# Safety-Guided Design & Analysis of Space Launch Vehicles

by

John M. Rising

B.S. Engineering, University of Southern California, 2014

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

June 2018

© 2018 John M. Rising. All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature redacted

Signature of Author _____

John M. Rising
System Design and Management Program
April 30, 2018

Signature redacted

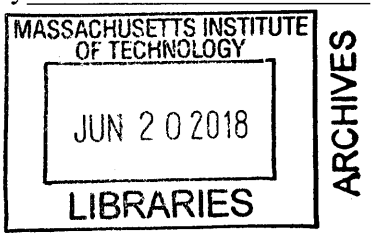
Certified by _____

Nancy G. Leveson, Ph.D., Professor
Department of Aeronautics and Astronautics
Thesis Supervisor

Signature redacted

Accepted by _____

John Rubin
Executive Director, System Design & Management Program



This Page Intentionally Left Blank

# Safety-Guided Design & Analysis of Space Launch Vehicles

by

John M. Rising

Submitted to the System Design and Management Program on 30 April 2018 in partial fulfillment of the requirements for the degree of Master of Science in Engineering and Management

## ABSTRACT

The advent of commercial launch systems has brought about a new age of space launch vehicle design. In order to survive in a competitive market, space launch providers must design systems with new technologies in shorter development times. This changing nature of space launch vehicle design requires a new way to perform safety analysis. Traditional hazard analysis techniques do not deliver adequate insight early in the design process, when most of the safety-related decisions are made. Early design decisions are often made using "lessons-learned" from previous launch systems, rather than interactive feedback from the new vehicle design actually being developed. Furthermore, traditional techniques use reliability theory as their foundation, resulting in the use of excessive design margin and redundancy as the "default" vehicle design choices. This equivocation of safety and reliability may have made sense for simpler launch vehicles of the past, but most modern space launch vehicle accidents have resulted from incorrect software specifications, component interaction accidents, and other design errors independent of the reliability of individual components. The space launch industry needs safety analysis methods and design processes that identify and correct these hazards early in the vehicle design process, when modifications to correct safety issues are more effective and less costly.

This work shows how Systems-Theoretic Process Analysis (STPA) can been used as a powerful tool to identify, mitigate, and possibly eliminate hazards throughout the entire space launch vehicle lifecycle. This work begins by reviewing traditional hazard analysis techniques and the changing nature of launch vehicle accidents. Next, it describes how STPA can be integrated into the space launch vehicle lifecycle to design safer systems. It then demonstrates the safety-guided design of a small-lift launch vehicle using STPA. Finally, this work shows how STPA can be used to satisfy regulatory and range safety requirements.

The thesis of this work is that integration of STPA into the design of space launch vehicles can make a significant contribution to reducing launch vehicle accidents.

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

This Page Intentionally Left Blank

# ACKNOWLEDGMENTS

I would first like to express my gratitude to Nancy Leveson. Her perspective and passion for systems safety is inspiring, and she provided invaluable insight to this work.

My parents, Mark Rising and Rosemary Rising, supported me innumerous ways throughout my journey to—and at—MIT.

I would also like to thank Relativity Space for allowing me to complete my degree while working.

Lastly, I would like to thank Mike Alsbury. Even though we did not know each other, my journey to MIT and interest in system safety began with him.

This Page Intentionally Left Blank

# TABLE OF CONTENTS

Abstract ..... 3

Acknowledgments ..... 5

Table of Figures ..... 10

Table of Tables ..... 11

Acronyms & Abbreviations ..... 13

1 Introduction ..... 15

1.1 Motivation ..... 15

1.2 Goals & Approach ..... 16

1.3 Definitions ..... 16

2 Overview of Safety Analysis Methods ..... 17

2.1 Event-Based Hazard Analyses ..... 17

2.1.1 Fault Tree Analysis (FTA) ..... 17

2.1.2 Failure Modes, Effects, and Criticality Analysis (FMECA) ..... 19

2.1.3 Preliminary Hazard Analysis (PHA) ..... 23

2.1.4 Summary of Event-Based Models ..... 24

2.2 Systems-Theoretic Methods ..... 27

2.2.1 Systems-Theoretic Accident Model and Processes ..... 27

2.2.2 Systems-Theoretic Process Analysis ..... 29

2.2.3 Use of STAMP and STPA on Aerospace Vehicles ..... 31

2.3 The Changing Nature of Launch Accidents ..... 32

2.3.1 Ariane 5 ..... 32

2.3.2 Titan/Centaur ..... 32

2.3.3 Fregat ..... 32

2.3.4 Falcon 1 Flight 3 ..... 33

2.3.5 Falcon 9 CRS-7 ..... 33

2.3.6 2014 Antares ..... 34
2.4 The Changing Nature of Launch Vehicle Design ..... 34
2.4.1 Reusability ..... 34
2.4.2 Small Satellite Market ..... 35
3 Launch Vehicle Design Process ..... 37
3.1 Systems Engineering Process ..... 37
3.2 Integration of STPA ..... 38
3.2.1 Stakeholder Analysis ..... 40
3.2.2 Requirements Engineering ..... 40
3.2.3 System Architecture ..... 40
3.2.4 System Design & Development ..... 40
3.2.5 Manufacturing & Integration ..... 41
3.2.6 Test & Validation ..... 41
3.2.7 Operation ..... 41
3.3 Designing for Safety ..... 41
3.3.1 Safety-Guided Design Process with STPA ..... 41
3.3.2 STAMP Model of the Design Process ..... 42
4 Design of a Launch Vehicle ..... 45
4.1 Stakeholder Analysis ..... 45
4.2 Conceptual Design ..... 46
4.3 Requirements & Constraints ..... 52
4.3.1 Refined Hazards ..... 53
4.4 System Architecture ..... 55
4.5 System Design ..... 59
4.5.1 Flight Safety System ..... 59
4.5.2 Second Stage Propulsion System ..... 76
5 STPA Range Safety and Regulatory Compliance ..... 91

5.1 14 CFR Part 400 ..... 91
5.1.1 Part 414 Subpart C ..... 91
5.1.2 Part 415 ..... 91
5.1.3 Part 417 ..... 92
5.2 EWR 127-1 ..... 94
5.2.1 Design Priority ..... 94
5.2.2 Software Safety ..... 94
5.3 RCC 319 ..... 97
6 Conclusions & Future Work ..... 99
6.1 Conclusions ..... 99
6.2 Future work ..... 100
6.2.1 Comparison with Traditional Methods ..... 100
6.2.2 Test Requirements and Operations ..... 100
6.2.3 Causal Scenario Generation ..... 100
6.2.4 Leading Safety Indicators ..... 100
6.2.5 Regulations and Range Safety Standards ..... 101
References ..... 103
Appendix A – Flight Safety System STPA Step 1 ..... 109
Safety Control Structure ..... 109
Unsafe Control Actions ..... 110
Safety Constraints ..... 124

# TABLE OF FIGURES

Figure 1. The cost of safety fixes increases exponentially with product lifecycle phase. Adapted from [49]. ..... 16
Figure 2. Integration of FMECAs into Space Vehicle Design [3]. ..... 22
Figure 3. A Generic Control Structure. ..... 28
Figure 4. The classic systems engineering v-model. ..... 37
Figure 5. NASA Space Flight Lifecycle [58]. ..... 38
Figure 6. Generalized Component Design Structure ..... 43
Figure 7. Design process flaws leading to hazards ..... 44
Figure 8. Safety control structure for the launch vehicle concepts during the launch phase. ..... 46
Figure 9. Safety control structure for an expendable air launch vehicle during pre-launch ..... 47
Figure 10. Example tradespace plot for a launch vehicle. The red line represents the Pareto frontier. ..... 56
Figure 11. Safety control structure for a liquid propulsion stage using a gas generator and helium pressurization system. ..... 57
Figure 12. Safety control structure for a liquid propulsion stage with an expander cycle and autogenous pressurization. ..... 57
Figure 13. Safety Control Structure of the Flight Safety System in the vehicle. ..... 60
Figure 14. Propulsion System Control Structure ..... 76
Figure 15. EWR 127-1 Software Safety Critical Functions requirements mapped to the generic STPA causal factors process model. ..... 96

# TABLE OF TABLES

Table 1. Typical failure severity and probability levels used in space vehicle FMECA analyses [3]. .....19
Table 2. Hazard severity and probability levels in MIL-STD-882E [4]. .....20
Table 3. A typical Preliminary Hazard Analysis format at SRR. Adapted from [7]. .....23
Table 4. A typical Preliminary Hazard Analysis format at PDR. Adapted from [7] .....23
Table 5. Typical Launch Vehicle Acceptable Risk Criteria. .....26
Table 6. Component failure rates assumed in most launch vehicle probabilistic failure computations [13]. .....26
Table 7. Human failure rates assumed in most launch vehicle probabilistic failure computations [13], [14]. .....27
Table 8. Simple Example of STPA Step 1. .....29
Table 9. Process State Oriented Context Tables. .....30
Table 10. Contribution to systems engineering activities by STPA. .....39
Table 11. Severity scale used for preliminary hazard analysis .....48
Table 12. Mitigatability scale used for preliminary hazard analysis .....48
Table 13. Severity and mitigatability of losses given identified hazards of the Expendable Ground Launch concept. .....49
Table 14. Severity and mitigatability of losses given identified hazards of the Expendable Air Launch concept. .....50
Table 15. Severity and mitigatability of losses given identified hazards of the Reusable Ground Launch concept. .....50
Table 16. Weighting Factors used in calculating *ORSRM*. .....51
Table 17. Concept *ORSRM* values. .....51
Table 18. Vehicle architectural decisions .....55
Table 19. Flight Safety System UCA context table. .....61
Table 20. Unsafe Control Actions for FSS provides power to termination devices [CA10] .....63
Table 21. Engine control unit UCA context table. .....77
Table 22. Partial list of unsafe control actions for the ECU .....81
Table 23. Examples of safety fixes to mitigate or eliminate causal scenarios. .....88

This Page Intentionally Left Blank

# ACRONYMS & ABBREVIATIONS

| | |
|---|---|
| **AFTS** | Automated Flight Termination System |
| **AP** | Ammonium Perchlorate |
| **Al-Li** | Aluminum-Lithium Alloy |
| **BFR** | Big Falcon Rocket |
| **BRM** | Baseline Reference Mission |
| **CCDL** | Cross-Channel Data Link |
| **CDR** | Critical Design Review |
| **CMD** | Command |
| **CNC** | Computer Numerical Control |
| **COPV** | Composite Overwrapped Pressure Vessel |
| **CPU** | Central Processing Unit |
| **CRS** | Commercial Resupply Services |
| **DSM** | Design Structure Matrix |
| **ECU** | Engine Control Unit |
| **ESA** | European Space Agency |
| **EMC** | Electromagnetic Compatibility |
| **EMI** | Electromagnetic Interference |
| **ESD** | Electrostatic Discharge |
| **EWR** | Eastern and Western Range |
| **FAA** | Federal Aviation Administration |
| **FMECA** | Finite Modes, Effects, and Criticality Analysis |
| **FSS** | Flight Safety System |
| **FTA** | Fault Tree Analysis |
| **FTS** | Flight Termination System |
| **GG** | Gas Generator |
| **GPOS** | General Purpose Operating System |
| **GPS** | Global Positioning System |
| **HAZOP** | Hazard and Operability Analysis |
| **He** | Helium |
| **HITL** | Hardware-in-the-loop |
| **HTPB** | Hydroxyl-Terminated Polybutadiene |
| **HTV** | H-II Transfer Vehicle |

| | |
|---|---|
| **ICBM** | Intercontinental Ballistic Missile |
| **JAXA** | Japanese Aerospace Exploration Agency |
| **JPL** | Jet Propulsion Laboratory |
| **KG** | Kilogram |
| **LOx** | Liquid Oxygen |
| **MDA** | Missile Defense Agency |
| **MIT** | Massachusetts Institute of Technology |
| **MPL** | Maximum Probable Loss |
| **$N_2$** | Nitrogen |
| **$N_2O_4$** | Dinitrogen Tetroxide |
| **NASA** | National Aeronautics and Space Administration |
| **$NO_2$** | Nitrous Oxide |
| **ORSRM** | Overall Residual Safety-Risk Metric |
| **PDR** | Preliminary Design Review |
| **PHA** | Preliminary Hazard Analysis |
| **PSI** | Pounds per Square Inch |
| **RCC** | Range Commanders Council |
| **RF** | Radio Frequency |
| **RP-1** | Rocket Propellant 1 |
| **RTOS** | Real Time Operating System |
| **SAD** | Safe-and-Arm Device |
| **SRR** | System Requirements Review |
| **SSCF** | Software Safety Critical Function |
| **STAMP** | Systems-Theoretic Accident Modeling Process |
| **STECA** | Systems-Theoretic Early Concept Analysis |
| **STPA** | Systems-Theoretic Process Analysis |
| **TBD** | To Be Determined |
| **TVCA** | Thrust Vector Control Actuators |
| **UCA** | Unsafe Control Action |
| **USA** | United States of America |
| **USAF** | United States Air Force |

# 1 INTRODUCTION

## 1.1 MOTIVATION

The causal factors of launch vehicle accidents are changing. Early accidents were often caused by electromechanical component failures, such as electrical shorts in flight computers and mechanical failures in propulsion systems. Efforts to eradicate such failures using traditional methods have proven successful. However, as launch vehicles and the organizations that operate them are becoming increasingly complex and innovative, systematic errors in specification and operation requirements are becoming much more common. Software and component interactions are increasingly implicated in accidents, but the reliability-based tools often used to evaluate safety are unable to predict or analyze software and component interactions. Furthermore, the growing popularity of autonomous flight termination systems (AFTS) reinforces the need for software safety analysis tools. Designers of launch systems need hazard analysis tools that are better equipped to handle these new causes of launch vehicle accidents.

A paradigm change is required. STPA, or Systems-Theoretic Process Analysis, is a new hazard analysis technique based on systems theory. In STPA, safety is viewed as a control problem, rather than a reliability problem. Safety emerges from enforcing constraints on a system's behavior. This leads to much more useful insights into systems engineering than traditional techniques and is much more naturally integrated into the systems engineering process. Safety is an emergent property of the design of a system that is best analyzed alongside system performance. Safety is freedom from undesired and unplanned loss events, and is thus necessary for a system to meet the objectives of stakeholders. In practice, however, safety is often isolated or separated from the system engineering process and introduced late in the design cycle, after the majority of safety-related design decisions have already been made. Expensive and not very effective solutions are then required, often at a performance penalty. For launch vehicles, this usually means adding redundancy or increasing the operational requirements of components far beyond their original specifications. Safety is thus often viewed as opposed to performance, rather than complementary.

Unlike reliability-based tools, STPA can be used throughout the standard system engineering process. High-level safety requirements can be generated early in the concept development phase with STPA to inform architectural decisions when the majority of safety-related decisions are made. These general requirements can be refined using STPA as development activities are completed and more information is discovered. Because STPA treats safety as a control problem, organizational and process elements of the

product lifecycle can be analyzed alongside launch vehicle design to evaluate systemic factors. This allows the design of the engineering organization to more effectively compliment the design of the vehicle.

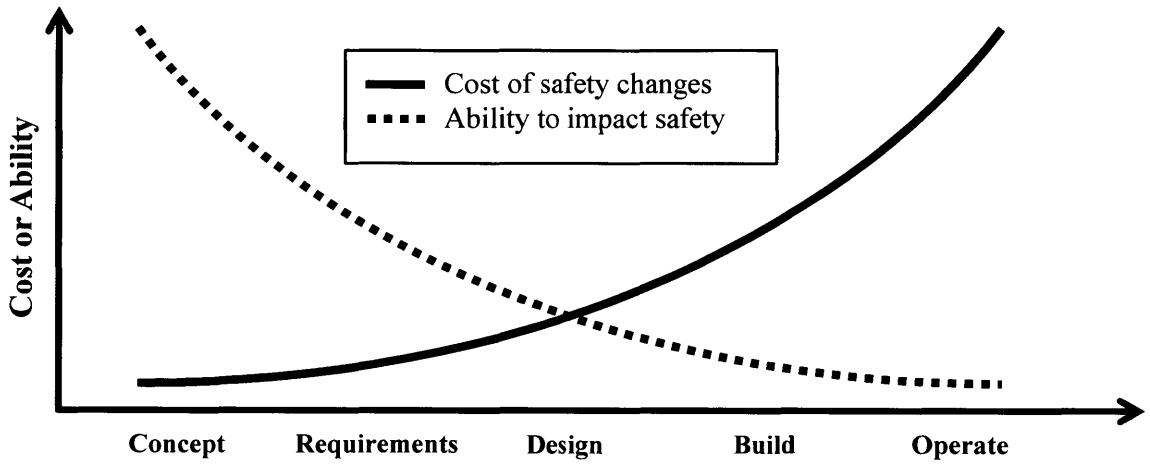



*Figure 1. The cost of safety fixes increases exponentially with product lifecycle phase. Adapted from [49].*

Integrating system safety analysis into the entire system engineering process at the outset results in a significant decrease in the cost of engineering for safety. The cost of a safety correction increases exponentially with lifecycle phase (Figure 1).

## 1.2 Goals & Approach

The goal of this research is to improve the safety of launch vehicles by demonstrating the application of STPA in the design of a two-stage expendable launch vehicle. Detailed safety requirements and constraints are generated and general guidelines for implementing safety-guided design of launch vehicles are developed. Compliance with regulatory and range requirements is also evaluated.

## 1.3 Definitions

Any discussion of safety requires some understanding of common terms. The following definitions are used in this thesis.

| | |
|---|---|
| **Accident** | An unplanned and undesired event that results in a loss |
| **Hazard** | A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident |
| **Hazard Analysis** | The process of identifying hazards and their potential causal factors |
| **Safety** | Freedom from accidents |

# 2 OVERVIEW OF SAFETY ANALYSIS METHODS

All safety analysis methods have the same goal: To identify potential causes of accidents so that they can be eliminated or at least controlled before an accident occurs. Mitigating and identifying hazards requires the analyst to have an understanding of how and why accidents occur. Traditional hazard analysis techniques use reliability theory as their foundation, and conceptualize the cause of an accident as a chain of linearly related failure events. STPA, on the other hand, conceptualizes the cause of an accident as the product of inadequate control or enforcement of safety-related constraints [1]. Each type of hazard analysis method can be characterized by the underlying accident causality model.

## 2.1 EVENT-BASED HAZARD ANALYSES

Event-based hazard analysis methods, which are also called "traditional" safety analysis methods, view accidents as the result of chains of failure events occurring in sequence over time. Each event provides the necessary and sufficient conditions to cause the next event, and so on, until an accident occurs.

To date, all U.S. and European launch vehicle programs use traditional safety analysis methods to evaluate mission safety. NASA, the FAA, and the U.S. Eastern and Western Ranges require that launch operators develop safety plans and demonstrate adherence to safety constraints based on the probability of loss of life, property, and mission. The two most common event-based methods used in launch vehicle reliability and safety assessment are (i) Fault Tree Analysis (FTA) and (ii) Failure Mode, Effects, and Criticality Analysis (FMECA).

### 2.1.1 Fault Tree Analysis (FTA)

FTA is the most widely used method for analyzing hazards in the aerospace industry. It is a top-down, deductive method, in which high-level hazardous events are defined and branches of component faults that could lead to an accident are identified and described. The probability of each component fault is then defined, enabling the probability of the overall accident to be calculated. FTA allows easy comparisons between designs to be made because it reduces safety to the probability of a hazard occurring: by simply reducing the probability of the accident, the system is deemed safer. This is often reinforced by the regulatory and range safety approach taken for launch vehicles, in which the regulator or range authority requires that the expected probability of a casualty per flight is less than an assigned threshold value.

FTA is presumably popular for its simplicity, but it has a few glaring disadvantages. First, the system must be completely designed and each individual component's reliability determined in order for the FTA

to be valid. Because the FTA occurs after the system has been completely designed, findings from the analysis are expensive to implement. FTA thus gives very little useful information to the designer in the early phases of design, when the most impactful safety-critical decisions are made. Frola and Miller found that 70% to 80% of design decisions related to safety are made in the concept development stage [2]. Thus, when the first FTA is conducted, traditionally to support the system's preliminary design review (PDR), only between 30% and 20% of safety-critical decisions are yet to be made. The reliability of each individual component is also nearly impossible to determine, so standard values are substituted or components are omitted. For launch vehicles, where components are often custom-built, standard values are often unreliable indicators of true component integrity. The FTA also often assumes that each component's reliability is independent of other components. In reality, the reliability of each component is often affected by the failures of others. This Boolean nature of component failures also neglects partial failures, operational phases, and timing-dependent events.

Because software is pure design abstracted from its physical realization [1] it does not fail, and certainly not randomly. Software components are thus usually omitted from the FTA. As software becomes more and more important in spacecraft systems, this omission makes the FTA results divorced from the reality of launch vehicle safety.

FTA also assumes that the fault tree is complete, that every component interaction is considered and defined. Launch vehicles contain hundreds of thousands of components, and each valid combination must be evaluated. Fault trees thus become extremely large and cumbersome to update as the system changes with time, further increasing the cost of a design change and increasing the likelihood that the hazard analysis contains conflicting assumptions or missing information.

Most of all, accidents with factors not related to component reliability are often undiscoverable. Design errors, such as software bugs or incorrect human controller models, cannot be analyzed using FTA. Often software is assumed never to fail, but software has been identified as a contributing factor or cause of many modern launch vehicle accidents.

### 2.1.2 Failure Modes, Effects, and Criticality Analysis (FMECA)

FMECA is another popular analysis technique that is an extension of Failure Modes and Effects Analysis. Although it is a bottom-up reliability analysis technique, it is often used in hazard analysis of spacecraft and launch vehicles (Aerospace Corporation FMECA Report). In FMECA, the safety engineer(s) identifies failure modes for each component or function (*failure modes*), describes the effects of each failure mode (*effects*), and assigns a probability and severity of occurrence (*criticality*). Launch service providers usually use MIL-STD-882 or a 4-level scale to qualitatively evaluate and categorize the severity and probability of each failure. A typical 4-level scale recommended for use in spacecraft FMECA by the Aerospace Corporation [3] is shown in Table 1.

*Table 1. Typical failure severity and probability levels used in space vehicle FMECA analyses [3].*

| Severity Level | Severity Category |
|---|---|
| 1 | Catastrophic Loss of Mission or Life |
| 2 | Degraded Mission |
| 3 | Loss of Redundancy |
| 4 | Negligible |

| Probability Level | Probability of Occurrence ($P_o$) |
|---|---|
| Probable | $P_o > 0.01$ |
| Occasional | $0.0001 < P_o \leq 0.01$ |
| Remote | $0.00001 < P_o \leq 0.0001$ |
| Extremely Remote | $P_o \leq 0.00001$ |

Severity Level 3, Loss of Redundancy, does not make much sense. If the redundancy does not result in loss or degradation of mission or life, then the loss of redundancy is inconsequential. MIL-STD-882E provides much more useful levels of severity and probability:

*Table 2. Hazard severity and probability levels in MIL-STD-882E [4].*

| Severity Categories | | |
|---|---|---|
| **Description** | **Severity Category** | **Mishap Result Criteria** |
| Catastrophic | 1 | Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M |
| Critical | 2 | Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M. |
| Marginal | 3 | Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M. |
| Negligible | 4 | Could result in one or more of the following: injury or occupational illness not resulting in a lost work day, minimal environmental impact, or monetary loss less than $100K. |

| Probability Levels | | | |
|---|---|---|---|
| **Description** | **Level** | **Specific Individual Item** | **Fleet or Inventory** |
| Frequent | A | Likely to occur often in the life of an item. | Continuously experienced. |
| Probable | B | Will occur several times in the life of an item. | Will occur frequently. |
| Occasional | C | Likely to occur sometime in the life of an item. | Will occur several times. |
| Remote | D | Unlikely, but possible to occur in the life of an item. | Unlikely, but can reasonably be expected to occur. |
| Improbable | E | So unlikely, it can be assumed occurrence may not be experienced in the life of an item. | Unlikely to occur, but possible. |
| Eliminated | F | Incapable of occurrence. This level is used when potential hazards are identified and later eliminated. | Incapable of occurrence. This level is used when potential hazards are identified and later eliminated. |

FMECAs are used to identify and limit critical failures and single point failures, prevent failure mode propagation, and identify reliability critical items. The implementation of FMECA across the space domain is varied. Best practices for performing FMECAs in the space domain have been developed, but The Aerospace Corporation found that FMECA is not being used effectively in unmanned space vehicle development [3].

Like FTA, use of FMECA usually involves very large data sets and requires the entire system to be designed and tested in order to estimate probabilities of failure. Although standard component failure probabilities exist, the majority of launch vehicle hardware is developed specifically for each vehicle's operating environment. Furthermore, component interactions and the effects of multiple failures are not captured. Because formal FMECAs are bottoms-up analyses, they become large extremely quickly and require significant effort to manage change.

One strength FMECAs have over FTAs is that FMECAs can be performed at a functional block level early in the design process and refined as the design matures. Thus, it is more likely that the functional hazard analysis is comprehensive, as high-level functions can be increasingly decomposed and completeness checked at each level. In practice, functional analyses are often not performed and do not guide design until late in vehicle development [3]. A diagram showing the Aerospace Corporation's recommended integration of FMECA into the space vehicle systems engineering process is shown in Figure 2.

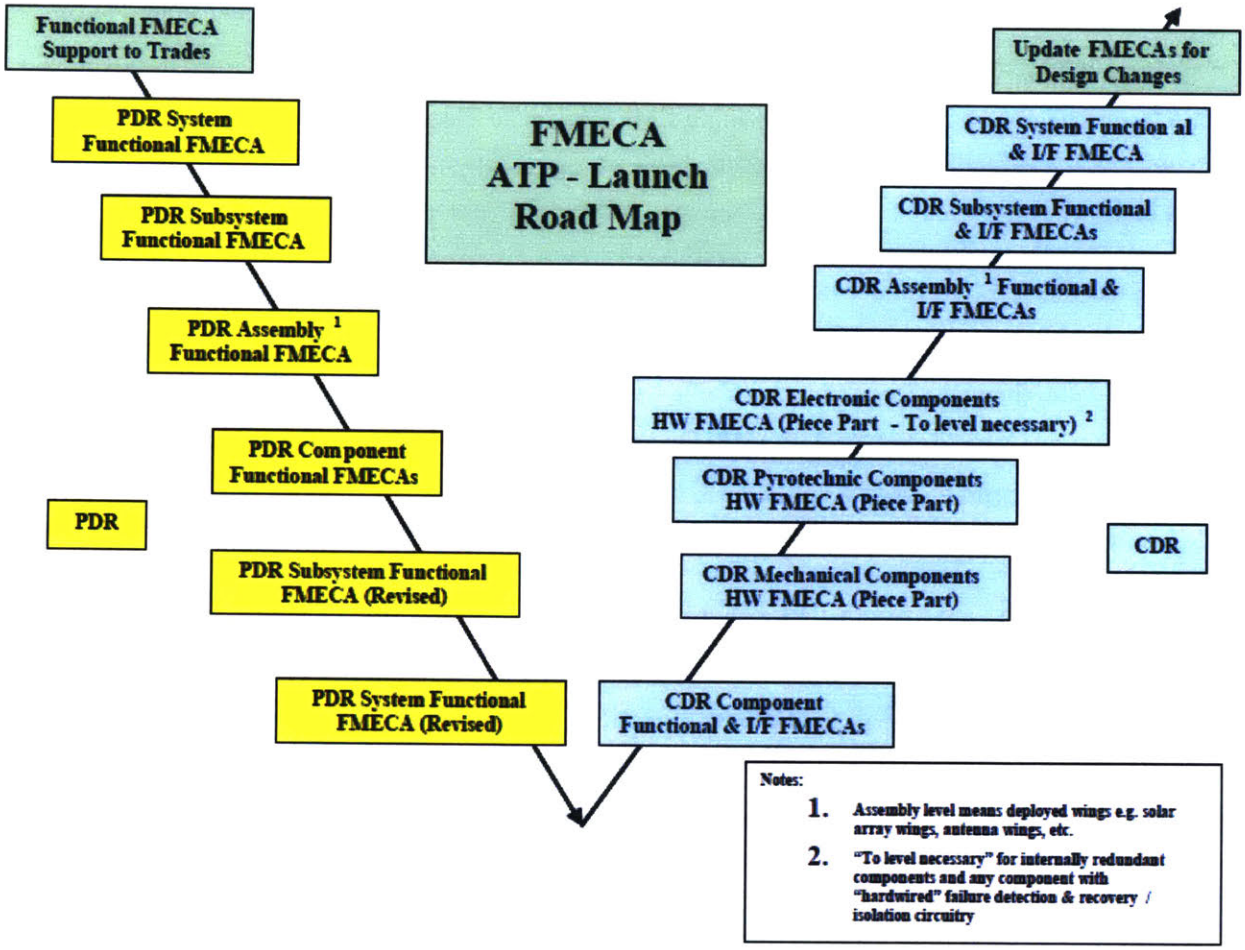



*Figure 2. Integration of FMECAs into Space Vehicle Design [3].*

In this process, FMECAs are performed in early concept development, during PDRs and CDRs, and as designs change after CDR. There are many separate analyses that must be crosschecked to ensure consistency. The consequences of a design change on safety, therefore, become much more difficult to determine, as multiple safety analyses must be updated. Many trivial cases must be considered, and unplanned cross-system effects are difficult to identify. FMECAs are typically performed by separate groups, and designers making critical safety decisions often consult experience and engineering judgment rather than the result of these analyses to make engineering design decisions. Furthermore, it is not possible to use FMECAs to evaluate software, though virtually all functions in spacecraft today are implemented through software. Despite attempts to extend the FMECA method, these analyses have shown limited success in reducing software-related accidents [5] and FMEA/FMECA standards themselves state that the analysis cannot be performed on software, or claim that FMECA can be performed on software to a limited extent but provide no evidence to demonstrate that this is true [6].

### 2.1.3 Preliminary Hazard Analysis (PHA)

In order to supplement FMECA and FTA analyses, a Preliminary Hazard Analysis (PHA) is often conducted to identify potentially hazardous conditions of the conceptual design and to develop a preliminary set of recommendations on how those hazards can be eliminated or controlled. Output of a PHA is used to develop early safety requirements, prepare design specifications, and initiate the hazard tracking and risk resolution processes. A PHA is usually recorded in tables. NASA typically uses the format in Table 3 at System Requirements Reviews (SRR) and the format in Table 4 at Preliminary Design Reviews (PDR).

