Systems-Theoretic Process Analysis of space launch vehicles

Citation: Rising, John M. and Nancy G.Leveson. "Systems-Theoretic Process Analysis of space launch vehicles." Journal of Space Safety Engineering 5, 3-4 (September–December 2018): 153-183 © 2018 International Association for the Advancement of Space Safety

As Published: http://dx.doi.org/10.1016/j.jsse.2018.06.004

Publisher: Elsevier BV

Persistent URL: https://hdl.handle.net/1721.1/122988

Contents lists available at ScienceDirect

The Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

Systems-Theoretic Process Analysis of space launch vehicles

John M. Rising[a,*], Nancy G. Leveson[b]

[a] Massachusetts Institute of Technology, USA
[b] Aeronautics and Astronautics, Massachusetts Institute of Technology, USA

ABSTRACT

This article demonstrates how Systems-Theoretic Process Analysis (STPA) can be used as a powerful tool to identify, mitigate, and eliminate hazards throughout the space launch system lifecycle. Hazard analysis techniques commonly used to evaluate launch vehicle safety use reliability theory as their foundation, but most modern space launch vehicle accidents have resulted from design errors or other factors independent of component reliability. This article reviews safety analysis methods as they are applied to space launch vehicles, and demonstrates that they are unable to treat many of the causal factors associated with modern launch accidents. Next, it describes how STPA can be applied to the design of space launch vehicles to treat these casual factors. Safety-guided design with STPA is then demonstrated with a hypothetical small-lift launch vehicle, launch safety system, and upper stage propulsion system.

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

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; N2, Nitrogen; N2O4, Dinitrogen Tetroxide; NASA, National Aeronautics and Space Administration; NO2, 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

[*] Corresponding author.
E-mail addresses: johnrising@alum.mit.edu (J.M. Rising), leveson@mit.edu (N.G. Leveson).

https://doi.org/10.1016/j.jsse.2018.06.004
Received 17 May 2018; Received in revised form 23 June 2018; Accepted 24 June 2018

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. Furthermore, 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, and ensure that appropriate organization controls are put in place.

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 (Fig. 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.

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

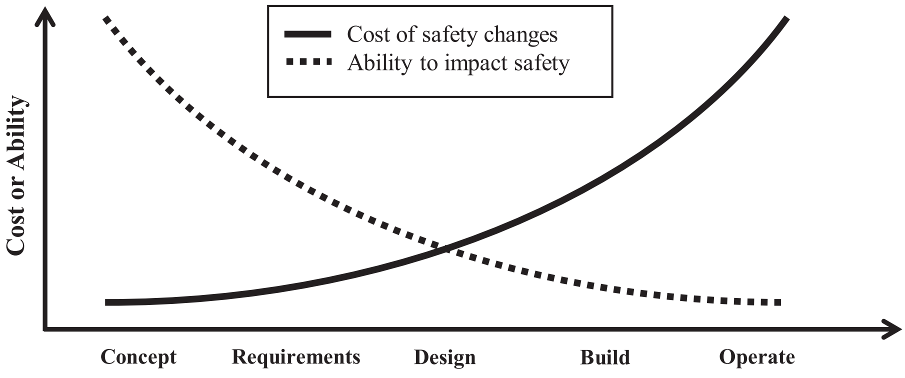


Fig. 1. The cost of safety fixes increases exponentially with product lifecycle phase. Adapted from [49].

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	$P_O \leq 0.00001$

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.

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 $1 M but less than $10 M.
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 $100 K but less than $1 M.
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 $100 K.

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.

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.

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).

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 Fig. 2.

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).

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

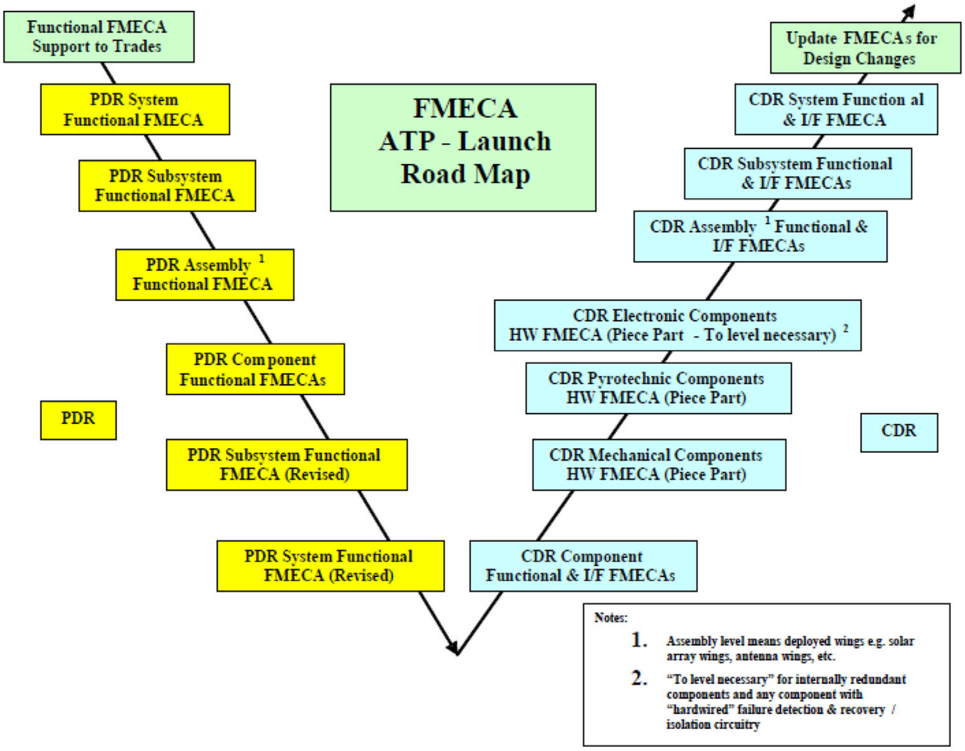

Functional FMECA Support to Trades
PDR System Functional FMECA
PDR Subsystem Functional FMECA
PDR Assembly 1 Functional FMECA
PDR Component Functional FMECAs
PDR
PDR Subsystem Functional FMECA (Revised)
PDR System Functional FMECA (Revised)
FMECA ATP - Launch Road Map
Update FMECAs for Design Changes
CDR System Function al & I/F FMECA
CDR Subsystem Functional & I/F FMECAs
CDR Assembly 1 Functional & I/F FMECAs
CDR Electronic Components HW FMECA (Piece Part - To level necessary) 2
CDR Pyrotechnic Components HW FMECA (Piece Part)
CDR
CDR Mechanical Components HW FMECA (Piece Part)
CDR Component Functional & I/F FMECAs
Notes:
1. Assembly level means deployed wings e.g. solar array wings, antenna wings, etc.
2. "To level necessary" for internally redundant components and any component with "hardwired" failure detection & recovery / isolation circuitry

Fig. 2. Integration of FMECAs into space vehicle design [3].

