes	No	No
SC-16: The nominal maneuvers must not be provided before receiving the approach initiation command	Yes	No	No
SC-17: The R-bar approaching control must not be provided when the orbit is violates the KOS	Yes	No	No
SC-18: The R-bar approaching control must not be provided when the laser reflection is not captured by the RVS	Yes	No	No
SC-19: The attitude control must be provided	Yes	No	No
SC-20: The abort maneuver must be provided when the abort command is provided	Yes	No	No
SC-21: The abort maneuver must be provided when the orbit violates the KOS	Yes	No	No

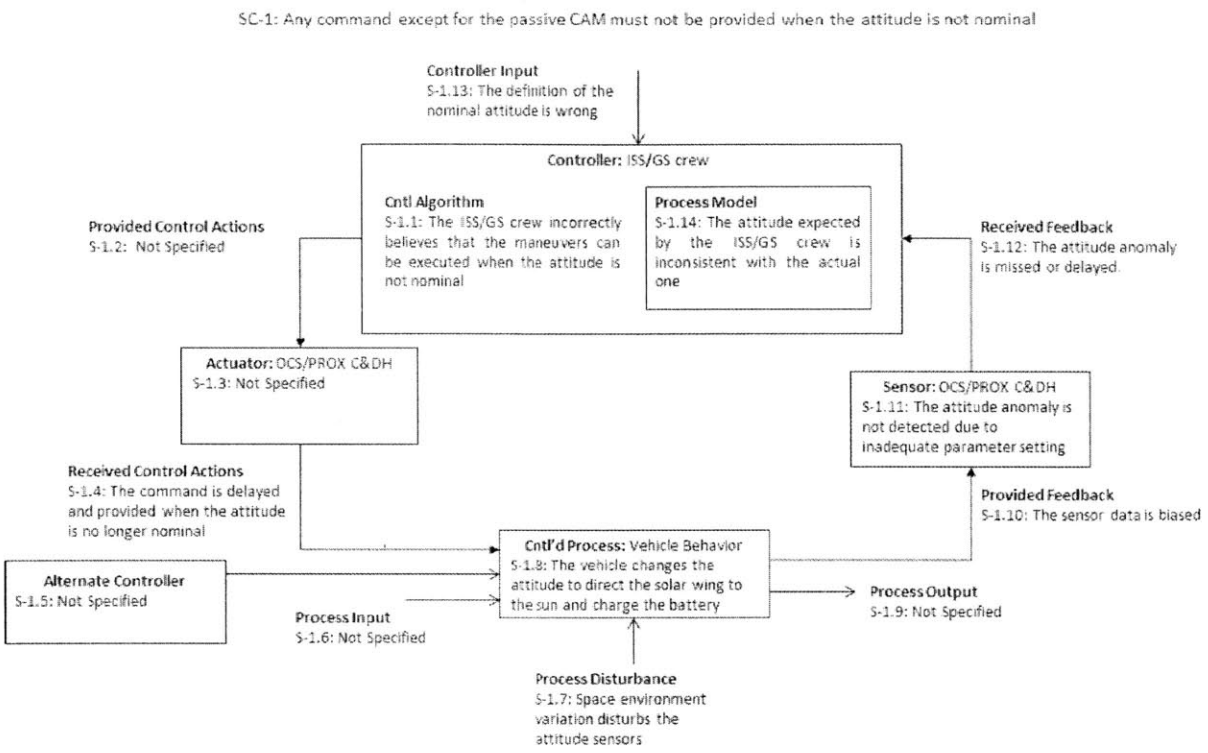


Figure A-1: Control Loop Diagram for the Safety Constraints (1/11)

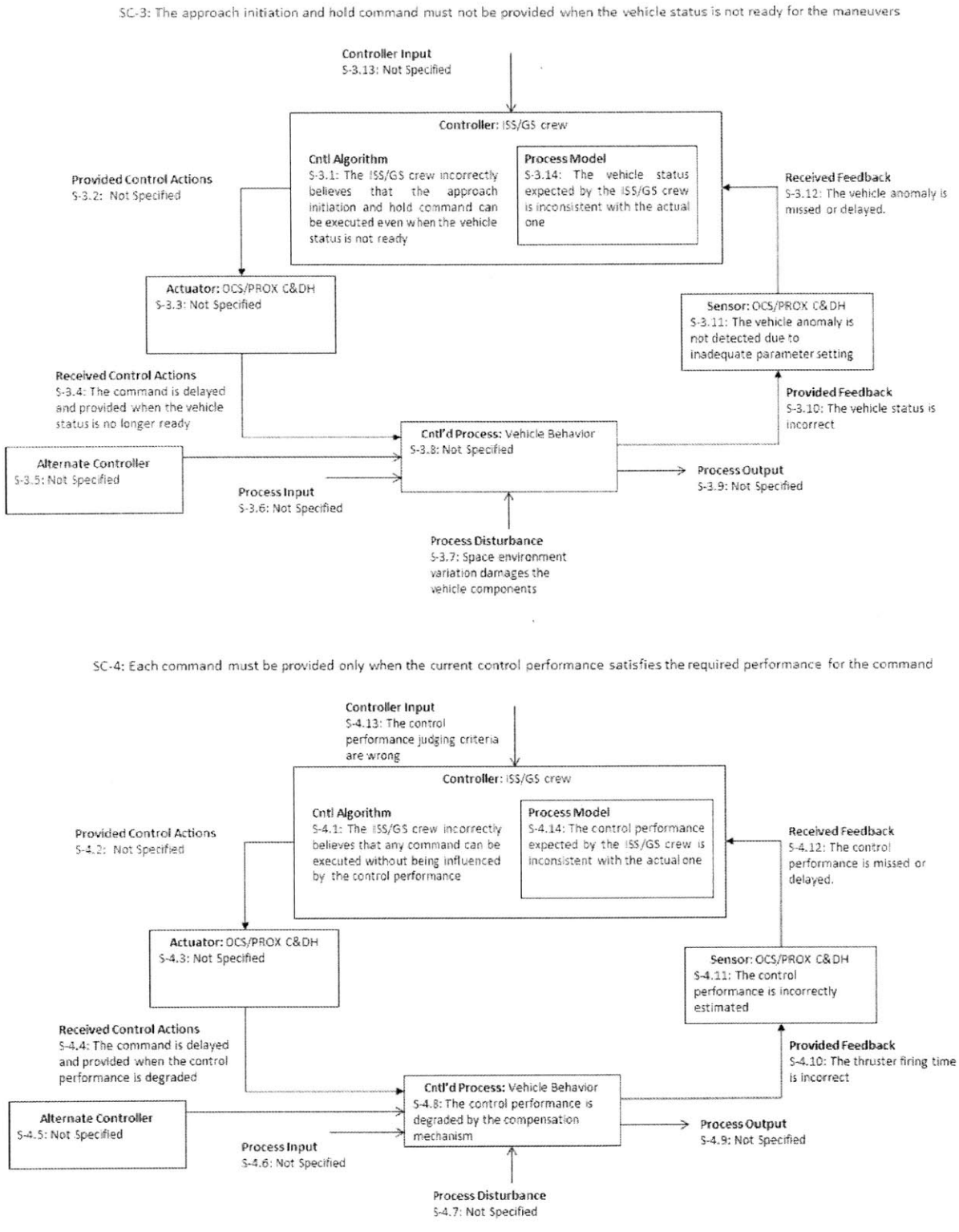


Figure A-1: Control Loop Diagram for the Safety Constraints (2/11)

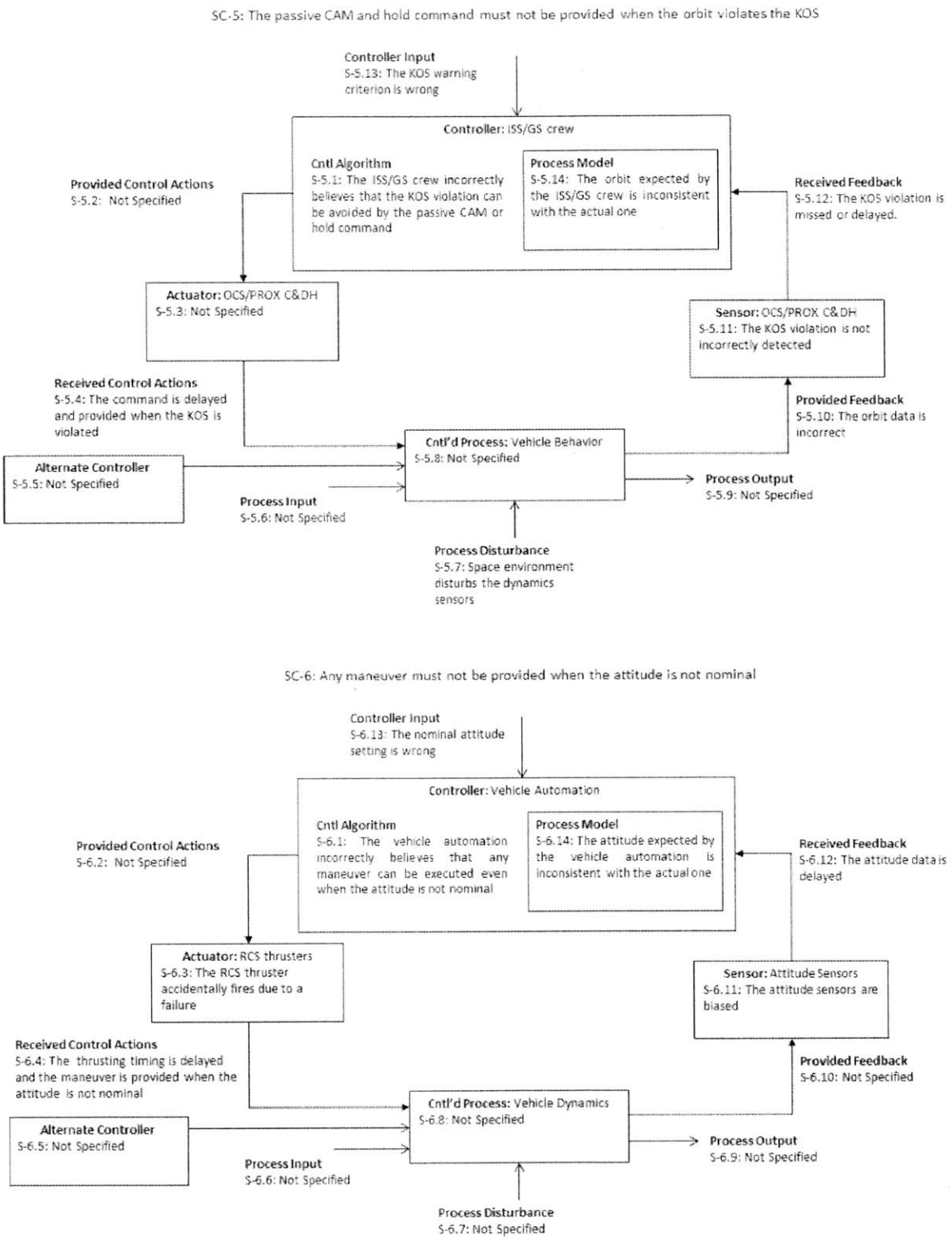


Figure A-1: Control Loop Diagram for the Safety Constraints (3/11)