*Table 3. A typical Preliminary Hazard Analysis format at SRR. Adapted from [7].*

| Hazardous Condition | Cause(s) | Effect and Applicable Project, Element, or Subsystem | Initiating/ Affected Element | Severity | Requirements | Hazard Elimination/ Control Provisions | Failure Tolerance | Recommendation |
|---|---|---|---|---|---|---|---|---|
| Use the checklist below to identify potentially hazardous conditions:<br>1. Can the system fail to operate as intended?<br>2. Can the system operate inadvertently?<br>3. Are there standard errors? | Enter brief description of how each hazardous condition is created. | Record the potential effect of each hazardous condition on critical equipment, personnel, or the public. | Identify the project/ element/ subsystem that initiates the event or is affected. | Identify the worst-case severity level: catastrophic, critical, or other. | Identify the existing or proposed safety requirement that will eliminate or control the hazardous condition. | Identify proposed hazard reduction methods for hazards. | Identify the level of failure tolerance required. | Provide recommendations for additional requirements, trade studies, or other options which may be needed to control or eliminate the hazardous condition. |

*Table 4. A typical Preliminary Hazard Analysis format at PDR. Adapted from [7].*

| Hazardous Condition | Cause(s) | Effect and Applicable Project, Element, or Subsystem | Initiating/ Affected Element | Severity / Likelihood of Occurrence | Requirements | Hazard Elimination/ Control Provisions | Verification | Failure Tolerance | Recommendation |
|---|---|---|---|---|---|---|---|---|---|
| Use the checklist below to identify potentially hazardous conditions:<br>4. Can the system fail to operate as intended?<br>5. Can the system operate inadvertently?<br>6. Are there standard errors? | Enter brief description of how each hazardous condition is created. | Record the potential effect of each hazardous condition on critical equipment, personnel, or the public. | Identify the project/ element/ subsystem that initiates the event or is affected. | Identify the worst-case severity level. Assess the control that are in place and assess the residual risk after the controls are applied. Specify the likelihood that the hazard could occur as a result of the residual risk. | Identify the existing or proposed safety requirement that will eliminate or control the hazardous condition. | Identify proposed hazard reduction methods for hazards. | Identify the methods used to verify the hazard controls. | Identify the level of failure tolerance required. | Provide recommendations for additional requirements, trade studies, or other options which may be needed to control or eliminate the hazardous condition. |

Because only a functional design of the system exists at the time a PHA is conducted, PHA relies heavily on mishap data from similar systems and lessons learned from other projects. A list of standard hazards from similar systems is usually checked to guide the analyst. Unfortunately, the likelihood and severity of a hazardous condition occurring cannot be known before any detailed design is done, and cannot ever be known for software-intensive systems. Thus, hazards are estimated based on experience. These estimates are not useful if the PHA is being conducted on a system that differs significantly from past systems. Analysts have found that specific hazards on real projects are often incorrectly dismissed early in the system development process as marginal or extremely unlikely [8]. Furthermore, the PHA assesses risks assuming that safety controls are in place. No assessment is made of the safety control structure itself.

### 2.1.4 Summary of Event-Based Models

The similarities among the traditional safety analysis methods such as FTAs and FMECAs arise from their common theoretical underpinning. These analyses explain accidents in terms of sequences of time-ordered events that have some probability of occurring. The events directly leading to an accident are identified as a cause or contributory conditions. FTAs and FMECAs, therefore, attempt to find plausible series of events that cause a hazardous condition that may lead to an accident. Traditional methods are premised on the proposition that safety is increased by reducing the probability of the event sequence that may lead to an accident. Engineer(s) use FTAs and FMECAs to remove the causative events or conditions, or add enough redundancy to reduce the likelihood of such causative events or conditions occurring to a comfortable level.

#### *2.1.4.1 Limitations of Traditional Models*

Because traditional safety analysis methods only consider hardware failures, they have limited utility to the designer of modern complex systems. Although FMECA and FTA analyses are able to identify components that are critical to the safety of systems, they do not inform the designer of functional design flaws or complex component interactions. These shortcomings may be partially overcome by experience, as systems are built and flown and interactions are discovered from accidents. This "fly-fix-fly" approach has been the norm for aviation and aerospace, resulting in architectural innovation in these industries being incremental and historically slow.

The dynamic forces that are propelling the commercial space launch market require that space launch vehicle innovation occur at an accelerated pace. Software plays an increasing role in space launch vehicles, and systems are becoming increasingly complex and different from their predecessors. At the same time, regulators and customers demand higher reliability than has been accepted in the

past. Advances in electronics have enabled reusability and the small satellite market, and new vehicles with limited flight heritage are attracting significant investment. Many companies in the commercial space launch market are taking a rapid iteration approach to identifying potential causes of accidents, where design specification errors are found by integrating and flying whole systems. Reused vehicles have an advantage over expendable vehicles in that they provide unique insight into unexpected component interactions, but only when those interactions do not cause accidents that destroy the vehicle [9]. This rapid iteration strategy to identifying hazards is effective but can be very expensive. If the first mission is safety-critical, such as on a crewed vehicle like the Space Shuttle or a missile defense system, the vehicle is carefully tested and controlled, and is also heavily analyzed using traditional safety analysis methods. This iteration approach is both time consuming and expensive, for the same reason: in order to use the traditional safety analysis methods to evaluate the systemic causes of accidents, vehicles must be mostly (or fully) designed.

Despite regulator recommendations to use traditional safety analysis methods to inform design [10], traditional safety analysis methods are often performed improperly and late in the development cycle of new space vehicles [3]. Software is unable to be analyzed using the traditional safety analysis methods, and the operating context the vehicle is assumed to operate in by the traditional analysis is often changed and improperly documented over the product lifecycle. Both the false equivocation of reliability with safety and the increasing role of software in launch vehicle accidents warrant the consideration of new or additional safety analysis methods.

#### *2.1.4.2 Use of Event-based Analyses in Launch Vehicles*

Traditional safety analysis methods require the identification of events that cause a hazard, which in turn relies on extensive experience from past failures. Thus, traditional safety analysis methods tend to be effective only for standardized designs in slow-innovation technology sectors or for simple systems composed primarily of simple electromechanical devices. When technology changes rapidly, however, the effectiveness of learning from past failures is significantly more limited [11].

The primary objective of U.S. Government safety organizations for space vehicle activities has been the protection of people. The primary safety risk measures used to assess safety is the overall expected number of casualties or the overall probability of a casualty to individuals or a theoretical most-exposed individual. Over time, these protection objectives have expanded to include the maximum probable loss (MPL) that will result from launch operations [12]. The MPL is a combined measure of damage and injury that may occur from a launch event. In order to address safety in the requirements generation phase of launch vehicle design, reliability or statistical requirements are written to provide constraints on vehicle operation and design. This approach is codified into the FAA launch vehicle licensing process,

which uses probabilistic expectations of casualties to determine acceptable mission risk. Eastern Western Range (EWR) requirements follow a similar approach. Some standard values used by the FAA, EWR, and the Range Commanders Council (RCC) are shown in Table 5.

*Table 5. Typical Launch Vehicle Acceptable Risk Criteria.*

| Probabilistic Requirement | Standard Value |
|---|---|
| Loss-of-crew | $5 \times 10^{-3}$ |
| Casualty expectation per launch to public | $10^{-4}$ |
| Casualty expectation per launch to individual | $10^{-6}$ |
| Probability of impact of water borne vessels | $10^{-5}$ |
| Probability of impact of aircraft | $10^{-6}$ |
| Fatality expectation per launch to public | $3 \times 10^{-5}$ |
| Fatality expectation per launch to individual | $1 \times 10^{-3}$ |

While these requirements define how safe is safe enough to fly a launch vehicle, these probabilistic requirements offer little guidance for the design of new space launch systems. Standard failure rates are assumed for overflight risk assessments early in the design process. Component failure rates that are commonly used in failure and risk computations are shown in Table 6.

*Table 6. Component failure rates assumed in most launch vehicle probabilistic failure computations [13].*

| Component Failure | Rate |
|---|---|
| Automatic Shutdown | $10^{-2}$ / demand |
| Emergency Shutdown System | $10^{-3}$ / demand |
| Defective Materials (Seals) | $10^{-4}$ / demand |
| Defective Pumps | $10^{-3}$ / year |
| Faulty Gasket | $10^{-5}$ / year |
| Brittle Fracture (Pipes) | $10^{-5}$ / year |
| Pipe Failure – 3′ rupture | $8 \times 10^{-5}$ / section-year |
| Spontaneous Failures (Tanks, etc.) | $10^{-6}$ / year |

These component failure rates are often applied improperly to human actions. Table 7 shows commonly applied human error rates that are recommended by the FAA Office of Commercial Space Transportation and the petroleum industry. These probabilities assume that (i) human errors are random and (ii) independent of whether the interface between a human and the system is well designed or poorly designed. These assumptions are invalid, and do not provide the designer useful information for evaluating the safety of a system.

*Table 7. Human failure rates assumed in most launch vehicle probabilistic failure computations [13], [14].*

| Task | Probability of Error/Task |
|---|---|
| Critical Routine | $10^{-3}$ |
| Non-Critical Routine: Errors of omission & commission | $10^{-2} - 10^{-3}$ |
| High Stress Operations | $10^{-1} - 10^{-2}$ |
| Responses after major accident during: | |
| 1. 1st minute | 1 |
| 2. 1st to +5 minutes | $9 \times 10^{-1}$ |
| 3. +5 minutes to +30 minutes | $10^{-1}$ |
| 4. +30 minutes to +several hours | $10^{-2}$ |

Using this event-based perspective, the engineer maximizes safety by maximizing reliability, effectively minimizing the probability of casualties resulting from a catastrophic failure along a given trajectory. Bounds are put on that trajectory, and the vehicle is destroyed if it approaches these limits. If a vehicle is crewed, systems are usually required to allow the crew to escape during the most probable failures. The focus of launch vehicle safety has been on mission safety and assurance. During handling and operations, launch service providers typically use traditional human-factors engineering and event-based failure modes analyses to assess the hazards associated with working on or with the vehicle.

In recent times, the objectives of launch vehicle safety have grown to include consideration of the protection of critical assets, infrastructure, cultural resources, and the environment. Still, this broader view of the objectives of space launch vehicle safety is relatively new [12]. Regardless of such individual objectives, in the more appropriate, generalized view of safety as *freedom from accidents (loss events)*, as defined in section 1.3, it is clear that the view of launch vehicle safety has been too narrow.

## 2.2 SYSTEMS-THEORETIC METHODS

### 2.2.1 Systems-Theoretic Accident Model and Processes

An alternative to event-based hazard analysis techniques is Systems-Theoretic Process Analysis (STPA), a hazard analysis technique based on STAMP. STAMP is an accident model founded on systems theory that changes the emphasis in system safety from preventing failures to enforcing safety constraints on system behavior [1]. Systems are viewed as hierarchies of interrelated components kept in a state of dynamic equilibrium by feedback control loops. Safety emerges from maintaining the appropriate constraints on the system's behavior. Systems are thus not treated as static and linear, as in the traditional safety analysis models, but as dynamic and adaptive to changes to itself and its environment.

An example of a simple control structure is shown in Figure 3. In it, a controller such as a human, hardware component, or software performs actions to influence a process. Sensors then provide feedback to the controller, which adapts its actions according to its model of the process.

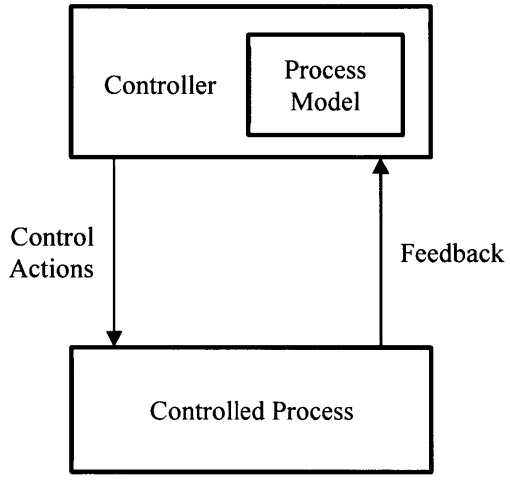



*Figure 3. A Generic Control Structure.*

Accidents occur when the safety control structure does not enforce the system safety constraints and hazardous states result. Hazardous states can occur due to unhandled environmental disturbances, unhandled or uncontrolled component failures, unsafe interactions among components, and inadequately coordinated control actions by multiple controllers [15].

STAMP models have been demonstrated to be more complete than most other models [1] [16] [17]. By focusing on systemic factors, STAMP reduces subjectivity, catches requirements flaws, and gives a more useful picture of the system to designers. Traditional safety analysis techniques have demonstrated limited ability to provide insight into component interactions, software errors, human errors, requirements incompleteness, and organizational and management flaws [1]. These shortcomings are often treated by analyzing each of these elements separately from the reliability analysis. This introduces further complexity into the hazard analysis and increases the likelihood that analysis errors are made. By treating the system as a control structure, STAMP considers both component interaction factors and component failures. The causes evaluated by STAMP are thus a superset of those identified by the traditional safety analysis techniques [15].

### 2.2.2 Systems-Theoretic Process Analysis

STPA is an iterative process that can be used at any stage of the system life cycle to provide insight into ensuring safety constraints are enforced. The two main steps to STPA are:

1. Identify potentially hazardous control actions.
2. Determine how each unsafe control action identified in step 1 could occur, i.e., the scenarios that can lead to hazardous control actions.

Prior to performing STPA, the system boundary and system goals must be defined. This enables high-level accidents to be identified based on stakeholder needs. System-level hazards are derived from these accidents to guide the analysis. The first step in STPA is to assess the safety controls provided by the system design and determine the potential for inadequate control. Control actions can be hazardous in four ways [1]:

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

Step 1 is typically performed by generating a table of control actions and identifying the context in which the action can be hazardous according to the above list. An example for a computer that coordinates the actions of multiple Computer Numerical Control (CNC) mills is shown below.

*Table 8. Simple Example of STPA Step 1.*

| Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|
| Send command to start mills | N/A | Mills are not correctly placed next to part<br><br>Mills are incorrectly mounted to machine<br><br>Mills are incorrectly configured | Mills are started before material is in place | N/A |

Because the control actions are finite and known, the STPA analyst can quickly check that all interactions between the controller and the process have been considered. Other table configurations are possible because there is no specified format for categorizing context or unsafe control actions in STPA. Another systematic method for identifying unsafe control actions is by evaluating each operating context directly

[18]. Two tables are required, depending on whether the control action is provided or not provided. An example is shown in Table 9.

*Table 9. Process State Oriented Context Tables.*

| Control Action | Process State Variable 1 | Process State Variable 2 | Process State Variable N | Hazardous Control Action? If provided any time in this context | If provided too early in this context | If provided too late in this context |
|---|---|---|---|---|---|---|
| Control Action A provided | | | | | | |

| Control Action | Process State Variable 1 | Process State Variable 2 | Process State Variable N | Hazardous if control action not provided? |
|---|---|---|---|---|
| Control Action A <u>not</u> provided | | | | |

This method has been demonstrated to be effective for systems with complex operating environments and for multiple controllers acting on the same process. From the above table, the list of unsafe control actions are found and the appropriate system safety constraints can be identified. Often multiple unsafe control actions can be mitigated with the same system safety constraint.

In step 2, guidance is provided to help engineers identify the scenarios or paths that could lead to each hazard. At this step, the high-level hazards from the stakeholder analysis are typically refined to lower-level hazards. The causal scenarios that could lead to these lower-level hazards are identified, and the mechanisms through which these controls can degrade over time are considered. Identifying the degradation in controls is an important and unique aspect of STPA that makes it particularly powerful for complex systems that operate over many years and many design variants, such as launch services. Complex systems tend to conditions or states of higher risk with time. A study of the organizational dynamics of the Space Shuttle program's dynamics showed that systemic risk not only increases with time, but that responding to accidents only shortly decreases total system risk while greatly increasing perceived system safety [19].

From this analysis, design and operational recommendations can be made. Component failures and unsafe interactions can be controlled through design, process, or social controls. STPA gives insights into which type of control is most appropriate.

### 2.2.3 Use of STAMP and STPA on Aerospace Vehicles

STAMP and STPA have been used in the analysis of a handful of aerospace vehicles. Comparisons of STPA directly with traditional techniques have demonstrated a clear superiority of STPA. In a comparison between an STPA analysis of the Japanese Aerospace Exploration Agency's H-II Transfer Vehicle (JAXA HTV) and an existing NASA Fault Tree Analysis, all of the hazards in the fault tree were identified by STPA, and there were causal factors that were identified by STPA only [20]. Some of the causal factors identified by STPA, but not the fault tree, were crew mistakes in operation, delayed activation commands, out-of-range radio disturbances, and wrong information or directives from the NASA/JAXA ground station.

JAXA also used STPA to evaluate the safety-guided design of JAXA's Crew Return Vehicle, as the organization found that traditional fault tree analyses were not useful in their conceptual design activities [21]. Embraer [22] and Boeing [23] have also used STPA to evaluate aircraft and workplace safety. Dunn evaluated the NASA GPM mission with STPA and created generalized control structures to guide other satellite design engineers [24]. Fleming and Leveson demonstrated improvements to the hazard analysis and certification of integrated modular avionics using STPA [25]. Owens and Crocker applied STAMP to evaluate spacecraft operator training [26].

STPA is also less costly than traditional safety analysis methods. Two people worked for three months to conduct a Non-Advocate safety analysis for the U.S. Missile Defense Agency's Ballistic Missile Defense System using STPA [27]. The analysis not only identified every causal factor in the previous traditional analysis, it also found enough undiscovered safety-critical problems that it took MDA 6 months to fix the newly discovered problems [28].

Other STAMP-based analysis tools have been used to conduct accident analyses and organizational evaluations. Notable examples include an accident analysis of the third Milstar satellite launch [1], and an independent evaluation of NASA's Independent Technical Authority organization [29]. Fleming created a STAMP-based approach to preliminary hazard analysis in conceptual design called STECA and demonstrated its application to the NextGen air traffic management modernization program [30]. An MIT-JPL collaboration applied STAMP and STPA to the design of an outer planet exploration mission [31]. Ball extended STPA to identify leading indicators in early-stage aerospace product development [32].

## 2.3 The Changing Nature of Launch Accidents

Notable software and specification failures abound in recent years. To demonstrate the increasing role of component interaction accidents, noteworthy examples are presented.

### 2.3.1 Ariane 5

In early 2018, an Ariane 5 lost contact with its ground station during flight. The vehicle continued to fly and inject its payloads into orbit, but at the wrong orbital parameters. The SES and Eutelsat satellites onboard the rocket were placed into an orbit at a 20.6 degree inclination, a significant departure from their intended 3 degree inclination. An investigation by an independent commission showed that the anomaly resulted from an incorrect value in the azimuth required for the alignment of the launcher's inertial units [33]. This bad specification was not caught during the standard quality checks carried out during the launch preparation plan. A causal factor that was not identified by the investigation, but that was reported by European media, was that a procedure to double-check the flight software before liftoff was cut in a cost reduction effort [34].

The same vehicle was also involved in one of the most famous software errors in launch history. Forty seconds into its maiden launch, the Ariane 5 veered off its intended flight path, broke up due to high aerodynamic loads, and exploded 8900 feet above the launch pad. The accident report identified "complete loss of guidance and attitude information" as the cause of the accident. This information was lost due to specification and design errors in the inertial reference system of the flight software, which itself was reused from Ariane 4. Both the back-up and active inertial reference systems were loaded with the same software, and key functions were not tested under simulated Ariane 5 flight conditions [35].

### 2.3.2 Titan/Centaur

Software development, testing, and quality assurance issues were also determined to be the cause of a 1999 launch of a Titan/Centaur rocket. During the burn of the Centaur upper stage, the vehicle experienced a roll instability due to a roll rate filter constant that was incorrectly entered into the Inertial Measurement System flight software file. The vehicle lost control and depleted the hydrazine in its reaction control system, leading to placement of the Milstar payload into an incorrect and unusable orbit [36].

### 2.3.3 Fregat

Component interaction accidents are not limited to software specifications. In a 2014 Soyuz launch, the vehicle's Fregat upper stage placed two Galileo navigation satellites into the wrong orbit. An ESA independent review board found that the Fregat main engine was commanded an erroneous thrust vector during the stage's second burn. This error was the result of the loss of inertial reference, as it was

operating outside of its normal operational envelope because two of the stage's attitude control thrusters failed. The attitude control thrusters failed because hydrazine froze in the thruster feed system, which was connected to the vehicle using the same support structure as cold helium lines. The support structure acted as a thermal bridge. According to the report, "[a]mbiguities in the design documents" allowed this design error to occur and "such bridges have also been seen on other Fegat stages now under production" [37]. The chief of the failure review board found that six of forty-five previously flown Fregat stages had flown a similar mission profile, but "it can only be supposed that they were among the majority of Fregats whose helium and hydrazine lines were not clamped together" [38]. The report recommended rework of the thermal analysis, design documents, and manufacture, assembly, integration, and inspection procedures of the supply lines [37]. None of these recommendations involved reviewing the design of other systems, or evaluating the social structure that enabled ambiguous design documents and design errors in the first place. In November 2017, a Fregat upper stage injected its payloads back into the Earth's atmosphere due to a guidance and navigation software error that was previously undetected [39]. In fact, there has been a Russian launch failure every year from 2004 to 2017 [40].

### 2.3.4 Falcon 1 Flight 3

During the third flight of the Falcon 1 vehicle, residual propellant in the first stage engine provided transient thrust during second stage separation. The thrust was sufficient to push the first stage into the second, preventing the second stage from completing its mission [41]. This issue was resolved on the following flight by increasing the delay between first stage main engine cutoff and the separation of the second stage. Another component interaction failure caused a Falcon 9 rocket to explode on the pad during preparation for the AMOS-6 mission. The most likely cause of the explosion was the trapping of liquid oxygen between the composite overwrap and buckled aluminum liner of the vehicle's upper stage helium tank, which solidified when cold helium was loaded into the tank [42].

### 2.3.5 Falcon 9 CRS-7

In the majority of the component failure incidents, the components failed because they did not meet the very specifications that were assumed in the hazard analysis. As an example, in a 2015 Falcon 9 accident, a strut in a second stage propellant tank failed at a fraction of its rated strength. After thousands of tests of material from the same supplier, the company found that a few failed at much lower forces than expected [43]. SpaceX attributed the cause as a manufacturing defect, but the NASA independent review team attributed the cause of the accident more broadly as a design error [44]. The NASA team found that "[t]he use of an industrial grade 17-4PH SS (precipitation-hardening stainless steel) casting in a critical load path under cryogenic conditions and flight environments, without substantial part screening, and without regard to manufacturer recommendation for a 4:1 factor of safety, represents a design error –

directly related to the F9-020 CRS-7 launch failure" [44]. Specifications for commercially procured wire ropes did not heed the manufacturer's caution to specify the ropes be pre-stretched. Reliability estimates used in these kinds of safety and mission assurance analysis do not include the probability of this kind of gross defect, and are incapable of analyzing the quality assurance organization.

### 2.3.6 2014 Antares

Furthermore, reliability estimates are often taken from the component's initial intended use, not the new context in which they are used. The 2014 Antares failure was linked to the contact of rotating and stationary components, but a NASA Independent Report Team was unable to identify a definitive cause for the contact identified as the proximate cause [45]. According to the NASA report, inadequate design robustness, foreign object debris, or a manufacturing defect identified with another engine was the technical root cause of the accident. The operator, Orbital Sciences Corporation, instead blamed a machining defect from when the component was originally manufactured in the Soviet Union nearly 40 years before the accident [46]. Regardless of the "root cause," NASA had identified that the "engines were not subjected to a thorough delta-qualification program to demonstrate their operational capability and margin for use on Antares." In short, the operating context changed, but the engine was not sufficiently analyzed or tested to demonstrate that it maintained reliability within this new context. The NASA team also found a lack of communication and increased technical risk with time, and attributed the lack of design insight into the engines to a "low level of confidence in loss-of-mission predictions made by Orbital ATK and Aerojet-Rocketdyne."

## 2.4 The Changing Nature of Launch Vehicle Design

The nature of launch vehicle design has changed as well. New market pressures have changed traditional launch paradigms and produced a burgeoning commercial launch industry.

### 2.4.1 Reusability

Reusable orbital launch vehicles have been seriously studied since the early 1960's. The first reusable orbital vehicle was the Space Transportation System, more commonly referred to as the Space Shuttle Program. The Space Shuttle Orbiter and Solid Rocket Motors were reusable, requiring extensive design innovations that pushed the limits of 1970's technology. Although many reusable vehicles were proposed and developed in the years after the Space Shuttle, it wasn't until 2010 that another reusable lifting-body vehicle, the USAF X-37B, flew and returned to orbit. In 2015, SpaceX landed its first stage booster at Cape Canaveral. Soon after, SpaceX became the first company to land and re-fly an entire stage with minimal refurbishment in 2017 [47]. SpaceX flew two refurbished boosters on the maiden flight of the Falcon Heavy, and landed those stages at Cape Canaveral after ascent [48]. The company's super-heavy

lift BFR vehicle, currently under development, will also be reusable, refuel in space, and use staged-combustion Raptor engines [49]. Blue Origin's New Glenn heavy lift vehicle will also reuse its boosters, which will also be powered by staged-combustion engines [50].

### 2.4.2 Small Satellite Market

The growing demand for worldwide imaging and telecommunications has spurred the development of small satellite constellations in low earth orbit. The launch market has responded with three solutions: placing small satellites as secondary payloads on large launch vehicles, mass deployment on single launch vehicles, and dedicated small launchers to resupply constellations. A survey of the small launch market found that at least 29 launch vehicles were in active development as of September 2016 [51]. This development is nearly entirely backed by venture capital, dramatically changing the goals and development pace of this sector of the market. These financial pressures, as well as the advent of new manufacturing technologies, have caused companies to make innovative design decisions, devise and develop new operational concepts, and take unusual development strategies. Nearly every launch vehicle company is making use of additive manufacturing to streamline the process of building rocket engines and spacecraft components [52]. Relativity Space has chosen to additively manufacture and the majority of its components, including the primary structure [53]. Rocket Lab USA, a New Zealand and US-based company, has developed electric pumps [54] to deliver propellants to its additively manufactured engines, and Virgin Orbit's air-launched vehicle uses additively manufactured engines and composite tanks without metallic liners [55]. Vector Space Systems has experimented with mobile launch systems to reach a target launch rate of 100 per year [56]. These rapid development cycles, ambitious use of new technologies, and nontraditional operational concepts pose new safety challenges in an industry with intense time and funding pressures.

This Page Intentionally Left Blank

# 3 LAUNCH VEHICLE DESIGN PROCESS

## 3.1 SYSTEMS ENGINEERING PROCESS

The history of modern systems engineering is inextricably tied to launch vehicle development. The Atlas Intercontinental Ballistic Missile (ICBM) was one of the first large scale applications of modern systems engineering, and the Apollo program was the first nonmilitary government program in which systems engineering was recognized as an essential function [57]. This heritage continues today. All major U.S. and European launch vehicle programs have followed some form of the classic systems engineering v-model (Figure 4).

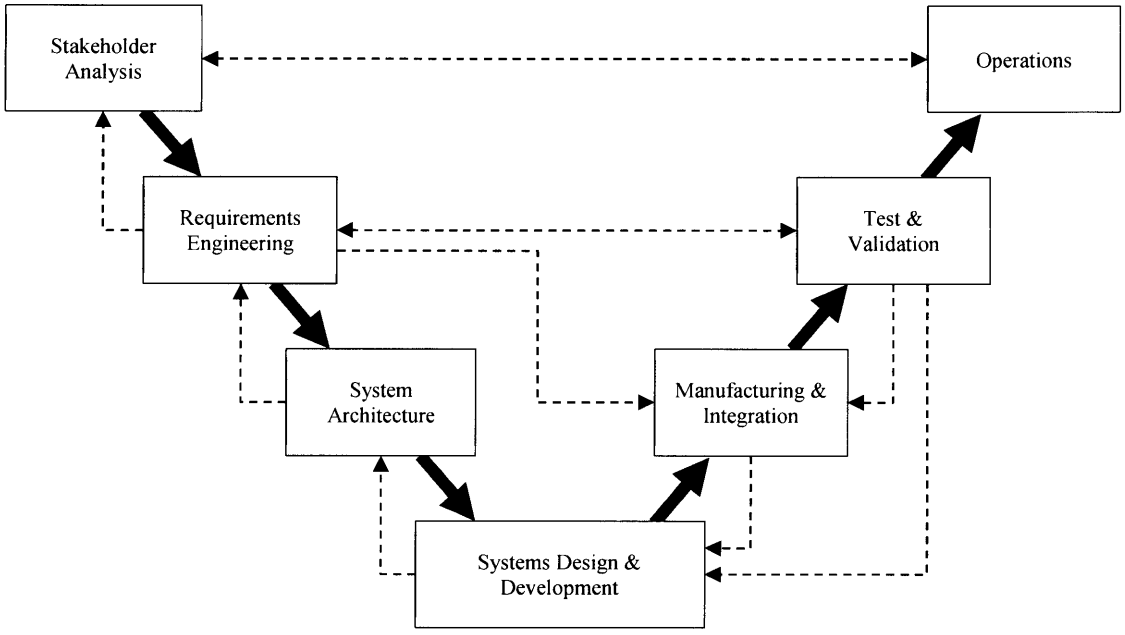
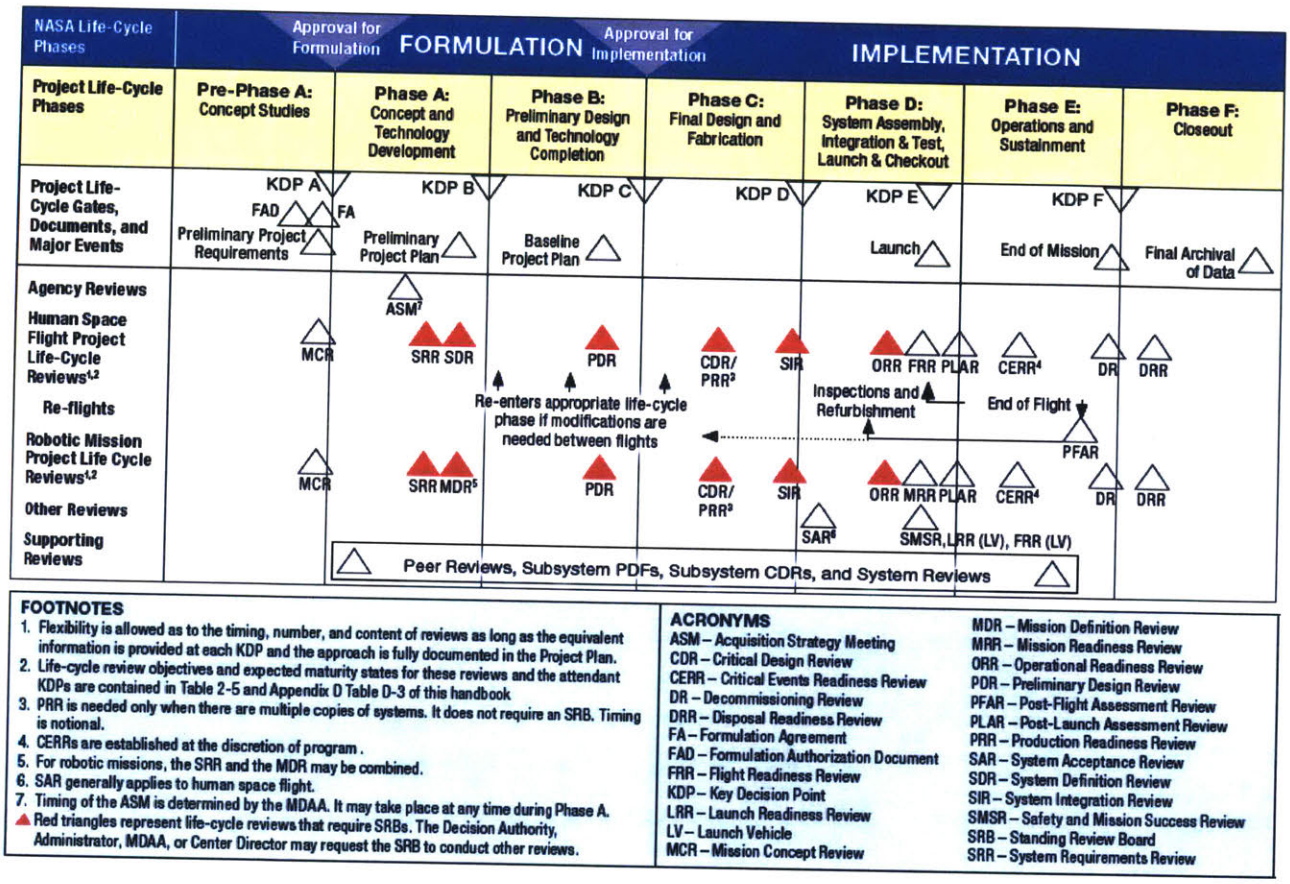



*Figure 4. The classic systems engineering v-model.*

Only a few of the most important feedback loops are shown in Figure 4. In practice, there is some form of information flow from each element to the others. The extent of this information flow and its criticality is dependent on the nature of the system being developed. Communication is critical in managing emergent properties of any complex system, especially safety. Enforcing safety constraints requires that information needed for decision-making is available to the right people at the right time.