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: 1. Can the system fail to operate as intended? 2. Can the system operate inadvertently? 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: 4. Can the system fail to operate as intended? 5. Can the system operate inadvertently? 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.

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	5×10^{-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	3×10^{-5}
Fatality expectation per launch to individual	1×10^{-3}

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	8×10^{-5} / section-year
Spontaneous failures (tanks, etc.)	10^{-6} / year

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.

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.

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.

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	9×10^{-1}
3. +5 minutes to + 30 minutes	10^{-1}
4. + 30 minutes to + several hours	10^{-2}

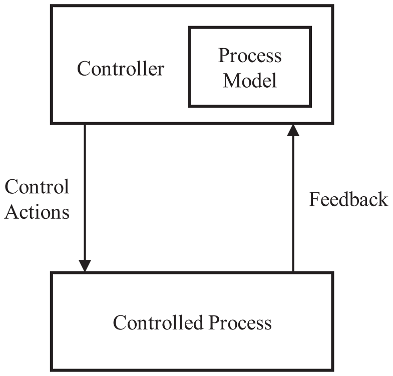


Fig. 3. A generic control structure.

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 Fig. 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.

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 in Table 8.

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.

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-

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 Mills are incorrectly mounted to machine Mills are incorrectly configured	Mills are started before material is in place	N/A

Table 9
Process state oriented context tables.

				Hazardous control action?		
Control action	Process state variable 1	Process state variable 2	Process state variable N	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 not provided				

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° inclination, a significant departure from their intended 3° 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.

The same vehicle was also involved in one of the most famous software errors in launch history. Forty seconds into its maiden launch in 1996, 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 [34].

2.3.2. *Delta III*

The first flight of Boeing's Delta III rocket in August 1998 ended in failure. The launch vehicle's guidance system misinterpreted a roll mode as a disturbance, and expended the hydraulic fluid for the solid rocket thrust vector control actuators trying to correct it. The vehicle then flew through a wind shear, yawed 25–35°, and began to breakup. The vehicle's safety system then destructed the vehicle. Similar to the maiden flight of Ariane 5 three years prior, Boeing modified the Delta II guidance system to work on the Delta III. Boeing did not identify the roll oscillation mode as the primary oscillation mode for Delta III because it was not the primary oscillation mode on Delta II [35].

2.3.3. *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].

2.3.4. 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].

2.3.5. 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].

2.3.6. 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.

2.3.7. 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."

Many of these accidents could have been identified if the appropriate system test or analysis was identified and prioritized at the beginning. When applied to the engineered system, STPA can identify the potential for these component interactions early in the design lifecycle and prioritize the appropriate analysis or test. When applied to the launch service organization, STPA can identify lacks of controls in engineering and operations processes.

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 refly 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.

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 (Fig. 4).

Only a few of the most important feedback loops are shown in Fig. 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 (Fig. 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.

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].

STPA is hierarchical and can be used across the entire product lifecycle, promoting traceability as the system evolves. Because a

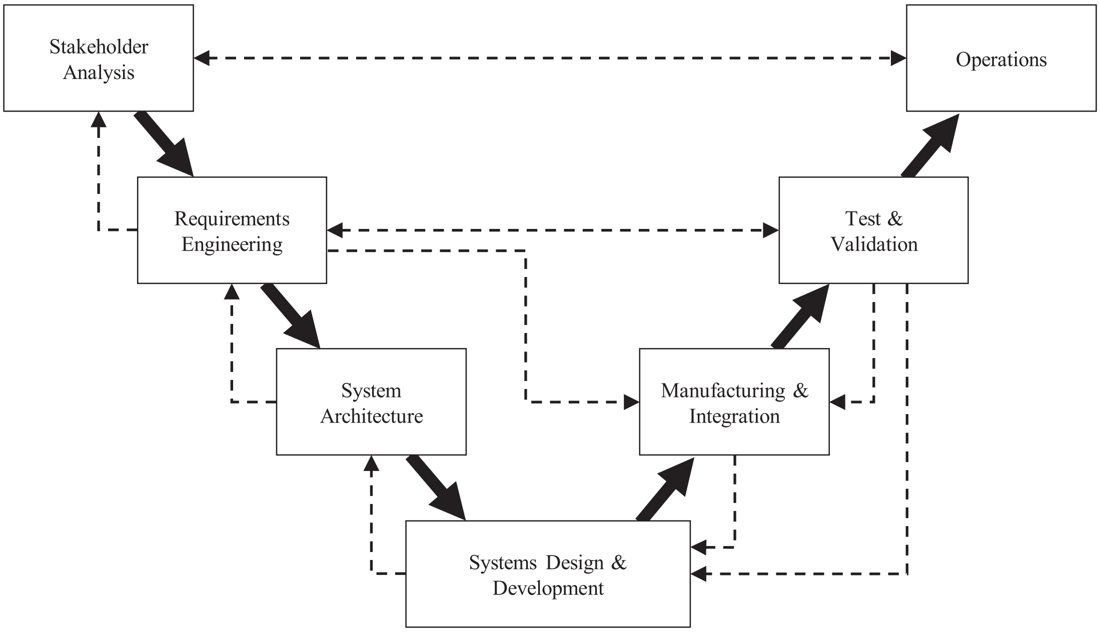
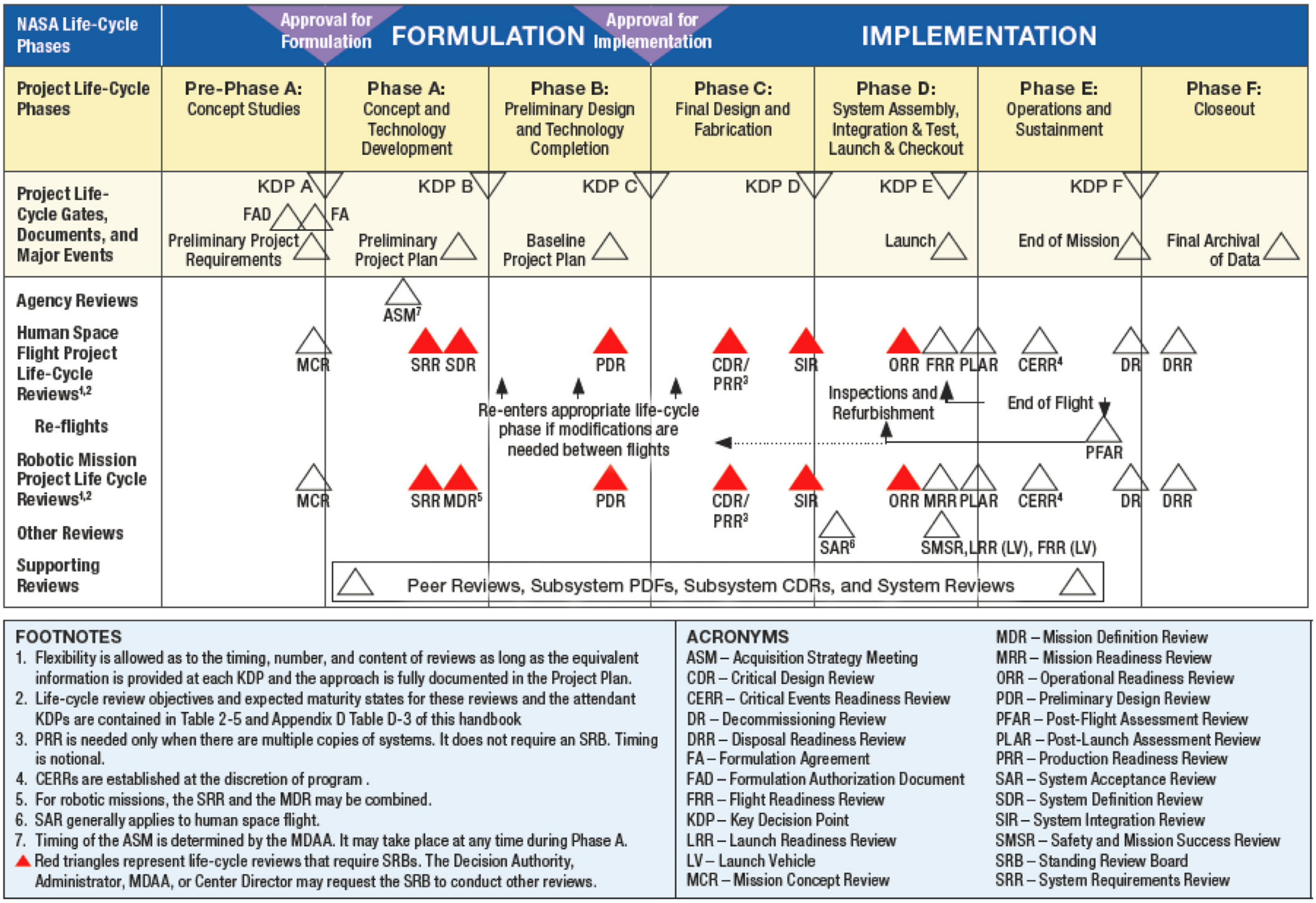


