AIAA SciTech Forum
11–15 & 19–21 January 2021, VIRTUAL EVENT
AIAA Scitech 2021 Forum

10.2514/6.2021-1122

Check for updates

Risk-Based Formal Requirement Elicitation for Automatic Spacecraft Maneuvering*

Kerianne L. Hobbs † and Alexander R. Collins ‡
Air Force Research Laboratory, Wright-Patterson AFB, OH, 45433

Eric M. Feron§ ¶
Georgia Institute of Technology, Atlanta, GA, 30318
King Abdullah University of Science and Technology (KAUST), Thuwal, 23955-6900, Kingdom of Saudi Arabia

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

As space continues to become more congested, automated techniques for spacecraft maneuvering become increasingly attractive for tasks such as collision avoidance, rendezvous and proximity operations, and station keeping. This work uses hazard analysis to elicit requirements for an autonomous spacecraft controller. Spacecraft maneuvers today are planned by human operators and conducted days to hours in advance. This represents a risk averse climate that is hesitant to rely on automation. In the absence of regulations governing automated maneuvering, a risk-based approach is a promising technique. First, top-down accidents, hazards, and safety constraints are identified. Second, a functional control model for an automatic collision avoidance system on a spacecraft in the context of a theoretical Space Traffic Management system is constructed using System Theoretic Accident Models and Processes (STAMP). Third, unsafe control actions, scenarios, and mitigating requirements are identified using Systems Theoretic Process Analysis (STPA). These requirements form the foundation for the development of automatic control designs for spacecraft. Finally, the safety constraints are formally specified as high level requirements as a path towards formal analysis of the system.

I. Introduction

After maneuvering to avoid a near collision of their Aeolus earth science satellite with SpaceX's Starlink 44 in September 2019, the European Space Agency (ESA) called for the development of an automated collision avoidance system [1]. This call joined a chorus of growing international demands for a Space Traffic Management (STM) system from sources such as the White House [2] and an AIAA position paper emphasizing that collision avoidance is the "top priority and metric for success of the STM Program" [3]. Current collision avoidance approaches largely depend on predictions made between 72 hours and a full week in advance. They are also reliant on human subject matter expert teams to design, evaluate, and upload safe maneuver trajectories to the spacecraft [4–9]. Coordination between different organizations is often accomplished via email [1, 6], with the potential for significant delays. As the space environment becomes even more congested and contested [10], the speed of subject-matter expert decisions may be insufficient to meet requirements and automation will be key to preserving use of space-based resources.

The Federal Communications Commission (FCC) [11, 12], Federal Aviation Administration (FAA) [13], Consultative Committee for Space Data Systems (CCSDS) [14], NASA Systems Engineering Handbook [15], and USAF Space and Missile Systems Center (SMC) Systems Engineering Primer & Handbook [16] all provide design guidance on spacecraft design and operations. However, this guidance focuses on radio frequencies for operation, debris removal, launch safety, spacecraft operations, and general development in a rigorous systems engineering process, and none of these sources provide requirements for design of automatic control systems. Aside from the author's previous work [17–19], there is no publicly available literature on spacecraft automatic maneuver system requirements. This is in part due to the often proprietary or classified nature of spacecraft programs. This research focuses on the use of system hazard analysis to identify safety requirements for a general automatic collision avoidance decision and control systems for spacecraft.

A number of factors, including ineffective safety engineering of spacecraft software, have been shown to cause spacecraft accidents [20]. While software is becoming more prevalent in aerospace, hazard analysis processes outside of

*Approved for Public Release. Case Number 88ABW-2020-1870.
†Research Aerospace Engineer, Autonomous Control Branch, 2210 8th Street, AIAA Member.
‡Research Aerospace Engineer, Autonomous Control Branch, 2210 8th Street, AIAA Member.
§Professor of Aerospace Engineering, School of Aerospace Engineering, 85 Fifth Street NW.
¶Professor of Computer, Electrical and Mathematical Sciences and Engineering, 4700 KAUST.