Review gates follow each of the major design and integration activities to ensure that risks and opportunities are evaluated before resources are allocated to the proceeding phase. NASA follows a phase-gate lifecycle process in the development of launch vehicles (Figure 5). The formulation phases of

the lifecycle correspond to the left side of the v-model, and the implementation phases correspond to the right side.




**FOOTNOTES**

1. Flexibility is allowed as to the timing, number, and content of reviews as long as the equivalent information is provided at each KDP and the approach is fully documented in the Project Plan.
2. Life-cycle review objectives and expected maturity states for these reviews and the attendant KDPs are contained in Table 2-5 and Appendix D Table D-3 of this handbook
3. PRR is needed only when there are multiple copies of systems. It does not require an SRB. Timing is notional.
4. CERRs are established at the discretion of program.
5. For robotic missions, the SRR and the MDR may be combined.
6. SAR generally applies to human space flight.
7. Timing of the ASM is determined by the MDAA. It may take place at any time during Phase A.

▲ Red triangles represent life-cycle reviews that require SRBs. The Decision Authority, Administrator, MDAA, or Center Director may request the SRB to conduct other reviews.

**ACRONYMS**

ASM – Acquisition Strategy Meeting
CDR – Critical Design Review
CERR – Critical Events Readiness Review
DR – Decommissioning Review
DRR – Disposal Readiness Review
FA – Formulation Agreement
FAD – Formulation Authorization Document
FRR – Flight Readiness Review
KDP – Key Decision Point
LRR – Launch Readiness Review
LV – Launch Vehicle
MCR – Mission Concept Review
MDR – Mission Definition Review
MRR – Mission Readiness Review
ORR – Operational Readiness Review
PDR – Preliminary Design Review
PFAR – Post-Flight Assessment Review
PLAR – Post-Launch Assessment Review
PRR – Production Readiness Review
SAR – System Acceptance Review
SDR – System Definition Review
SIR – System Integration Review
SMSR – Safety and Mission Success Review
SRB – Standing Review Board
SRR – System Requirements Review

*Figure 5. NASA Space Flight Lifecycle [58].*

The effect of design iterations and rework are more important than this linear process suggests [59]. Stakeholder needs and goals change with time, and the development of new technologies presents unexpected risks and opportunities that require adjustment. The systems engineering process must support system evolution without compromising safety. This chapter describes how STPA can be integrated into the product lifecycle to enable safety-guided design.

## 3.2 INTEGRATION OF STPA

The difference between safety-guided design and the usual design process is that hazard analysis is used throughout the systems engineering lifecycle to generate the safety constraints that are factored into design decisions as they are made. Safety-related information must be freely available and digestible to engineers. Because STPA is a hierarchical systems-theoretic tool, it fits naturally into the launch vehicle systems engineering process.

The systems engineering process starts with a stakeholder analysis. This analysis allows the system designers to agree on objectives and identify constraints on how goals can be achieved. With these high-level goals, a trade analysis is conducted to select a concept of operations and system architecture. Goals are refined further into requirements and constraints that drive the design and development process. Subsystems are designed, manufactured, and tested individually then integrated together to form the system, which is itself tested to validate that it meets the requirements, constraints, and goals. This process is repeated until an acceptable system results. Because the systems engineering process focuses on managing interfaces, requirements, and constraints, STPA is a particularly useful analysis tool. Unlike traditional methods, STPA is able to support early architectural trades and detailed engineering decisions. The contributions of STPA to systems engineering activities are shown in Table 10. Portions of content in this table are adapted from Leveson and Thomas' STPA Handbook [8].

*Table 10. Contribution to systems engineering activities by STPA.*

| Lifecycle Activity | Contributions by STPA |
|---|---|
| **Stakeholder Analysis & Concept Development** | • Identify safety and other system goals<br>• Generate initial system requirements<br>• Inform conceptual design trades by establishing safety evaluation criteria |
| **Requirements Engineering** | • Identification of system-level hazards and related constraints on system behavior<br>• Design of the engineering development organization<br>• Generate component or subsystem requirements |
| **System Architecture** | • Preliminary hazard and risk analysis to assist architectural design decisions<br>• Identify system integration and critical interface requirements |
| **Systems Design & Development** | • Assist design and development decision-making (safety-guided design)<br>• Design safety management organization |
| **Manufacturing & Integration** | • Support manufacturing control and workplace safety<br>• Evaluate system integration problems |
| **Test & Validation** | • Generation of system test and evaluation requirements<br>• Identify critical tests and testing regimes |
| **Operations** | • Generation of operational safety requirements & safety management plan<br>• Identify and monitor safety leading indicators |

STPA is hierarchical and can be used across the entire product lifecycle, promoting traceability as the system evolves. Because a systems model is required, assumptions are explicit throughout the design lifecycle and easily communicated across the engineering organization.

### 3.2.1 Stakeholder Analysis

The purpose of the stakeholder analysis is to determine the high-level goals of the system. Performance and mission capabilities, cost, schedule, reliability, safety, and operability goals are determined alongside any additional factors. Stakeholder networks can be evaluated to help identify external constraints and high-level losses that are important to mitigate. Both high-level goals and losses to be considered must be agreed upon by the launch vehicle stakeholders to establish goals for the safety program.

### 3.2.2 Requirements Engineering

Once the set of losses to be avoided has been agreed upon in stakeholder analysis, hazards can be formulated. This preliminary hazard analysis informs early requirements and constraints on the vehicle's behavior. The engineering organization is often put together around this time in order to support the development of the vehicle, and STPA can help inform the design of the engineering organization and development processes.

### 3.2.3 System Architecture

Using the high-level safety requirements, early-stage technical decisions that define the system's architecture are made. Permutations of design decisions, such as the number of stages, propellant types, engine configurations, and so on are analyzed and decisions made. STPA can be used to evaluate the control structures of these architectures and provide a preliminary hazard analysis to inform these decisions. These early technical decisions define the elements of the launch vehicle and the relationship between those elements. Risk analysis is usually not included in this phase because it is difficult to estimate. Development risk is typically handled by evaluating the Technology Readiness Level of each component, and high-level hazards are ranked by their severity and ability to mitigate. STPA can be used in this phase because a high-level control structure exists for each concept. Architectural hazards can then be identified and eliminated or reduced based strictly on the control structure, not the likelihood of each component failing, which cannot be determined in the architectural phase.

### 3.2.4 System Design & Development

Once the system's architecture is selected, subsystem features will be defined and designed. An internal control structure for the system is constructed, and functional requirements and constraints from the requirements phase are assigned to individual system components. STPA can be used to generate analyses of the hazards and inform opportunities for their elimination or mitigation. As performance and interface characteristics of system elements are discovered in the design process, additions and changes will likely be made to requirements and constraints. STPA can be used to generate safe design alternatives and continually evaluate safety as the design progresses.

### 3.2.5 Manufacturing & Integration

Key interfaces and components identified by STPA during design inform quality control and integration processes. STPA can also be applied to workplace safety during critical manufacturing and integration activities.

### 3.2.6 Test & Validation

Because STPA identifies key safety drivers, test requirements can be designed to ensure that the safety control structure functions as intended. The hazard analysis can be updated as unanticipated component interactions are discovered, and safety fixes can be proposed from the safety control structure. By evaluating the control structure, rather than component reliability, hazard elimination is a more natural step than increasing redundancy or safety factors, the most common design fixes late in the system lifecycle.

### 3.2.7 Operation

STPA allows the entire sociotechnical system to be analyzed, not just engineering components. Interactions between the organizational control structure and engineered components are explicit, allowing operational safety requirements to be analyzed alongside the vehicle's safety requirements. STPA can be used to evaluate the operating organization to assist in the creation of a safety management plan. Leading safety indicators can be identified with STPA and monitored to give operators the feedback required to maintain system safety.

## 3.3 Designing for Safety

Accidents involving software or system logic design often result from requirements incompleteness and unhandled scenarios in the functional design of the safety control system [1]. This section develops some launch vehicle design principles that derive directly from a model of the engineering design process. In STAMP, accidents are caused by inadequate control. The same is true in design.

### 3.3.1 Safety-Guided Design Process with STPA

Once the hazards, system-level safety requirements, and constraints have been identified, design can begin. The general process in safety-guided design [1] is:

1. Try to eliminate hazards from the conceptual design
2. If any hazards cannot be eliminated, identify the potential for their control at the system level.
3. Select a system control structure to enforce safety constraints.
4. Refine the constraints and design in parallel.

a. Identify hazardous control actions by each of the system components that would violate system constraints (STPA Step 1).
b. Determine what factors could lead to violation of the safety constraints (STPA Step 2).
c. Redesign to eliminate or control potentially unsafe control actions and behaviors.
d. Repeat 4a through 4c until all hazardous scenarios are eliminated, mitigated, or controlled.

A natural hierarchy of design choices exists to eliminate or control hazards. First, the designer should attempt to eliminate hazards by substituting or removing elements, decoupling interactions, eliminating environmental inputs that are known to induce human error, and reduce hazardous materials or conditions. These choices are usually made at the architectural level, and are the most effective and inexpensive to implement at the outset of engineering design. If hazards cannot be eliminated, they should be reduced by designing proper controls, introducing barriers, increasing safety factors, or adding redundancy. Designing controls and barriers is typically more cost effective than adding redundancy, especially in launch vehicles where the additional mass increases overall performance requirements on other components, driving the overall system cost higher. Hazards can also be controlled by reducing exposure to hazardous environments and adding containment devices. At the lowest level, if hazards cannot be eliminated, reduced, or controlled, efforts must be made to reduce the damage or losses from accidents [60].

### 3.3.2 STAMP Model of the Design Process

A generalized model of engineering design is developed here to show how design & specification errors can enter and propagate within a system. The lowest-level design process is composed of a designer, analysis or test, and the design itself (Figure 6). In this model, the designer is a single human or group of humans.

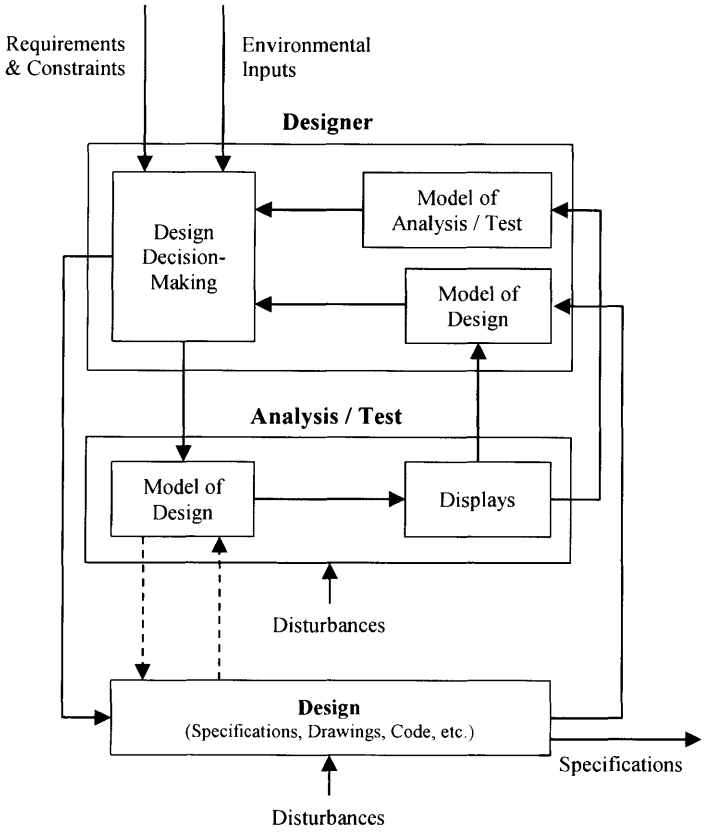



*Figure 6. Generalized Component Design Structure.*

The basic components of the design process are the same as in general controller operation: control inputs and other relevant external information sources, control algorithms, and process models. The designer has mental models of the design and analysis/test process, and uses these models to make design decisions. The design decisions are input into the design and analysis/test until design requirements and constraints are satisfied. Disturbances can enter the design, analysis, and test processes. The context and environment of human controllers is also an important factor. The environment in which engineers operate, the procedures they use, the control loops in which they operate, the processes they control, and the training they receive are all key parts of preventing errors in engineering design by controlling the designers' mental models [1].

Each of the elements in the design control loop can be examined to identify where inadequate design can occur. As with any control structure, an accident occurs because either safety constraints are not enforced or appropriate control actions are provided but not followed (Figure 7).

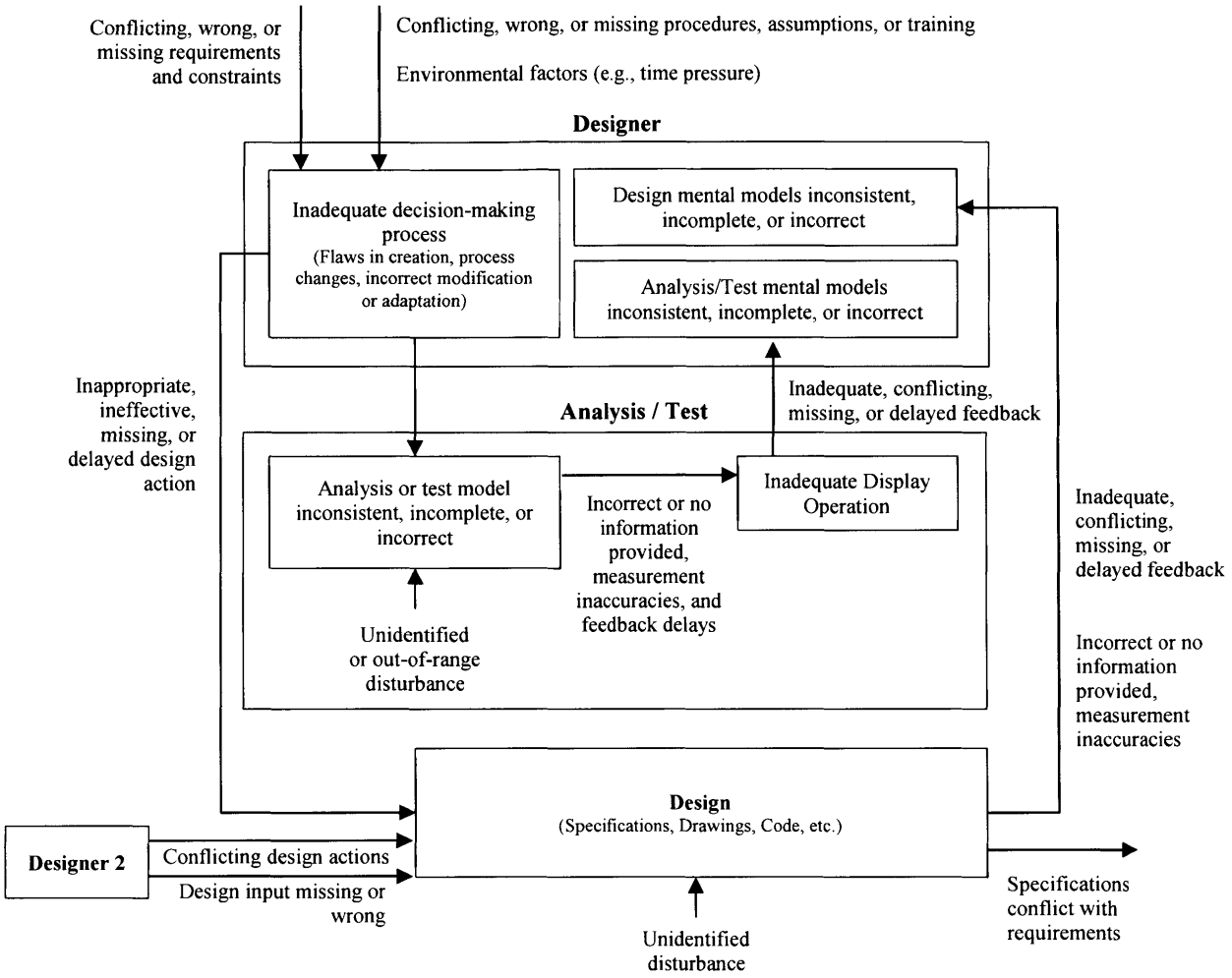



*Figure 7. Design process flaws leading to hazards.*

This model can be used as a guide while conducting hazard analyses of design processes or to help identify sources of design errors in organizations. Designers have multiple process models to maintain: mental models of the design, as well as mental models of any supporting analysis and testing. The engineering organization and systems engineering process should support designers in maintaining these models. When design and analysis are intertwined, as in modern model-based systems engineering, designers should have feedback to ensure that information passed between automated design and test activities is not inadequate, conflicting, missing, or delayed. Connections between analysis/test and design should be made traceable and obvious.

Furthermore, coordination between designers is key to ensuring safe design. Inconsistency between process models can lead to hazardous design decisions. Careful design of communication channels is required in any organization designing safety-critical systems such as space launch vehicles. A more comprehensive set of safety-guided design recommendations can be found in [1].

# 4 DESIGN OF A LAUNCH VEHICLE

This section demonstrates the use of the STPA in the design of a small-lift launch vehicle that is part of a commercial small satellite launch service.

## 4.1 STAKEHOLDER ANALYSIS

At the outset of the conceptual design phase, only high-level goals, accidents, hazards, and constraints can be identified. First, the goals of the system are chosen by stakeholders. For the purposes of this example vehicle, the stakeholder-defined goal(s) are:

- **G1.** Transport small satellite payloads to low earth orbit reliably, affordably, and frequently
- **G2.** Ensure the protection of the public, property, and the national security and foreign policy interests of the United States
- **G3.** Provide the value and capital required to sustain and grow the company

The goals of customers, company, investors, and government regulators should be included in one or more of these system-level goals. Often, these goals are defined by the project charter or set in law in the development of public launch vehicles, such as the Space Launch System or Space Transportation System. Before safety analysis begins, the accidents or mishaps of primary importance to these stakeholders should be identified and ranked. For this launch vehicle, the set of system-level losses, $\mathcal{A}$, to be avoided are:

- **A1.** Loss of life or injury to people
- **A2.** Loss of or damage to public property
- **A3.** Loss of mission
- **A4.** Loss of or damage to launch facilities
- **A5.** Loss of capital (beyond loss-of-mission)

Although the goals and accidents are relatively trivial at this stage, it is important to state them explicitly to promote completeness and establish traceability. In systems where the business context is important, business strategic goals and losses can be defined and analyzed alongside engineering safety.

## 4.2 CONCEPTUAL DESIGN

Once goals and accidents are defined, conceptual designs of the system are created and their high-level hazards compared to aid the selection of the concept of operations. Expendable ground launch, expendable air launch, and reusable ground launch concepts are evaluated. Each of these concepts has a functional control structure that can be analyzed directly with STPA. Each generally has four operating phases: prelaunch, launch, orbit, and reentry. For each of these operability phases of the launch process, the corresponding control structure can be drawn to generate generic classes of hazards that are associated with each concept. In the launch phase, the three concepts have the same generic control structure (Figure 8).

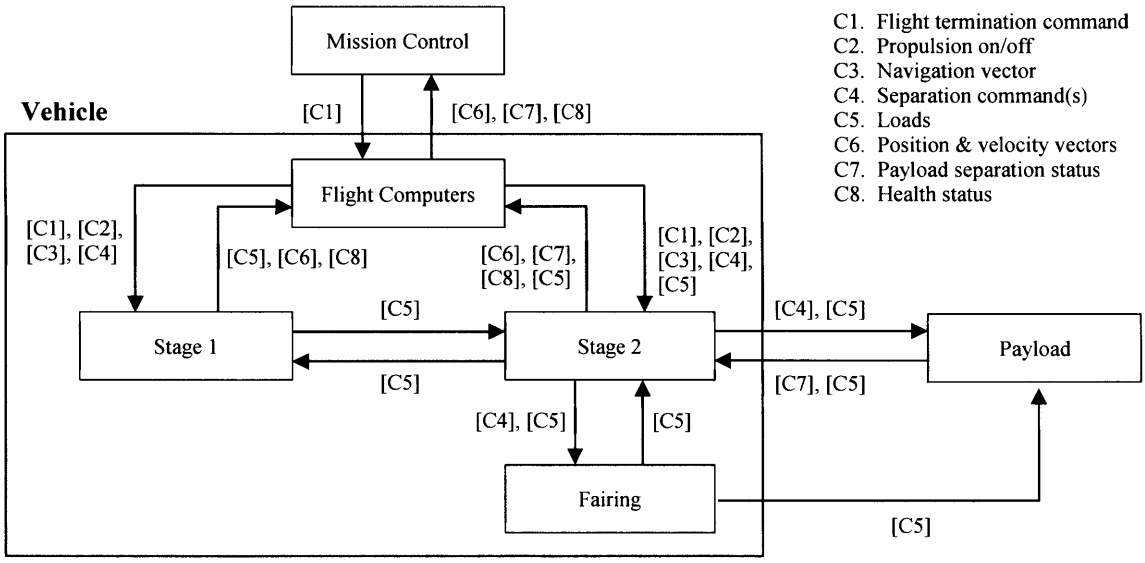



*Figure 8. Safety control structure for the launch vehicle concepts during the launch phase.*

During the pre-launch, orbit, and reentry phases the control structures are different for each of the three concepts. The preliminary control structures for each phase can be drawn and compared against each other to generate hazards and draw insights into the safety of each system. An example control structure for an expendable air launch system is shown in Figure 9.

**EXPENDABLE AIR LAUNCH – *Pre-Launch Phase***

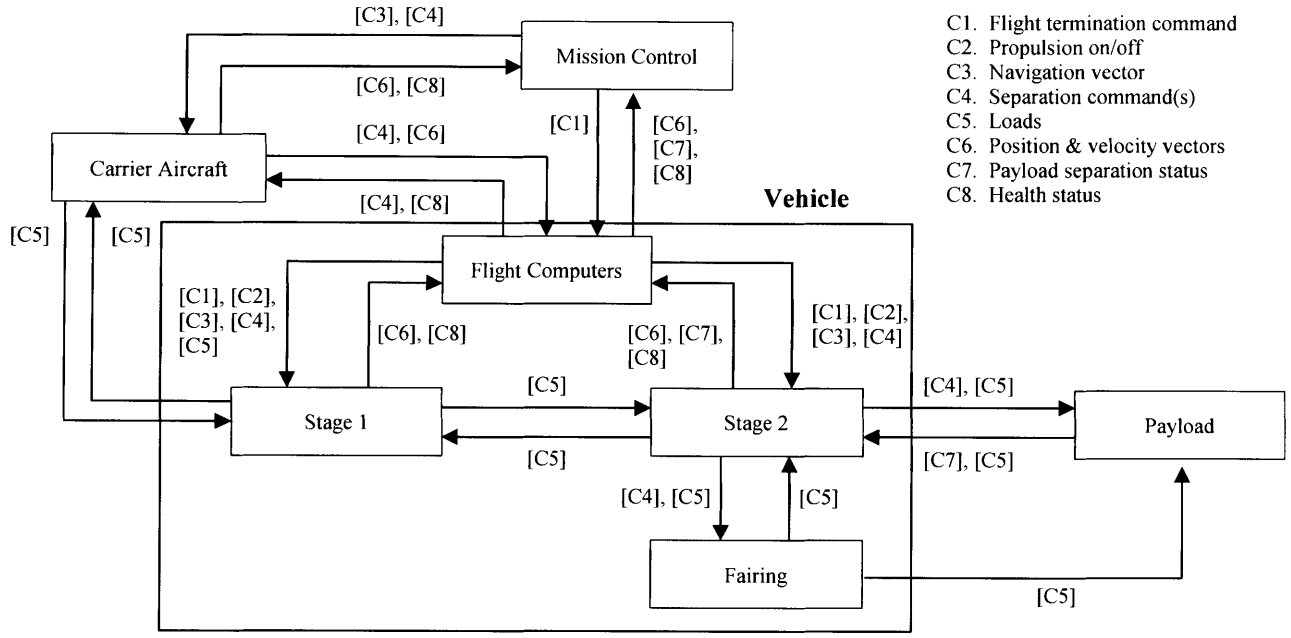



*Figure 9. Safety control structure for an expendable air launch vehicle during pre-launch.*

A formal model of each system, such as the one in Figure 9, allows engineering teams to explicitly state assumptions as conceptual designs are considered. This facilitates constructive critique and gives insights into the goals and hazards of the system before any formal analysis takes place. As conceptual control structures are refined, high-level hazards can be generated based on experience and insights from the exercise. The set of system-level hazards common to each concept are:

- **H1.** Payload damaged during pre-launch or launch [A3]
- **H2.** Vehicle structural integrity is lost [A1, A2, A3, A4, A5]
- **H3.** Vehicle leaves designated flight corridor [A1, A2, A3, A4, A5]
- **H4.** Loss of vehicle control within flight corridor [A1, A2, A3, A4, A5]
- **H5.** Payload inserted into the wrong orbit [A2, A3, A5]
- **H6.** Incorrect or missing separation event [A1, A2, A3]
- **H7.** Uncontrolled release of thermal energy or non-structural material [A1, A2, A3, A4, A5]
- **H8.** Vehicle unable to launch when scheduled [A5]

*Payload damaged during pre-launch or launch* (H1) refers to any change to the physical condition of the payload that negatively effects its performance. Hazards H2, H3, H4, and H7 are all dangerous conditions that can cause every system-level accident. Although these hazards could occur without an accident, (e.g., the vehicle could leave and reenter the flight corridor), these are still dangerous conditions

that should be controlled by design. *Payload inserted into the wrong orbit* (H5) includes orbits that are recoverable by payload propulsion, but which causes a lifetime, availability, or other performance loss. *Incorrect or missing separation event* (H6) includes separation of ground support equipment upon liftoff, stage separation, and payload separation. *Vehicle unable to launch when scheduled* (H8) includes any unplanned delay that may result in a loss of capital to customers, the launch provider, or other stakeholders. Each hazard is linked to the corresponding high-level accident for traceability.

As unsafe control actions and requirements are generated in STPA, they will be linked to the hazards to ensure each safety requirement and constraint is linked to system goals. To aid the selection of concepts, a preliminary hazard assessment can be made to estimate of the ability to eliminate or control each hazard. The likelihood of each hazard is unknown at this point, but the severity and ability to mitigate each hazard with respect to each loss can be compared. There is no formal way to estimate likelihood accurately this early in the design process, as virtually no design information is available, and psychological research has shown that humans are bad at estimating the likelihood of unusual events [61]. However, mitigation potential can be assessed, as the possibility for introducing future design features to mitigate, prevent, or control hazards is often known. Mitigatability is thus chosen instead of likelihood for the preliminary hazard assessment. The scales used to assess severity and mitigatability of launch vehicle concepts are shown in Table 11 and Table 12.

*Table 11. Severity scale used for preliminary hazard analysis*

| Severity | Human (A1) | Mission (A3) | Property (A2, A4, A5) |
|---|---|---|---|
| **16** | Loss of life | Complete mission loss | >200% project cost or schedule lost |
| **9** | Severe injury or illness | Primary mission objectives incomplete | >100% project cost or schedule lost |
| **4** | Minor injury or illness | Secondary mission objectives incomplete | >50% project cost or schedule lost |
| **1** | Less than minor injury or illness | Tertiary mission objectives incomplete | <50% project cost or schedule lost |

*Table 12. Mitigatability scale used for preliminary hazard analysis*

| Scale | Mitigation Result |
|---|---|
| **1** | Complete elimination of hazard |
| **2** | Ability to prevent hazard |
| **3** | Ability to control hazard |
| **4** | Ability to reduce losses |

The mitigatability scale follows the same safety-guided design priority outlined in 3.3.1. A variant of this scale has also been used to evaluate space mission safety in architectural design [62].

Even though designs may have common hazards, the severity and ability to mitigate may be very different. For example, certain types of hazards, such as unwanted mechanical contact between components, is more easily detected in reused vehicles (which can be inspected after flight) than expendable vehicles (which cannot be inspected after flight).