Fig. 4. The classic systems engineering v-model.


NASA Life-Cycle Phases
Approval for Formulation
FORMULATION
Approval for Implementation
IMPLEMENTATION
Project Life-Cycle Phases
Pre-Phase A: Concept Studies
Phase A: Concept and Technology Development
Phase B: Preliminary Design and Technology Completion
Phase C: Final Design and Fabrication
Phase D: System Assembly, Integration & Test, Launch & Checkout
Phase E: Operations and Sustainment
Phase F: Closeout
Project Life-Cycle Gates, Documents, and Major Events
KDP A
KDP B
KDP C
KDP D
KDP E
KDP F
FAD
FA
Preliminary Project Requirements
Preliminary Project Plan
Baseline Project Plan
Launch
End of Mission
Final Archival of Data
Agency Reviews
ASM7
Human Space Flight Project Life-Cycle Reviews1,2
MCR
SRR SDR
PDR
CDR/ PRR3
SIR
ORR FRR PLAR
CERR4
DR
DRR
Re-flights
Re-enters appropriate life-cycle phase if modifications are needed between flights
Inspections and Refurbishment
End of Flight
PFAR
Robotic Mission Project Life Cycle Reviews1,2
MCR
SRR MDR5
PDR
CDR/ PRR3
SIR
ORR MRR PLAR
CERR4
DR
DRR
Other Reviews
SAR6
SMSR, LRR (LV), FRR (LV)
Supporting Reviews
Peer Reviews, Subsystem PDFs, Subsystem CDRs, and System Reviews

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

Fig. 5. NASA space flight lifecycle [58].

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

Table 10
Contribution to systems engineering activities by STPA.

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

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 (Fig. 6). In this model, the designer is a single human or group of humans.

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 (Fig. 7).

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:

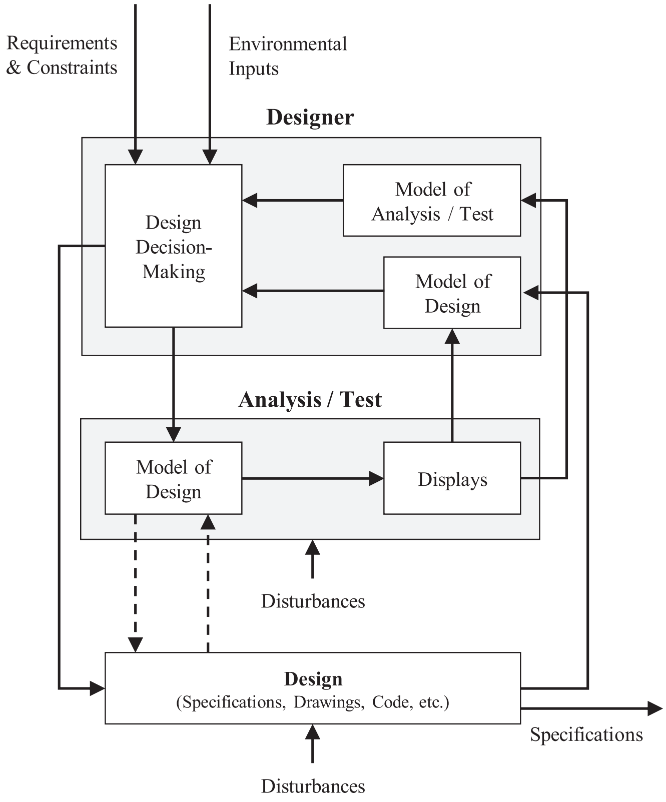


Fig. 6. Generalized component design structure.

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 (Fig. 8).

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 Fig. 9.