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

Systems Theoretic Accident Models and Processes (STAMP) and Systems Theoretic Process Analysis (STPA) often fall short of identifying software hazards [21, 22]. STAMP and STPA have been used to analyze spacecraft [23], an aircraft rapid decompression event [24], space launch vehicles [25], safety and cyber security for integrating unmanned aircraft in the national airspace system [26], the NextGen air traffic management system [27, 28] manned-unmanned teaming of aircraft [29, 30], and the takeoff phase of a complex UAV [31], among others. A combination of intent specifications [32], STAMP, and STPA have been applied to a spacecraft in low Earth orbit [33]. However, previous research has not specifically considered hazards for automated maneuvering, and a complete set of safety constraints, and requirements from the process have not been presented.

The primary contributions of this work are to complete the following steps in the process of deriving requirements from hazard analysis for a *spacecraft automatic collision avoidance maneuver system in the context of a hypothetical STM system*:

- Application of STAMP to generate a functional control model of an automatic spacecraft maneuver system within an STM context.
- Adaptation of STAMP from a single-level model to a multi-level model with each model diving deeper into subsystem and component interactions.
- Application of STPA to generate accidents, hazards, safety constraints, and unsafe control actions.
- Identification of patterns for repeatability of the approach for specific applications.
- Examples of formal safety requirement specifications.

First, top-down accidents, hazards, and safety constraints are identified. Second, a functional control model for an automatic collision avoidance system on a spacecraft in the context of a theoretical Space Traffic Management system is constructed using System Theoretic Accident Models and Processes (STAMP). Third, unsafe control actions, scenarios, and mitigating requirements are identified using Systems Theoretic Process Analysis (STPA). These requirements form the foundation for the development of automatic control designs for spacecraft. Finally, the safety constraints are formally specified as high level requirements as a path towards formal analysis of the system.

II. Preliminaries

This section provides background information on the STAMP and STPA methods used to conduct the hazard analysis, as well as the formal logic and mathematical syntax used to formalize system requirements. A hazard assessment methodology using the STAMP modeling framework and the STPA framework was selected because it can be applied early in a design process, incorporates human interaction, and allows for analysis of hazards in the presence of feedback between systems. Many alternative hazard analysis techniques such as failure modes and effects analysis are designed for physical systems with stochastic failure rates, do not include humans or software in the modeling process, are linear and unidirectional. STAMP and STPA can be conducted iteratively from the earliest stage of system design until completion, with refinement as design decisions are made. While STAMP and STPA can provide indication of unsafe actions that could be translated to safety requirements, they are qualitative, not quantitative, and thus cannot provide a risk level or percent reliability. Formal and mathematical requirements presented in this work help bridge that gap. Formal specification and analysis ensures that requirements are unambiguous and free of conflict.

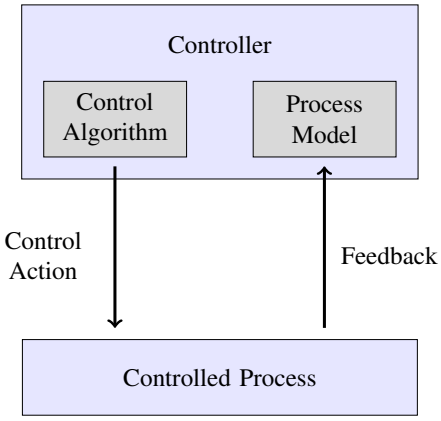


Fig. 1 Components of a STAMP functional control block diagram.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

A. Systems Theoretic Accident Models and Processes

STAMP is a functional control block diagram model of complex systems described in [34], and briefly summarized here. The basic structure of the diagram is shown in Fig. 1 Each of the blocks in the system are functional blocks rather than physical component blocks. This facilitates multiple physical instantiations that satisfy functional requirements. The diagram is also hierarchical: blocks at higher levels have control over blocks at lower levels. Each functional block is either a controller or a controlled process but can be both depending on its location in the diagram and relationship to other blocks. Every controller has a control algorithm that describes how it decides its output and a process model that describes how it uses inputs to construct a model of the world. This model also works for humans, where the control algorithm is how the human can interact with the system, and the process model is the human's mental model of the system. Down arrows in the diagram are control actions while up arrows are feedback. Missing feedback arrows quickly identify likely design vulnerabilities. While not explicitly stated in previous work, STAMP also facilitates nesting of subsystems within larger systems, and can be expanded to explore multiple levels of a system design.