*Table 13. Severity and mitigatability of losses given identified hazards of the Expendable Ground Launch concept.*

| | **Severity** | | | | | **Mitigatability** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **A1** | **A2** | **A3** | **A4** | **A5** | **A1** | **A2** | **A3** | **A4** | **A5** |
| **H1** | -- | -- | 16 | -- | -- | -- | -- | 2 | -- | -- |
| **H2** | 4 | 4 | 16 | 9 | 4 | 2 | 2 | 3 | 2 | 2 |
| **H3** | 16 | 16 | 16 | 9 | 4 | 2 | 2 | 2 | 2 | 2 |
| **H4** | 1 | 4 | 16 | 9 | 4 | 1 | 2 | 2 | 2 | 2 |
| **H5** | -- | 1 | 9 | -- | 1 | -- | 2 | 4 | -- | 4 |
| **H6** | 1 | 1 | 16 | 1 | -- | 1 | 1 | 2 | 2 | -- |
| **H7** | 16 | 16 | 16 | 16 | 9 | 1 | 1 | 4 | 2 | 3 |
| **H8** | -- | -- | -- | -- | 1 | -- | -- | -- | -- | 2 |

Table 13 shows the severity, $\mathcal{S}$, and mitigatability, $\mathcal{M}$, of each high-level hazard associated with the expendable ground launch concept with respect to the losses that could occur. *Vehicle leaves flight corridor* (H3) has particularly high severity but also high mitigatability, as range tracking and flight termination systems are extremely mature and reliable. The tables for the air launch and reusable ground launch concepts are shown in Table 14 and Table 15, respectively.

*Table 14. Severity and mitigatability of losses given identified hazards of the Expendable Air Launch concept.*

| | Severity | | | | | Mitigatability | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **A1** | **A2** | **A3** | **A4** | **A5** | **A1** | **A2** | **A3** | **A4** | **A5** |
| **H1** | -- | -- | 16 | -- | -- | -- | -- | 2 | -- | -- |
| **H2** | 16 | 4 | 16 | 9 | 4 | 2 | 2 | 3 | 3 | 2 |
| **H3** | 16 | 16 | 16 | 9 | 4 | 2 | 2 | 2 | 2 | 2 |
| **H4** | 1 | 4 | 16 | 9 | 4 | 1 | 2 | 2 | 2 | 2 |
| **H5** | -- | 1 | 9 | -- | 1 | -- | 2 | 4 | -- | 4 |
| **H6** | 16 | 1 | 16 | 16 | -- | 2 | 1 | 2 | 4 | -- |
| **H7** | 16 | 16 | 16 | 16 | 9 | 3 | 1 | 4 | 2 | 3 |
| **H8** | -- | -- | -- | -- | 1 | -- | -- | -- | -- | 2 |

*Table 15. Severity and mitigatability of losses given identified hazards of the Reusable Ground Launch concept.*

| | Severity | | | | | Mitigatability | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **A1** | **A2** | **A3** | **A4** | **A5** | **A1** | **A2** | **A3** | **A4** | **A5** |
| **H1** | -- | -- | 16 | -- | -- | -- | -- | 2 | -- | -- |
| **H2** | 4 | 4 | 16 | 9 | 4 | 2 | 2 | 3 | 3 | 2 |
| **H3** | 16 | 16 | 16 | 16 | 4 | 2 | 2 | 2 | 2 | 2 |
| **H4** | 1 | 4 | 16 | 16 | 4 | 1 | 2 | 2 | 3 | 2 |
| **H5** | -- | 1 | 9 | -- | 1 | -- | 2 | 4 | -- | 4 |
| **H6** | 1 | 1 | 16 | 1 | -- | 1 | 1 | 2 | 2 | -- |
| **H7** | 16 | 16 | 16 | 16 | 9 | 1 | 1 | 4 | 3 | 3 |
| **H8** | -- | -- | -- | -- | 1 | -- | -- | -- | -- | 2 |

By these metrics, the severity of *loss of life or injury to people* (A1) is highest for air launch. Naturally, there will be differences in opinion over the severity and mitigatability of each hazard. Differences in opinion reveal assumptions about the execution of each concept, such as whether structural hazards on reusable vehicles are inherently more mitigatable because data can presumably be gathered from multiple flights. The level of hazard mitigation assumed inherent in each design, as an example, will drive the assumed severity of the loss. These assumptions should be documented to inform future analyses and design decisions.

**AA1.** All concepts use two stages with conventional bipropellant liquid propulsion from an existing U.S. range

**AA2.** Air launch vehicles are dropped horizontally from a manned carrier aircraft over the open ocean with a crew escape system

**AA3.** Reusable stages land vertically on land within 10 miles of the launch site

**AA4.** All vehicles use conventional propulsion technologies with equivalent technology readiness

Weighting factors can then be used to create a safety risk metric, Overall Residual Safety-Risk Metric ($ORSRM$), to evaluate each concept:

$$ORSRM = \sum_{i=1}^{N_A} \sum_{j=1}^{N_H} w_i(\mathcal{S}_j + \mathcal{M}_j)$$

Where $N_A$ is the number of accidents to be considered (5), $N_H$ is the number of high-level hazards (8), $w_{A_i}$ is the weight for accident $i$, $\mathcal{S}_j$ is the severity of hazard $j$, and $\mathcal{M}_j$ is the hazard mitigatability. Weighting factors should be chosen based on the relative acceptability of losses from the program stakeholders. Each high-level loss can be grouped by human (A1), mission (A3), resources (A2, A4, A5), or other custom metrics. For the purpose of this analysis, the following weighting factors are used:

*Table 16. Weighting Factors used in calculating ORSRM.*

| Accident | Weight ($w_i$) |
|---|---|
| Human (A1) | 10 |
| Mission (A3) | 5 |
| Resources (A2, A4, A5) | 1 |

The corresponding $ORSRM$ values for each concept are:

*Table 17. Concept ORSRM values.*

| Concept | $ORSRM$ |
|---|---|
| Expendable Ground Launch | 1241 |
| Expendable Air Launch | 1532 |
| Reusable Ground Launch | 1231 |

The expendable air launch concept has a higher $ORSRM$ primarily due to the increased severity of hazards to the carrier aircraft. For the purpose of the following sections, the expendable ground-launch concept is chosen.

## 4.3 REQUIREMENTS & CONSTRAINTS

A set of high-level safety constraints can be generated by restating these hazards as constraints. Two general classes of constraints are used: inverted conditions and conditional statements. Inverted conditions simply state that a condition must be enforced, and have the form <System> & <Condition to Enforce>. Conditional statements define how the system must prevent or minimize losses in case the hazard does occur. They have the form if <hazards> occurs, then <what needs to be done to prevent or minimize a loss>.

- **SC1.** Payload must not be damaged under worst-case pre-launch, launch, and orbit environments [H1]
- **SC2.** Vehicle must maintain structural integrity under worst-case pre-launch, launch, and orbit conditions [H2]
- **SC3.** Vehicle must not exit flight corridor [H3]
- **SC4.** If vehicle approaches flight corridor limits, then the violation must be detected and measures taken to prevent loss of life or injury to people [H3]
- **SC5.** Flight path control shall be maintained during launch and orbit [H4]
- **SC6.** The payload shall be injected into the intended orbit within TBD tolerance [H5]
- **SC7.** Uncommanded separation events shall not occur [H6]
- **SC8.** Separation events must occur within TBD seconds of command [H6]
- **SC9.** Uncontrolled vehicle energy or material release must not cause injury or death to public persons [H3, H7]
- **SC10.** Toxic, corrosive, and energetic materials must not be released within range of humans or other systems [H7]
- **SC11.** Vehicle structural integrity must be maintained under worst-case conditions [H2]

Some of these constraints can be stated in the positive as "shall" requirements that can be tested and verified, whereas others must be stated in the negative as "must not" constraints. For the purpose of this exercise, all safety requirements and constraints are written as constraints so that multiple naming conventions are not required.

Additional safety constraints are created as part of the first part of STPA in the architectural and design phases. These safety constraints are informed by the unsafe control actions that can be provided by vehicle elements and the specific scenarios that could lead to unsafe control actions.

### 4.3.1 Refined Hazards

Hazards can be further refined to assist downstream analyses. The refined hazards associated with the launch vehicle are:

- **H1.** Payload damaged during pre-launch or launch [A3]
  - **H1.1.** Payload environment standards (cleanliness, ESD/EMI/EMC, radiation, temperature, pressures, loads) are not maintained
  - **H1.2.** Incorrect application of electrical signal or power applied to the payload during ground processing or launch
  - **H1.3.** Toxic, corrosive, or energetic materials contact payload
  - **H1.4.** Payload contacts fairing, other payloads, or itself during launch
  - **H1.5.** Premature actuation of payload elements
- **H2.** Vehicle structural integrity is lost [A1, A2, A3, A4, A5]
  - **H2.1.** Insufficient strength provided by vehicle structural elements
  - **H2.2.** Thrust too high or asymmetric during launch
  - **H2.3.** Aerodynamic pressure too high or asymmetric during launch
- **H3.** Vehicle leaves designated flight corridor [A1, A2, A3, A4, A5]
  - **H3.1.** Thrust continues to be applied as vehicle approaches flight corridor boundary
  - **H3.2.** Asymmetric thrust maneuvers vehicle toward flight corridor boundary
  - **H3.3.** Insufficient steering to turn vehicle away from flight corridor boundary
  - **H3.4.** Steering maneuvers vehicle out of flight corridor
  - **H3.5.** Launch vehicle, launch vehicle debris, payload, or payload debris impacts land outside flight corridor
- **H4.** Loss of vehicle control within flight corridor [A1, A2, A3, A4, A5]
  - **H4.1.** Forces required to maintain flight path are not provided during launch
  - **H4.2.** Thrust is insufficient during takeoff or launch
  - **H4.3.** Thrust is provided during pre-launch
  - **H4.4.** Propulsion components operate outside of intended operating conditions
  - **H4.5.** Insufficient or missing communication with ground elements
- **H5.** Payload inserted into the wrong orbit [A1, A2, A3, A4]
  - **H5.1.** Missing or incorrect payload separation command is provided
  - **H5.2.** Minimum separation between vehicle and payload(s) is not maintained
- **H6.** Incorrect or missing separation event [A3]
  - **H6.1.** Insufficient mechanical contact between separation elements is not provided
  - **H6.2.** Initiating energy is provided to separation mechanism prior to intended separation

**H6.3.** Release velocity is insufficient during separation

**H7.** Uncontrolled release of thermal energy or non-structural material [A1, A2, A3, A4]

**H7.1.** Separation of reactive and energetic materials is not maintained

**H7.2.** Insufficient containment of toxic, corrosive, or energetic materials during pre-launch, launch, or orbit

**H7.3.** Minimum separation distance between moving and stationary components is not maintained

**H7.4.** Feed system cleanliness not maintained

**H7.5.** Damage to the environment

**H8.** Vehicle unable to launch when scheduled [A5]

**H8.1.** Day-of-flight operational parameters exceed operational envelope

**H8.2.** Incorrect or missing payload requirements

## 4.4 System Architecture

The goal of system architecture is to map functional requirements to formal elements. Propellants, engines, pressurization system type, and other high-level design decisions are made at this stage by laying out the options for each primary vehicle function and estimating the performance benefit and cost of each valid permutation of the options. The architectural decisions for the expendable ground-launch concept are shown in Table 18.

*Table 18. Vehicle architectural decisions.*

| ID | Parameter | Option A | Option B | Option C | Option D | Option E | Option F |
|---|---|---|---|---|---|---|---|
| **AD1** | Stage 1 fuel | RP-1 | Hydrogen | Methane | HTPB | Hydrazine | -- |
| **AD2** | Stage 1 oxidizer | LOx | $N_2O_4$ | AP | -- | -- | -- |
| **AD3** | Stage 2 fuel | RP-1 | Hydrogen | Methane | HTPB | Hydrazine | -- |
| **AD4** | Stage 2 oxidizer | LOx | $N_2O_4$ | AP | -- | -- | -- |
| **AD5** | Stage 1 engine cycle | Gas Generator | Staged Combustion | Open Expander | Closed Expander | Tapoff | Electric |
| **AD6** | Stage 2 engine cycle | Gas Generator | Staged Combustion | Open Expander | Closed Expander | Tapoff | Electric |
| **AD7** | Stage 1 pressurization | $N_2$ | He | Autogenous | Self-pressurizing | -- | -- |
| **AD8** | Stage 2 pressurization | $N_2$ | He | Autogenous | Self-pressurizing | -- | -- |
| **AD9** | Payload capacity to BRM | 100 kg | 200 kg | 300 kg | 500 kg | 1000 kg | 2000 kg |
| **AD10** | Primary Structure Material | Al-Li | Carbon Composite | -- | -- | -- | -- |

With this matrix of decisions, a performance model can be created to evaluate the architectures corresponding to each valid combination of decisions. This model sizes the vehicle and estimates the cost, technical risk, and performance of each option to aid selection. The designer can then use the resulting data to select the most desirable architecture. Performance metrics are usually plotted on a two-dimensional tradespace, where the independent variable axis is a cost metric and the dependent variable axis is a performance metric. An example is given in Figure 10.

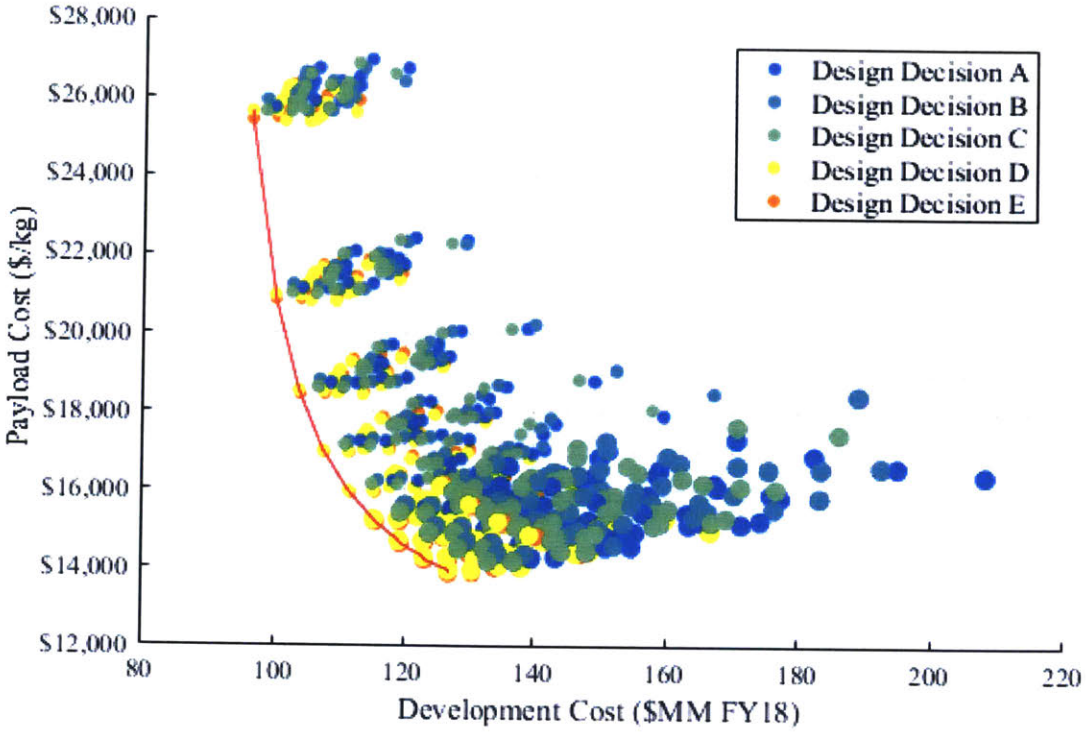



*Figure 10. Example tradespace plot for a launch vehicle. The red line represents the Pareto frontier.*

Although this method allows the designer to select optimal performance for a given cost, safety and other emergent properties cannot be enumerated in any meaningful way in this tradespace. A method such as STPA must be used to identify architecture-specific hazards and give the designer a sense of the impact of architectural decisions on system safety. Many of the architectural decisions in Table 18 are also decisions about the nature of the safety control structure. The control structure of each architecture can be drawn to facilitate a preliminary hazard analysis using STPA. Examples of the control structures for some of the architectures are shown in Figure 11 and Figure 12.

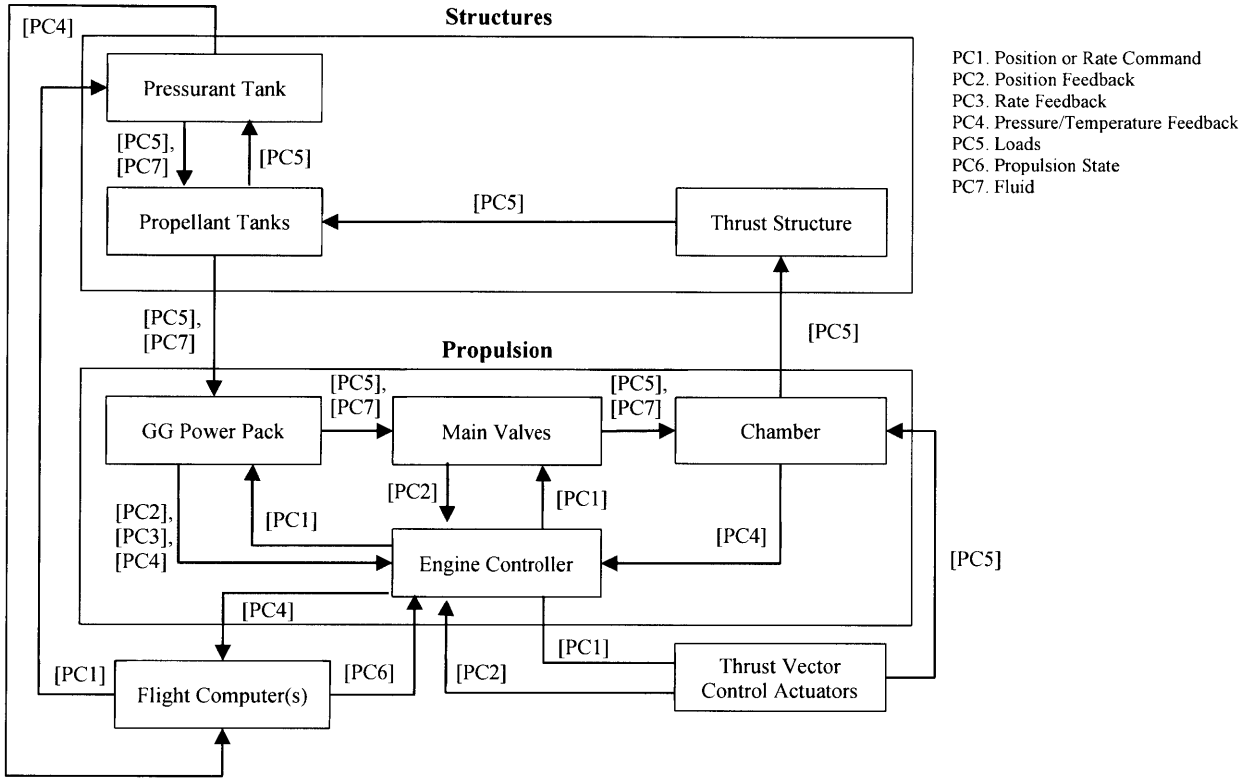



*Figure 11. Safety control structure for a liquid propulsion stage using a gas generator and helium pressurization system.*

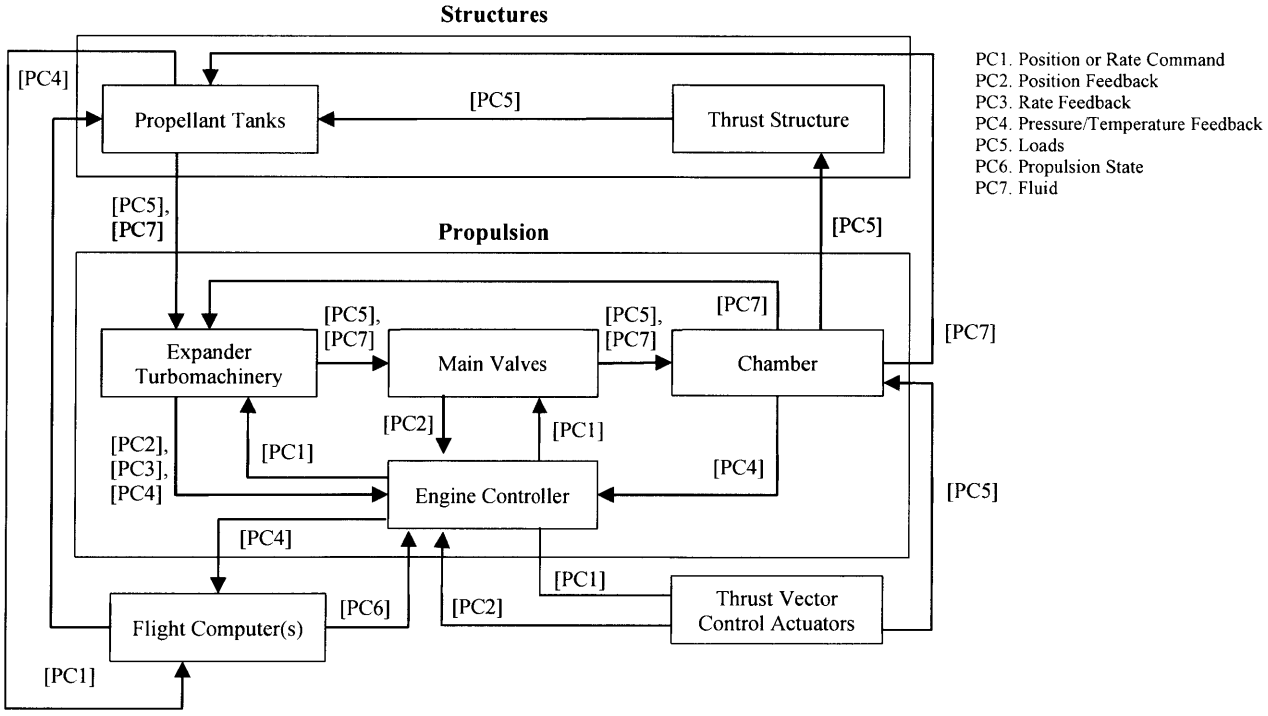



*Figure 12. Safety control structure for a liquid propulsion stage with an expander cycle and autogenous pressurization.*

STPA can then be used to evaluate the safety of each architecture under consideration. The unsafe control actions of each of the two architectures shown in Figure 11 and Figure 12 are very different, even though both are expendable ground launch vehicles with liquid propulsion systems. This early safety analysis gives the designer an idea of the safety constraints and potential influence of architectural decisions on safety. As an example, the safety constraints for the expander cycle (especially those constraints that concern errors in the engine controller process model), may be easier to control due to the thermodynamic coupling of chamber cooling performance to turbomachinery performance and the absence of an additional combustion device. However, an expander cycle may require a spin start system to start the cycle and is sensitive to the performance of the chamber cooling channels. STPA gives the designer a structured way to evaluate the safety constraints and requirements of each architecture under consideration, and thus allows the designer to select the architecture that best meets stakeholder objectives.

## 4.5 System Design

STPA is equally well equipped for detailed analysis of subsystems. Two critical subsystems, a flight termination system (FTS) and the second stage propulsion system are chosen for further analysis to demonstrate the use of STPA.

### 4.5.1 Flight Safety System

#### *4.5.1.1 System Definition*

The flight safety system (FSS) is a range safety tool used to mitigate losses in the event the vehicle strays off course or experiences a mechanical failure that could result in loss greater than complete termination of the flight. An FSS consists of a flight termination system, a method to track the vehicle, and a method to receive status data from the vehicle.

When the vehicle approaches the flight corridor, the deviation is detected and the FTS terminates the flight of the vehicle. The FSS may also contain a method to input commands to the flight control system to place the vehicle into recovery mode. The flight safety system consists of passive antennas, one or more receivers, independent and redundant power, a safe-and-arm device (SAD), and a decision-making unit. The decision-making unit interfaces with batteries, the receiver, the umbilical, onboard telemetry, and SAD.

#### *4.5.1.2 Losses & Hazards*

The losses and hazards are picked directly from the vehicle system losses and hazards. The vehicle-level losses the FSS is designed to prevent are:

**A1.** Loss of life or injury to people

**A2.** Loss of or damage to public property

**A4.** Loss of or damage to launch facilities

The corresponding vehicle-level hazards for the FSS are:

**H3.** Vehicle leaves designated flight corridor [A1, A2, A3, A4, A5]

**H7.** Uncontrolled release of thermal energy or non-structural material [A1, A2, A3, A4, A5]

To prevent these hazards, the vehicle must satisfy the following constraints:

**SC3.** Vehicle must not exit flight corridor [H3]

**SC9.** Uncontrolled vehicle energy or material release must not cause injury or death to public persons [H3, H7]

**SC10.** Toxic, corrosive, and energetic materials must not be released within range of humans or other systems [H7]

#### *4.5.1.3 Safety Control Structure*

The control structure of the flight safety system and flight termination system within the context of the vehicle is shown in Figure 13.

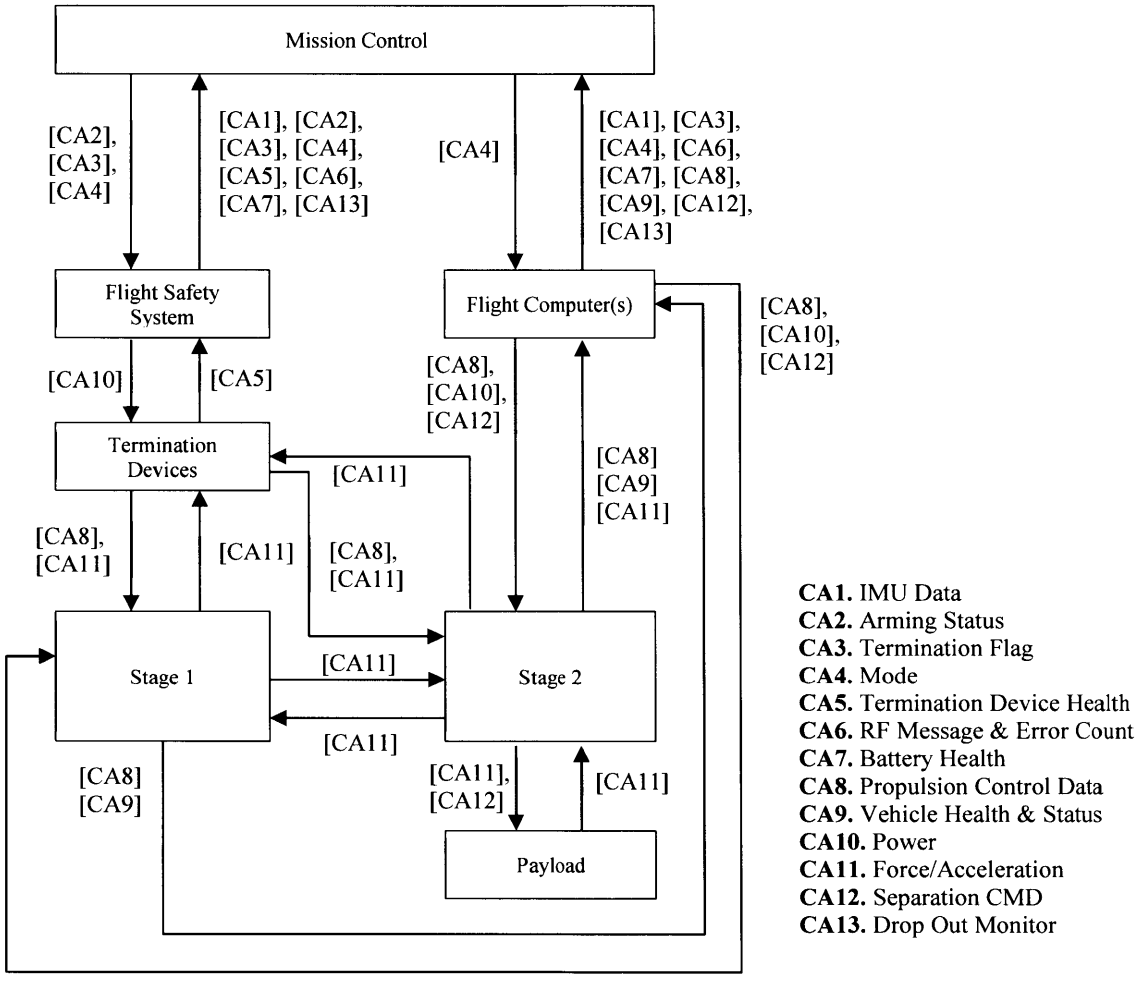



*Figure 13. Safety Control Structure of the Flight Safety System in the vehicle.*

#### *4.5.1.4 Unsafe Control Actions (STPA Step 1)*

Unsafe control actions can be derived directly from the control structure. For brevity, Table 19 shows a subset of the unsafe control actions that could be provided in the system.