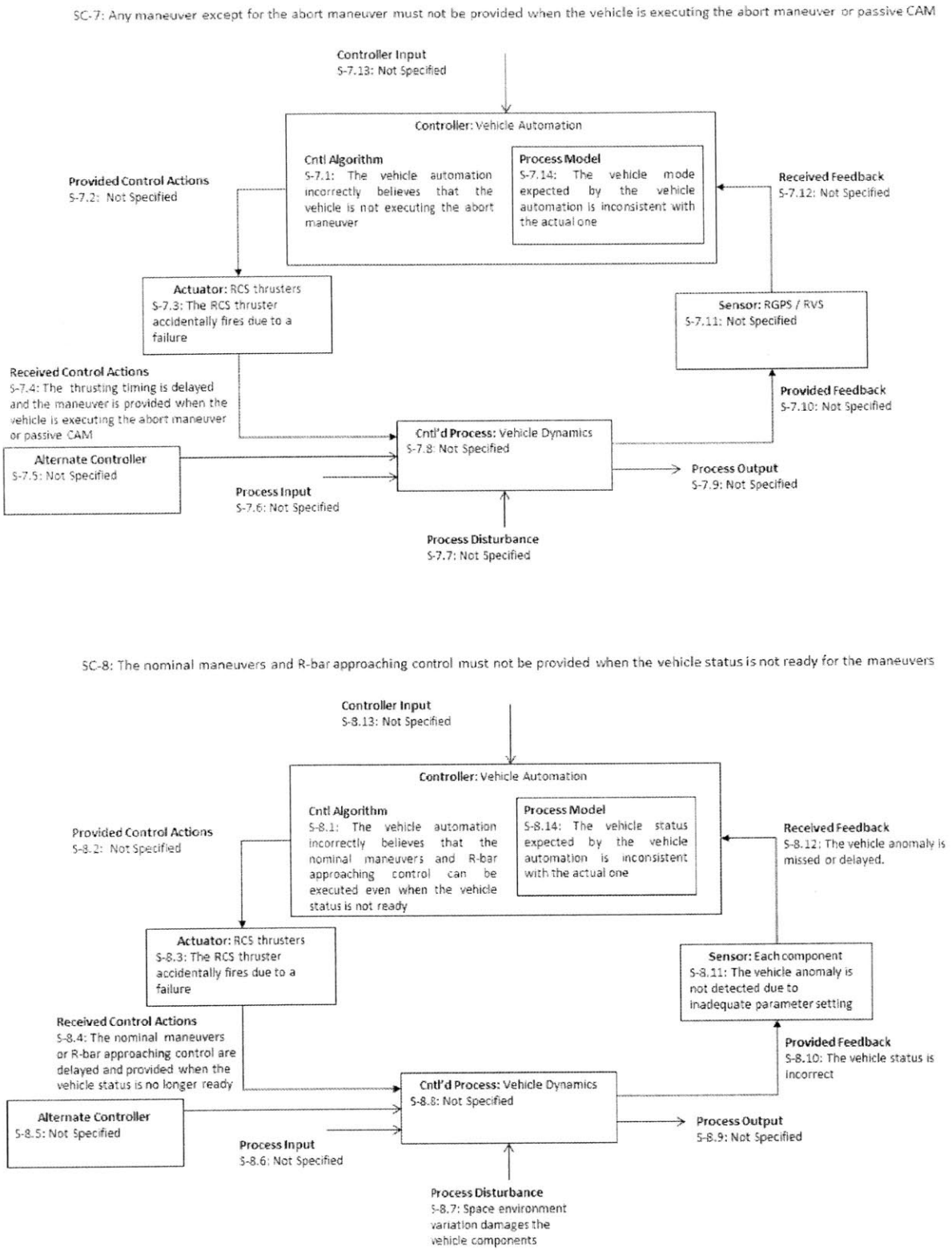
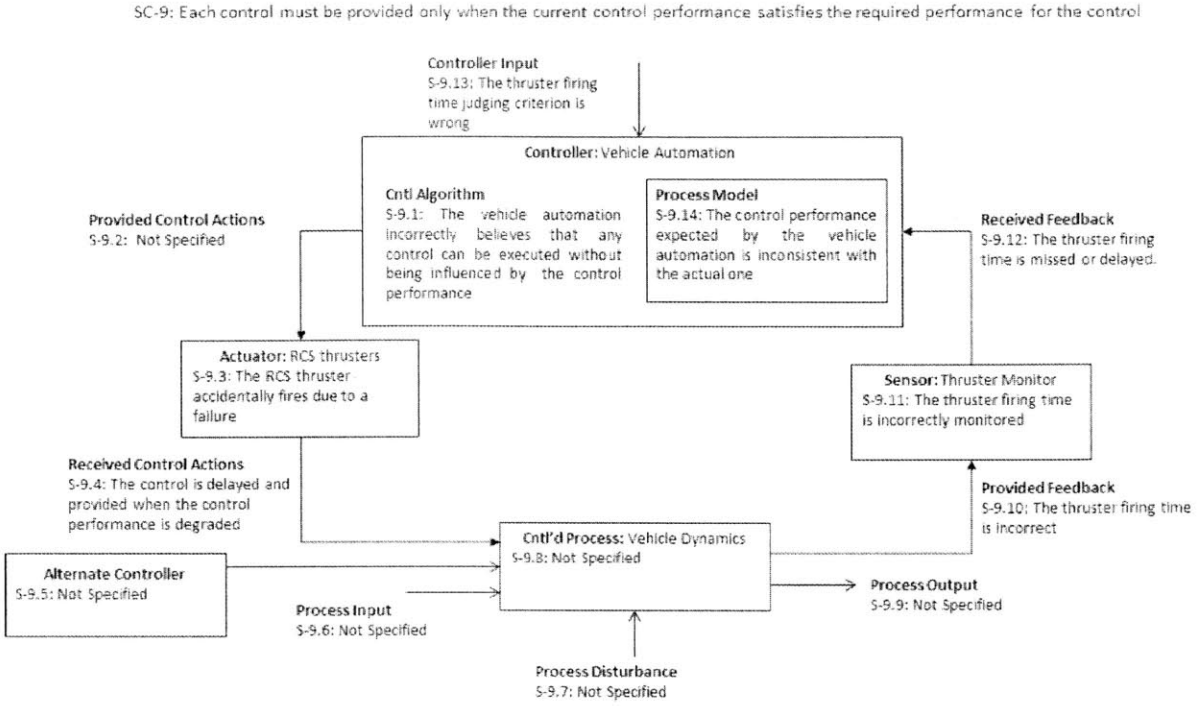


Figure A-1: Control Loop Diagram for the Safety Constraints (4/11)