B. Systems Theoretic Process Analysis

Systems Theoretic Process Analysis (STPA) is a hazard analysis methodology described in [34], and briefly summarized here. Three initial steps provide the foundation for the rest of the STPA analysis. The first step is to identify *accidents*, which are undesired or unplanned events that result in some type of loss or undesired outcome, such as human injury or mission failure. The second step is to identify *hazards*, defined as a system state or set of conditions that would lead to an accident in a worst-case environment. Each hazard should tie directly to one or more accidents. The third step is to identify *safety constraints*, which are constraints that can be implemented to reduce the risk level of the hazards.

Having completed these three steps, *unsafe control actions* can be identified by analyzing the STAMP diagram. Unsafe control actions consist of four components: a controller, control action, unsafe control action type, and context. Each control action (down arrow) in the STAMP model is evaluated for four possible unsafe control action types:

- Provided (in an inappropriate context)
- Not provided (in a context where it should be)
- Duration (a continuous control action is provided for too long or too short a duration)
- Timing (a control action is provided too early or too late)

In this research, automatic maneuver system requirements are generated based on the safety constraints and unsafe control actions that constrain behavior and highlight the need for additional requirements or feedback to maintain safety.

C. Formal Specification and Analysis

Formal specification creates an unambiguous description of the system for users, designers, programmers, and testers. Formal specification may use a variety of different logics and languages such as first order logic [35], propositional logic [35] and temporal logics [36–39]. Safety constraints in this research are expressed in *past time linear temporal logic* (ptLTL), which uses temporal operators to describe the past states of an execution trace relative to the current point of reference [39]. A list of ptLTL symbols is listed in precedence order in Table 1.

Table 1 Summary of Past Time Linear Temporal Logic (ptLTL) Symbols.

Symbol	Description	Translation	Alternative Symbols
$\Box$	historically/always	"always"	$[*]$
$\bigcirc^{-1}$	previous step	"previously"	
$\neg$	negation	"not"	!
$\cup$	until	"until"	U
$\wedge$	conjunction	"and"	
$\vee$	disjunction	"or"	
$\Rightarrow$	implication	"implies"	$->$
$\Leftrightarrow$	logical equivalence	"is equivalent to"	$<->$

In this research, the safety constraints were formally specified and analyzed using the Specification and Analysis of Requirements (SpeAR) tool. SpeAR is an open source tool that enables requirements specification in a constrained natural language with the formal semantics of ptLTL. Once the requirements are captured, SpeAR can be used to conduct automated realizability, logical entailment, logical consistency, and traceability analysis. The scope of the analysis in this paper is limited to logical consistency analysis because the focus is on development of safety requirements with limited implementation details. Logical consistency analysis verifies that the safety constraints are free of conflicts for N steps. Understanding the future analysis capabilities and underlying solvers for logical entailment and traceability analysis informs how the specifications are written so that they remain useful as design decisions refine the system abstraction.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

III. Results

In this section, the results of the STAMP, STPA, and formalization activities are described. First accidents, hazards, and safety constraints are identified for the automatic spacecraft maneuvering problem as part of the STPA process. Next, a STAMP model is created for a generic spacecraft in the context of an STM framework. The STAMP model features a spacecraft in communication with a ground station that receives updates about other spacecraft from a space surveillance network. The STAMP model is then analyzed for unsafe control actions using STPA and requirements are generated. Finally, the requirements formalization process and safety constraint patterns identified in the research are described.