A formal model of each system, such as the one in Fig. 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

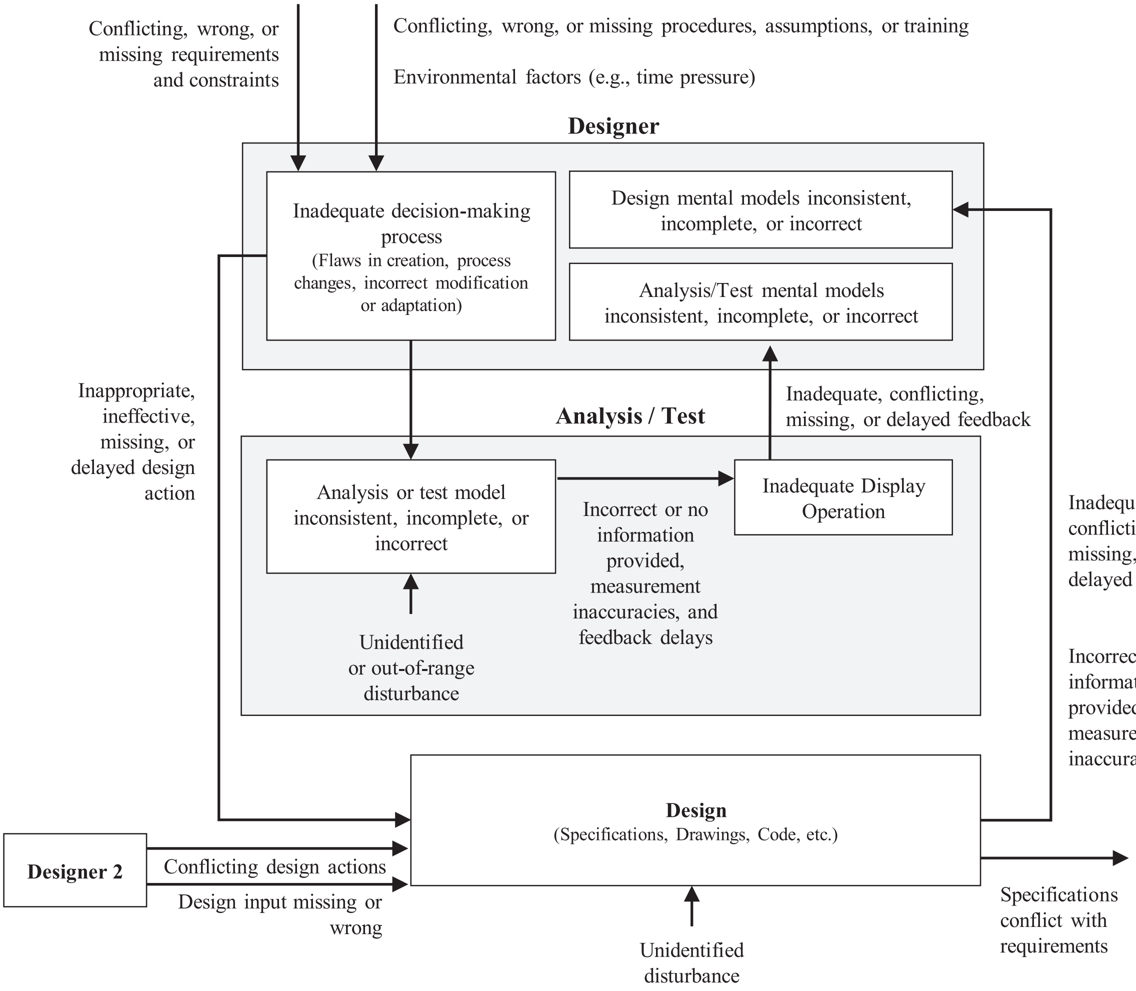

Conflicting, wrong, or missing requirements and constraints
Conflicting, wrong, or missing procedures, assumptions, or training
Environmental factors (e.g., time pressure)
Designer
Inadequate decision-making process
(Flaws in creation, process changes, incorrect modification or adaptation)
Design mental models inconsistent, incomplete, or incorrect
Analysis/Test mental models inconsistent, incomplete, or incorrect
Inappropriate, ineffective, missing, or delayed design action
Inadequate, conflicting, missing, or delayed feedback
Analysis / Test
Analysis or test model inconsistent, incomplete, or incorrect
Incorrect or no information provided, measurement inaccuracies, and feedback delays
Inadequate Display Operation
Unidentified or out-of-range disturbance
Inadequate, conflicting, missing, or delayed feedback
Incorrect or no information provided, measurement inaccuracies
Design
(Specifications, Drawings, Code, etc.)
Designer 2
Conflicting design actions
Design input missing or wrong
Unidentified disturbance
Specifications conflict with requirements

Fig. 7. Design process flaws leading to hazards.

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

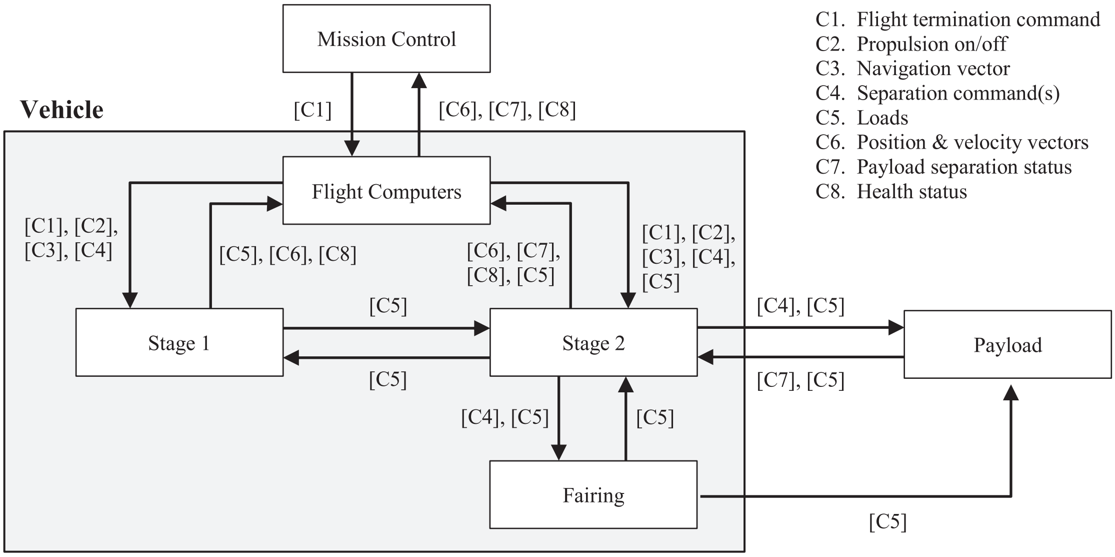


Fig. 8. Safety control structure for the launch vehicle concepts during the launch phase.