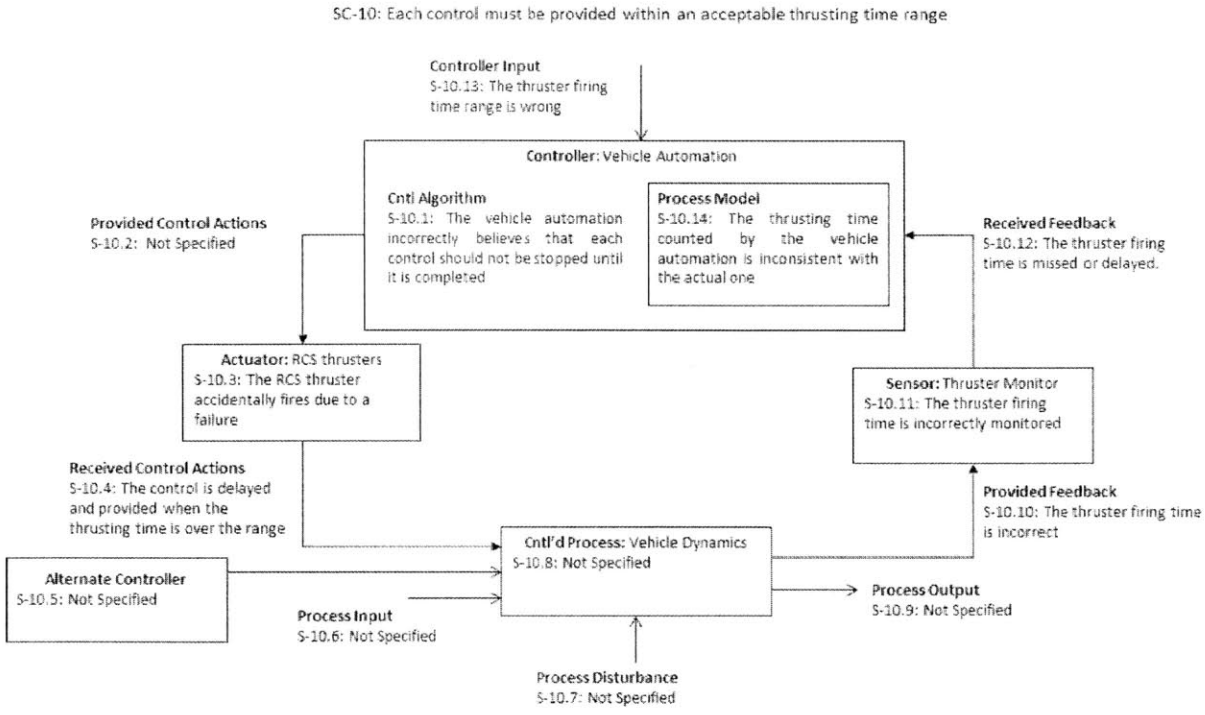
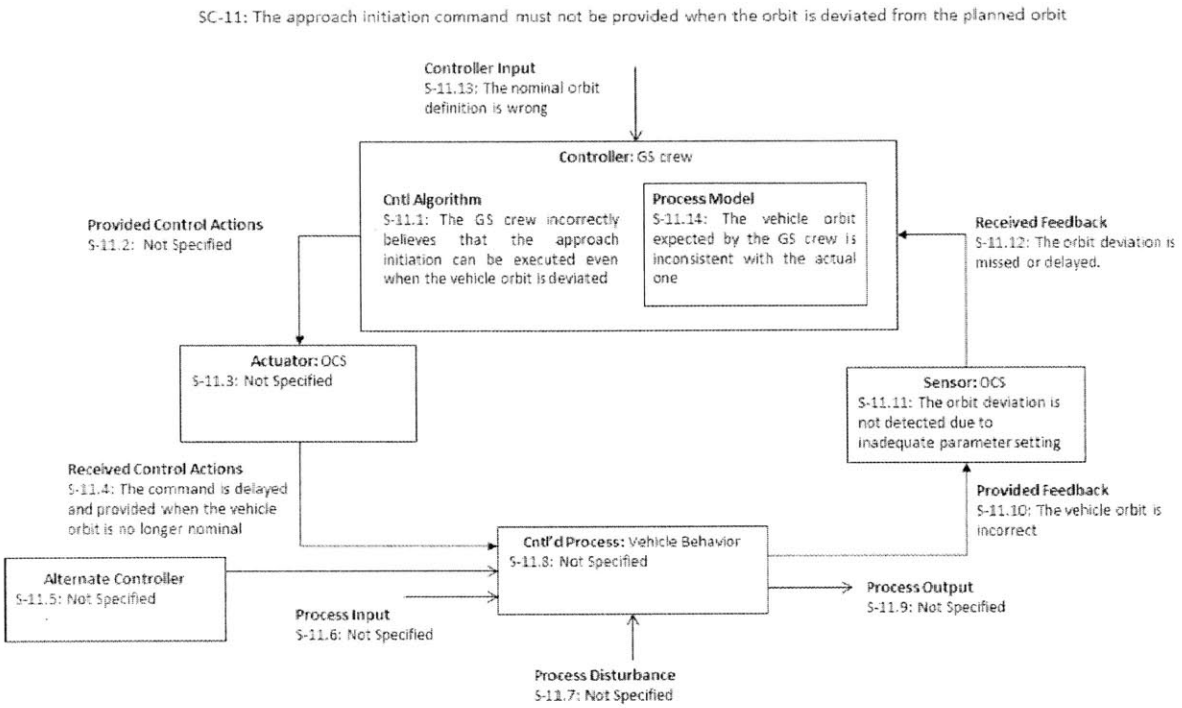


Figure A-1: Control Loop Diagram for the Safety Constraints (5/11)



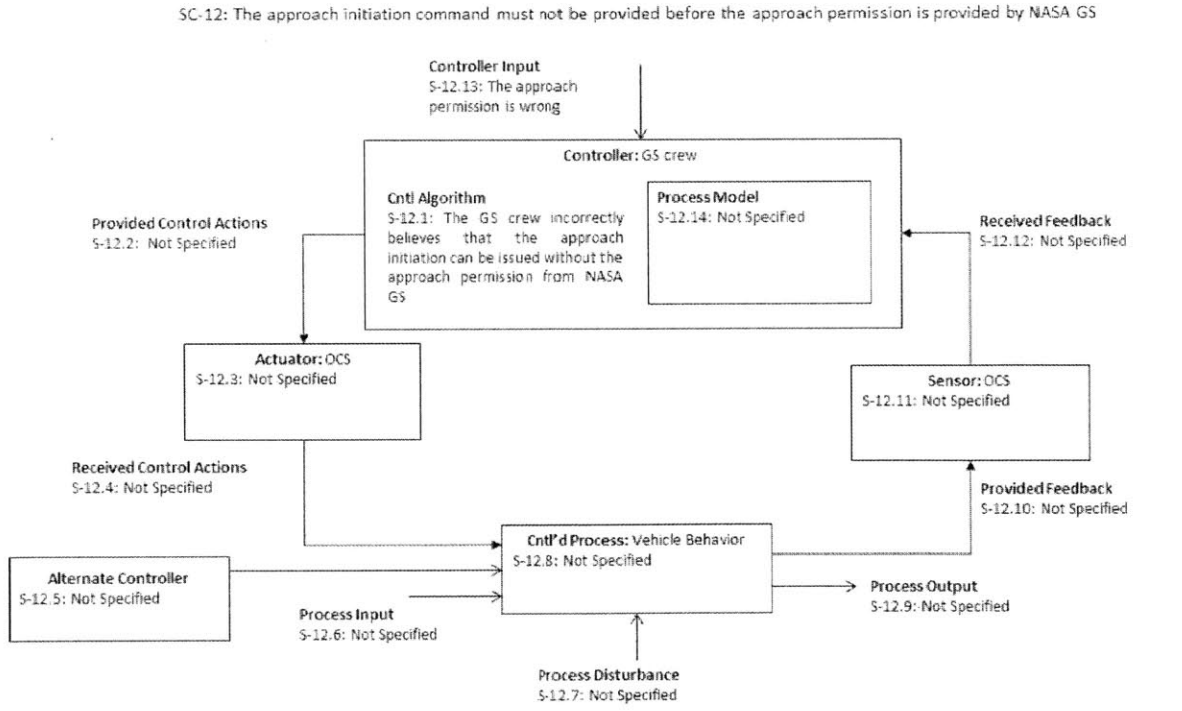
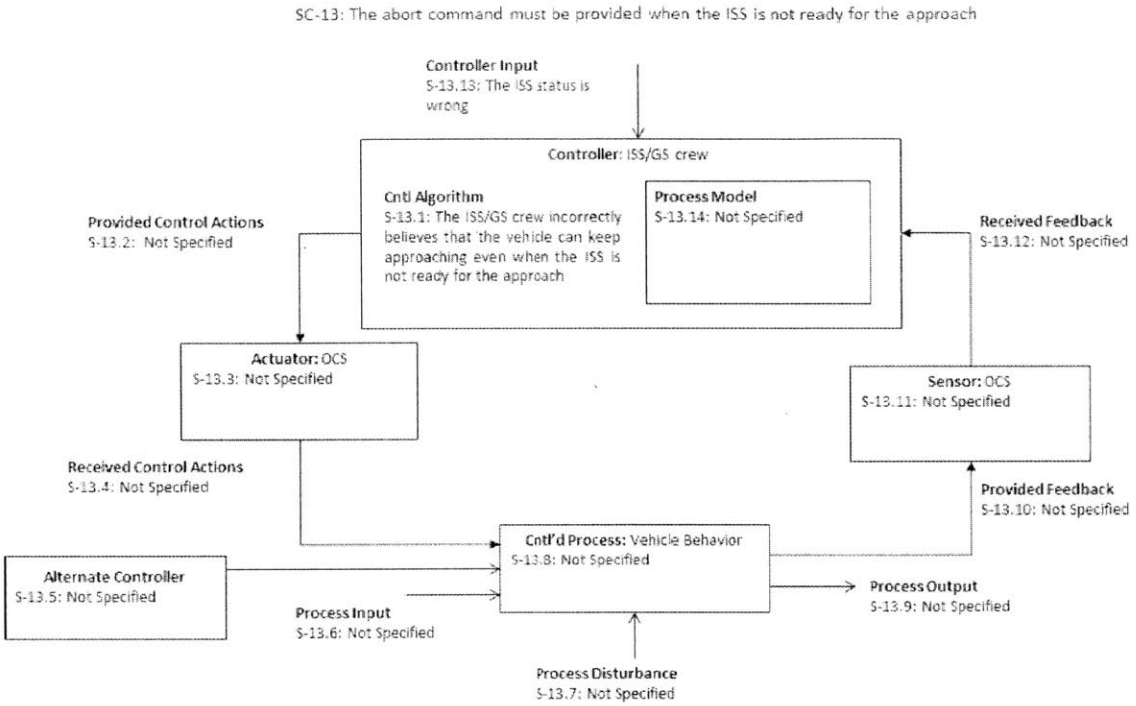


Figure A-1: Control Loop Diagram for the Safety Constraints (6/11)