*Table 19. Flight Safety System UCA context table.*

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Safety System | FSS provides power to termination devices [CA10] | **UCA1:** FSS does not provide power to termination devices when termination flag is active and SAD is armed [H3] [H7]<br><br>**UCA2:** FSS does not provide power to termination devices when vehicle approaches flight corridor boundary during launch [H3]<br><br>**UCA3:** FSS does not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy during launch [H7] | **UCA4:** FSS provides power to termination devices when termination flag is not active [H7]<br><br>**UCA5:** FSS provides power to termination devices when SAD is unarmed or safed [H7]<br><br>**UCA6:** FSS provides power to termination devices when in test mode [H7]<br><br>**UCA7:** FSS provides power to termination devices when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [H7]<br><br>**UCA8:** FSS provides power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [H3] [H7] | **UCA9:** FSS provides power to termination devices out of order [H3] [H7]<br><br>**UCA10:** FSS provides power to termination devices too late (< TBD seconds from receipt of termination flag) [H3] [H7] | **UCA11:** FSS stops providing power to termination devices before termination is complete [H3] [H7] |
| Mission Control | Mission Control provides arming status to FSS [CA2] | **UCA12:** Mission control does not provide arm command to FSS during launch [H3]<br><br>**UCA13:** Mission control does not provide safe command to FSS during ground operations and test prior to liftoff [H7] | **UCA14:** Mission control provides arm command during ground operations and test prior to liftoff [H7]<br><br>**UCA15:** Mission control provides safe command to FSS during launch [H3] | N/A | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Mission Control | Mission control provides termination flag to FSS [CA3] | **UCA16:** Mission control does not provide termination flag to FSS when vehicle approaches flight corridor boundary [H3]<br><br>**UCA17:** Mission control does not provide termination flag to FSS when vehicle experiences catastrophic uncontrolled release of energy [H7] | **UCA18:** Mission control provides termination flag to FSS when resulting debris and energy may contact humans, public property, or launch facility [H7]<br><br>**UCA19:** Mission control provides termination flag to FSS when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [H7] | **UCA20:** Mission control provides termination flag to FSS during mission control testing with live termination mechanisms [H7]<br><br>**UCA21:** Mission control provides termination flag to FSS in orbit [H7]<br><br>**UCA22:** Mission control provides termination flag to FSS before fill/drain operations of energetic material has begun [H7] | **UCA23:** Mission control stops providing termination flag to FSS before termination flag received [H7] |
| Mission Control | Mission control provides active mode or flight mode command to FSS [CA4] | **UCA24:** Mission control does not provide active mode to FSS during terminal counts [H3] | **UCA25:** Mission control provides active mode to FSS during ground operations and test [H7]<br><br>**UCA26:** Mission control provides non-External Power mode command to FSS during ground operations and test [H7] | **UCA27:** Mission control provides active mode to FSS before terminal count [H7] | **UCA28:** Mission control stops providing mode to FSS during launch [H7] |
| Stage 1 | Stage 1 provides force/acceleration to FSS [CA11] | **UCA29:** Stage 1 does not provide TBD acceleration to FSS during liftoff [H7] | **UCA30:** Stage 1 provides >TBD quasi-static acceleration to FSS during launch [H7] [H3]<br><br>**UCA31:** Stage 1 provides excessive (TBD) dynamic or shock acceleration to FSS during launch [H7] [H3] | **UCA32:** Stage 1 provides TBD acceleration to FSS prior to liftoff [H7] [H3]<br><br>**UCA33:** Stage 1 provides excessive force (blast, debris, etc.) to FSS before termination [H7] | **UCA34:** Stage 1 provides excessive force (blast, debris, etc.) to FSS during termination [H7] [H3] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Safety System | FSS provides Mode to Mission Control [CA4] | **UCA35:** FSS does not provide Mode to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8]<br><br>**UCA36:** FSS does not provide Mode to Mission Control before FSS is disabled [H7] [H3] | **UCA37:** FSS provides incorrect or delayed Mode to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8] | **UCA38:** N/A | **UCA39:** N/A |

The corresponding safety constraints for the first eleven unsafe control actions are shown in Table 20. This table corresponds to the contexts under which the FSS providing power to the termination devices can lead to a hazard.

*Table 20. Unsafe Control Actions for FSS provides power to termination devices [CA10]*

| Unsafe Control Actions | Safety Constraints |
|---|---|
| **UCA1**: FSS does not provide power to termination devices when termination flag is active and SAD is armed [H3] [H7] | **SC1:** FSS must provide power to termination devices when termination flag is active and SAD is armed |
| **UCA2:** FSS does not provide power to termination devices when vehicle approaches flight corridor boundary during launch [H3] | **SC2:** FSS must provide power to termination devices when vehicle approaches flight corridor boundary during launch |
| **UCA3:** FSS does not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy during launch [H7] | **SC3:** FSS must provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy during launch |
| **UCA4:** FSS provides power to termination devices when termination flag is not active [H7] | **SC4:** FSS must not provide power to termination devices when termination flag is not active |
| **UCA5:** FSS provides power to termination devices when SAD is unarmed or safed [H7] | **SC5:** FSS must not provide power to termination devices when SAD is unarmed or safed |
| **UCA6:** FSS provides power to termination devices when in test mode [H7] | **SC6:** FSS must not provide power to termination devices when in test mode |
| **UCA7:** FSS provides power to termination devices when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [H7] | **SC7:** FSS must not provide power to termination devices when vehicle is within flight corridor and is not releasing or about to release uncontrolled energy |
| **UCA8:** FSS provides power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [H3] [H7] | **SC8:** FSS must not provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility |
| **UCA9:** FSS provides power to termination devices out of order [H3] [H7] | **SC9:** FSS must not provide power to termination devices out of order |
| **UCA10:** FSS provides power to termination devices too late (< TBD seconds from receipt of termination flag) [H3] [H7] | **SC10:** FSS must not provide power to termination devices too late (< TBD seconds from receipt of termination flag) |
| **UCA11:** FSS stops providing power to termination devices before termination is complete [H3] [H7] | **SC11:** FSS must not stop providing power to termination devices before termination is complete |

#### *4.5.1.5 Causal Scenarios (STPA Step 2)*

More useful design information can be gathered by considering the causal scenarios that could lead to an unsafe control action. Unsafe control actions can be caused by unsafe controller behavior and inadequate feedback and other inputs. Some of the causal scenarios that could lead to the first eleven unsafe control actions for the flight safety system follow.

**UCA1:** FSS does not provide power to termination devices when termination flag is active and SAD is armed

Scenario 1 for UCA1: Physical mechanism(s) in the FSS or power supply fail(s) due to mechanical or thermal environment, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA1: The FSS provides intermittent power, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA1: The FSS provides insufficient or excessive power, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. Insufficient or excessive power may be provided because power draw exceeds the design specifications of the power supply, or the design specifications of the power supply do not meet the power supply performance. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA1: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. A wrong connection may be caused by incorrect specifications or the belief that the connect is correct by design or integration personnel As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 5 for UCA1: A single-event effect causes the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 6 for UCA1: Foreign object debris, dust, or other physical contaminant causes the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 7 for UCA1: FSS does not switch on internal power prior to takeoff, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 8 for UCA1: FSS never enters an active state, causing the FSS to not provide power to termination devices when termination flag is active and SAD is armed [UCA1]. The FSS may not switch to an active state due to incorrect state criteria, incorrect software configuration, or erroneous input. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

**UCA2:** FSS does not provide power to termination devices when vehicle approaches flight corridor boundary

Scenario 1 for UCA2: Physical mechanism(s) in the FSS or power supply fail(s) due to mechanical or thermal environment, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA2: The FSS provides intermittent power, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA2: The FSS provides insufficient or excessive power, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. Insufficient or excessive power may be provided because power draw exceeds the design specifications of the power supply, or the design specifications of the power supply do not meet the power supply performance. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA2: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 5 for UCA2: A single-event effect causes the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 6 for UCA2: Foreign object debris, dust, or other physical contaminant causes the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 7 for UCA2: IMU measurement inaccuracy or delays misinform vehicle position, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA1]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 8 for UCA2: FSS does not switch on internal power prior to takeoff, causing the FSS to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 9 for UCA2: FSS never enters an active state, causing the FSS to not provide power to not provide power to termination devices when vehicle approaches flight corridor boundary [UCA2]. The FSS may not switch to an active state due to incorrect state criteria, incorrect software

configuration, or erroneous input. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

**UCA3:** FSS does not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy

Scenario 1 for UCA3: Physical mechanism(s) in the FSS or power supply fail(s) due to mechanical or thermal environment, causing the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA3: The FSS provides intermittent power, causing the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA3: The FSS provides insufficient or excessive power, causing the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. Insufficient or excessive power may be provided because power draw exceeds the design specifications of the power supply, or the design specifications of the power supply do not meet the power supply performance. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA3: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 5 for UCA3: A single-event effect causes the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 6 for UCA3: Delay in sensing impending catastrophic uncontrolled release of energy, translation of sensor data into termination flag, and processing of termination flag by FSS causes FSS to not provide power to termination devices when vehicle experiences uncontrolled release of energy [UCA3]. This delay may be caused by excessive execution time or the mechanical response time of the sensor. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 7 for UCA3: Foreign object debris, dust, or other physical contaminant causes the FSS to not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy [UCA3]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 8 for UCA3: Delay in sensing off-nominal conditions and subsequent termination command by the Range Safety Officer causes FSS to not provide power to termination devices when vehicle experiences uncontrolled release of energy [UCA3]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

**UCA4:** FSS provides power to termination devices when termination flag is not active

Scenario 1 for UCA4: Physical mechanism(s) in the FSS or power supply fail(s) due to mechanical or thermal environment, causing the FSS to provide power to termination devices when termination flag is not active [UCA4]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the energy or material may be released uncontrolled [H7].

Scenario 2 for UCA4: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to provide power to termination devices when termination flag is not active [UCA4]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, the energy or material may be released uncontrolled [H7].

Scenario 3 for UCA4: A single-event effect causes the FSS to provide power to termination devices when termination flag is not active [UCA4]. As a result, the energy or material may be released uncontrolled [H7].

Scenario 4 for UCA4: Foreign object debris, dust, or other physical contaminant in the FSS or power supply causes the FSS to provide power to termination devices when termination flag is not active [UCA4]. As a result, the energy or material may be released uncontrolled [H7].

**UCA5:** FSS provides power to termination devices when SAD is unarmed or safed

Scenario 1 for UCA5: Physical mechanism(s) in the FSS or power supply fail(s), causing the FSS to provide power to termination devices when SAD is safed [UCA5]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the energy or material may be released uncontrolled [H7].

Scenario 2 for UCA5: A current path exists between the FSS and the termination devices, causing the FSS to provide power to termination devices when SAD is safed [UCA5]. As a result, the energy or material may be released uncontrolled [H7].

Scenario 3 for UCA5: Foreign object debris, dust, or other physical contaminant in the FSS or power supply causes the FSS to provide power to termination devices when SAD is safed [UCA5]. As a result, the energy or material may be released uncontrolled [H7].

Scenario 4 for UCA5: A single-event effect in the SAD occurs alongside one of the other scenarios, causing the FSS to provide power to termination devices when SAD is safed [UCA5]. As a result, the energy or material may be released uncontrolled [H7].

**UCA6:** FSS provides power to termination devices when in test mode

Scenario 1 for UCA6: SAD is not safed when FSS enters test mode and termination flag is received, causing the FSS to provide power to termination devices when in test mode [UCA6]. SAD may not be safed because the requirement was not communicated to test personnel or test configuration files, SAD appears to be safed but is actually armed, or software configuration is incorrect. As a result, uncontrolled energy or material may be released [H7].

Scenario 2 for UCA6: FSS provides excessive power to armed SAD when in test mode, causing the FSS to provide power to termination devices when in test mode [UCA6]. FSS provides excessive power because the incorrect arming voltage is supplied. As a result, uncontrolled energy or material may be released [H7].

Scenario 3 for UCA6: Foreign object debris, dust, or other undesired physical contaminant causes the FSS to provide power to termination devices when in test mode [UCA6]. As a result, uncontrolled thermal energy may be released [H7].

Scenario 4 for UCA6: A current path exists between the FSS and the termination devices, causing the FSS to provide power to termination devices when in test mode [UCA6]. As a result, uncontrolled thermal energy may be released [H7].

**UCA7:** FSS provides power to termination devices when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy

Scenario 1 for UCA7: Vehicle inertial measurement is missing, delayed or incorrect, causing the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

Scenario 2 for UCA7: Conflicting inertial or sensor data indicates a false situation, causing the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

Scenario 3 for UCA7: Mechanical failure of sensors, communication lines, or power causes the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

Scenario 4 for UCA7: Voting system does not operate properly, causing the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

Scenario 5 for UCA7: Physical mechanism(s) in the FSS or power supply fail(s), causing the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, uncontrolled energy or material may be released [H7].

Scenario 6 for UCA7: Foreign object debris, dust, or other physical contaminant causes the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

Scenario 7 for UCA7: Unclear vehicle state causes the Range Safety Officer to provide a termination flag to the FSS, causing the FSS to provide power to termination devices when the vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]. As a result, uncontrolled energy or material may be released [H7].

**UCA8:** FSS provides power to termination devices when resulting debris and energy may contact humans, public property, or launch facility

Scenario 1 for UCA8: Vehicle inertial measurement is missing, delayed or incorrect, causing the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

Scenario 2 for UCA8: Conflicting inertial data indicates a false situation, causing the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

Scenario 3 for UCA8: Failure in sensors, communication lines, or power causes the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

Scenario 4 for UCA8: Physical mechanism(s) in the FSS or power supply fail(s), causing the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, uncontrolled energy or material may be released [H7].

Scenario 5 for UCA8: Failure in sensors, communication lines, or power causes the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

Scenario 6 for UCA8: Foreign object debris, dust, or other physical contaminant causes the FSS to provide power to termination devices when resulting debris and energy may contact humans, public

property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

Scenario 7 for UCA8: Unclear vehicle state causes the Range Safety Officer to provide a termination flag to the FSS, causing the FSS to provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]. As a result, uncontrolled energy or material may be released [H7].

**UCA9:** FSS provides power to termination devices out of order

Scenario 1 for UCA9: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to provide power to termination devices out of order [UCA9]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA9: One or more termination device(s) do not activate when power applied, causing the FSS to provide power to termination devices out of order [UCA9]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA9: Physical mechanism(s) in the FSS or power supply fail(s) due to environmental loads, causing the FSS to provide power to termination devices out of order [UCA9]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA9: Resistive load or system delays are unanticipated in design, causing the FSS to provide power to termination devices out of order [UCA9]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 5 for UCA9: Termination schedule, if any, is incorrectly specified, causing the FSS to provide power to termination devices out of order [UCA9]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 6 for UCA9: FSS timer(s) are incorrectly set, causing the FSS to provide power to termination devices out of order [UCA9]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

**UCA10:** FSS provides power to termination devices too late (<TBD seconds from receipt of termination flag)

Scenario 1 for UCA10: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA10: One or more termination device(s) do not activate when power applied, causing the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA10: Physical mechanism(s) in the FSS or power supply fail(s) due to environmental loads, causing the FSS to provide power to termination devices too late [UCA10]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., excessive shock environment during stage separation). As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA10: Resistive load or system delays are unanticipated in design, causing the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 5 for UCA10: FSS timer(s) are incorrectly set, causing the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 6 for UCA10: Delays in receiver/decoder cause the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 7 for UCA10: Delays in processing termination flag in termination logic cause the FSS to provide power to termination devices too late [UCA10]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

**UCA11:** FSS stops providing power to termination devices before termination is complete

Scenario 1 for UCA11: The physical connection between the FSS and the termination devices is wrong, broken, or intermittent, causing the FSS to stop providing power to termination devices before termination is complete [UCA11]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 2 for UCA11: FSS power is insufficient, causing the FSS to stop providing power to termination devices before termination is complete [UCA11]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 3 for UCA11: Uncontrolled release of energy or material breaks continuity between FSS elements and the termination devices, causing the FSS to stop providing power to termination devices before termination is complete [UCA11]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

Scenario 4 for UCA11: Energy released by termination devices breaks continuity between FSS power elements and the termination devices, causing the FSS to stop providing power to termination devices before termination is complete [UCA11]. As a result, the vehicle or parts of the vehicle may leave the flight corridor [H3] and energy or material may be released uncontrolled [H7].

#### *4.5.1.6 Design Decisions*

Each of these scenarios can then be evaluated, and design changes can be proposed to eliminate or mitigate hazards. The effectiveness of each can be compared, and steps 1 and 2 performed again to see the impact on design changes. This gives the designer a way to assess quickly and objectively the effects of a design change on safety. In the case of the flight termination system, a few design options are available to the designer to eliminate or reduce the likelihood of the identified causal scenarios. Some of the design decisions available are:

- Autonomous vs. traditional flight termination system
- Design margins
- Operating System (RTOS vs. GPOS)
- Design review criteria and process
- Minimum workmanship screening levels and acceptable performance variability
- Test plans (stress testing, sign checks, mapping, acceptance test procedures, qualification tests, HITL, etc.)
- Tracking sources (GPS, inertial, C-band beacon, etc.)
- Error detection and correction (dual redundant elements in lockstep, triple redundant, etc.)
- Arming devices
- Communications bus type and harnessing (Ethernet, CAN, FLEXray, serial, etc.)
- RF coupling antennas or separate Tx/Rx
- Battery type and configuration
- Partitioning of software functions into modules and concurrent loops in real-time systems
- Hardware and software self-checking and error correction
- Watchdog timers and circuits
- Electromagnetic interference and compatibility protection
- Redundant message transmission and cross-strapping
- Vibration isolation
- Thrust termination only vs. vehicle breakup and deflagration
- Ordnance initiation type (redundant, single stick with two contacts, thrust termination only, etc.)
- FPGA or microprocessor
- Thermal management systems
- Encoder/decoder type
- Etc.

### 4.5.2 Second Stage Propulsion System

The design of the second stage propulsion system is chosen for further analysis. As part of propulsion system preliminary design, functional responsibilities are assigned to specific components and assemblies.

#### *4.5.2.1 Safety Control Structure*

For the purpose of this exercise, the second stage propulsion system is composed of the engine, gas generator (GG) power pack, main valves, and an engine controller. The engine controller, thrust vector control actuators (TVCA), and propellant tanks receive and send data back to the main flight computer. Loads from the engine are transferred to the vehicle body and tanks via a thrust structure. The control structure is shown in Figure 14.

**PC1.** Position or Rate Command
**PC2.** Position Feedback
**PC3.** Rate Feedback
**PC4.** Pressure/Temperature Feedback
**PC5.** Loads
**PC6.** Propulsion on/off
**PC7.** Health Status
**PC8.** Power

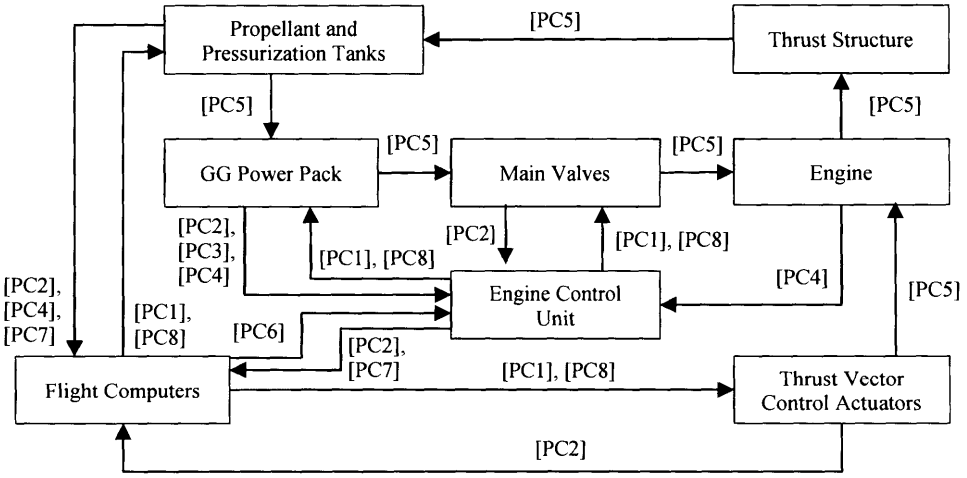



*Figure 14. Propulsion System Control Structure.*

#### *4.5.2.2 Unsafe Control Actions (STPA Step 1)*

Unsafe control actions can be identified from this control structure. Table 21 shows some of the unsafe control actions that could be provided by the engine control unit (ECU).

*Table 21. Engine control unit UCA context table.*

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Engine Control Unit | GG valves open commands | **UCA1:** ECU does not provide GG open command during startup sequence [H4.2] [H4.1] [H5] | **UCA2:** ECU provides GG open command during shutdown [H4.4] [H2]<br><br>**UCA3:** ECU provides GG open command when downstream pressure is higher than upstream pressure [H7.1] [H7.4]<br><br>**UCA4:** ECU provides GG valves open commands when there is insufficient propellant in pumps [H7] [H4.4]<br><br>**UCA5:** ECU provides GG valves open command when there is insufficient propellant to GG [H4.2] [H4.4] [H7]<br><br>**UCA6:** ECU provides GG valves open commands during abort [H4.4] [H2]<br><br>**UCA7:** ECU provides excessive GG open command power [H7.2] [H4.2]<br><br>**UCA8:** ECU provides GG open command when upstream propellant pressures are out of range [H4.4] | **UCA9:** ECU provides GG open command >TBD milliseconds from main valve cracking [H7] [H4.4]<br><br>**UCA10:** ECU provides GG valves open command <TBD seconds before GG ignition source provided [H7] [H4.4]<br><br>**UCA11:** ECU provides GG open command <TBD milliseconds from main valve cracking [H7] [H4.4] | **UCA12:** ECU stops providing GG open command power before valves are fully open [H4.2] [H4.4] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Engine Control Unit | GG valves close commands | **UCA13:** ECU does not provide GG valves close commands during shutdown [H4.4] [H7.2]<br><br>**UCA14:** ECU does not provide GG valves close commands during abort [H4.4] [H7.2] [H7] | **UCA15:** ECU provides GG valve close command during startup [H4.2] | **UCA16:** ECU provides GG close command >TBD seconds before main valves close [H4.4] [H4.2]<br><br>**UCA17:** ECU provides GG close command too late (<TBD seconds after main valves close) [H4.4] | **UCA18:** ECU stops providing GG close command power before valves are fully closed [H4.1] [H7.2] |
| Engine Controller | GG ignition source command | **UCA19:** ECU does not provide GG ignition source command during startup sequence [H4.2] | **UCA20:** ECU provides GG ignition source command during pre-launch [H7] | **UCA21:** ECU provides GG ignition source command before stage separation [H7] [H2]<br><br>**UCA22:** ECU provides GG ignition source command outside of startup window [H4.3] [H7]<br><br>**UCA23:** ECU provides GG ignition source power >TBD seconds before flow enters GG [H7] [H4.2] | **UCA24:** ECU stops providing GG ignition source command before GG is lit [H4.2]<br><br>**UCA25:** ECU provides GG ignition source command too long [H4.4] [H4.2] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Engine Controller | Igniter valves open commands | **UCA26:** ECU provides igniter valves open commands during shutdown [H4.4] [H2.2] [H7]<br><br>**UCA27:** ECU provides igniter valves open commands during abort [H4.4] [H7.2] [H2.2] [H7] | **UCA28:** ECU provides igniter valves open commands when downstream pressure is higher than upstream pressure [H7.1] [H7.2] [H7.4] | **UCA29:** ECU provides igniter valves open commands too late (>TBD seconds after main valve open commands) [H7] [H4.4]<br><br>**UCA30:** ECU provides igniter valves open commands too early (>TBD seconds before main valve open commands) [H7]<br><br>**UCA31:** ECU provides igniter valves open commands before stage separation [H7] [H2] | **UCA32:** ECU stops providing igniter valves open commands power before valves are fully open [H4.2] [H7]<br><br>**UCA33:** ECU provides igniter valves open commands too long (>TBD milliseconds) [H4.4] |
| Engine Controller | Igniter valves close commands | **UCA34:** ECU does not provide igniter valves close commands during shutdown [H4.4] [H2.2] [H7]<br><br>**UCA35:** ECU does not provide igniter valves close commands during abort [H4.4] [H7.2] [H2.2] [H7] | N/A | **UCA36:** ECU provides the igniter valves close commands too late (>TBD milliseconds) after chamber ignition [H4.4] [H7.1]<br><br>**UCA37:** ECU provides the igniter valves close commands too early (>TBD milliseconds) before chamber ignition [H4.2]<br><br>**UCA38:** ECU provides igniter valves close commands out of order [H4.4] [H7.1] [H7.4] | **UCA39:** ECU stops providing igniter valves close commands before igniter valves are fully closed [H4.4] [H7.1] [H7.2] [H7.4] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Engine Controller | MV open commands | **UCA40:** ECU does not provide MV open commands during startup [H4.2] [H5] | **UCA41:** ECU provides MV open commands during abort [H4.4] [H7.2] [H2.2] [H7]<br><br>**UCA42:** ECU provides MV open commands during shutdown [H4.4] [H2.2] [H7]<br><br>**UCA43:** ECU provides MV open commands when downstream pressure is greater than upstream pressure [H7.1] [H7.2] [H7.4]<br><br>**UCA44:** ECU provides MV open commands when igniter is not on [H7.2] [H4.2] | **UCA45:** ECU provides MV open commands before startup [H4.2] [H7.2]<br><br>**UCA46:** ECU provides MV open commands out of order [H7.2] [H4.4]<br><br>**UCA47:** ECU provides MV open commands too late (>TBD milliseconds) after pump spool up [H4.4]<br><br>**UCA48:** ECU provides MV open commands too soon (>TBD milliseconds) after stage separation [H2] | **UCA49:** ECU stops providing MV open commands before valves are fully open [H4.2] [H4.4] [H5] |
| Engine Controller | MV close commands | **UCA50:** ECU does not provide MV close commands during shutdown [H7.2] [H5] [H7.2]<br><br>**UCA51:** ECU does not provide MV close commands during abort [H7.2] [H5] [H7.2] | **UCA52:** ECU provides MV close commands during normal operations [H4.2] [H4.4]<br><br>**UCA53:** ECU provides MV close commands when pump power is above TBD level [H4.4] | **UCA54:** ECU provides MV close commands before shutdown or abort [H4.2] [H4.4]<br><br>**UCA55:** ECU provides MV close commands out of order [H4.4] [H7]<br><br>**UCA56:** ECU provides MV close commands before desired orbital parameters reached [H5] | **UCA57:** ECU stops providing MV close commands too early (before valves are fully open) [H4.4] [H7.2] [H5] |

The unsafe control actions can be translated into constraints on behavior. For the purpose of demonstration, only the unsafe control actions corresponding to the engine controller providing GG open commands will be considered. Table 22 shows the safety constraints on the engine controller that can be identified from the unsafe control actions in Table 21.

*Table 22. Partial list of unsafe control actions for the ECU.*

| Unsafe Control Actions | Safety Constraints |
|---|---|
| **UCA1:** ECU does not provide GG open command during startup sequence | **SC1:** ECU must provide GG open command during startup sequence |
| **UCA2:** ECU provides GG open command during shutdown | **SC2:** ECU must not provide GG open command during shutdown |
| **UCA3:** ECU provides GG open command when downstream pressure is higher than upstream pressure | **SC3:** ECU must not provide GG open command when downstream pressure is higher than upstream pressure |
| **UCA4:** ECU provides GG valves open commands when there is insufficient propellant in pumps | **SC4:** ECU must not provide GG open command when there is insufficient propellant in pumps |
| **UCA5:** ECU provides GG valves open command when there is insufficient propellant to GG | **SC5:** ECU must not provide GG open command when there is insufficient propellant to start GG |
| **UCA6:** ECU provides GG valves open commands during abort | **SC6:** ECU must not provide GG open command during abort |
| **UCA7:** ECU provides excessive GG open command power | **SC7:** ECU must provide <TBD GG open command power |
| **UCA8:** ECU provides GG open command when upstream propellant pressures are out of range | **SC8:** ECU must not provide GG open command when upstream propellant pressures are out of range |
| **UCA9:** ECU provides GG open command >TBD milliseconds from main valve cracking | **SC9:** ECU must not provide GG open command >TBD milliseconds from main valve cracking |
| **UCA10:** ECU provides GG valves open command <TBD seconds before GG ignition source provided | **SC10:** ECU must not provide GG open command <TBD milliseconds before GG ignition source provided |
| **UCA11:** ECU provides GG open command <TBD milliseconds from main valve cracking | **SC11:** ECU must not provide GG open command <TBD milliseconds from main valve cracking |
| **UCA12:** ECU stops providing GG open command power before valves are fully open | **SC12:** ECU must not stop providing GG open command power before valves are fully open |

#### *4.5.2.3 Causal Factors (STPA Step 2)*

Once unsafe control actions are identified, the causal scenarios that could lead to unsafe control actions can be found. Unsafe control actions can be caused by unsafe controller behavior and inadequate feedback and other inputs. Some of the causal scenarios that could lead to the first six unsafe control actions are identified in this section.

**UCA1:** ECU does not provide GG open command during startup sequence

Scenario 1 for UCA1: The ECU physical controller fails due to environmental loads during the startup sequence, causing the GG valve open command to not be provided [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 2 for UCA1: The ECU physical controller receives incorrect timing data from the main flight computer, causing the GG valve open command to not be provided during the startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 3 for UCA1: The ECU physical controller provides intermittent power, causing the GG valve open command to not be provided during the startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 4 for UCA1: The physical connection between the ECU and the GG valve actuators is wrong, broken, or intermittent, causing the GG valve open command to not be provided during the startup sequence [UCA1]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 5 for UCA1: The correct GG valve open command timing or redlines are not passed to designers/developers or are incorrectly specified, causing the GG valve open command to not be provided during the startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 6 for UCA1: A redundant ECU provides a conflicting GG valve open command, causing the GG valve open command to not be provided during startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 7 for UCA1: Actuation channels are incorrectly mapped in ECU software, causing the GG valve open command to not be provided during startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5].

Scenario 8 for UCA1: ECU incorrectly receives or interprets a signal satisfying abort conditions during the startup sequence, causing the GG valve open command to not be provided during startup sequence [UCA1]. As a result, forces required to maintain flight path may not be provided [H4.1] [H4.2] and the payload may be inserted into the wrong orbit [H5]. This incorrect signal may be received if any of the following occur:

- Sensor feedback (GG/engine pressures, valve positions, etc.) is delayed due to filtering used
- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect due to wrong or missing sensor mapping in ECU software

- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect or missing due to electromagnetic interference
- Mechanical failure of harnesses or switches
- Mechanical failure of sensors
- No sensor feedback exists

Some scenarios may cause multiple unsafe control actions. For example, UCA Scenario 5, *the correct GG valve open command timing is not passed to designers/developers or is incorrectly specified*, could also cause UCA3, UCA4, UCA5, UCA9, or UCA10.

**UCA2:** ECU provides GG open command during shutdown

Scenario 1 for UCA2: The ECU physical controller fails due to environmental loads during or before the shutdown sequence, causing the GG valve open command to be provided during shutdown [UCA2]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 2 for UCA2: The ECU physical controller receives incorrect timing data from the main flight computer, causing the GG valve open command to be provided during shutdown [UCA2]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 3 for UCA2: The physical connection between the ECU and the GG valve actuators is wrong, broken, or intermittent, causing the GG valve open command to be provided during shutdown [UCA2]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 4 for UCA2: The correct GG valve open command timing or redlines are not passed to designers/developers or are incorrectly specified, causing the GG valve open command to be provided during shutdown [UCA2]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 5 for UCA2: A redundant ECU provides conflicting valve commands during shutdown, causing the GG valve open command to be provided during shutdown [UCA2]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 6 for UCA2: Actuation channels are incorrectly mapped in ECU software, causing the GG valve open command to be provided during shutdown [UCA2]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

**UCA3:** EC provides GG open command when downstream pressure is higher than upstream pressure

Scenario 1 for UCA3: The ECU physical controller fails due to environmental loads during or before the shutdown sequence, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy.