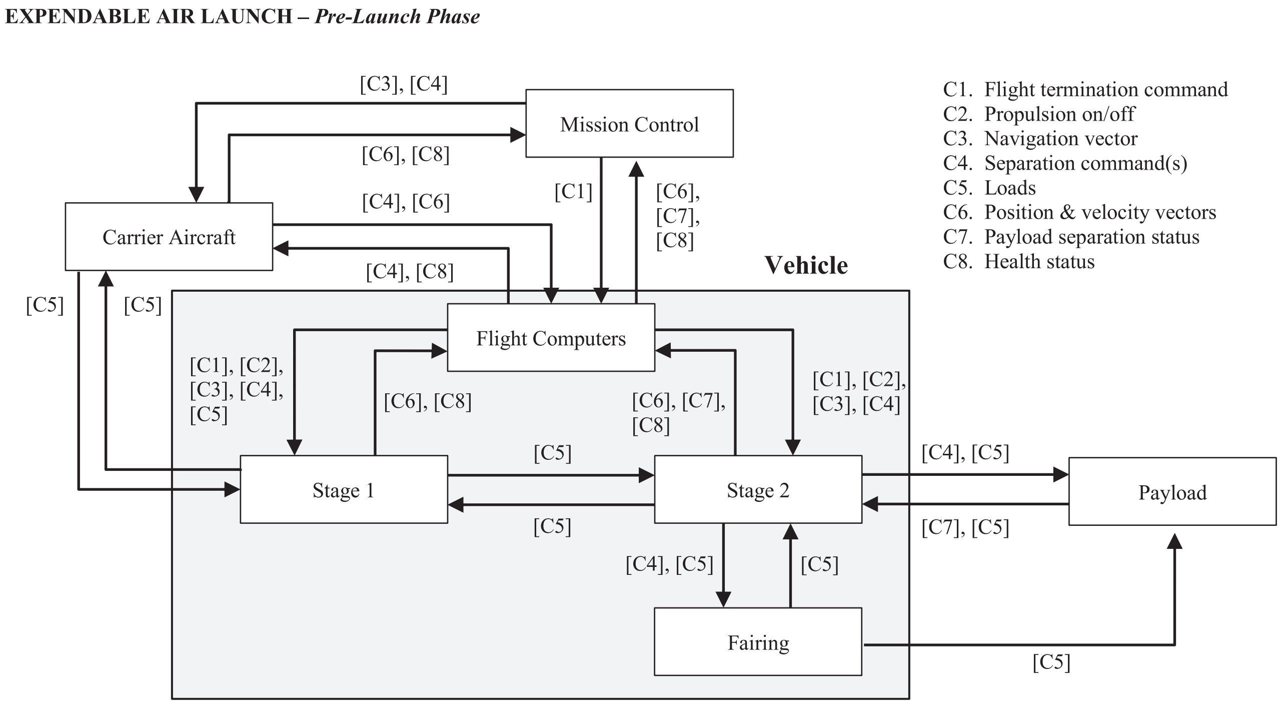


Fig. 9. Safety control structure for an expendable air launch vehicle during pre-launch.

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

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 Tables 11 and 12.

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

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 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

flight) than expendable vehicles (which cannot be inspected after flight).

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.

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 mitigatability 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.

1. All concepts use two stages with conventional bipropellant liquid propulsion from an existing U.S. range
2. Air launch vehicles are dropped horizontally from a manned carrier aircraft over the open ocean with a crew escape system
3. Reusable stages land vertically on land within 10 miles of the launch site
4. 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).

The corresponding *ORSRM* values for each concept are shown in Table 17.

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.

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

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

Table 17
Concept ***ORSRM*** values.

Concept	*ORSRM*
Expendable Ground Launch	1241
Expendable Air Launch	1532
Reusable Ground Launch	1231

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
  H1.5. 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.

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

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	–	–	–	–

Fig. 10.

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 Figs. 11 and 12.

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 Figs. 11 and 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

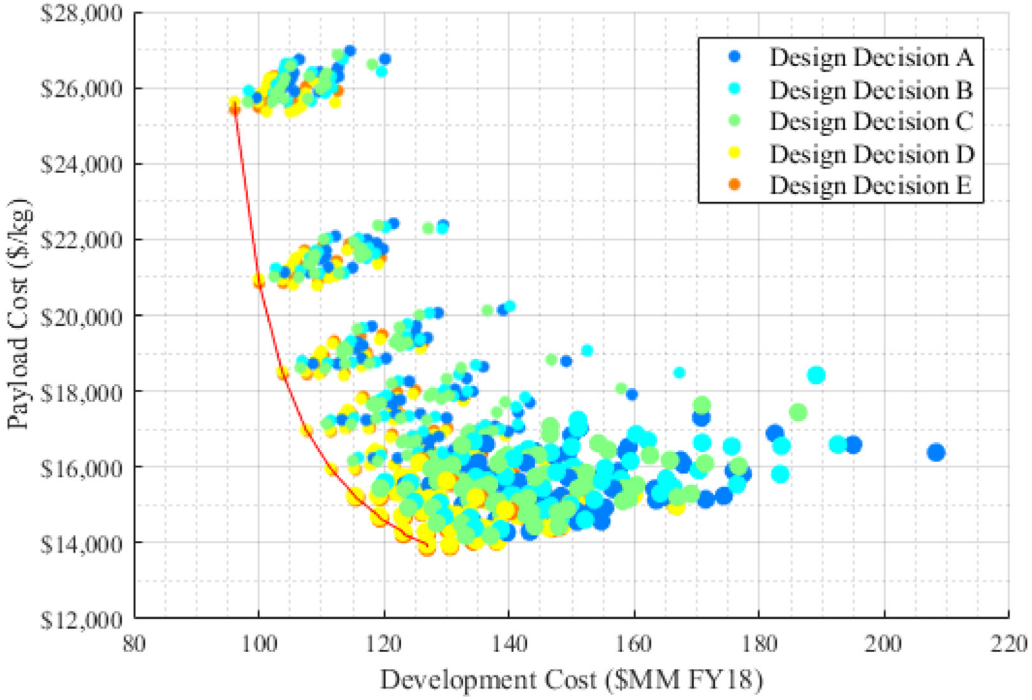


Fig. 10. Example tradespace plot for a launch vehicle. The red line represents the Pareto frontier. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