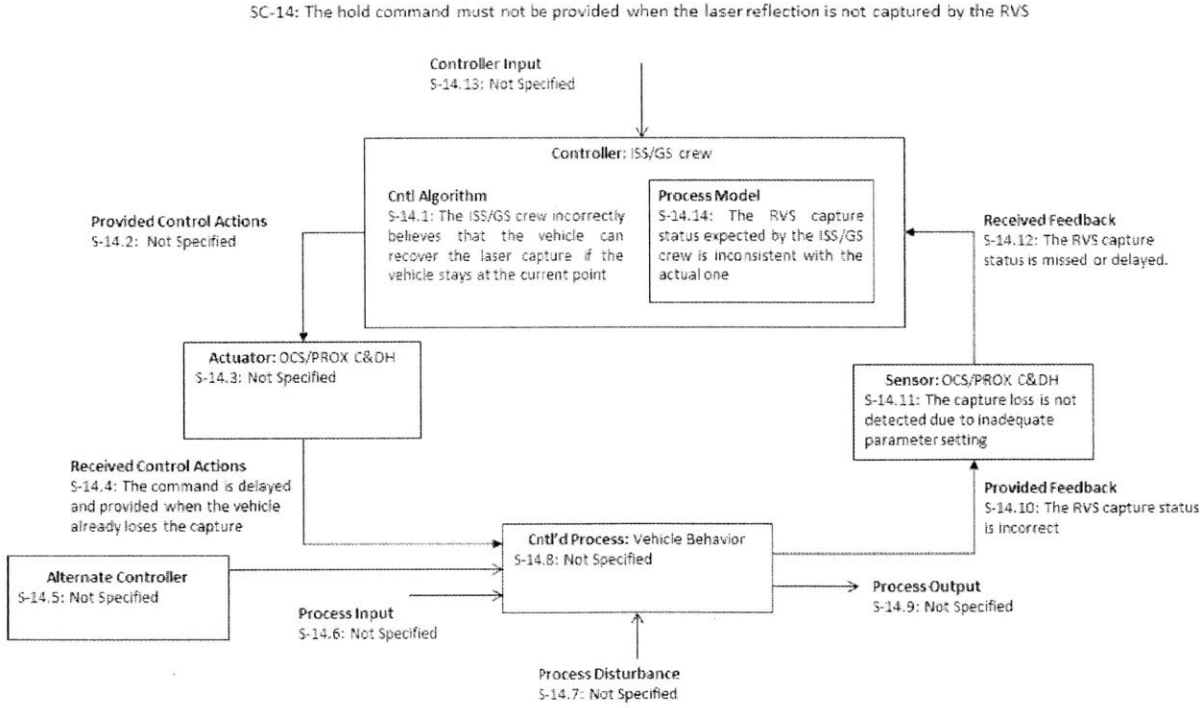
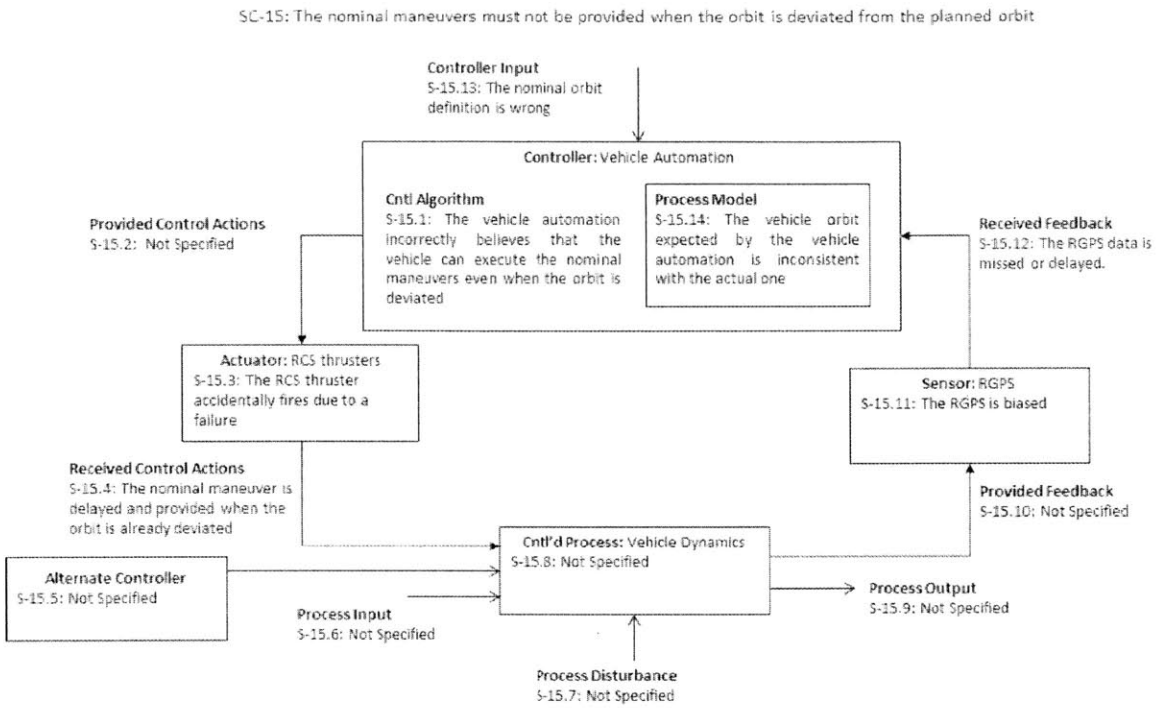


Figure A-1: Control Loop Diagram for the Safety Constraints (7/11)



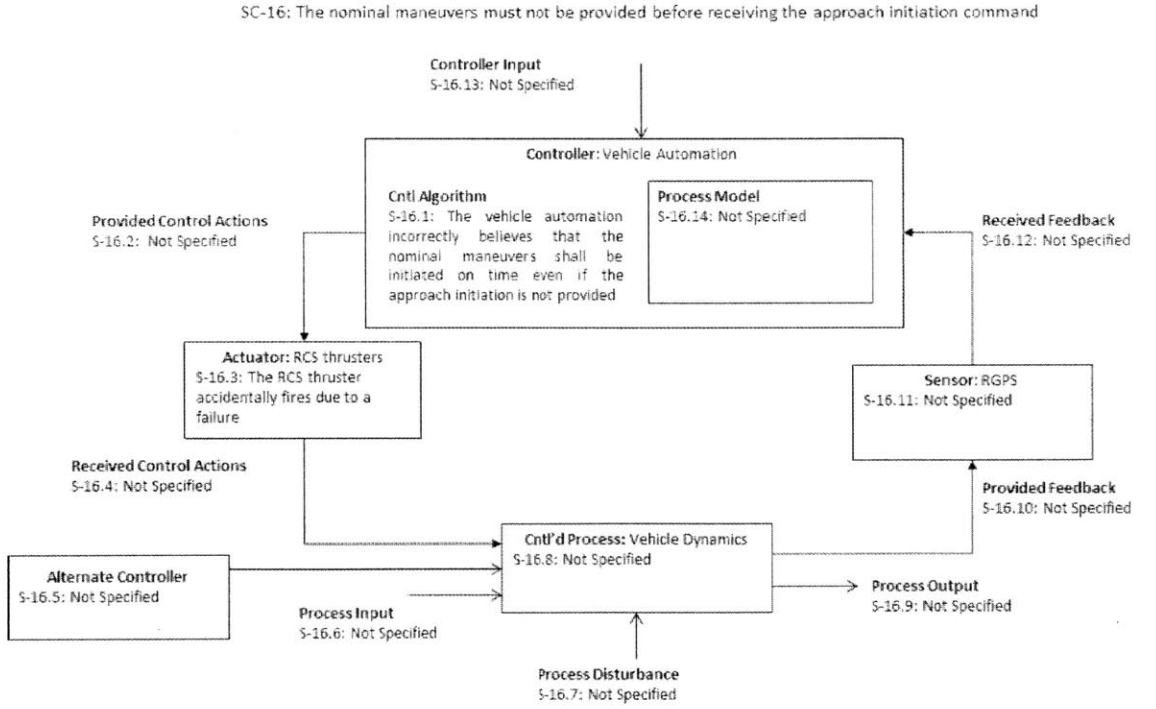
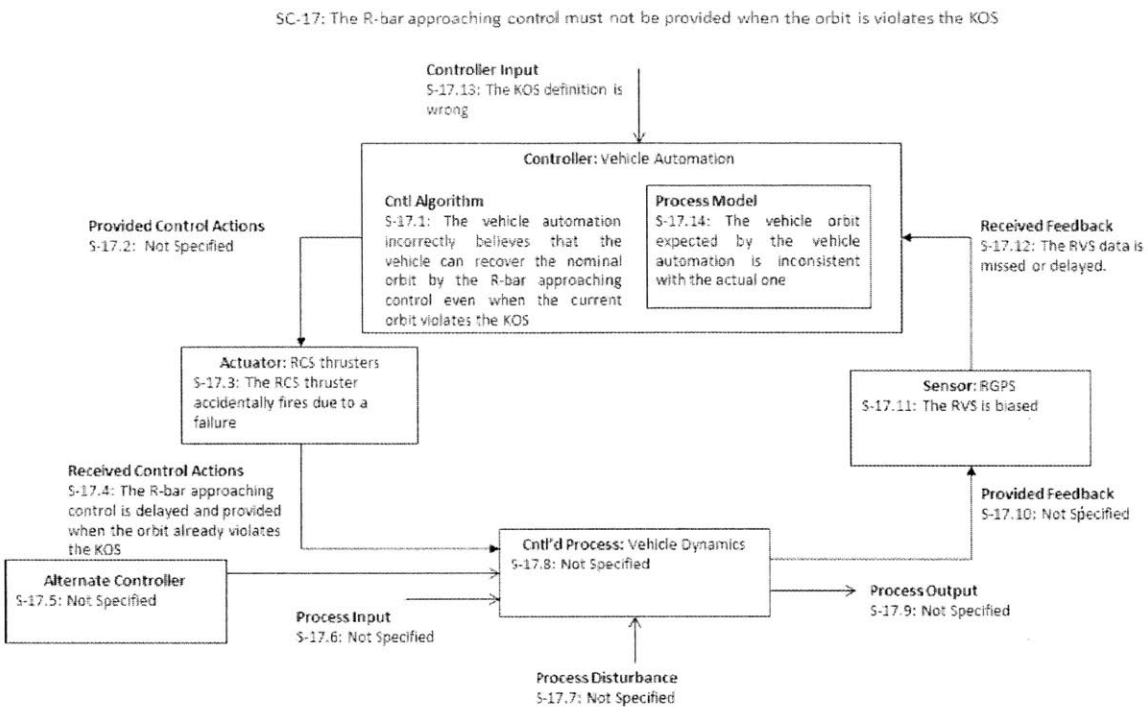