Scenario 2 for UCA3: The ECU physical controller receives incorrect timing data from the main flight computer, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy.

Scenario 3 for UCA3: The physical connection between the ECU and the GG valve actuators is wrong, broken, or intermittent, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy.

Scenario 4 for UCA3: The correct GG valve open command timing or redlines are not passed to designers/developers or are incorrectly specified, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy.

Scenario 5 for UCA3: A redundant ECU provides conflicting valve commands during shutdown, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy.

Scenario 6 for UCA3: Actuation channels are incorrectly mapped in ECU software, causing the GG valve open command to be provided when downstream pressure is higher than upstream pressure [UCA3]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 7 for UCA3: The ECU incorrectly detects a positive pressure difference across the GG valves [UCA3]. As a result, fluid may flow into the feed system [H7.1] [H7.4] and cause uncontrolled release of energy. This incorrect signal may be received if any of the following occur:

- Sensor feedback (GG/engine pressures, valve positions, etc.) is delayed due to filtering used
- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect due to wrong sensor mapping in ECU software
- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect or missing due to electromagnetic interference
- Mechanical failure of harnesses or switches
- Mechanical failure of sensors
- No sensor feedback exists

**UCA4:** The ECU provides GG valves open commands when there is insufficient propellant in pumps

Scenario 1 for UCA4: Actuation channels are incorrectly mapped in the ECU software, causing the ECU to provide GG valves open commands at the wrong time (when there is insufficient propellant in pumps) [UCA4]. As a result, turbomachinery may overspin, causing uncontrolled release of energy [H7] or degraded pump performance [H4.4].

Scenario 2 for UCA4: ECU incorrectly switches to an operating state after propellant supply is depleted [UCA4]. This may be caused by an incorrect command from the FSS or an ECU process model flaw. Uncontrolled release of thermal energy or thrust force may result [H7].

Scenario 3 for UCA4: The physical connection between the ECU and the GG valve actuators is wrong, broken, or intermittent, causing the ECU to provide GG valves open commands at the wrong time (when there is insufficient propellant in pumps) [UCA4]. A wrong connection may be caused by incorrect specifications or the belief that the connection is correct by design or integration personnel. Uncontrolled release of thermal energy or thrust force may result [H7].

Scenario 4 for UCA4: The correct GG valve open command timing or redlines are not passed to designers/developers or are incorrectly specified, causing the ECU to provide GG valves open commands at the wrong time (when there is insufficient propellant in pumps) [UCA4]. Uncontrolled release of thermal energy or thrust force may result [H7].

Scenario 5 for UCA4: The ECU incorrectly detects the presence of fluid in pumps. As a result, ECU may provide GG valves open commands and turbomachinery may overspin and/or pumps may

cavitate [UCA4], causing uncontrolled release of energy [H7] or degraded pump performance [H4.4]. This incorrect signal may be received if any of the following occur:

- Sensor feedback (GG/engine pressures, valve positions, etc.) is delayed due to filtering used
- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect due to wrong sensor mapping in ECU software
- Sensor feedback (GG/engine pressures, valve positions, etc.) is incorrect or missing due to electromagnetic interference
- Mechanical failure of harnesses or switches
- Mechanical failure of sensors
- No sensor feedback exists

**UCA5:** ECU provides GG valves open command when there is insufficient propellant to GG

Scenario 1 for UCA5: Valve actuator maps in the ECU are missing or incorrect, causing the ECU to provide GG valves open commands at the wrong time (when there is insufficient propellant to GG) [UCA5]. As a result, the GG does not start or runs at reduced flow rate, which may cause insufficient performance [H4.2] or operation at an undesired operating condition [H4.4] that causes uncontrolled release of energy [H7].

Scenario 2 for UCA5: ECU incorrectly switches state during a transient event, and the ECU provides GG valves open command when there is insufficient propellant in the GG [UCA5]. This may be caused by an incorrect command from the FSS or an ECU process model flaw. As a result, the GG operates at an off-design mixture ratio, which may cause insufficient performance [H4.2] or operation at an undesired operating condition [H4.4] that causes uncontrolled release of energy [H7].

Scenario 3 for UCA5: Propellant line to GG valves is blocked by a closed valve or foreign object debris when GG open command provided by ECU [UCA5]. As a result, the GG does not start or runs at reduced flow rate, which may cause insufficient performance [H4.2] or operation at an undesired operating condition [H4.4] that causes uncontrolled release of energy [H7].

Scenario 4 for UCA5: Propellant lines or tanks to GG valves leak. As a result, the GG does not start or runs at reduced flow rate, which may cause insufficient performance [H4.2] or operation at an undesired operating condition [H4.4] that causes uncontrolled release of energy [H7].

**UCA6:** ECU provides GG open commands during abort

Scenario 1 for UCA6: Physical mechanism(s) on the ECU fail(s) due to environmental loads during or before an abort, causing the GG valve open command to be provided during the abort [UCA6]. This environment may be during manufacturing (e.g., excessive thermal gradients during soldering), testing (e.g., improper humidity control in environmental chamber during acceptance testing), or flight (e.g., structural dynamics in engine bay). As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 2 for UCA6: The ECU physical controller receives incorrect timing data from the main flight computer, causing the GG valve open command to be provided during abort [UCA6]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 3 for UCA6: The physical connection between the ECU and the GG valve actuators is wrong, broken, or intermittent, causing the GG valve open command to be provided during abort [UCA6]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 4 for UCA6: The correct GG valve abort command timing or redlines are not passed to designers/developers or are incorrectly specified, causing the GG valve open command to be provided during abort [UCA6]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

Scenario 5 for UCA6: A redundant ECU provides conflicting valve commands during abort, causing the GG valve open command to be provided during abort [UCA6]. As a result, the GG and turbomachinery may operate while the main valves are closed or about to close [H4.4] and structural integrity may be lost [H2].

#### *4.5.2.4 Design Options*

Each of these scenarios can then be evaluated, and design changes can be proposed to eliminate or mitigate the hazards. The effectiveness of each can be compared, and steps 1 and 2 performed again to see the impact on design changes. This gives the designer a way to assess quickly and objectively the effects of the safety fix. In the case of the gas generator control actions above, a few design options are available to the designer to eliminate or reduce the likelihood of causal scenarios. Some examples are shown in Table 23.

*Table 23. Examples of safety fixes to mitigate or eliminate causal scenarios.*

| Safety Fix | Scenarios Eliminated or Mitigated |
|---|---|
| ECU self-checking | Scenario 6 for UCA1, Scenario 5 for UCA2, Scenario 5 for UCA3, Scenario 5 for UCA6 |
| FC self-checking | Scenario 2 for UCA1, Scenario 4 for UCA1, Scenario 2 for UCA2, Scenario 3 for UCA2, Scenario 2 for UCA3, Scenario 2 for UCA4, Scenario 2 for UCA5, Scenario 2 for UCA6 |
| Cross-checking and Cross-Channel Data Link (CCDL) | Scenario 6 for UCA1, Scenario 5 for UCA2, Scenario 5 for UCA3, Scenario 7 for UCA3, Scenario 2 for UCA6, Scenario 5 for UCA6 |
| Redundant message transmission | Scenario 2 for UCA4, Scenario 2 for UCA5, Scenario 2 for UCA6 |
| ECU vibration isolators | Scenario 1 for UCA1, Scenario 3 for UCA1, Scenario 4 for UCA1, Scenario 1 for UCA2, Scenario 3 for UCA2, Scenario 1 for UCA2, Scenario 3 for UCA3, Scenario 3 for UCA4, Scenario 3 for UCA4, Scenario 1 for UCA6, Scenario 3 for UCA6 |
| Fluid line filters | Scenario 3 for UCA4, Scenario 3 for UCA5 |
| Redundant GG valve(s) | Scenario 1 for UCA5, Scenario 3 for UCA5 |
| Change grounding scheme | Scenario 3 for UCA1, Scenario 8 for UCA1, Scenario 7 for UCA3 |
| Redundant sensors | Scenario 8 for UCA1, Scenario 7 for UCA3, Scenario 5 for UCA4 |
| Check valves | Scenario 4 for UCA3, Scenario 3 for UCA5 |
| Change inlet connection (e.g., orbital tube weld) | Scenario 3 for UCA4, Scenario 4 for UCA5 |
| End-to-end sensor filtering and delay verification testing | Scenario 8 for UCA1, Scenario 5 for UCA4 |
| Sensor/actuator mapping and continuity verification | Scenario 4 for UCA1, Scenario 7 for UCA1, Scenario 8 for UCA1, Scenario 3 for UCA2, Scenario 6 for UCA2, Scenario 3 for UCA3, Scenario 6 for UCA3, Scenario 7 for UCA3, Scenario 1 for UCA4, Scenario 3 for UCA4, Scenario 5 for UCA4, Scenario 1 for UCA5, Scenario 3 for UCA6 |
| Filtering & actuation response verification | Scenario 2 for UCA1, Scenario 2 for UCA2, Scenario 7 for UCA3 |
| ECU/FSS valve sequence independent verification | Scenario 2 for UCA1, Scenario 5 for UCA1, Scenario 2 for UCA2, Scenario 4 for UCA2, Scenario 2 for UCA3, Scenario 4 for UCA3, Scenario 2 for UCA4, Scenario 4 for UCA4, Scenario 2 for UCA5, Scenario 2 for UCA6, Scenario 4 for UCA6 |

Many of these safety fixes are avionics/ECU architecture dependent. For example, the ECU may act as a passive controller that just provides power to valves based on commands from the flight computer, rather than controlling engine and valve commands from states programmed into each ECU. Furthermore, safety fixes concerning software or controller process models, such as valve sequence verification and sensor/actuator mapping, mitigate many of the scenarios identified.

Causal scenarios that cannot be eliminated should be mitigated through crossing/channelizing, self-checking/voting, and switching/bussing. Care should be taken to ensure that this redundancy does not introduce additional design errors. The corresponding solution should depend on the likelihood of the causal scenario occurring, the severity of the hazard, and the likelihood of the hazard leading to an accident.

This Page Intentionally Left Blank

# 5 STPA RANGE SAFETY AND REGULATORY COMPLIANCE

## 5.1 14 CFR PART 400

The Commercial Space Launch Act of 1984 empowers the FAA Office of Commercial Space Transportation to authorize and regulate launches and reentries of launch vehicles carried out within the United States or by U.S. citizens. Commercial space transportation regulations are located in Title 14 of the Code of Federal Regulations (CFR). This section addresses the applicability and compliance of STPA to fulfill FAA commercial space transportation regulations for uncrewed launch vehicles.

### 5.1.1 Part 414 Subpart C

14 CFR Part 414 Subpart C defines the safety approval review and issuance process for FAA launch licenses. The FAA determines approval based on (i) FAA or other appropriate Federal regulations, (ii) government-developed or adopted standards, (iii) industry consensus performance-based criteria or standards, and (iv) applicant-developed criteria. Applicant-developed criteria must define the system design and minimum performance, quality assurance system requirements, production acceptance test specifications, and operational safety monitoring system characteristics. The design requirements generated by STPA can be used to define these criteria. The safety monitoring system is defined by the safety control structure. System safety requirements are generated by STPA, and design choices made to eliminate or mitigate the identified hazards define the quality assurance system requirements and inform the production acceptance test specifications.

### 5.1.2 Part 415

#### *5.1.2.1 Subpart C*

14 CFR Part 415 describes the requirements for obtaining a license to launch a launch vehicle other than a reusable launch vehicle. If the vehicle is launched from a federal launch range, launch service providers must comply with 14 CFR Part 415 Subpart C. Subpart C requires an applicant to maintain and document the organization's safety organization, and define the lines of communication and approval authority for all launch safety decisions. The organizational safety control structure created for an STPA analysis of the safety organization states these lines of communication and approval authority, and thus satisfies §415.33.

14 CFR 415.35 requires the applicant to demonstrate acceptance flight risk. §415.35(a) requires the applicant to satisfy minimum expected casualty requirements. §415.35(b) requires the applicant to identify the hazards and risks associated with public health and safety and safety of property associated

with the flight of the vehicle. §415.35(c) requires the vehicle to be designed to ensure the flight risks meet the criteria of §415.35(a) by describing the (i) launch vehicle structure, (ii) hazardous and safety-critical systems, and (iii) drawings and schematics for each system. §415.35(d) requires the launch vehicle to be operated in a manner consistent with §415.35(c)(2). An STPA analysis of the launch vehicle identifies the hazardous and safety critical systems, and contains the operational contexts in the analysis. The STPA analysis thus satisfies §415.35(c)(2) and §415.35(d). Furthermore, an STPA analysis will inform the accident investigation plan required by §415.41.

#### *5.1.2.2 Subpart F*

14 CFR Part 415 Subpart F defines the safety review and approval requirements for the launch of expendable launch vehicles from non-federal launch sites. Similar to §415.35, §415.105 requires all hazards associated with the launch vehicle to be determined during pre-application consultation. This identification can be performed with STPA. 14 CFR Part 415 Subpart F also requires flight, ground, computing systems and software, flight safety system design, and end-of-launch safety plans. Many aspects of these plans can be addressed by STPA. Part 415 Subpart F largely refers to Part 417 requirements, so the specific application of STPA to these requirements will be addressed in the section of this chapter devoted to Part 417.

### 5.1.3 Part 417

14 CFR Part 417 defines the responsibilities of a launch operator conducting a licensed launch of an expendable launch vehicle. §417.25 requires a post-launch report to be filed to the FAA 90 days after launch. This post-launch report must identify deviations from expected performance and the associated corrective actions. STPA can provide the safety requirements to be checked in the post-launch report and provide a method to quickly evaluate design changes proposed as corrective actions.

#### *5.1.3.1 Subpart B – Launch Safety Responsibilities*

Similar to §415.33, §417.103 requires the launch provider to document and maintain a safety organization. The lines of communication and approval authority are part of the safety control structure required for the STPA analysis.

§417.107 defines requirements for flight safety. §417.107(a) requires launch vehicles to have a flight safety system. §417.107(b)-(e) set public risk criteria and thresholds on the use of a flight safety system, and the analysis used to determine injury or casualties. These thresholds set the "TBD" values in the corresponding requirements generated by the STPA analysis.

§417.113 requires launch operators to satisfy launch safety rules. The safety constraints generated by an STPA of the launch system can be used to generate these launch safety rules. These rules include

constraints related to ground safety, flight-commit criteria, flight termination rules, flight safety system safing, and launch crew work shift and rest rules.

§417.115 requires all flight communication, and ground systems and equipment that is used to protect the public from adverse effects of a launch to undergo testing. STPA can inform the test plans by providing the safety constraints that are supposed to be satisfied.

§417.117 requires a launch operator to conduct reviews of safety-critical processes and systems. STPA provides the requirements and safety constraints that must be satisfied and reviewed.

§417.123 requires a launch operator to document a system safety process and identify all safety-critical functions associated with computing systems and software. STPA can be used as the backbone of the system safety process and identify safety-critical functions.

§417.127 requires a launch operator to identify any unique hazards not otherwise addressed by Part 417, and demonstrate that these hazards are mitigated. STPA can be used to identify these hazards alongside hazards and causal scenarios that are addressed in Part 417.

#### *5.1.3.2 Subpart C – Flight Safety Analysis*

§417.205 states that a flight safety analysis must demonstrate that a launch operator will control the risk to the public from hazards associated with launch vehicle flight. The analysis is required to demonstrate control of risks to the public by demonstrating that each identified risk meets §417.107(b), through hazard isolation, or a combination of hazard isolation and control of risks. STPA can be used to identify hazards and propose mitigations or demonstrate their elimination. The remaining requirements in this subpart concern the analysis required to demonstrate that each hazard is satisfactorily mitigated or eliminated.

#### *5.1.3.3 Subpart D – Flight Safety System*

§417.301 through §417.311 contains flight safety system requirements. These requirements state that performance specifications must be provided for each subsystem to demonstrate that safety requirements are met. STPA can provide safety constraints for the flight safety system and inform the selection of performance specifications in design.

#### *5.1.3.4 Subpart E – Ground Safety*

§417.405 requires launch operators to perform a safety analysis for all launch vehicle ground hardware. The analysis is required to identify each hazard, associated cause, and each hazard control. STPA satisfies each of these three requirements.

## 5.2 EWR 127-1

Easter and Western Range (EWR) 127-1 provides range safety requirements for users of the launch ranges at Cape Canaveral Air Force Station and Vandenberg Air Force Base. Appendix 1B of this document requires a range user to establish a safety management system to implement provisions of EWR 127-1. Section 1.4 of this appendix requires the range user to perform preliminary hazard analyses, subsystem hazard analyses, system hazard analyses, operating and support hazard analyses, and safety assessments. Each of these hazard analyses are required to consider certain program elements such as equipment, hazardous materials, interfaces, design criteria, environmental constraints, testing, facilities, training, human error, and equipment safeguards.

Unlike FMECA and other traditional hazard techniques, STPA addresses all of these elements in a single integrated analysis because each element is part of the safety control structure. Additionally, the range user is required to perform a safety assessment to identify all safety features of system hardware, software, and design and to identify procedural, hardware, software related hazards [63]. An STPA of the system also addresses this requirement.

### 5.2.1 Design Priority

EWR 127-1 identifies priority of system safety precedence to: (1) design to eliminate or reduce hazards, (2) incorporate safety devices, (3) provide warning devices, and (4) develop procedures and training [63]. However, EWR 127.1 states that a system should be designed to tolerate a minimum number of credible failures by introducing inhibits, which must be of an electrical or mechanical nature. This design priority is similar to the design priority in 3.3.1 of this document but does not prioritize eliminating hazards above reducing hazards.

### 5.2.2 Software Safety

Software safety is handled by determining software safety critical functions (SSCF) and imposing general safety design requirements on those functions. A few example requirements from EWR 127-1 are below:

> **EWR 127-1 3.16.2.2a:** The system shall power up in a safe state.
>
> **EWR 127-1 3.16.2.2b:** The system shall not enter an unsafe or hazardous state after an intermittent power transient or fluctuation.
>
> **EWR 127-1 3.16.2.2c:** The system shall gracefully degrade to a secondary mode of operations or shutdown in the event of a total power loss so that potentially unsafe states are not created.

**EWR 127-1 3.16.2.3c:** The software shall be capable of detecting the following input/output errors: (1) Improper entries, (2) Improper sequences of entries, (3) Improper sequences of operations, (4) Invalid output, (5) Timing.

**EWR 127-1 3.16.2.4b:** If a failure or error is detected within a flight SSCF or associated safety critical hardware, the system shall: (1) Maintain the FTS in an ARMED state throughout the flight even if errors are detected, (2) Reject erroneous input, (3) Ensure all detected SSCF (FTS) related system errors are transmitted via telemetry to the range, (4) Notify the operator if an ARM or SAFE logic pattern other than ARM or SAFE code is present.

The set of software critical safety function requirements in EWR 127-1 are designed to ensure safety design requirements have been "correctly and completely implemented in SSCF code" [63]. No mention is made to ensuring that the design requirements are correct other than 3.16.3.6(b)(l), which requires that reused software shall be analyzed for correctness of design assumptions and requirements. The implicit assumption is that the design requirements are correct in a new system but not necessarily in a reused system. This is false, as many of the causes of recent spacecraft and launch vehicle accidents have been related to requirement errors. The EWR requirements are a subset of the requirements that would be

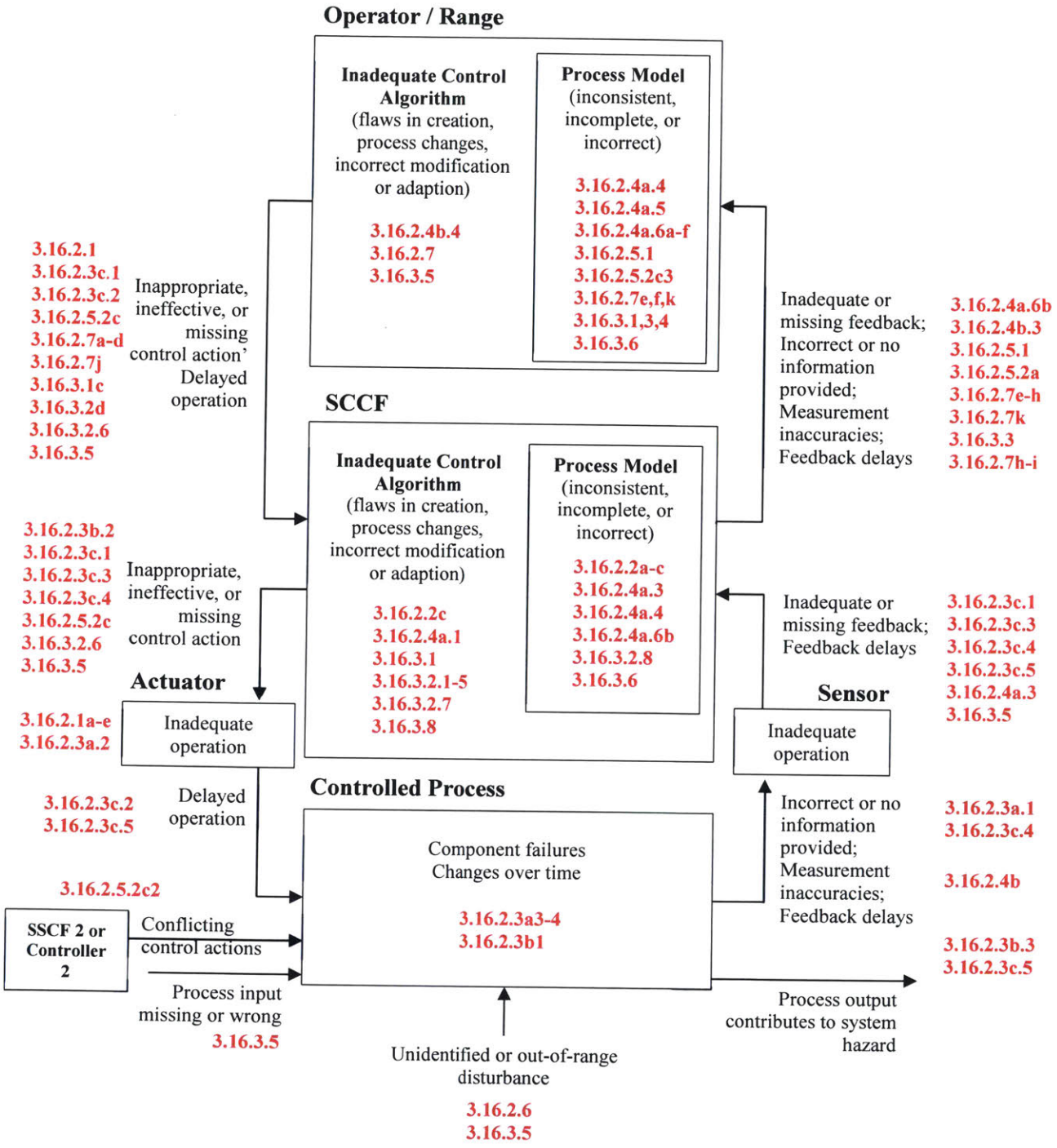



*Figure 15. EWR 127-1 Software Safety Critical Functions requirements mapped to the generic STPA causal factors process model.*

found by STPA during design for this reason. Figure 15 shows that each of the EWR127-1 SSCF requirements maps directly to one or more of the generic causal factors considered by the final step of STPA. This demonstrates that STPA is able to identify all SSCF requirements, but not that the SSCF requirements are complete. Conflicting control actions from secondary SSCF's are only handled in the

context of interlocks and processor voting logic in the presence of single event upsets. Conflicting control action hazards in the flight termination system are eliminated by requiring each FTS to be completely independent of other controllers. Process output that could contribute to system hazards are handled in other aspects of the safety requirements documentation.

STPA provides a systematic and complete method of identifying hazards caused by unsafe control actions and information flow. It is thus uniquely suited to demonstrate fulfillment of EWR 127-1 requirements, and most importantly identifies errors in requirements not addressed by EWR 127-1.

## 5.3 RCC 319

Range Commands Council (RCC) 319 provides a commonality standard for flight termination systems on launch vehicles. Unlike EWR 127-1, finding design and development errors is directly addressed in software. RCC 319-14 Appendix A states that the equations and algorithms of the flight termination system design documents must be reviewed to ensure that they satisfy range user requirements. The range user requirements in RCC 319-14 include notes to clarify the goals and intent of individual requirements, and a tailoring process for removing requirements that do not apply to a flight termination system is provided. This procedure helps ensure requirements are correct beyond verification and validation reviews and is thus more likely to catch design errors than EWR 127-1 and FAA Part 417.

This Page Intentionally Left Blank

# 6 CONCLUSIONS & FUTURE WORK

The advent of the commercial space launch market has brought about a new age of space launch vehicle design. In order to survive in a competitive market, space launch providers must design systems with new technologies in shorter development times. The changing nature of space launch vehicle design requires a new way to perform safety analysis. Traditional hazard analysis techniques do not deliver adequate insight early in the vehicle design process, when most of the safety-related decisions are made. Early design decisions are often made using "lessons-learned" from previous vehicle systems, rather than interactive feedback from the new vehicle design actually being developed. Furthermore, traditional techniques use reliability theory and event-based hazard analyses as their foundation, resulting in the use of expanded design margin and redundancy as the "default" vehicle design choices.

## 6.1 CONCLUSIONS

This thesis addressed the problem that traditional hazard analysis tools are unable to identify and correct safety-related design errors in modern launch vehicles. Chapter 2 gave an overview of safety analysis methods currently used in launch vehicle design, and critiqued the effectiveness of those techniques. Section 2.2 introduced safety analysis techniques based on systems theory and examined some of the uses of Systems-Theoretic Process Analysis (STPA) on aerospace vehicles to date. The changing nature of launch vehicle accidents was demonstrated through the launch vehicle accidents chronicled in section 2.3, and the changing nature of launch vehicle design spurred by the commercial launch market was described in section 2.4. Methods for integrating STPA into the launch vehicle lifecycle were discussed in chapter 3, followed by a more detailed description of how STPA can be used to develop principles for safety-guided launch vehicle design processes. Chapter 4 formulated a more detailed model which showed how STPA can be applied to the real-world safety-guided design processes of a small-lift launch vehicle. Finally, chapter 5 showed how STPA could be used to comply with current regulatory, range, and safety standards.

The space launch industry needs safety analysis methods and design processes which identify and correct safety issues early in the vehicle design process, when modifications to correct safety issues are more effective and less costly. The integration of Systems-Theoretic Process Analysis (STPA) into the safety-guided design of small lift space launch vehicles can make a significant contribution to reducing accidents without compromising efficient and cost-effective design. This work shows how STPA can be a powerful tool to identify, mitigate, and possibly eliminate hazards throughout the entire space launch vehicle design lifecycle. It offers a thorough, concrete model of how STPA can be applied to the concept

evaluation, system requirements, system architecture, and system design phases of a hypothetical two-stage small-lift launch vehicle. It also shows how STPA can inform and guide manufacturing, testing, operations, and regulatory compliance.

## 6.2 FUTURE WORK

### 6.2.1 Comparison with Traditional Methods

The limited scope of this thesis prevented a comprehensive application of STPA to an existing space launch system. Applying STPA to an existing launch system would allow a side-by-side comparison of STPA relative to an existing FMECA would robustly test STPA's effectiveness.

### 6.2.2 Test Requirements and Operations

The safety constraints generated by STPA are often stated in the negative, e.g., "The ECU must not provide", rather than as a testable positive, e.g., "The ECU must provide." Methods for testing these safety constraints in launch systems should be devised to aid vehicle design, and designers should favor architectures with testable safety constraints. Methods for testing safety constraints would clearly increase safety.

Launch vehicle operations and manufacturing were not addressed in this thesis. An evaluation of the launch operations control structure would give valuable insight into the strengths and weaknesses of launch operations safety as it is currently practiced.

### 6.2.3 Causal Scenario Generation

The causal scenarios identified in section 4.5.1.5 and section 4.5.2.3 are representative but incomplete. The author is not an expert in avionics hardware or software and generated these scenarios to represent the types of hazards that should be considered.

### 6.2.4 Leading Safety Indicators

The results of an STPA analysis of the launch vehicle organization would deliver insight into the leading safety indicators universal to all launch vehicle providers. In particular, valuable insight would be gained by providing ways to identify (i) degradation of important safety-related design information within the engineering organization, (ii) shifts in working environment that are most likely to affect safety, and (iii) changes in operational context or design evolution with respect to the safety analysis. Some work has been done on these subjects, but to the best of this author's knowledge, not in the context of the design of a launch vehicle other than the Space Shuttle.

### 6.2.5 Regulations and Range Safety Standards

The author found that regulatory requirements and range safety standards, such EWR 127-1, could be easily linked to unsafe control actions identified in step 1 of the FSS safety analysis. However, many of these regulations and requirements do not address requirements or design errors. EWR 127-1 in particular focuses on component failures and is insufficient to identify and diagnose design flaws. Furthermore, none of these regulations or standards include identification of leading indicators of safety issues. Results of all tests and mishaps are required to be recorded and reported, but leading indicators of safety that do not lead to a mishap are not addressed. Generating causal scenarios for the FSS safety analysis provided in Appendix A – Flight Safety System STPA Step 1 would give further insight into the completeness of these regulations and standards and may generate recommendations for improving those regulations.

This Page Intentionally Left Blank

# REFERENCES


[1] N. G. Leveson, Engineering a Safer World, Cambridge, MA, USA: The MIT Press, 2011.

[2] F. Frola and C. Miller, *System safety in aircraft management,* Washington, DC, USA: Logistics Management Institute, 1984.

[3] R. J. Duphily, "Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide," The Aerospace Corporation, El Segundo, CA, 2009.

[4] Department of Defense, *MIL-STD-882E System Safety,* 2012.

[5] H. Pentti and H. Atte, "Failure Mode and Effects Analysis of Software-Based Automation Systems," The Radiation and Nuclear Safety Authority, Helsinki, Finland, 2002.

[6] *Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA),* Geneva: International Electrotechnical Commission, 2006.

[7] NASA, "Methodology for Conduct of Project Constellation Hazard Analyses," Houston, TX, USA, 2006.

[8] N. G. Leveson and J. P. Thomas, "STPA Handbook," Cambridge, MA, USA, 2018.

[9] H. Koenigsmann, *Smallsat Symposium Keynote Address,* Mountain View, CA, USA, 2018.

[10] AST-1, "AC 431.35-2A Reusable Launch and Reentry Vehicle Systems Safety Process," U.S. Department of Transportation Federal Aviation Administration Office of Commercial Spacec Transportation, Washington, D.C., USA, 2005.