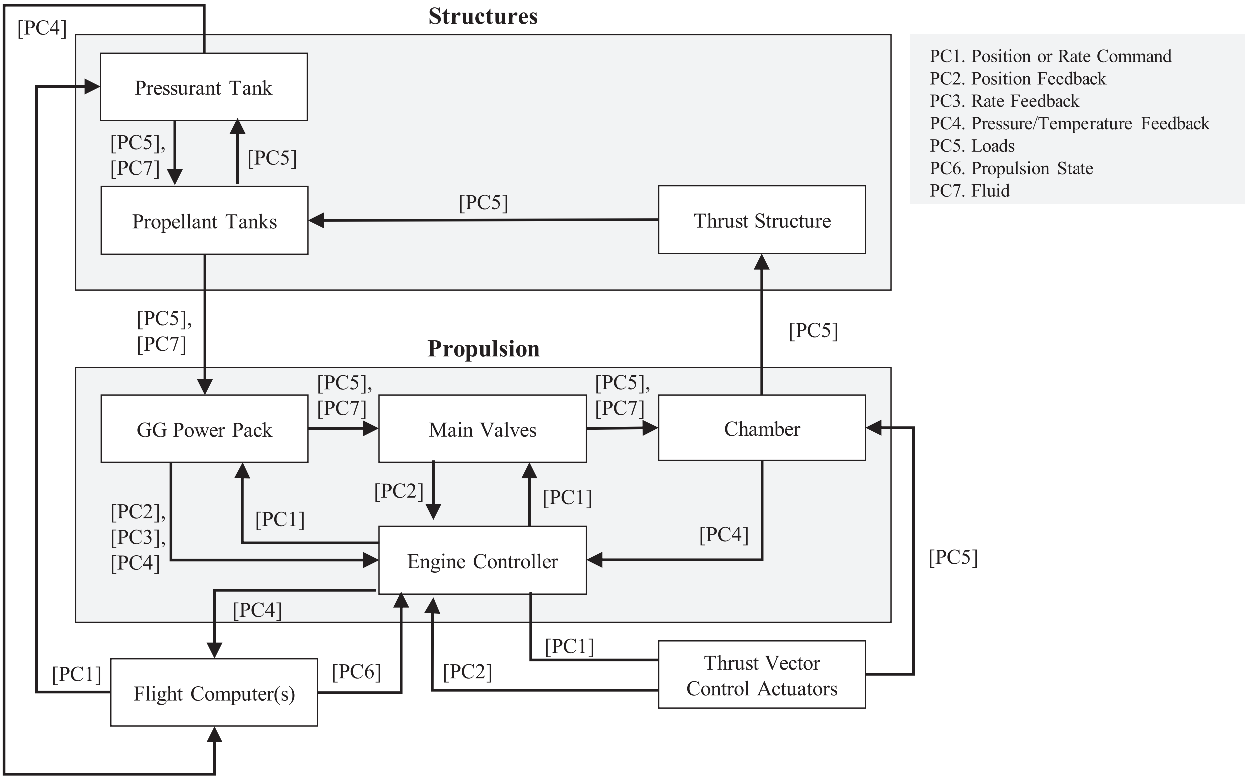


Fig. 11. Safety control structure for a liquid propulsion stage using a gas generator and helium pressurization system.

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
A3. Loss of or damage to launch facilities

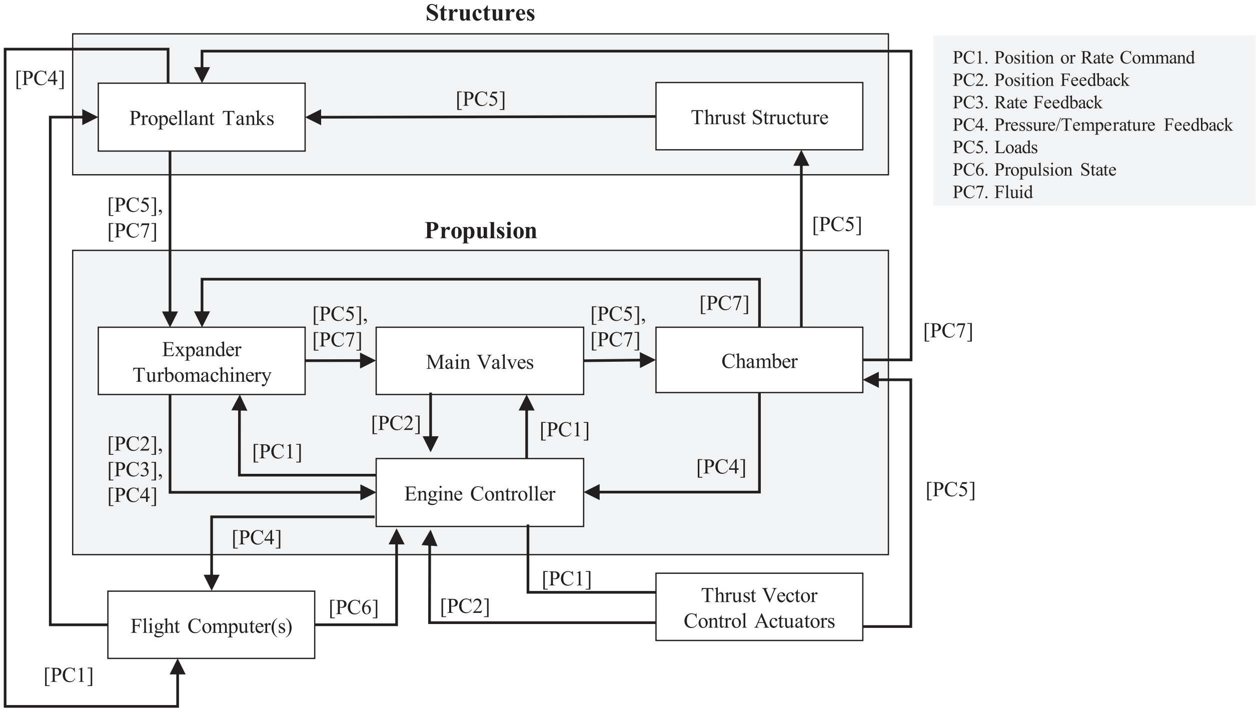


Fig. 12. Safety control structure for a liquid propulsion stage with an expander cycle and autogenous pressurization.