Figure A-1: Control Loop Diagram for the Safety Constraints (8/11)



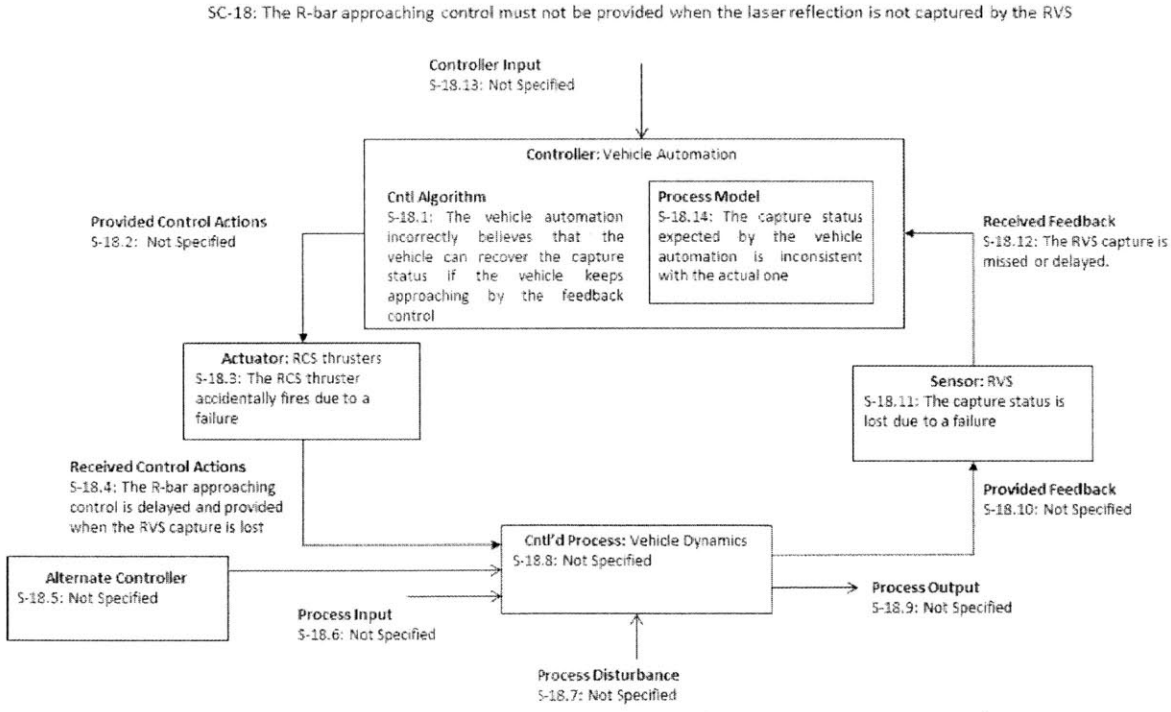


Figure A-1: Control Loop Diagram for the Safety Constraints (9/11)

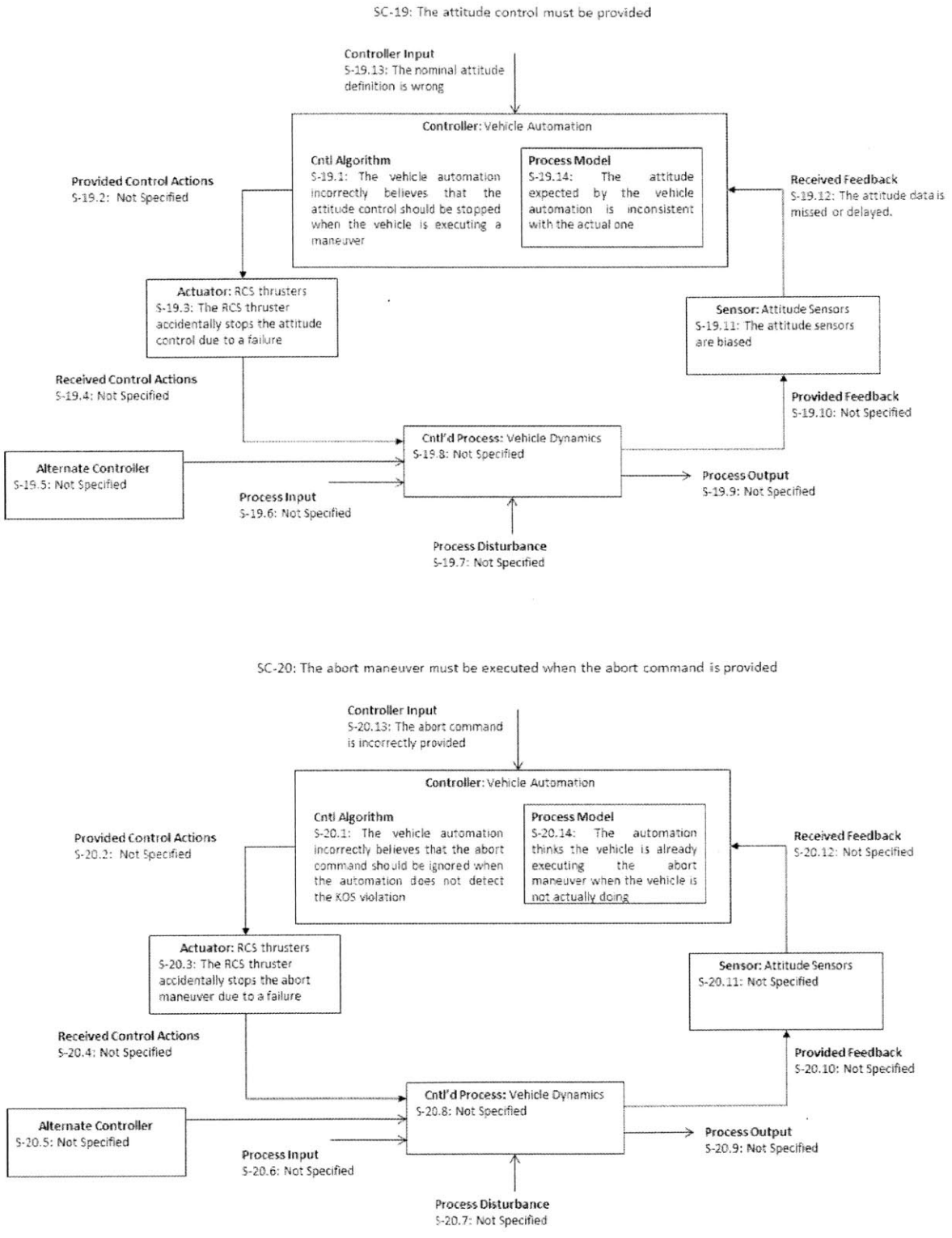


Figure A-1: Control Loop Diagram for the Safety Constraints (10/11)

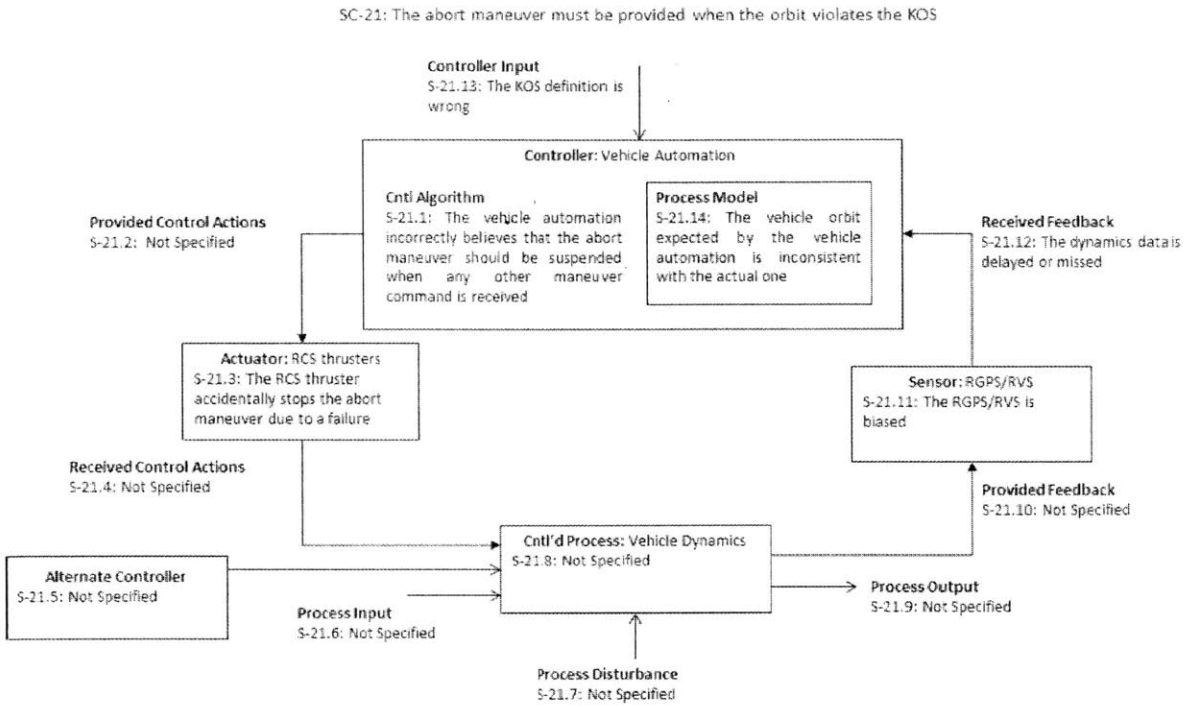


Figure A-1: Control Loop Diagram for the Safety Constraints (11/11)