[11] N. G. Leveson, "Evaluating Accident Models using Recent Aerospace Accidents," Massachusetts Institute of Technology, Cambridge, MA, USA, 2001.

[12] J. M. Haber, "Launch and reentry safety objectives," *The Journal of Space Safety Engineering,* vol. 4, no. 1, pp. 22-28, 2017.

[13] Transportation Systems Center and United States Office of Commercial Space Transportation, Licensing Program Division, "Hazard Analysis of Commercial Space Transportation," U.S.

Department of Transportation, Office of Commercial Space Transportation, Licensing Programs Division, Washington, DC, USA, 1995.

[14] S. Hope, "Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry," Concawe, The Hauge, Netherlands, 1982.

[15] N. G. Leveson, An STPA Primer, 1 ed., Cambridge, MA, USA: MIT Partnership for a Systems Approach to Safety, 2015.

[16] A. Richard, "A Qualitative Comparative Analysis of STAMP and SOAM in ATM Occurrence Investigation," Lund University, Lund, Sweden, 2008.

[17] S. D. Ito, "Assuring Safety in High-Speed Magnetically Levitated (Maglev) Systems.," Cambridge, MA, USA, 2008.

[18] J. Thomas, "Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis," Cambridge, MA, USA, 2013.

[19] N. G. Leveson, "Technical and Managerial Factors in the NASA Challenger and Columbia Losses: Looking Forward to the Future," *Controversies in Science and Technology,* vol. 2, 2008.

[20] T. Ishimatsu, N. G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto and H. Nakao, "Modeling and Hazard Analysis Using STPA," in *Proceedings of the 4th Conference of the International Association for the Advancement of Space Safety*, Huntsville, AL, USA, 2010.

[21] H. Nakao, M. Katahira, Y. Miyamoto and N. G. Leveson, *Safety Guided Design of Crew Return Vehicle in Concept Design Phase using STAMP/STPA,* 2011.

[22] A. Scarinci, F. X. de Oliveira, R. Moraes, A. I. Quilici, D. Patrick and D. da Costa Ribeiro, "A Complete STPA Application to the Air Management System of Embraer Regional Jets Family," in *MIT STAMP Workshop*, Cambridge, MA, USA, 2017.

[23] E. Howard, K. Belvin, S. Murray, L. Juhnke, L. Hettinger and M. France, "STAMP In Workplace Safety," in *MIT STAMP Workshop*, Cambridge, MA, USA, 2017.

[24] N. C. Dunn, "Satellite System Safety Analysis Using STPA," Cambridge, MA, USA, 2011.

[25] C. H. Fleming and N. G. Leveson, "Improving Hazard Analysis and Certification of Integrated Modular Avionics," *Journal of Aerospace Information Systems,* vol. 11, no. 6, 2014.

[26] B. D. Owens and A. R. Crocker, "SimSup's Loop: A control theory approach to spacecraft operator training," in *Aerospace Conference, 2015 IEEE*, Big Sky, MT, USA, 2015.

[27] S. J. Pereira, G. Lee and J. Howard, "A System-Theretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System," in *Proceedings of the 2006 AIAA Missile Sciences Conference*, Monterey, CA, 2006, 2006.

[28] J. Thomas, *Systems Theoretic Process Analysis Tutorial v9,* Cambridge, MA, USA, 2013.

[29] N. G. Leveson, N. Dulac, B. Barrett, J. Carroll, J. Cutcher-Gershenfeld and S. Friedenthal, "Risk Analysis of NASA Independent Technical Authority," Cambridge, MA, USA, 2005.

[30] C. H. Fleming, "Safety-Driven Early Concept Analysis and Development," Cambridge, MA, USA, 2015.

[31] B. D. Owens, M. S. Herring, N. Dulac, N. G. Leveson, M. D. Ingham and K. A. Weiss, "Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission," in *IEEE Aerospace Conference*, Big Sky, MT, USA, 2008.

[32] A. J. Ball, "Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development," Cambridge, MA, USA, 2015.

[33] Arianespace, "Résultats de la Commission d'Enquête Indépendante concernant la déviation de trajectoire observée lors de la mission VA241," Évry, France, 2018.

[34] Spaceflight101, "Ariane 5 VA241 Anomaly Analysis," 26 January 2018. [Online]. Available: http://spaceflight101.com/ariane-5-va241/ariane-5-va241-anomaly-analysis/. [Accessed 24 February 2018].

[35] J. L. Lions, "Ariane 5 Flight 501 Failure Report by the Inquiry Board," Paris, France, 1996.

[36] J. G. Pavlovich, "Formal Report of the Investigation of the 30 April 1999 Titan IV B/Centaur TC-14/Milstar-3 (B32)," U.S. Air Force, 1999.

[37] Arianespace, "Soyuz Flight VS09: Independent Inquiry Board announces definitive conclusions concerning the Fregat upper stage anomaly," Paris, France, 2014.

[38] P. B. de Selding, "Soyuz Team Takes Steps To Prevent Repeat of Galileo Launch Failure, including the Premature Celebration," SpaceNews, Paris, France, 2014.

[39] M. Bodner, "Russian looks past Soyuz-2 failure to Soyuz-5," *SpaceNews,* 6 December 2017.

[40] J. McDowell, "JSR Launch Vehicle Database," 28 December 2017. [Online]. Available: http://planet4589.org/space/lvdb/. [Accessed 28 February 2018].

[41] Space Exploration Technologies, "Falcon 1, Flight 3 Mission Summary," 8 August 2008. [Online]. Available: http://www.spacex.com/news/2013/02/11/falcon-1-flight-3-mission-summary. [Accessed 24 February 2018].

[42] Space Exploration Technologies, "Anomaly Updates," 2 January 2017. [Online]. Available: http://www.spacex.com/news/2016/09/01/anomaly-updates. [Accessed 24 February 2018].

[43] J. Foust, "Falcon 9 Failure Linked To Upper Stage Tank Strut," *SpaceNews,* 20 July 2015.

[44] National Aeronautics and Space Administration, "SpaceX CRS-7 Accident Investigation Report Public Summary," 2018.

[45] NASA Independent Review Team, "Orb-3 Accident Investigation Report Executive Summary," National Aeronautics and Space Administration, 2015.

[46] J. Foust, "NASA and Orbital Reach Differing Conclusions on Antares Failure," *SpaceNews,* 29 October 2015.

[47] K. Chang, "SpaceX Launches a Satellite With a Partly Used Rocket," The New York Times, 30 March 2017. [Online]. Available: https://www.nytimes.com/2017/03/30/science/spacex-launches-a-satellite-with-a-partly-used-rocket.html.

[48] K. Chang, "Falcon Heavy, in a Roar of Thunder, Carries SpaceX's Ambition Into Orbit," The New York Times, 18 February 2018. [Online]. Available: https://www.nytimes.com/2018/02/06/science/falcon-heavy-spacex-launch.html.

[49] J. Foust, "Musk unveils revised version of giant interplanetary launch system," SpaceNews, 29 September 2017. [Online]. Available: http://spacenews.com/musk-unveils-revised-version-of-giant-interplanetary-launch-system/.

[50] C. Gebhardt, "Blue Origin remains on course for 2020 debut of New Glenn heavy lift rocket," NASA Spaceflight, 10 November 2017. [Online]. Available: https://www.nasaspaceflight.com/2017/11/blue-origin-2020-debut-new-glenn-rocket/.

[51] C. Niederstrasser and W. Frick, "Small Launch Vehicles - A 2016 State of the Industry Survey," in *67th International Astronautical Congress*, Guadalajara, Mexico, 2016.

[52] A. Boyle, "Blastoff for 3-D printing: How Virgin Orbit harnesses high tech for low-cost rockets," GeekWire, 14 October 2017. [Online]. Available: https://www.geekwire.com/2017/virgin-orbit-3d-printing-rockets/.

[53] J. Foust, "Relativity Space aims to 3D print entire launch vehicles," SpaceNews, 5 December 2017. [Online]. Available: http://spacenews.com/relativity-space-aims-to-3d-print-entire-launch-vehicles/. [Accessed 19 March 2018].

[54] "Rocket Lab Reveals First Battery-Powered Rocket for Commercial Launches to Space," Rocket Lab, 31 May 2015. [Online]. Available: https://www.rocketlabusa.com/news/updates/rocket-lab-reveals-first-battery-powered-rocket-for-commercial-launches-to-space/.

[55] C. Bergin, "Virgin Galactic preparing for busy LauncherOne future," NASA Spaceflight, 30 June 2016. [Online]. Available: https://www.nasaspaceflight.com/2016/06/virgin-galactic-prepare-busy-launcherone-future/.

[56] S. Masunaga, "In the latest twist for space start-ups, a rocket roars off a country road in Georgia," *Los Angeles Times,* 4 August 2017.

[57] R. C. Booton and S. Ramo, "The Development of Systems Engineering," *IEEE Transactions on Aerospace and Electronic Systems,* Vols. AES-20, no. 4, pp. 306-310, 1984.

[58] NASA, "NPR 7120.5E, NASA Space Flight Program and Project Management Requirements," 2011.

[59] O. L. de Weck, "Fundamentals of Systems Engineering," MIT OpenCourseWare, Cambridge, MA, 2015.

[60] N. G. Leveson, "Safeware: System Safety and Computers," Addison-Wessley, 1995.

[61] A. Tversky and D. Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science,* vol. 185, no. 4157, pp. 1124-1131, 27 September 1974.

[62] N. Dulac and N. G. Leveson, "Incorporating Safety Risk in Early System Architecture Trade Studies," *AIAA Journal of Spacecraft and Rockets,* vol. 46, no. 2, 2009.

[63] "EWR 127-1, Eastern Western Range Safety Requirements," 1999.

[64] W. Young, "A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Against Cyber Disruptions," Cambridge, MA, USA, 2017.

[65] B. C. Paulson, "Designing to Reduce Construction Costs," *Journal of the Construction Division,* vol. 102, no. 4, pp. 587-592, 1976.

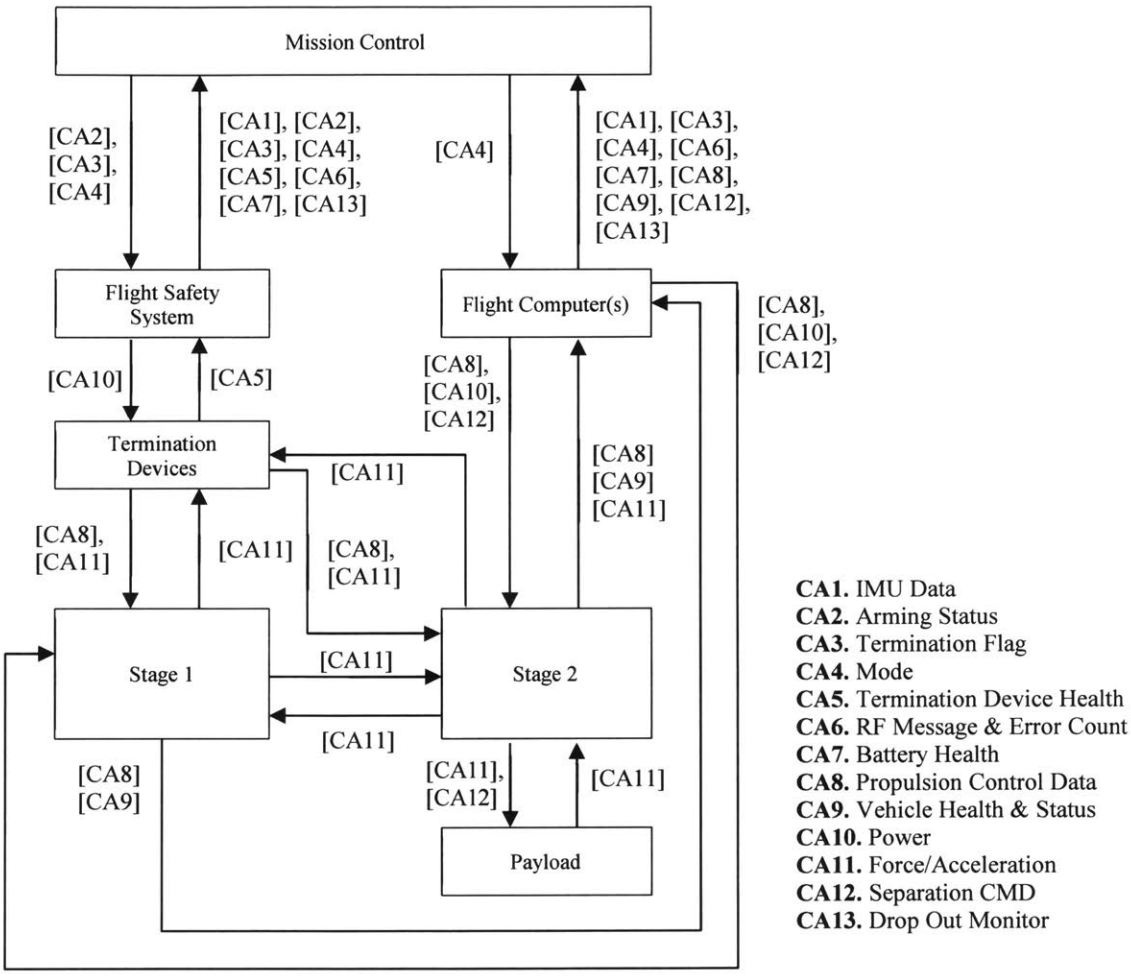
[66] J. Blair, R. Ryan, L. Schutzenhofer and W. Humphries, "NASA/TP-2001-210992. Launch Vehicle Design Process: Characterization, Technical Integration, and Lessons Learned," National Aeronautics and Space Administration, MSFC, Alabama, USA, 2001.

[67] S. R. Hirshorn, "NASA Systems Engineering Handbook, NASA/SP-2016-6104 Rev 2," National Aeronautics and Space Administration, Washington, DC, USA, 2016.

[68] F. Crawley, M. Preston and B. Tyler, Hazop: Guide to Best Practice: Guidelines to Best Practice for the Process and Chemical Industries, Inst. of Chemical Enigneers, 2008.

# APPENDIX A – FLIGHT SAFETY SYSTEM STPA STEP 1

## SAFETY CONTROL STRUCTURE




**CA1.** IMU Data
**CA2.** Arming Status
**CA3.** Termination Flag
**CA4.** Mode
**CA5.** Termination Device Health
**CA6.** RF Message & Error Count
**CA7.** Battery Health
**CA8.** Propulsion Control Data
**CA9.** Vehicle Health & Status
**CA10.** Power
**CA11.** Force/Acceleration
**CA12.** Separation CMD
**CA13.** Drop Out Monitor

## UNSAFE CONTROL ACTIONS

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Safety System | FSS provides power to termination devices [CA10] | **UCA1:** FSS does not provide power to termination devices when termination flag is active and SAD is armed [H3] [H7]<br><br>**UCA2:** FSS does not provide power to termination devices when vehicle approaches flight corridor boundary during launch [H3]<br><br>**UCA3:** FSS does not provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy during launch [H7] | **UCA4:** FSS provides power to termination devices when termination flag is not active [H7]<br><br>**UCA5:** FSS provides power to termination devices when SAD is unarmed or safed [H7]<br><br>**UCA6:** FSS provides power to ordnance termination devices when in test mode [H7]<br><br>**UCA7:** FSS provides power to termination devices when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [H7]<br><br>**UCA8:** FSS provides power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [H3] [H7] | **UCA9:** FSS provides power to termination devices out of order [H7]<br><br>**UCA10:** FSS provides power to termination devices too late (> TBD seconds from receipt of termination flag) [H7] | **UCA11:** FSS stops providing power to termination devices before termination is complete [H3] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Mission Control | Mission Control provides arming status to FSS [CA2] | **UCA12:** Mission control does not provide arm command to FSS before launch [H3]<br><br>**UCA13:** Mission control does not provide safe command to FSS during ground operations and test prior to liftoff [H7] | **UCA14:** Mission control provides arm command during manned ground operations and non-armed test prior to liftoff [H7]<br><br>**UCA15:** Mission control provides safe command to FSS during launch [H3] | **UCA16:** Mission control provides safe command to FSS before vehicle no longer poses viable threat to people or property [H7] | N/A |
| Mission Control | Mission control provides termination flag to FSS [CA3] | **UCA17:** Mission control does not provide termination flag to FSS when vehicle approaches flight corridor boundary [H3]<br><br>**UCA18:** Mission control does not provide termination flag to FSS when vehicle experiences catastrophic uncontrolled release of energy [H7] | **UCA19:** Mission control provides termination flag to FSS when resulting debris and energy may contact humans, public property, or launch facility [H7]<br><br>**UCA20:** Mission control provides termination flag to FSS when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [H7] | **UCA21:** Mission control provides termination flag to FSS during pre-launch testing with live termination mechanisms [H7]<br><br>**UCA22:** Mission control provides termination flag to FSS when vehicle altitude >TBD [H7]<br><br>**UCA23:** Mission control provides termination flag to FSS before fill/drain operations of energetic material has begun [H7] | **UCA24:** Mission control stops providing termination flag to FSS before termination flag received [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Mission Control | Mission control provides mode to FSS [CA4] | **UCA25:** Mission control does not provide active mode to FSS during terminal count [H3] | **UCA26:** Mission control provides active mode to FSS during ground operations and non-active test [H7]<br><br>**UCA27:** Mission control provides a non-External Power mode command to FSS during ground operations and test [H7]<br><br>**UCA28:** Mission control provides a mode that cancels termination once termination has been received [H3] [H7] | **UCA29:** Mission control provides active mode to FSS before terminal count [H7] | **UCA30:** Mission control stops providing mode to FSS before FSS is disabled [H7] |
| Stage 1 | Stage 1 provides force/acceleration to FSS [CA11] | **UCA31:** Stage 1 does not provide >TBD acceleration to FSS during liftoff [H7] | **UCA32:** Stage 1 provides >TBD quasi-static acceleration to FSS during launch [H7] [H3]<br><br>**UCA33:** Stage 1 provides excessive (TBD) dynamic or shock acceleration to FSS during launch [H7] [H3] | **UCA34:** Stage 1 provides TBD acceleration to FSS prior to liftoff [H7] [H3]<br><br>**UCA35:** Stage 1 provides excessive force (blast, debris, etc.) to FSS before termination [H7] | **UCA36:** Stage 1 provides excessive force (blast, debris, etc.) to FSS during termination [H7] [H3] |
| Flight Safety System | FSS provides IMU data to Mission Control [CA1] | **UCA37:** FSS does not provide IMU data to Mission Control during launch [H3] | **UCA38:** FSS provides incorrect or delayed IMU data to Mission Control during launch [H3] | N/A | N/A |
| Flight Safety System | FSS provides Arming Status to Mission Control [CA2] | **UCA39:** FSS does not provide Arming Status to Mission Control during pre-launch or launch [H7] | **UCA40:** FSS provides incorrect or delayed Arming Status to Mission Control during pre-launch, launch, orbit, or reentry [H7] | N/A | N/A |
| Flight Safety System | FSS provides Termination Flag to Mission Control [CA3] | **UCA41:** FSS does not provide Termination Flag to Mission Control when Termination Flag is active [H3] [H7] | **UCA42:** FSS provides incorrect or delayed Termination Flag to Mission Control during launch [H3] [H7] | N/A | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Safety System | FSS provides Mode to Mission Control [CA4] | **UCA43:** FSS does not provide Mode to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8]<br><br>**UCA44:** FSS does not provide Mode to Mission Control before FSS is disabled [H7] [H3] | **UCA45:** FSS provides incorrect or delayed Mode to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8] | N/A | N/A |
| Flight Safety System | FSS provides Termination Device Health to Mission Control [CA5] | N/A | **UCA46:** FSS provides incorrect, missing, or delayed Termination Device Health to Mission Control during pre-launch [H7] [H8] | N/A | N/A |
| Flight Safety System | FSS provides RF Message & Error to Mission Control [CA6] | **UCA47:** FSS does not provide RF Link Message to Mission Control during pre-launch or launch [H7] [H3] [H8]<br><br>**UCA48:** FSS does not provide RF Error Count to Mission Control during pre-launch or launch [H7] [H8] | **UCA49:** FSS provides incorrect RF Link Message to Mission Control during pre-launch or launch [H7] [H3] [H8]<br><br>**UCA50:** FSS provides incorrect RF Error Count to Mission Control during pre-launch or launch [H7] [H8] | N/A | N/A |
| Flight Safety System | FSS provides Battery Health to Mission Control [CA7] | **UCA51:** FSS does not provide Battery Health to Mission Control during pre-launch or launch [H7] [H3]<br><br>**UCA52:** FSS does not provide Battery Health to Mission Control before FSS is disabled [H7] [H3] | **UCA53:** FSS provides incorrect or delayed Battery Health to Mission Control during pre-launch or launch [H7] [H3] | N/A | N/A |
| Flight Safety System | FSS provides Umbilical Drop Out Monitor to Mission Control [CA13] | **UCA54:** FSS does not provide Umbilical Drop Out Monitor to Mission Control [H7] [H3] [H8] | **UCA55:** FSS provides incorrect or delayed Umbilical Drop Out Monitor to Mission Control [H7] [H3] [H8] | **UCA56:** FSS provides Umbilical Drop Out Monitor to Mission Control late (>TBD seconds from liftoff) [H7] [H3] [H8] | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Mission Control | Mission Control provides Mode to Flight Computers [CA4] | **UCA57:** Mission Control does not handover vehicle control to Flight Computers before liftoff [H8] | **UCA58:** Mission Control provides BIT mode to Flight Computers during launch [H7] [H3] [H6] | N/A | N/A |
| Flight Computers | Flight Computers provide IMU data to Mission Control [CA1] | **UCA59:** Flight Computers do not provide IMU data to Mission Control during launch, orbit, and reentry [H3] [H4] | **UCA60:** Flight Computers provide incorrect or delayed IMU data to Mission Control during launch [H7] [H3] [H6] | N/A | N/A |
| Flight Computers | Flight Computers provide Termination Flag to Mission Control [CA3] | **UCA61:** Flight Computers do not provide Termination Flag status to Mission Control during pre-launch or launch [H7] [H3] [H8] | **UCA62:** Flight Computers provide incorrect or delayed Termination Flag status to Mission Control during pre-launch or launch [H7] [H3] [H8] | N/A | **UCA63:** Flight Computers stop sending Termination Flag status to Mission Control before received by Mission Control [H7] [H3] [H8] |
| Flight Computers | Flight Computers provide Mode to Mission Control [CA4] | **UCA64:** Flight Computers do not provide Flight Computer mode or health status to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8] | **UCA65:** Flight Computers provide incorrect or delayed Flight Computer mode or health status to Mission Control during pre-launch, launch, orbit, or reentry [H7] [H3] [H8] | N/A | **UCA66:** Flight computers stop providing Flight Computer mode before received by Mission Control [H7] [H3] |
| Flight Computers | Flight Computers provide RF Message & Error Count to Mission Control [CA6] | **UCA67:** Flight Computers do not provide RF Link Message to Mission Control during pre-launch or launch [H7] [H3] [H8]<br><br>**UCA68:** Flight Computers do not provide RF Error Count to Mission Control during pre-launch or launch [H7] [H8] | **UCA69:** FSS provides incorrect or delayed RF Link Message to Mission Control during pre-launch or launch [H7] [H3] [H8]<br><br>**UCA70:** FSS provides incorrect or delayed RF Error Count to Mission Control during pre-launch or launch [H7] [H8] | N/A | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Computers | Flight Computers provide Battery Health to Mission Control [CA7] | **UCA71:** Flight Computers do not provide Battery Health to Mission Control during pre-launch, launch, orbit, or reentry [H3] [H4] [H7] [H8] | **UCA72:** Flight Computers provide incorrect or delayed Battery Health to Mission Control during pre-launch, launch, orbit, or reentry [H3] [H4] [H7] [H8] | N/A | N/A |
| Flight Computers | Flight Computers provide Propulsion Control Data to Mission Control [CA8] | **UCA73:** Flight Computers do not provide Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [H2] [H3] [H4] [H7] [H8] | **UCA74:** Flight Computers provide incorrect Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [H2] [H3] [H4] [H7] [H8] | **UCA75:** Flight Computers provide delayed Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [H2] [H3] [H4] [H7] [H8] | N/A |
| Flight Computers | Flight Computers provide Vehicle Health & Status to Mission Control [CA9] | **UCA76:** Flight Computers do not provide Vehicle Health & Status to Mission Control during pre-launch, launch, orbit, or reentry [H2] [H3] [H4] [H7] [H8] | **UCA77:** Flight Computers provide incorrect Vehicle Health & Status to Mission Control during pre-launch, launch, orbit, or reentry [H2] [H3] [H4] [H7] [H8] | **UCA78:** Flight Computers provide delayed Vehicle Health & Status to Mission Control during pre-launch, launch, orbit, or reentry [H2] [H3] [H4] [H7] [H8] | N/A |
| Flight Computers | Flight Computers provide Separation CMD to Mission Control [CA12] | **UCA79:** Flight Computers do not provide stage separation command flag to Mission Control once commanded [H6]<br><br>**UCA80:** Flight Computers do not provide fairing separation command flag to Mission Control once commanded [H6]<br><br>**UCA81:** Flight Computers do not provide payload separation command flag to Mission Control once commanded [H6] | **UCA82:** Flight Computers provide incorrect or delayed stage separation confirmation to Mission Control [H6]<br><br>**UCA83:** Flight Computers provide incorrect or delayed fairing separation confirmation to Mission Control [H6]<br><br>**UCA84:** Flight Computers provide incorrect or delayed payload separation confirmation to Mission Control [H6] | **UCA85:** Flight Computers provide stage separation confirmation to Mission Control before stage separation has been confirmed [H6]<br><br>**UCA86:** Flight Computers provide fairing separation confirmation to Mission Control before fairing separation has been confirmed [H6]<br><br>**UCA87:** Flight Computers provide payload separation confirmation to Mission Control before payload separation has been confirmed [H6] | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Computers | Flight Computers provide Drop Out Monitor to Mission Control [CA13] | **UCA88:** Flight Computers do not provide Umbilical Drop Out to Mission Control when umbilical connection is lost [H6] | **UCA89:** Flight Computers provide incorrect or delayed Umbilical Drop Out to Mission Control [H6] | N/A | N/A |
| Flight Computers | Flight Computers provide Propulsion Control Data to Stage 1 [CA8] | **UCA90:** Flight Computers do not provide liftoff commands to Stage 1 [H4] [H8]<br><br>**UCA91:** Flight Computers do not provide thrust vector information to Stage 1 [H3] [H4]<br><br>**UCA92:** Flight Computers do not provide propulsion shutdown commands to Stage 1 [H3] [H4] [H7]<br><br>**UCA93:** Flight Computers do not provide pressure or valve controls to Stage 1 [H3] [H4] [H7]<br><br>**UCA94:** Flight Computers do not provide shutdown commands to Stage 1 before propellant below TBD level [H7] | **UCA95:** Flight Computers provide liftoff commands to Stage 1 during pre-launch [H7]<br><br>**UCA96:** Flight Computers provide incorrect or delayed thrust vector information to Stage 1 [H3] [H4] [H7]<br><br>**UCA97:** Flight Computers provide incorrect or delayed pressure or valve set points to Stage 1 [H3] [H4] [H7]<br><br>**UCA98:** Flight Computers provide incorrect or delayed throttle to Stage 1 [H5] [H2]<br><br>**UCA99:** Flight Computers provide startup or excessive purge to Stage 1 propulsion during or shortly after stage separation [H2] [H4] [H7] | **UCA100:** Flight Computers provide startup to Stage 1 after liftoff [H3] [H4] [H7]<br><br>**UCA101:** Flight Computers provide shutdown to Stage 1 too early (>TBD seconds before performance target reached) [H2]<br><br>**UCA102:** Flight Computers provide shutdown to Stage 1 too late (>TBD seconds after performance target reached) [H2] | **UCA103:** Flight Computers provide purge, pressurization, or vent commands to Stage 1 too long [H3] [H4] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Computers | Flight Computers provide Power to Stage 1 [CA10] | **UCA104:** Flight Computers do not provide sufficient Power to Stage 1 components [H2] [H4] [H7] | **UCA105:** Flight Computers provide excessive Power (>TBD) to Stage 1 components [H2] [H4] [H7]<br><br>**UCA106:** Flight Computers provide intermittent Power to Stage 1 components [H2] [H4] [H7] | **UCA107:** Flight Computers provide power to Stage 1 components too early (>TBD seconds before liftoff) [H8] [H7] | **UCA108:** Flight Computers stop providing power to Stage 1 components during pre-launch and launch [H2] [H4] [H7]<br><br>**UCA109:** Flight Computers provide power to Stage 1 components too long [H2] [H4] [H7] |
| Flight Computers | Flight Computers provide Separation Command to Stage 1 [CA12] | **UCA110:** Flight Computers do not provide stage separation command during scheduled stage separation [H6] | **UCA111:** Flight Computers provide stage separation command during pre-launch or stage 1 launch [H6] | **UCA112:** Flight Computers provide stage separation command before Stage 1 thrust below TBD [H2] [H4] [H6] [H7]<br><br>**UCA113:** Flight Computers provide stage separation command too late (>TBD seconds after timed separation) [H4] [H5] | **UCA114:** Flight Computers stop providing stage separation command before stage separation is complete [H2] [H4] [H6] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Computers | Flight Computers provide Propulsion Control Data to Stage 2 [CA8] | **UCA115:** Flight Computers do not provide startup commands to Stage 2 [H4] [H5]<br><br>**UCA116:** Flight Computers do not provide thrust vector information to Stage 2 [H3] [H4] [H5]<br><br>**UCA117:** Flight Computers do not provide propulsion shutdown commands to Stage 2 [H3] [H4] [H5] [H7]<br><br>**UCA118:** Flight Computers do not provide pressure or valve controls to Stage 2 [H3] [H4] [H7]<br><br>**UCA119:** Flight Computers do not provide body rates to Stage 2 RCS [H3] [H4] [H7]<br><br>**UCA120:** Flight Computers do not provide shutdown commands to Stage 2 before propellant level is below TBD [H7] | **UCA121:** Flight Computers provide startup commands to Stage 2 during pre-launch or Stage 1 burn [H7] [H2]<br><br>**UCA122:** Flight Computers provide incorrect or delayed thrust vector information to Stage 2 [H3] [H4] [H7]<br><br>**UCA123:** Flight Computers provide incorrect or delayed pressure or valve set points to Stage 2 [H3] [H4] [H5] [H7]<br><br>**UCA124:** Flight Computers provide incorrect or delayed throttle to Stage 2 propulsion [H5] [H2]<br><br>**UCA125:** Flight Computers provide incorrect or delayed RCS control during payload separation [H1] [H6] | **UCA126:** Flight Computers provide startup commands to Stage 2 >TBD seconds before stage separation [H3] [H4] [H7]<br><br>**UCA127:** Flight Computers provide shutdown commands to Stage 2 too early (>TBD seconds before performance target reached) [H2]<br><br>**UCA128:** Flight Computers provide shutdown commands to Stage 2 too late (>TBD seconds after performance target reached) [H2] | N/A |
| Flight Computers | Flight Computers provide Power to Stage 2 [CA10] | **UCA129:** Flight Computers do not provide sufficient Power to Stage 2 components [H2] [H4] [H7] | **UCA130:** Flight Computers provide excessive (>TBD) Power to Stage 2 components [H2] [H4] [H7]<br><br>**UCA131:** Flight Computers provide intermittent Power to Stage 2 components [H2] [H4] [H7] | **UCA132:** Flight Computers provide Power to Stage 2 components too early (>TBD seconds before liftoff) [H8] [H7] | **UCA133:** Flight Computers stop providing power to Stage 2 components [H2] [H4] [H7]<br><br>**UCA134:** Flight Computers provide power to Stage 2 components too long (>TBD) or too many cycles [H2] [H4] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Flight Computers | Flight Computers provide Separation Command to Stage 2 [CA12] | **UCA135:** Flight Computers do not provide fairing separation command during scheduled fairing separation [H6]<br><br>**UCA136:** Flight Computers do not provide payload separation command during scheduled payload separation [H6] [H5] | **UCA137:** Flight Computers provide fairing separation command during pre-launch, Stage 1 launch, or stage separation [H6] | **UCA138:** Flight Computers provide payload separation command before Stage 2 thrust below TBD [H2] [H4] [H6] [H7]<br><br>**UCA139:** Flight Computers provide fairing separation command too late (>TBD seconds after separation command) [H4] [H5]<br><br>**UCA140:** Flight Computers provide fairing separation command when fairing pressure >TBD psi [H2] [H4] [H6] [H7]<br><br>**UCA141:** Flight Computers provide payload separation command too early (<TBD seconds before fairing separation) [H2] [H4] [H6] [H7] | **UCA142:** Flight Computers stop providing fairing separation command before fairing separation is complete [H2] [H4] [H6] [H7]<br><br>**UCA143:** Flight Computers stop providing payload separation command before payload separation is complete [H2] [H4] [H6] [H7] |
| Stage 2 | Stage 2 provides Propulsion Data to Flight Computers [CA8] | **UCA144:** Stage 2 does not provide propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | **UCA145:** Stage 2 provides incorrect or intermittent propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | **UCA146:** Stage 2 provides delayed propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | N/A |
| Stage 2 | Stage 2 provides Vehicle Health & Status to Flight Computers | **UCA147:** Stage 2 does not provide Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | **UCA148:** Stage 2 provides incorrect or intermittent Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | **UCA149:** Stage 2 provides delayed Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | N/A |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Stage 2 | Stage 2 provides Force/Acceleration to Flight Computer(s) | **UCA150:** Stage 2 does not provide sufficient force to Flight Computer(s) to maintain mechanical or electrical connections [H3] [H4] [H5] [H6] [H7] [H8] | **UCA151:** Stage 2 provides excessive force or acceleration to Flight Computer(s) [H3] [H4] [H5] [H6] [H7] | N/A | **UCA152:** Stage 2 provides force or acceleration greater than TBD to Flight Computer(s) >TBD seconds [H3] [H4] [H5] [H6] [H7] |
| Stage 1 | Stage 1 provides Propulsion Data to Flight Computers [CA8] | **UCA153:** Stage 1 does not provide propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | **UCA154:** Stage 1 provides incorrect or intermittent propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | **UCA155:** Stage 1 provides delayed propulsion sensor data to Flight Computers [H2] [H4] [H7] [H8] | N/A |
| Stage 1 | Stage 1 provides Vehicle Health & Status to Flight Computers [CA9] | **UCA156:** Stage 1 does not provide Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | **UCA157:** Stage 1 provides incorrect or intermittent Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | **UCA158:** Stage 1 provides delayed Vehicle Health & Status data to Flight Computers [H2] [H4] [H7] [H8] | N/A |
| Stage 2 | Stage 2 provides Force/Acceleration to Payload [CA11] | **UCA159:** Stage 2 does not provide sufficient force to Payload to maintain mechanical or electrical connections [H1] [H2] [H4] [H5] [H6] [H7] | **UCA160:** Stage 2 provides excessive Force/Acceleration to Payload [H1] [H2] [H4] [H5] [H6] [H7]<br><br>**UCA161:** Stage 2 provides contact force to Payload after payload separation [H1] [H2] [H4] [H5] [H6] [H7] | N/A | **UCA162:** Stage 2 provides force or acceleration to Payload too long/too many cycles [H1] [H2] [H4] [H5] [H6] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Stage 2 | Stage 2 provides Separation CMD to payload [CA12] | **UCA163:** Stage 2 does not provide separation command to Payload [H5] [H6] | **UCA164:** Stage 2 provides separation command to Payload during pre-launch or launch [H1] [H5] [H7] [H6] | **UCA165:** Stage 2 provides separation command to Payload before Stage 2 thrust <TBD [H1] [H5] [H7]<br><br>**UCA166:** Stage 2 provides payload separation command too late (>TBD seconds after target separation time reached) [H5]<br><br>**UCA167:** Flight Computers provide payload separation command too early (>TBD seconds before target separation time is reached) [H5] | **UCA168:** Stage 2 stops providing separation command to Payload before Payload has separated [H5] |
| Stage 2 | Stage 2 provides Force/Acceleration to Stage 1 [CA11] | **UCA169:** Stage 2 does not provide sufficient force to maintain mechanical or electrical connections to Stage 1 during pre-launch and launch [H2] [H6] [H7] | **UCA170:** Stage 2 provides excessive Force/Acceleration to Stage 1 [H2] [H6] [H7] | N/A | **UCA171:** Stage 2 provides force or acceleration to Stage 1 too long/too many cycles [H2] [H6] [H7] |
| Stage 1 | Stage 1 provides Force/Acceleration to Stage 2 [CA11] | **UCA172:** Stage 1 does not provide sufficient force to maintain mechanical or electrical connections to Stage 2 [H2] [H6] [H7] | **UCA173:** Stage 1 provides excessive force/acceleration to Stage 2 [H2] [H6] [H7] | N/A | **UCA174:** Stage 1 provides force or acceleration to Stage 2 too long/too many cycles [H2] [H6] [H7] |
| Stage 1 | Stage 1 provides Force/Acceleration to Termination Devices [CA11] | **UCA175:** Stage 1 does not provide sufficient force to Termination Devices to maintain mechanical or electrical connections during pre-launch and launch [H7] [H3] | **UCA176:** Stage 1 provides excessive Force/Acceleration to Termination Devices [H7] [H3] | N/A | **UCA177:** Stage 1 provides Force/ Acceleration to Termination Devices too long/too many cycles [H3] [H6] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Stage 2 | Stage 2 provides Force/Acceleration to Termination Devices [CA11] | **UCA178:** Stage 2 does not provide sufficient force to Termination Devices to maintain mechanical or electrical connections during pre-launch and launch [H7] [H3] | **UCA179:** Stage 2 provides excessive Force/Acceleration to Termination Devices [H7] [H3] | N/A | **UCA180:** Stage 2 provides Force/ Acceleration to Termination Devices too long/too many cycles [H3] [H6] [H7] |
| Termination Devices | Termination Devices provide Propulsion Control Data to Stage 1 [CA8] | **UCA181:** Termination Devices do not stop Stage 1 thrust during termination [H3] [H7] | **UCA182:** Termination Devices provide Stage 1 thrust termination when Termination Flag is not active [H7] | N/A | **UCA183:** Termination Devices stop terminating Stage 1 thrust before thrust below TBD [H3] [H7] |
| Termination Devices | Termination Devices provide Force/Acceleration to Stage 1 [CA11] | **UCA184:** Termination Devices do not provide sufficient Force/Acceleration to Stage 1 to send vehicle and payload debris on safe ballistic trajectory [H3]<br><br>**UCA185:** Termination Devices do not provide sufficient Force/Acceleration to Stage 1 to distribute and burn propellants [H7]<br><br>**UCA186:** Termination Devices do not provide sufficient Force/Acceleration to Stage 1 to depressurize pressurized vessels within flight corridor [H7] | **UCA187:** Termination Devices provide sufficient Force/Acceleration to Stage 1 to detonate propellants [H7]<br><br>**UCA188:** Termination Devices provide sufficient Force/Acceleration to Stage 1 to accelerate debris beyond flight corridor or safed area at launch pad [H3] [H7] | **UCA189:** Termination Devices provide Force/Acceleration to Stage 1 before Stage 2 is terminated [H3]<br><br>**UCA190:** Termination Devices provide Force/Acceleration to Stage 1 before Stage 1 thrust is terminated [H3]<br><br>**UCA191:** Termination Devices burn or provide Force/Acceleration to Stage 1 >TBD seconds after termination [H7] | N/A |
| Termination Devices | Termination Devices provide Propulsion Control Data to Stage 2 [CA8] | **UCA192:** Termination Devices do not stop Stage 2 thrust during termination [H3] [H7] | **UCA193:** Termination Devices provide thrust termination to Stage 2 when termination flag is not active [H7] | N/A | **UCA194:** Termination Devices stop terminating Stage 2 thrust before thrust below TBD [H3] [H7] |