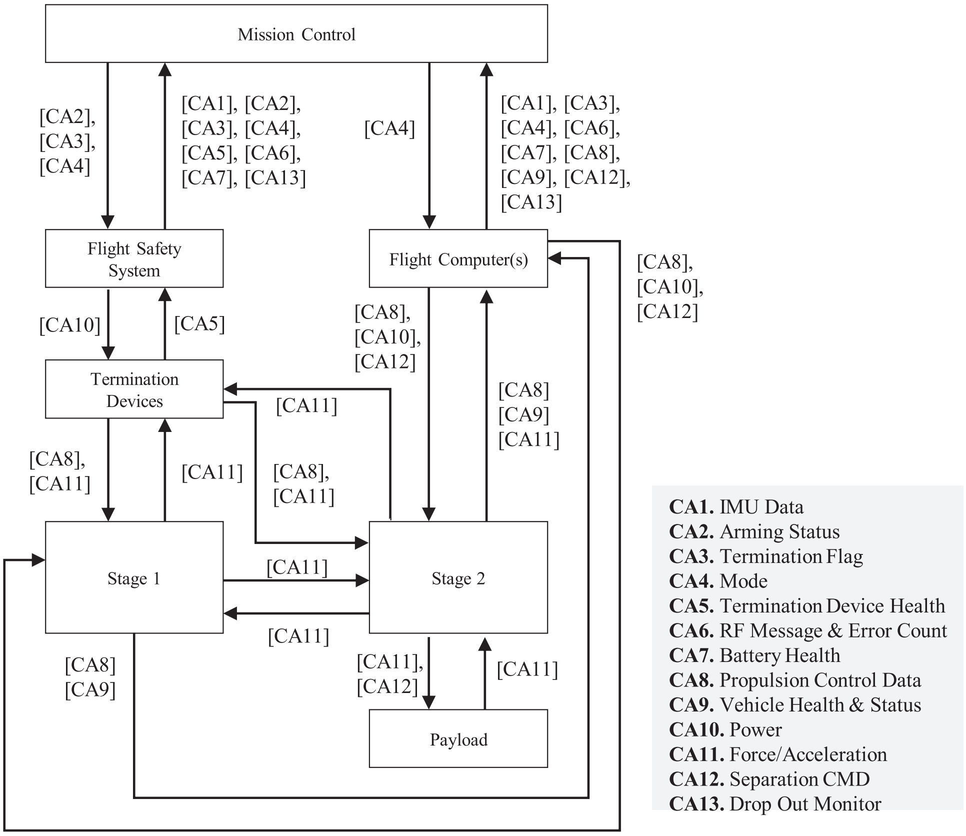


Fig. 13. Safety control structure of the flight safety system in the vehicle.

Accidents A1 and A2 concern public safety. Protecting the public is the primary function of an FSS, and any elements of this analysis that link back to A1 and A2 are critical to public safety. 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 Fig. 13.

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.

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.

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

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] **UCA2:** FSS does not provide power to termination devices when vehicle approaches flight corridor boundary during launch [H3] **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] **UCA5:** FSS provides power to termination devices when SAD is unarmed or safed [H7] **UCA6:** FSS provides power to termination devices when in test mode [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 [H7] **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] **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] **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] **UCA15:** Mission control provides safe command to FSS during launch [H3]	N/A	N/A
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] **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] **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] **UCA21:** Mission control provides termination flag to FSS in orbit [H7] **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] **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] **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] **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]
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] **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

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

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.

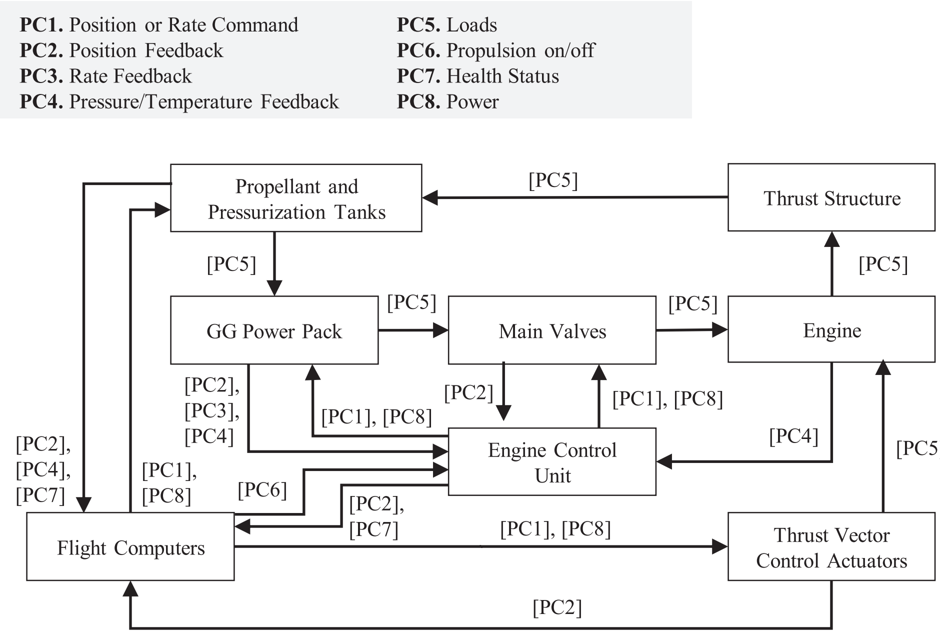


Fig. 14. Propulsion system control structure.

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 Fig. 14.

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).

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.

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

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] **UCA3:** ECU provides GG open command when downstream pressure is higher than upstream pressure [H7.1] [H7.4] **UCA4:** ECU provides GG valves open commands when there is insufficient propellant in pumps [H7] [H4.4] **UCA5:** ECU provides GG valves open command when there is insufficient propellant to GG [H4.2] [H4.4] [H7] **UCA6:** ECU provides GG valves open commands during abort [H4.4] [H2] **UCA7:** ECU provides excessive GG open command power [H7.2] [H4.2] **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] **UCA10:** ECU provides GG valves open command < TBD seconds before GG ignition source provided [H7] [H4.4] **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]
Engine Control Unit	GG valves close commands	**UCA13:** ECU does not provide GG valves close commands during shutdown [H4.4] [H7.2] **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] **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] **UCA22:** ECU provides GG ignition source command outside of startup window [H4.3] [H7] **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] **UCA25:** ECU provides GG ignition source command too long [H4.4] [H4.2]
Engine Controller	Igniter valves open commands	**UCA26:** ECU provides igniter valves open commands during shutdown [H4.4] [H2.2] [H7] **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] **UCA30:** ECU provides igniter valves open commands too early (> TBD seconds before main valve open commands) [H7] **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] **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] **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] **UCA37:** ECU provides the igniter valves close commands too early (> TBD milliseconds) before chamber ignition [H4.2] **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]
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] **UCA42:** ECU provides MV open commands during shutdown [H4.4] [H2.2] [H7] **UCA43:** ECU provides MV open commands when downstream pressure is greater than upstream	**UCA45:** ECU provides MV open commands before startup [H4.2] [H7.2] **UCA46:** ECU provides MV open commands out of order [H7.2] [H4.4] **UCA47:** ECU provides MV open commands too late (> TBD milliseconds) after pump spool up [H4.4]	**UCA49:** ECU stops providing MV open commands before valves are fully open [H4.2] [H4.4] [H5]