Table A-4: Causal Scenarios and Design Recommendation (1/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-1: Any command except for the passive CAM must not be provided when the attitude is not nominal	**S-1.1**: Because the ISS/GS crew incorrectly believes that the maneuvers can be executed when the attitude is not nominal, the ISS/GS crew provides the commands when the attitude is not nominal **S-1.4**: Because the command is delayed, the command is provided when the attitude is not nominal **S-1.7**: Because an unexpected space environment variation disturbs the attitude sensors, the ISS/GS crew provides the commands when the attitude is not nominal **S-1.10**: Because the sensor data is biased, the ISS/GS crew incorrectly believes the attitude is nominal and provides the commands when the attitude is not nominal **S-1.11**: Because the attitude anomaly is not detected due to inadequate parameter setting in the OCS/PROX C&DH, the ISS/GS crew incorrectly believes the attitude is nominal and provides the commands when the attitude is not nominal **S-1.12**: Because the attitude anomaly is missed or delayed, the ISS/GS crew incorrectly believes the attitude is nominal and provides the commands when the attitude is not nominal **S-1.13**: Because the definition of the nominal attitude is wrong, the ISS/GS crew incorrectly believes the attitude is nominal and provides the commands when the attitude is not nominal. **S-1.14**: Because the attitude expected by the ISS/GS crew is inconsistent with the actual one, the ISS/GS crew provides the commands when the attitude is not nominal	The vehicle automation shall autonomously judge if the attitude is nominal. The vehicle automation shall reject any command execpt for the passive CAM when the attitude is not nominal. (S-1.1, 1.4, 1.7, 1.10, 1.11, 1.12, 1.13, 1.14)
SC-2: Any command except for the abort must not be provided when the vehicle is executing the abort maneuver or passive CAM	**S-2.4**: Because the command is delayed, the command is provided when the vehicle is executing the abort maneuver or passive CAM **S-2.5**: Because the GS/ISS crew issues the abort or passive CAM when the ISS/GS crew issues the other command, the command is provided when the vehicle is executing the abort maneuver or passive CAM **S-2.8**: Because the vehicle autonomously executes the abort maneuver, the command is provided when the vehicle is executing the abort maneuver **S-2.12**: Because the vehicle mode is missed or delayed, the command is provided when the vehicle is executing the abort maneuver **S-2.14**: Because the ISS/GS crew incorrectly believes that the vehicle is not in the CAM mode when the vehicleis actually in the CAM mode, the command is provided when the vehicle is executing the abort maneuver	The vehicle automation shall reject any command execpt for the abort command when the vehicle is in the CAM mode. (S-2.4, 2.5, 2.8, 2.12, 2.14)
SC-3: The approach initiation and hold command must not be provided when the vehicle status is not ready for the maneuvers	**S-3.1**: Because the ISS/GS crew incorrectly believes that the approach initiation and hold command can be executed even when the vehicle status is not ready, the comand is provided when the vehicle status is not ready for the maneuvers **S-3.4**: Because the approach initiation or hold command is delayed, the comand is provided when the vehicle status is not ready for the maneuvers **S-3.7**: Because space environment variation damages the vehicle components, the ISS/GS crew provides the approach initiation or hold command when the vehicle status is not ready for the maneuvers **S-3.10**: Because the vehicle status is incorrect, the ISS/GS crew provides the approach initiation or hold command when the vehicle status is not ready for the maneuvers **S-3.11**: Because the vehicle anomaly is not detected due to inadequate parameter setting, the ISS/GS crew provides the approach initiation or hold command when the vehicle status is not ready for the maneuvers **S-3.12**: Because the vehicle anomaly is missed or delayed, the ISS/GS crew provides the approach initiation or hold command when the vehicle status is not ready for the maneuvers **S-3.14**: Because the vehicle status expected by the ISS/GS crew is inconsistent with the actual one, the ISS/GS crew provides the approach initiation or hold command when the vehicle status is not ready for the maneuvers	The vehicle automation shall autonomously judge if the vehicle status is ready for the maneuvers. The vehicle automation shall reject the approach initiation command and hold command when the vehicle status is not ready for the maneuvers (S-3.1, 3.4, 3.7, 3.10, 3.11, 3.12, 3.14)

Table A-4: Causal Scenarios and Design Recommendation (2/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-4: Each command must be provided only when the current control performance satisfies the required performance for the command	**S-4.1**: Because the ISS/GS crew incorrectly believes that any command can be executed without being influenced by the control performance, the command is provided when the performance is less than the required level **S-4.4**: Because the command is delayed, the command is provided when the performance is less than the required level **S-4.8**: Because the control performance is degraded by the compensation mechanism, the command is provided when the performance is less than the required level **S-4.10**: Because the thruster firing time is incorrect and consequently the estimated control performance is also incorrect, the command is provided when the performance is less than the required level **S-4.11**: Because the control performance is incorrectly estimated, the command is provided when the performance is less than the required level **S-4.12**: Because the control performance is missed or delayed, the command is provided when the performance is less than the required level **S-4.13**: Because the control performance judging criteria are wrong, the command is provided when the performance is less than the required level **S-4.14**: The control performance expected by the ISS/GS crew is inconsistent with the actual one, the command is provided when the performance is less than the required level	Based on the control performance, the available commands shall be displayed on the OCS/PROX C&DH. (S-4.1, 4.14) The control performance shall be recovered by reconfiguring the thrusters. (S-4.4, 4.8) The thruster firing time and control performance shall be verified by checking the consistency with the dynamics data. (S-4.10, 4.11, 4.12) The control perfromance judging criteria shall be verified based on the flight data before the final approaching operation (S-4.13)
SC-5: The passive CAM and hold command must not be provided when the orbit violates the KOS	**S-5.1**: Because the ISS/GS crew incorrectly believes that the KOS violation can be avoided by the passive CAM or hold command, the command is provided when the orbit violates the KOS **S-5.4**: Because the command is delayed, the passive CAM or hold command is provided when the KOS is violated **S-5.7**: Because space environment disturbs the dynamics sensors, the passive CAM or hold command is provided when the KOS is violated **S-5.10**: Because the orbit data is incorrect, the passive CAM or hold command is provided when the KOS is violated **S-5.11**: Because the KOS violation is not incorrectly warned, the passive CAM or hold command is provided when the KOS is violated **S-5.12**: Because the KOS violation is missed or delayed, the passive CAM or hold command is provided when the KOS is violated. **S-5.13**: Because the KOS warning criterion is wrong, the passive CAM or hold command is provided when the KOS is violated. **S-5.14**: Because the orbit expected by the ISS/GS crew is inconsistent with the actual one, the passive CAM or hold command is provided when the KOS is violated.	The vehicle automation shall autonomously judge if the orbit violates the KOS. The vehicle automation shall reject any the passive CAM and hold command when the KOS is volated. (S-5.1, 5.4, 5.7, 5.10, 5.11, 5.12, 5.13, 5.14)
SC-6: Any maneuver must not be provided when the attitude is not nominal	**S-6.1**: Because the vehicle automation incorrectly believes that any maneuver can be executed even when the attitude is not nominal, a maneuver is provided when the attitude is not nominal **S-6.3**: Because the RCS thruster accidentally fires due to a failure, a maneuver is provided when the attitude is not nominal **S-6.11**: Because the attitude sensors are biased, a maneuver is provided when the attitude is not nominal. **S-6.12**: Because the attitude data is delayed, a maneuver is provided when the attitude is not nominal. **S-6.13**: Because the nominal attitude setting is wrong, a maneuver is provided when the attitude is not nominal. **S-6.14**: Becuse the attitude expected by the vehicle automation is inconsistent with the actual one, a maneuver is provided when the attitude is not nominal.	The vehicle automation shall autonomously judge if the attitude is nominal. The vehicle automation shall stop any maneuver when the attitude is not nominal. (S-6.1) The vehicle automation shall close the thruster valve when the attitude is not nominal. (S-6.3) The attitude data shall be always verified by two types of sensors (STT & IRU) (S-6.11, 6.12, 6.14) The nominal attitude shall be adjusted during the operation (S-6.13)