| Controller | Control Action | Not Providing Causes Hazard | Providing Causes Hazard | Wrong Timing or Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| Termination Devices | Termination Devices provide Force/Acceleration to Stage 2 [CA11] | **UCA195:** Termination Devices do not provide sufficient Force/Acceleration to Stage 2 to send vehicle and payload debris on safe ballistic trajectory [H3]<br><br>**UCA196:** Termination Devices do not provide sufficient Force/Acceleration to Stage 2 to distribute and burn propellants [H7] | **UCA197:** Termination Devices provide sufficient Force/Acceleration to Stage 2 to detonate propellants [H7]<br><br>**UCA198:** Termination Devices provide sufficient Force/Acceleration to Stage 2 to accelerate debris beyond flight corridor or uninhabited area at launch pad [H3] [H7]<br><br>**UCA199:** Termination Devices provide termination Force/Acceleration to Stage 2 when altitude >TBD [H7] | **UCA200:** Termination Devices provide Force/Acceleration to Stage 2 before Stage 1 is terminated [H3]<br><br>**UCA201:** Termination Devices provide Force/Acceleration to Stage 2 before Stage 2 thrust is terminated [H3]<br><br>**UCA202:** Termination Devices burn or provide Force/Acceleration to Stage 2 >TBD seconds after termination [H7] | N/A |
| Payload | Payload provides Force/Acceleration to Stage 2 [CA11] | **UCA203:** Payload does not provide sufficient Force/Acceleration to Stage 2 to maintain mechanical or electrical contact during pre-launch, launch and orbit [H2] [H7] | **UCA204:** Payload provides excessive Force/Acceleration to Stage 2 [H1] [H2] [H7] | **UCA205:** Payload contacts Stage 2 after separation [H1] [H2] [H7] | N/A |

## SAFETY CONSTRAINTS

**SC1:** FSS must provide power to termination devices when termination flag is active and SAD is armed [UCA1]

**SC2:** FSS must provide power to termination devices when vehicle approaches flight corridor boundary during launch [UCA2]

**SC3:** FSS must provide power to termination devices when vehicle experiences catastrophic uncontrolled release of energy during launch [UCA3]

**SC4:** FSS must not provide power to termination devices when termination flag is not active [UCA4]

**SC5:** FSS must not provide power to termination devices when SAD is unarmed/safed [UCA5]

**SC6:** FSS must not provide power to ordnance termination devices when in test mode [UCA6]

**SC7:** FSS must not provide power to termination devices when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA7]

**SC8:** FSS must not provide power to termination devices when resulting debris and energy may contact humans, public property, or launch facility [UCA8]

**SC9:** FSS must not provide power to termination devices out of order [UCA9]

**SC10:** FSS must not provide power to termination devices >TBD seconds from receipt of termination flag [UCA10]

**SC11:** FSS must not stop providing power to termination devices before termination is complete [UCA11]

**SC12:** Mission Control must provide ARM command to FSS before launch [UCA12] and during ground operations and test prior to liftoff [UCA13]

**SC13:** Mission Control must not provide ARM command during manned ground operations and non-armed test prior to liftoff [UCA14]

**SC14:** Mission Control must not provide SAFE command to FSS during launch [UCA15] or before vehicle no longer poses viable threat to people or property [UCA16]

**SC15:** Mission Control must provide termination flag to FSS when vehicle approaches flight corridor boundary [UCA17]

**SC16:** Mission Control must provide termination flag to FSS when vehicle experiences catastrophic uncontrolled release of energy [UCA18]

**SC17:** Mission Control must not provide termination flag to FSS when resulting debris and energy may contact humans, public property, or launch facility [UCA19]

**SC18:** Mission Control must not provide termination flag to FSS when vehicle is within flight corridor boundary and is not releasing or about to release uncontrolled energy [UCA20]

**SC19:** Mission Control must not provide termination flag to FSS during pre-launch testing with live termination mechanisms [UCA21]

**SC20:** Mission Control must not provide termination flag to FSS when vehicle altitude >TBD [UCA22]

**SC21:** Mission Control must not provide termination flag to FSS before fill/drain operations of energe3ic material has begun [UCA24]

**SC22:** Mission Control must not stop providing termination flag to FSS before termination flag received [UCA24]

**SC23:** Mission Control must provide active mode to FSS during terminal count [UCA25]

**SC24:** Mission Control must not provide active mode to FSS during ground operations and non-active test [UCA26]

**SC25:** Mission Control must not provide a non-External Power mode command to FSS during ground operations and test [UCA27]

**SC26:** Mission Control must not cancel termination once termination has been received [UCA28]

**SC27:** Mission Control must not provide active mode to FSS before terminal count [UCA29]

**SC28:** Mission Control must not stop providing mode to FSS before FSS is disabled [UCA30]

**SC29:** Stage 1 must provide >TBD acceleration to FSS during liftoff [UCA31]

**SC30:** Stage1 must not provide >TBD quasi-static acceleration to FSS during launch [UCA32]

**SC31:** Stage 1 must not provide excessive (TBD) dynamic or shock acceleration to FSS during launch [UCA33]

**SC32:** Stage 1 must not provide greater than TBD acceleration to FSS prior to liftoff [UCA34]

**SC33:** Stage 1 must not provide excessive force (blast, debris, etc.) to FSS before [UCA35] or after [UCA36] termination

**SC34:** FSS must provide IMU data to Mission Control during launch [UCA37]

**SC35:** FSS must not provide incorrect or delayed IMU data to Mission Control during launch [UCA38]

**SC36:** FSS must provide Arming Status to Mission Control during pre-launch or launch [UCA39]

**SC37:** FSS must not provide incorrect or delayed Arming Status to Mission Control during pre-launch, launch, orbit, or reentry [UCA40]

**SC38:** FSS must provide Termination Flag to Mission Control when Termination Flag is active [UCA41]

**SC39:** FSS must not provide incorrect or delayed (>TBD latency) Termination Flag to Mission Control during launch [UCA42]

**SC40:** FSS must provide mode to Mission Control during pre-launch, launch, orbit, and reentry [UCA43]

**SC41:** FSS must provide mode to Mission Control before FSS is disabled [UCA44]

**SC42:** FSS must not provide incorrect or delayed mode to Mission Control during pre-launch, launch, orbit, or reentry [UCA45]

**SC43:** FSS must not provide incorrect, missing, or delayed Termination Device Health to Mission Control during pre-launch [UCA46]

**SC44:** FSS must provide RF Link Message [UCA47] and RF Error Count [UCA48] to Mission Control during pre-launch or launch

**SC45:** FSS must not provide incorrect RF Link Message [UCA49] or incorrect RF Error Count [UCA50] to Mission Control during pre-launch or launch

**SC46:** FSS must provide Battery Health to Mission Control during pre-launch or launch [UCA51] and before FSS is disabled [UCA52]

**SC47:** FSS must not provide incorrect or delayed Battery Health to Mission Control during pre-launch or launch [UCA53]

**SC48:** FSS must provide Umbilical Drop Out Monitor to Mission Control [UCA54]

**SC49:** FSS must not provide incorrect or delayed (>TBD latency) Umbilical Drop Out Monitor to Mission Control [UCA55]

**SC50:** FSS must not provide Umbilical Drop Out Monitor to Mission Control >TBD seconds from liftoff [UCA56]

**SC51:** Mission Control must handover vehicle control to Flight Computers before liftoff [UCA57]

**SC52:** Mission Control must not provide BIT mode to Flight Computers during launch [UCA58]

**SC53:** Flight Computers must provide IMU data to Mission Control during launch, orbit, and reentry [UCA59]

**SC54:** Flight Computers must not provide incorrect or delayed (>TBD latency) IMU data to Mission Control during launch [UCA60]

**SC55:** Flight Computers must provide Termination Flag status to Mission Control during pre-launch or launch [UCA61]

**SC56:** Flight Computers must not provide incorrect or delayed (>TBD latency) Termination Flag status to Mission Control during pre-launch or launch [UCA62]

**SC57:** Flight Computers must not stop sending Termination Flag status to Mission Control before received by Mission Control [UCA63]

**SC58:** Flight Computers must provide Flight Computer mode or health status to Mission Control during pre-launch, orbit, and reentry [UCA64]

**SC59:** Flight Computers must not provide incorrect or delayed (>TBD latency) Flight Computer mode or health status to Mission Control during pre-launch, launch, orbit, and reentry [UCA65]

**SC60:** Flight Computers must not stop providing Flight Computer mode before received by Mission Control [UCA66]

**SC61:** Flight Computers must provide RF Link Message [UCA67] and RF Error Count [UCA68] to Mission Control during pre-launch, launch, and orbit

**SC62:** FSS must not provide incorrect or delayed (>TBD latency) RF Link Message to Mission Control during pre-launch and launch [UCA69]

**SC63:** FSS must not provide incorrect or delayed (>TBD latency) RF Link Message to Mission Control during pre-launch and launch [UCA70]

**SC64:** Flight Computers must provide Battery Health to Mission Control during pre-launch, launch, orbit, and reentry [UCA71]

**SC65:** Flight Computers must not provide incorrect or delayed (>TBD latency) Battery Health to Mission Control during pre-launch, launch, orbit, or reentry [UCA72]

**SC66:** Flight Computers must provide Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [UCA73]

**SC67:** Flight Computers must not provide incorrect Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [UCA74]

**SC68:** Flight Computers must not provide delayed (>TBD latency) Propulsion Control Data to Mission Control during pre-launch, launch, orbit, and reentry [UCA75]

**SC69:** Flight Computers must provide Vehicle Health & Status to Mission Control during pre-launch, launch, orbit, and reentry [UCA76]

**SC70:** Flight Computers must not provide incorrect Vehicle Health & Status to Mission Control during pre-launch, launch, orbit, or reentry [UCA77] with a delay or latency greater than TBD [UCA78]

**SC71:** Flight Computers must provide stage separation [UCA79], fairing separation [UCA80], and payload separation [UCA81] command flags to Mission Control as soon as commanded

**SC72:** Flight Computers must not provide incorrect or delayed stage separation confirmation to Mission Control [UCA82]

**SC73:** Flight Computers must not provide incorrect or delayed fairing separation confirmation to Mission Control [UCA83]

**SC74:** Flight Computers must not provide incorrect or delayed payload separation confirmation to Mission Control [UCA84]

**SC75:** Flight Computers must not provide stage separation confirmation to Mission Control before stage separation has been confirmed [UCA85]

**SC76:** Flight Computers must not provide fairing separation confirmation to Mission Control before fairing separation has been confirmed [UCA86]

**SC77:** Flight Computers must not provide payload separation confirmation to Mission Control before payload separation has been confirmed [UCA87]

**SC78:** Flight Computers must provide Umbilical Drop Out to Mission Control when umbilical connection is lost [UCA88]

**SC79:** Flight Computers must not provide incorrect or delayed Umbilical Drop Out to Mission Control [UCA89]

**SC80:** Flight Computers must provide liftoff commands to Stage 1 [UCA90]

**SC81:** Flight Computers must provide thrust vector information to Stage 1 [UCA91]

**SC82:** Flight Computers must provide propulsion shutdown commands to Stage 1 [UCA92]

**SC83:** Flight Computers must provide pressure or valve controls to Stage 1 [UCA93]

**SC84:** Flight Computers must provide shutdown commands to Stage 1 before propellant below TBD level [UCA94]

**SC85:** Flight Computers must not provide liftoff commands to Stage 1 during pre-launch [UCA95]

**SC86:** Flight Computers must not provide incorrect or delayed thrust vector information to Stage 1 [UCA96]

**SC87:** Flight Computers must not provide incorrect or delayed pressure or valve set points to Stage 1 [UCA97]

**SC88:** Flight Computers must not provide incorrect or delayed throttle to Stage 1 [UCA98]

**SC89:** Flight Computers must not provide startup or excessive purge to Stage 1 propulsion during or shortly after stage separation [UCA99]

**SC90:** Flight Computers must not provide startup commands to Stage 1 after liftoff [UCA100]

**SC91:** Flight Computers must not provide shutdown to Stage 1 within TBD seconds of reaching performance target [UCA101] [UCA102]

**SC92:** Flight Computers must not provide purge, pressurization, or vent commands to Stage 1 too long (>TBD seconds) [UCA103]

**SC93:** Flight Computers must provide sufficient Power to Stage 1 components [UCA104]

**SC94:** Flight Computers must not provide excessive Power (>TBD) to Stage 1 components [UCA105]

**SC95:** Flight Computers must provide constant and regulated Power to Stage 1 components [UCA106]

**SC96:** Flight Computers must not provide power to Stage 1 components less than TBD seconds before liftoff [UCA107]

**SC97:** Flight Computers must not stop providing power to Stage 1 components during pre-launch and launch [UCA108]

**SC98:** Flight Computers must not provide power to Stage 1 components too long (>TBD seconds) [UCA109]

**SC99:** Flight Computers must provide stage separation command to Stage 1/interstage within TBD seconds of scheduled stage separation [UCA110]

**SC100:** Flight Computers must not provide stage separation command during pre-launch or stage 1 launch [UCA111], before Stage 1 thrust below TBD [UCA112], or >TBD seconds after timed separation [UCA113]

**SC101:** Flight Computers must not stop providing stage separation command before stage separation is complete [UCA114]

**SC102:** Flight Computers must provide startup commands to Stage 2 [UCA115]

**SC103:** Flight Computers must provide thrust vector information to Stage 2 [UCA116]

**SC104:** Flight Computers must provide propulsion shutdown commands to Stage 2 [UCA117]

**SC105:** Flight Computers must provide pressure and valve control to Stage 2 [UCA118]

**SC106:** Flight Computers must provide body rates to Stage 2 RCS [UCA119]

**SC107:** Flight Computers must provide shutdown commands to Stage 2 before propellant level is below TBD [UCA120]

**SC108:** Flight Computers must not provide startup commands to Stage 2 during pre-launch and Stage 1 burn [UCA121]

**SC109:** Flight Computers must not provide incorrect or delayed thrust vector information to Stage 2 [UCA122]

**SC110:** Flight Computers must not provide incorrect or delayed pressure and valve set points to Stage 2 [UCA123]

**SC111:** Flight Computers must not provide incorrect or delayed throttle to Stage 2 propulsion [UCA124]

**SC112:** Flight Computers must not provide incorrect or delayed RCS control during payload separation [UCA125]

**SC113:** Flight Computers must not provide startup commands to Stage 2 >TBD seconds before stage separation [UCA126]

**SC114:** Flight Computers must provide shutdown commands to Stage 2 within TBD seconds of reaching performance target [UCA127] [UCA128]

**SC115:** Flight Computers must provide sufficient Power to Stage 2 components [UCA129]

**SC116:** Flight Computers must not provide excessive (>TBD) Power to Stage 2 components [UCA130]

**SC117:** Flight Computers must provide constant and regulated Power to Stage 2 components [UCA131]

**SC118:** Flight Computers must not provide Power to Stage 2 components >TBD seconds before liftoff [UCA132]

**SC119:** Flight Computers must not stop providing power to Stage 2 components [UCA133]

**SC120:** Flight Computers must not provide power to Stage 2 components too long (>TBD) or too many cycles (>TBD) [UCA134]

**SC121:** Flight Computers must provide fairing separation command during schedule fairing separation [UCA135]

**SC122:** Flight Computers must provide payload separation command during scheduled payload separation [UCA136]

**SC123:** Flight Computers must not provide fairing separation command during pre-launch, Stage 1 launch, or stage separation [UCA137]

**SC124:** Flight Computers must not provide payload separation before Stage 2 thrust below TBD [UCA138]

**SC125:** Flight Computers must not provide fairing separation command when fairing pressure >TBD psi [UCA140], <TBD seconds before intended fairing separation [UCA141], or >TBD seconds before intended fairing separation [UCA139] [UCA135]

**SC126:** Flight Computers must not stop providing fairing separation command before fairing separation is complete [UCA142] or before payload separation is complete [UCA143]

**SC127:** Stage 2 must provide correct and constant propulsion sensor data to Flight Computers [UCA154] [UCA145] with <TBD delay/latency [UCA146]

**SC128:** Stage 2 must provide correct and constant Vehicle Health & Status data to Flight Computers [UCA147] [UCA148] with <TBD delay/latency [UCA149]

**SC129:** Stage 2 must provide sufficient force to Flight Computer(s) to maintain mechanical and electrical connections [UCA150]

**SC130:** Stage 2 must not provide excessive (>TBD) Force/Acceleration [UCA151], or Force/Acceleration greater than TBD for greater than TBD seconds [UCA152] to Flight Computer(s)

**SC131:** Stage 1 must provide correct and constant propulsion sensor data to Flight Computers [UCA153][UCA154] under TBD delay/latency [UCA155]

**SC132:** Stage 1 must provide correct and constant Vehicle Health & Status data to Flight Computers [UCA157] [UCA156] under TBD delay/latency [UCA158]

**SC133:** Stage 2 must provide sufficient force to Payload to maintain mechanical and electrical connections [UCA159]

**SC134:** Stage 2 must not provide excessive (>TBD) Force/Acceleration to Payload [UCA160] or >TBD Force/Acceleration to Payload for TBD seconds or TBD cycles [UCA162]

**SC135:** Stage 2 must not contact Payload after payload separation [UCA161]

**SC136:** Stage 2 must provide separation command to Payload [UCA163]

**SC137:** Stage 2 must not provide separation command to Payload during pre-launch and launch [UCA164] or before Stage 2 thrust <TBD [UCA165]

**SC138:** Stage 2 must not provide payload separation command >TBD seconds after target separation time reached [UCA166] or >TBD seconds before target separation time is reached [UCA167]

**SC139:** Stage 2 must not stop providing separation command to Payload before Payload has separated [UCA168]

**SC140:** Stage 2 must provide sufficient force to maintain mechanical and electrical connections to Stage 1 during pre-launch and launch [UCA169]

**SC141:** Stage 2 must not provide excessive (>TBD) force/acceleration to Stage 1 [UCA170] or greater than TBD Force/Acceleration to Stage 1 greater than TBD seconds or for greater than TBD cycles [UCA171]

**SC142:** Stage 1 must provide sufficient force to maintain mechanical or electrical connections to Stage 2 [UCA172]

**SC143:** Stage 1 must not provide excessive (>TBD) Force/Acceleration to Stage 2 [UCA173] or greater than TBD Force/Acceleration to Stage 2 greater than TBD seconds or for greater than TBD cycles [UCA174]

**SC144:** Stage 1 must provide sufficient force to Termination Devices to maintain mechanical and electrical connections during pre-launch and launch [UCA175]

**SC145:** Stage 1 must not provide excessive (>TBD) Force/Acceleration to Termination Devices [UCA176] or greater than TBD Force/Acceleration to Termination Devices greater than TBD seconds or greater than TBD cycles [UCA177]

**SC146:** Stage 2 must provide sufficient force to Termination Devices to maintain mechanical and electrical connections during pre-launch and launch [UCA178]

**SC147:** Stage 2 must not provide excessive Force/Acceleration to Termination Devices [UCA179], or greater than TBD Force/Acceleration to Termination Devices greater than TBD seconds or greater than TBD cycles [UCA180]

**SC148:** Termination Devices must stop Stage 1 thrust during termination [UCA181]

**SC149:** Termination Devices must not provide Stage 1 thrust termination when Termination Flag is not active [UCA182]

**SC150:** Termination Devices must not stop terminating Stage 1 thrust before thrust below TBD [183]

**SC151:** Termination Devices must provide sufficient Force/Acceleration to Stage 1 to send vehicle and payload debris on safe ballistic trajectory [UCA184], distribute and burn propellants [UCA 185], and depressurize pressurized vessels within flight corridor [UCA186]

**SC152:** Termination Devices must not provide sufficient Force/Acceleration to Stage 1 to detonate propellants [UCA187] or accelerate debris beyond flight corridor or safed area at launch pad [UCA188]

**SC153:** Termination Devices must not provide Force/Acceleration to Stage 1 before Stage 2 is terminated [UCA189], before Stage 1 thrust is terminated [UCA183] [UCA190], and greater than TBD seconds after termination [UCA191]

**SC154:** Termination Devices must stop Stage 2 thrust during termination [UCA192]

**SC155:** Termination Devices must not provide thrust termination to Stage 2 when Termination Flag is not active [UCA193] and thrust below TBD [UCA194]

**SC156:** Termination Devices must provide sufficient Force/Acceleration to Stage 2 to send vehicle and payload debris on safe ballistic trajectory [UCA195] and to distribute and burn propellants [UCA196]

**SC157:** Termination Devices must not provide sufficient Force/Acceleration to Stage 2 to detonate propellants [UCA197], accelerate debris beyond flight corridor or safed area at launch pad [UCA198], and when altitude >TBD [UCA199]

**SC158:** Termination Devices must not provide Force/Acceleration to Stage 2 before Stage 1 is terminated [UCA200], Stage 2 thrust is terminated [UCA192] [UCA 201], and greater than TBD seconds after termination [UCA202]

**SC159:** Payload must provide sufficient Force/Acceleration to Stage 2 to maintain mechanical and electrical connect during pre-launch, launch, and orbit [UCA203]

**SC160:** Payload must not provide excessive (>TBD) Force/Acceleration to Stage 2 [UCA204]

**SC161:** Payload must not contact Stage 2 after separation [UCA205]