(*continued on next page*)

Table 21 (*continued*)

Controller	Control action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
			pressure [H7.1] [H7.2] [H7.4] **UCA44:** ECU provides MV open commands when igniter is not on [H7.2] [H4.2]	**UCA48:** ECU provides MV open commands too soon (> TBD milliseconds) after stage separation [H2]	
Engine Controller	MV close commands	**UCA50:** ECU does not provide MV close commands during shutdown [H7.2] [H5] [H7.2] **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] **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] **UCA55:** ECU provides MV close commands out of order [H4.4] [H7] **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]

- 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

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

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

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

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.

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.

5. Conclusions

Traditional hazard analysis tools are unable to identify and correct safety-related design errors in modern launch vehicles. This article demonstrates that Systems-Theoretic Process Analysis, integrated into the design cycle ("safety-guided design"), is a solution. 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 space launch vehicles can make a significant contribution to reducing accidents without compromising efficient and cost-effective design. STPA was applied to the concept evaluation, requirements, architecture, and design phases of a hypothetical two-stage small-lift launch vehicle. The resulting analysis was shown to provide valuable safety-related insight into design decisions not possible with traditional safety techniques.

References

[1] N.G. Leveson, Engineering a Safer World, CambridgeThe MIT Press, MA, USA, 2011.
[2] F. Frola, C. Miller, System Safety in Aircraft Management, Logistics Management Institute, Washington, DC, USA, 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, 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, J.P. Thomas, STPA Handbook, Cambridge, MA, USA, 2018.
[9] H. Koenigsmann, Smallsat Symposium Keynote Address, Mountain View, 2018.
[10] Federal Aviation Administration Advisory Circular, "AC 431.35-2A Reusable Launch and Reentry Vehicle Systems Safety Process," U.S. Department of Transportation Federal Aviation Administration Office of Commercial Space 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, J. Space Saf. Eng. 4 (1) (2017) 22–28.
[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, first ed., MIT Partnership for a Systems Approach to Safety, Cambridge, MA, USA, 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 Sci. Technol. 2 (2008) 237–261.
[20] T. Ishimatsu, N.G. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, H. Nakao, Modeling and hazard analysis using STPA, 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, N.G. Leveson, Safety guided design of crew return vehicle in concept design phase using STAMP/STPA, Proceedings of the 5th IAASS Conference, 2011, pp. 497–501.
[22] A. Scarinci, F.X. de Oliveira, R. Moraes, A.I. Quilici, D. Patrick, D. da Costa Ribeiro, A complete STPA application to the air management system of Embraer regional jets family, Proceedings of the MIT STAMP Workshop, Cambridge, MA, USA, 2017.
[23] E. Howard, K. Belvin, S. Murray, L. Juhnke, L. Hettinger, M. France, STAMP In Workplace Safety, Proceedings of the 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, N.G. Leveson, Improving hazard analysis and certification of integrated modular avionics, J. Aerosp. Inf. Syst. 11 (6) (2014) 397–411.
[26] B.D. Owens, A.R. Crocker, SimSup's loop: a control theory approach to spacecraft operator training, *Proceedings of the IEEE Aerospace Conference* (Big Sky), MT, USA, 2015.
[27] S.J. Pereira, G. Lee, J. Howard, A system-theretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system, Proceedings of the AIAA Missile Sciences Conference, Monterey, CA, 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, 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, K.A. Weiss, Application of a safety-driven design methodology to an outer planet exploration mission, *Proceedings of the 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] J.L. Lions, Ariane 5 Flight 501 Failure Report by the Inquiry Board, European Space Agency, Paris, France, 1996.
[35] The Boeing Company, Boeing changes delta III control software, http://boeing.mediaroom.com/1998-10-15-Boeing-Changes-Delta-III-Control-Software, (1998) [Accessed 23 June 2018].
[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, Arianespace, 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, 2017 6 December.
[40] J. McDowell, JSR launch vehicle database, http://planet4589.org/space/lvdb/, (2017) [Accessed 28 February 2018].
[41] Space Exploration Technologies, Falcon 1, Flight 3 mission summary, http://www.spacex.com/news/2013/02/11/falcon-1-flight-3-mission-summary, (2008) [Accessed 24 February 2018].
[42] Space Exploration Technologies, Anomaly updates, http://www.spacex.com/news/2016/09/01/anomaly-updates, (2017) [Accessed 24 February 2018].
[43] J. Foust, Falcon 9 Failure Linked To Upper Stage Tank Strut, SpaceNews, 2015 20 July.
[44] National Aeronautics and Space Administration, SpaceX CRS-7 Accident Investigation Report Public Summary, National Aeronautics and Space Administration, 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, 2015 29 October.
[47] K. Chang, SpaceX Launches a Satellite With a Partly Used Rocket, The New York Times, 2017, 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, 2018, 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, 2017, 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, 2017, https://www.nasaspaceflight.com/2017/11/blue-origin-2020-debut-new-glenn-rocket/.
[51] C. Niederstrasser, W. Frick, Small launch vehicles - a 2016 state of the industry survey, Proceedings of the 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,, 2017, https://www.geekwire.com/2017/virgin-orbit-3d-printing-rockets/.
[53] J. Foust, Relativity Space Aims to 3D Print Entire Launch Vehicles, SpaceNews, 2017, 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, 2015. 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, 2016, 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, 2017 4 August.
[57] R.C. Booton, S. Ramo, The development of systems engineering, IEEE Trans. Aerosp. Electr. Syst. AES-20 (4) (1984) 306–310.
[58] NASA, NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, NASA, 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-Wesley, 1995.
[61] A. Tversky, D. Kahneman, Judgment under uncertainty: heuristics and biases, Science 185 (4157) (1974) 1124–1131 27 September.
[62] N. Dulac, N.G. Leveson, Incorporating safety risk in early system architecture trade studies, AIAA J. Spacecr. Rockets 46 (2) (2009).