Table A-4: Causal Scenarios and Design Recommendation (3/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-7: Any maneuver except for the abort maneuver must not be provided when the vehicle is executing the abort maneuver or passive CAM	**S-7.1**: Because the vehicle automation incorrectly believes that the vehicle is not executing the abort maneuver or passive CAM, a maneuver except for the abort is provided when the vehicle is actually executing the abort maneuver or passive CAM **S-7.3**: Because the RCS thruster accidentally fires due to a failure, a maneuver is provided when the vehicle is executing the abort maneuver or passive CAM **S-7.4**: Because the thrusting timing is delayed, a maneuver is provided when the vehicle is executing the abort maneuver or passive CAM **S-7.14**: Because the vehicle mode expected by the vehicle automation is inconsistent with the actual one, a maneuver is provided when the vehicle is executing the abort maneuver or passive CAM	The vehicle automation shall manage the vehicle flight mode by itself. The vehicle automation shall prohibit any maneuver when the vehicle is in the CAM mode. (S-7.1) The vehicle automation shall close the thruster valve when the vehicle is in the CAM mode. (S-7.3, 7.4) The GS crew shall monitor if the vehicle behavior and the mode are consistent (S-7.14)
SC-8: The nominal maneuvers and R-bar approaching control must not be provided when the vehicle status is not ready for the maneuvers	**S-8.1**: Because the vtehicle automation incorrectly believes that the nominal maneuvers and R-bar approaching control can be executed even when the vehicle status is not ready, those maneuvers are provided when the vehicle status is not ready **S-8.3**: Because the RCS thruster accidentally fires due to a failure, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is not ready **S-8.4**: Because the nominal maneuvers or R-bar approaching control are delayed, those maneuvers are provided when the vehicle status is no longer ready **S-8.7**: Because space environment variation damages the vehicle components, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is not ready **S-8.10**: Because the vehicle status is incorrect, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is actually not ready **S-8.11**: Because the vehicle anomaly is not detected due to inadequate parameter setting, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is actually not ready **S-8.12**: Becauase the vehicle anomaly is missed or delayed, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is not ready. **S-8.14**: Because the vehicle status expected by the vehicle automation is inconsistent with the actual one, the nominal maneuvers and R-bar approaching control are provided when the vehicle status is not ready.	The vehicle automation shall autonomously judge which maneuver is avilable in the current vehicle status. The vehicle automation shall stop any maneuver except for the abort maneuver when the vehicle status is not ready for it (S-8.1, 8.7) The vehicle automation shall close the thruster valve when the vehicle status is not ready. (S-8.3, 8.4) The vehicle status shall be verified by comparing with multiple component status (S-8.10, 8.11, 8.12, 8.14)
SC-9: Each control must be provided only when the current control performance satisfies the required performance for the control	**S-9.1**: Because the vehicle automation incorrectly believes that any control can be executed without being influenced by the control performance, a control is provided when the current control performance does not satisfy the required performance for the control **S-9.3**: Because the RCS thruster accidentally fires due to a failure, a control is provided when the current control performance does not satisfy the required performance for the control. **S-9.4**: Because the control is delayed, it is provided when the control performance is degraded **S-9.10**: Because the thruster firing time is incorrect, a control is provided when the current control performance does not satisfy the required performance for the control. **S-9.11**: Because the thruster firing time is incorrectly monitored, a control is provided when the current control performance does not satisfy the required performance for the control. **S-9.12**: Because the thruster firing time is missed or delayed, a control is provided when the current control performance does not satisfy the required performance for the control. **S-9.13**: Because the thruster firing time judging criterion is wrong, a control is provided when the current control performance does not satisfy the required performance for the control. **S-9.14**: Because the control performance expected by the vehicle automation is inconsistent with the actual one, a control is provided when the current control performance does not satisfy the required performance for the control.	The GS crew shall monitor each control result and judge if the successive maneuvers can be executed. If not, the GS crew shall issue the abort or passive CAM command. (S-9.1, 9.14) The vehicle automation shall close the thruster valve when the vehicle is executing the passive CAM. (S-9.3, 9.4) The thruster firing time and control performance shall be verified by checking the consistency with the dynamics data. (S-9.10, 9.11, 9.12) The thruster firing time judging criterion shall be verified based on the flight data before the final approaching operation (S-9.13)

Table A-4: Causal Scenarios and Design Recommendation (4/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-10: Each control must be provided within an acceptable thrusting range	**S-10.1**: Because the vehicle automation incorrectly believes that each control should not be stopped until it is completed, the control is provided over the acceptable thrusting range **S-10.3**: Because the RCS thruster accidentally fires due to a failure, the control is provided over the acceptable thrusting range **S-10.4**: Because the control is delayed, it is provided when the thrusting time is over the range **S-10.10**: Because the thruster firing time is incorrect, the control is provided over the acceptable thrusting time range **S-10.11**: Because the thruster firing time is incorrectly monitored, the control is provided over the acceptable thrusting time range **S-10.12**: Because the thruster firing time is missed or delayed, the control is provided over the acceptable thrusting time range **S-10.13**: Because the thruster firing time range is wrong, the control is provided over the actual range **S-10.14**: Because the thrusting time counted by the vehicle automation is inconsistent with the actual one, the control is provided over the actual range	The vehicle automation shall count the thruster firing time. If the firing time is over the acceptable firing time range, the vehicle automation shall autonomously stop thrusting. (S-10.1) The vehicle automation shall close the thruster valve when the firing time is over the acceptable firing time range. (S-10.3, 10.4) The GS crew shall monitor each control result (thrusting time & dynamics data) and judge if the control is completed within the acceptable time range. If not, the GS crew shall issue the command to stop the maneuver. (S-10.10, 10.11, 10.12, 10.13, 10.14)
SC-11: The approach initiation command must not be provided when the orbit is deviated from the planned orbit	**S-11.1**: Because the GS crew incorrectly believes that the approach initiation can be executed even when the vehicle orbit is deviated, the command is provided when the orbit is deviated **S-11.4**: Because the approach initiation is delayed, the command is provided when the vehicle orbit is no longer nominal **S-11.10**: Because the vehicle orbit is incorrect, the approach initiation is provided when the orbit is deviated **S-11.11**: Because the orbit deviation is not detected due to inadequate parameter setting on the OCS, the approach initiation is provided when the orbit is deviated **S-11.12**: Because the orbit deviation is missed or delayed, the approach initiation is provided when the orbit is deviated **S-11.13**: Because the nominal orbit definition is wrong, the approach initiation is provided when the orbit is deviated **S-11.14**: Because the vehicle orbit expected by the GS crew is inconsistent with the actual one, the approach initiation is provided when the orbit is deviated	The vehicle automation shall autonomously if judge the orbit is nominal. If not, the autonomation shall reject the approach initiation command. (S-11.1, 11.4, 11.10, 11.11, 11.12, 11.13, 11.14)
SC-12: The approach initiation command must not be provided before the approach permission is provided by NASA GS	**S-12.1**: Because the GS crew incorrectly believes that the approach initiation can be issued without the approach permission from NASA GS, the approach initiation is provided before the approach permission is provided	The approach permission shall be notified to the GS crew. The approach permission shall be displayed on the OCS. (S-12.1)
SC-13: The abort command must be provided when the ISS is not ready for the approach	**S-13.1**: Because the ISS/GS crew incorrectly believes that the vehicle can keep approaching even when the ISS is not ready for the approach, the abort command is not provided when the ISS is not ready for the approach **S-13.13**: Because the ISS status is wrong, the abort command is not provided when the ISS is not ready for the approach	The ISS crew and NASA GS shall monitor the ISS status and notify it to the GS crew. The ISS/GS crew shall issue the abort command when the ISS is not ready for the approach. (S-13.1, 13.13)

Table A-4: Causal Scenarios and Design Recommendation (5/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-14: The hold command must not be provided when the laser reflection is not captured by the RVS	**S-14.1**: Because the ISS/GS crew incorrectly believes that the vehicle can recover the laser capture if the vehicle stays at the current point, the hold command is provided when the RVS capture is lost **S-14.4**: Because the hold command is delayed, it is provided when the vehicle already loses the capture **S-14.10**: Because the RVS capture status is incorrect, the hold command is provided when the RVS capture is actually lost **S-14.11**: Because the capture loss is not detected due to inadequate parameter setting on the OCS/PROX C&DH, the hold command is provided when the RVS capture is actually lost **S-14.12**: Because the RVS capture status is missed or delayed, the hold command is provided when the RVS capture is actually lost **S-14.14**: Because the RVS capture status expected by the ISS/GS crew is inconsistent with the actual one, the hold command is provided when the RVS capture is actually lost	The vehicle automation shall autnomously check the RVS capture status. If the capture is lost, the vehicle shall autonomously executes the abort maneuver. (S-14.1, 14.4, 14.10, 14.11, 14.12, 14.14)
SC-15: The nominal maneuvers must not be provided when the orbit is deviated from the planned orbit	**S-15.1**: Because the vehicle automation incorrectly believes that the vehicle can execute the nominal maneuvers even when the orbit is deviated, the nominal maneuvers are provided when the orbit is deviated **S-15.3**: Because the RCS thruster accidentally fires due to a failure, the nominal maneuvers are provided when the orbit is deviated **S-15.4**: Because the nominal maneuvers are delayed, it is provided when the orbit is already deviated **S-15.11**: Because the RGPS is biased, the nominal maneuvers are provided when the orbit is deviated **S-15.12**: Because the RGPS data is missed or delayed, the nominal maneuvers are provided when the orbit is deviated **S-15.13**: Because the nominal orbit definition is wrong, the nominal maneuvers are provided when the orbit is deviated **S-15.14**: Because the vehicle orbit expected by the vehicle automation is inconsistent with the actual one, the nominal maneuvers are provided when the orbit is deviated	The vehicle automation shall autonomously if judge the orbit is nominal. If not, the autonomation shall stop the nominal maneuvers. (S-15.1, 15.14) The vehicle automation shall close the thruster valve when the firing time is over the acceptable firing time range. (S-15.3, 15.4) The quality of GPS data shall be checked during the operation. (S-15.11, 15.12) The nominal orbit definition shall be checked before the final approaching operation (S-15.13)
SC-16: The nominal maneuvers must not be provided before receiving the approach initiation command	**S-16.1**: The vehicle automation incorrectly believes that the nominal maneuvers shall be initiated on time even if the approach initiation is not provided	The vehicle automation shall not initiate the nominal maneuver sequence without receiving the approach initiation command (S-16.1)
SC-17: The R-bar approaching control must not be provided when the orbit violates the KOS	**S-17.1**: Because the vehicle automation incorrectly believes that the vehicle can recover the nominal orbit by the R-bar approaching control even when the current orbit violates the KOS, the R-bar approaching control is provided when the orbit violates the KOS **S-17.3**: Because the RCS thruster accidentally fires due to a failure, the R-bar approaching control is provided when the orbit violates the KOS **S-17.4**: Because the R-bar approaching control is delayed, it is provided when the orbit already violates the KOS **S-17.11**: Because the RVS is biased, the R-bar approaching control is provided when the orbit actually violates the KOS **S-17.12**: Because the RVS data is missed or delayed, the R-bar approaching control is provided when the orbit actually violates the KOS. **S-17.13**: Because the KOS definition is wrong, the R-bar approaching control is provided when the orbit actually violates the KOS. **S-17.14**: Because the vehicle orbit expected by the vehicle automation is inconsistent with the actual one, the R-bar approaching control is provided when the orbit actually violates the KOS.	The vehicle automation shall automously judge the KOS violation. If the violation is detected, the automation shall immidiately stop the current operation and execute the abort maneuver. (S-17.1, 17.3, 17.4) The RVS data shall be verified by the RGPS data (S-17.11, 17.12) When the RVS data is lost, the automation shall immidiately stop the current operation and execute the abort maneuver. (S-17.12) The GS crew shall monitor the KOS violation and issue the abort command when the violation is found. (S-17.14) The KOS definition shall be checked before the final approaching operation (S-17.13)

Table A-4: Causal Scenarios and Design Recommendation (6/6)

Safety Constraint	Causal Scenario	Design Recommendation
SC-18: The R-bar approaching control must not be provided when the laser reflection is not captured by the RVS	**S-18.1**: Because the vehicle automation incorrectly believes that the vehicle can recover the capture status if the vehicle keeps approaching by the feedback control, the R-bar approaching control is provided when the RVS capture is lost **S-18.3**: Because the RCS thruster accidentally fires due to a failure, the R-bar approaching control is provided when the RVS capture is lost **S-18.4**: Because the R-bar approaching control is delayed, it is provided when the RVS capture is lost **S-18.11**: Because the capture status is lost due to a failure, the R-bar approaching control is provided when the RVS capture is lost **S-18.12**: Because the RVS capture is missed or delayed, the R-bar approaching control is provided when the RVS capture is lost **S-18.14**: Because the capture status expected by the vehicle automation is inconsistent with the actual one, the R-bar approaching control is provided when the RVS capture is lost	The vehicle automation shall autnomously check the RVS capture status. If the capture is lost, the vehicle shall autonomously executes the abort maneuver. (S-18.1, 18.3, 18.4, 18.11, 18.12) The GS crew shall monitor the RVS capture status. If the status is lost, the GS crew shall issue the abort command (S-18.14)
SC-19: The attitude control must be provided	**S-19.1**: Because the vehicle automation incorrectly believes that the attitude control should be stopped when the vehicle is executing a maneuver, the attitude control is not provided **S-19.3**: Because the RCS thruster accidentally stops the attitude control due to a failure, the attitude control is not provided **S-19.11**: Because the attitude sensors are biased, the attitude control is not provided **S-19.12**: Because the attitude data is missed or delayed, the attitude control is not provided. **S-19.13**: Because the nominal attitude definition is wrong, the attitude control is not provided. **S-19.14**: Because the attitude expected by the vehicle automation is inconsistent with the actual one, the attitude control is not provided.	The attitude control shall be prioritized than any other control in the compensation mechanism (S-19.1, 19.3) The attitude data shall be always verified by two types of sensors (STT & IRU) (S-19.11, 19.12, 19.14) The nominal attitude definition shall be checked before the final approaching operation (S-19.13)
SC-20: The abort maneuver must be executed when the abort command is provided	**S-20.1**: Because the vehicle automation incorrectly believes that the abort command should be ignored when the automation does not detect the KOS violation, the abort maneuver is not executed when the abort command is provided **S-20.3**: Because the RCS thruster accidentally stops the abort maneuver due to a failure, the abort maneuver is not executed when the abort command is provided **S-20.14**: Because the automation incorrectly thinks the vehicle is already executing the abort maneuver when the vehicle is not actually doing, the abort maneuver is not executed when the abort command is provided	The abort command shall be accepted when it is provided, and the abort maneuver shall be immidiately executed. (S-20.1) The vehicle automation shall complete the abort maneuver by using the compensation mechanism. (S-20.3) The vehicle shall accept the abort command even when it is already in the CAM mode (S-20.14)
SC-21: The abort maneuver must be provided when the orbit violates the KOS	**S-21.1**: Because the vehicle automation incorrectly believes that the abort maneuver should be suspended when any other maneuver command is received, the abort maneuver is not provided when the orbit violates the KOS **S-21.3**: Because the RCS thruster accidentally stops the abort maneuver due to a failure, the abort maneuver is not provided when the orbit violates the KOS **S-21.11**: Because the RGPS/RVS is biased, the abort maneuver is not provided when the orbit violates the KOS **S-21.12**: Because the dynamics data is delayed or missed, the abort maneuver is not provided when the orbit violates the KOS **S-21.13**: Because the KOS definition is wrong, the abort maneuver is not provided when the orbit violates the KOS **S-21.14**: Because the vehicle orbit expected by the vehicle automation is inconsistent with the actual one, the abort maneuver is not provided when the orbit violates the KOS	The abort maneuver shall be prioritized than any other maneuver. (S-21.1) The vehicle automation shall complete the abort maneuver by using the compensation mechanism. (S-21.3) The quality of GPS data shall be checked during the operation. The RVS data shall be verified by the RGPS data (S-21.11, 21.12) The GS crew shall monitor the orbit and issue the abort command when it violates the KOS (S-21.13, 21.14)

Table A-5: Context Table (1/3)

#	Control Action	ISS Status	Vehicle Orbit	Vehicle Attitude	Vehicle Mode	Vehicle Status	Control Performance	RVS Capture	Control Duration	Not Providing Causes Hazards	Providing Causes Hazards	
1	Approach Initiation	*	Deviated	*	*	*	*	*	-	No	Yes	UCA-1.1
2		*	*	Off-Nominal	*	*	*	*	-	No	Yes	UCA-1.2
3		*	*	*	CAM	*	*	*	-	No	Yes	UCA-1.3
4		*	*	*	*	Not Ready	*	*	-	No	Yes	UCA-1.4
5		*	*	*	*	*	< AI	*	-	No	Yes	UCA-1.5
6		Not Ready	*	*	*	*	*	*	-	No	Yes	UCA-1.6
7	Passive CAM	*	KOS	*	*	*	*	*	-	No	Yes	UCA-2.1
8		*	*	*	Abort	*	*	*	-	No	Yes	UCA-2.2
9		*	*	*	*	*	< Attitude Control	*	-	No	Yes	UCA-2.3
10	Abort	Not Ready	*	*	*	*	*	*	-	Yes	No	UCA-3.1
11		*	*	Off-Nominal	*	*	*	*	-	No	Yes	UCA-3.2
12		*	*	*	*	*	< Abort	*	-	No	Yes	UCA-3.3

Table A-5: Context Table (2/4)

#	Control Action	ISS Status	Vehicle Orbit	Vehicle Attitude	Vehicle Mode	Vehicle Status	Control Performance	RVS Capture	Control Duration	Not Providing Causes Hazards	Providing Causes Hazards	
13	Hold	*	KOS	*	*	*	*	*	-	No	Yes	UCA-4.1
14		*	*	Off-Nominal	*	*	*	*	-	No	Yes	UCA-4.2
15		*	*	*	CAM	*	*	*	-	No	Yes	UCA-4.3
16		*	*	*	*	Not Ready	*	*	-	No	Yes	UCA-4.4
17		*	*	*	*	*	< Hold	*	-	No	Yes	UCA-4.5
18		*	*	*	*	*	*	Off	-	No	Yes	UCA-4.6
19	Nominal Maneuvers	*	Deviated / KOS	*	*	*	*	*	*	No	Yes	UCA-5.1
20		*	*	Off-Nominal	*	*	*	*	*	No	Yes	UCA-5.2
21		*	*	*	CAM	*	*	*	*	No	Yes	UCA-5.3
22		*	*	*	*	Not Ready	*	*	*	No	Yes	UCA-5.4
23		*	*	*	*	*	< AI	*	*	No	Yes	UCA-5.5
24		Not Ready	*	*	*	*	*	*	*	No	Yes	UCA-5.6
25		*	*	*	*	*	*	*	Too long	No	Yes	UCA-5.7
26		*	*	*	*	*	*	ON	*	No	Yes	New UCA-5.8

Table A-5: Context Table (3/4)

#	Control Action	ISS Status	Vehicle Orbit	Vehicle Attitude	Vehicle Mode	Vehicle Status	Control Performance	RVS Capture	Control Duration	Not Providing Causes Hazards	Providing Causes Hazards	
27	R-bar Approaching Control	*	KOS	*	*	*	*	*	*	No	Yes	UCA-6.1
28		*	*	Off-Nominal	*	*	*	*	*	No	Yes	UCA-6.2
29		*	*	*	CAM	*	*	*	*	No	Yes	UCA-6.3
30		*	*	*	*	Not Ready	*	*	*	No	Yes	UCA-6.4
31		*	*	*	*	*	< R-bar	*	*	No	Yes	UCA-6.5
32		*	*	*	*	*	*	Off	*	No	Yes	UCA-6.6
33		Not Ready	*	*	*	*	*	*	*	No	Yes	New UCA-6.7
34		*	Outside the RVS range	*	*	*	*	On	*	No	Yes	New UCA-6.8
35	Attitude Control	*	*	*	*	*	> Attitude Control	*	*	Yes	No	UCA-7.1
36		*	*	*	*	*	< Attitude Control	*	*	No	Yes	UCA-7.2
37		*	*	*	*	*	*	*	Too long	No	Yes	UCA-7.3

Table A-5: Context Table (4/4)

#	Control Action	ISS Status	Vehicle Orbit	Vehicle Attitude	Vehicle Mode	Vehicle Status	Control Performance	RVS Capture	Control Duration	Not Providing Causes Hazards	Providing Causes Hazards	
38	Abort Maneuver	Not Ready	*	*	*	*	*	*	*	Yes	No	UCA-8.1
39		*	KOS	*	*	*	*	*	*	Yes	No	UCA-8.2
40		*	*	Off-Nominal	*	*	*	*	*	No	Yes	UCA-8.3
41		*	*	*	*	*	< Abort	*	*	No	Yes	UCA-8.4
42		*	*	*	*	*	*	*	Too Short	No	Yes	UCA-8.5
43		*	*	*	*	*	*	*	Too long	No	Yes	UCA-8.6
44		*	Outside the RVS range	*	*	*	*	On	*	No	Yes	New UCA-8.7