A. Accidents, Hazards and Safety Constraints

The first step in the STAMP and STPA process was identifying top-down accidents, hazards, and safety constraints for spacecraft automatic maneuvers. Accident and hazard identification was primarily accomplished by interviewing stakeholders. Two primary *accidents* related to automatic or autonomous spacecraft maneuvering were identified, as follows:

[A1] Spacecraft is damaged or destroyed.
[A2] Spacecraft is unable to complete its mission.

These accidents tie to specific hazards and safety constraints as described in Table 2. The rationale for each hazard and safety constraint are described in depth in the Appendix. The accidents and hazards are obviously not mutually exclusive.

B. STAMP Model

The second step in this research was to develop a STAMP model of a generic sample spacecraft, as shown in figure 2. The sparsely populated elements of the STAMP model include the expected functional components that will interact with an automatic maneuver system from the spacecraft up through informing and controlling agencies, and down to the automatic maneuver system inside the controller subsystem. This STAMP model was designed to facilitate STPA, so controlling function blocks are divided into a control algorithm and process model. Functional blocks that do not control other blocks are modeled as controlled processes. Arrows pointing into each functional block (generally also pointing down) are generally control inputs or other data, while out arrows (generally pointing up) are feedback. Specific functional signals between components are labeled with a description. Recognizing that control inputs occur at multiple levels of a system, this is a three-level model. The first level includes a space surveillance network (SSN), a ground station (GS) block, and a spacecraft (SC) block, which will each be described further in the next several sections.

The space surveillance network (SSN) functional control block could include a current space situational awareness agency, or a future space traffic control agency. The SSN functional block maintains a catalog of spacecraft, updates two-line element (TLE) sets (or some other future standard data format) describing spacecraft properties, independently predicts conjunctions, and issues collision warnings. The SSN may also request ground-based observations of satellites from radars, telescopes, and other resources to maintain a current catalog. The control output of the SSN includes updates to individual spacecraft states based on ground observations as well as event-triggered collision warnings. The SSN can accept observation requests from spacecraft owner/operators in the ground station (GS) block, as well as data such as onboard GPS-based position and velocity which may be higher accuracy than ground-based measurements. While the current state of information exchange between the SSN functional block and GS block is accomplished via emails and phone calls [1, 6], a future space traffic control system could include alternative, less human-centric, automatic communications.

Table 2 Hazards and Safety Constraints

[A1]	[A2]		
✓	✓	[H1] Spacecraft maneuver causes ground communication loss.	[C1] Spacecraft shall maintain attitude requirements for communication with ground station.
✓		[H2] Spacecraft is on a collision course with another spacecraft or debris.	[C2] Spacecraft maneuvers shall maintain safe separation with another spacecraft or debris. [C2alt] Spacecraft maneuvers shall safely approach spacecraft during autonomous rendezvous, proximity operations and docking.
✓		[H3] Spacecraft maneuver is aggressive enough to cause damage.	[C3] Spacecraft shall maneuver below acceleration threshold to cause damage.
✓	✓	[H4] Spacecraft maneuver leads to uncontrollable state.	[C4] Spacecraft maneuver shall maintain controllability.
✓	✓	[H5] Spacecraft generates insufficient power to maintain operations.	[C5] Spacecraft shall maintain attitude requirements for sufficient power generation.
	✓	[H6] Spacecraft loses data transfer with the ground.	[C6] Spacecraft shall maintain attitude requirements for data transfer with ground station.
✓	✓	[H7] Spacecraft damaged or destroyed by an unsafe attitude.	[C7] Spacecraft shall adhere to attitude keep out zone geometries.
✓	✓	[H8] Spacecraft exceeds unsafe attitude duration.	[C8] Spacecraft shall limit duration of unfavorable attitudes.
✓	✓	[H9] Spacecraft expends excess fuel.	[C9a] Spacecraft shall not maneuver if an insufficient amount of time has passed since the last maneuver. [C9b] Spacecraft shall not maneuver if the cumulative maneuver time within a past time frame exceeds a threshold total time. [C9c] Spacecraft shall not maneuver if the fuel level is below an operator-specified threshold. [C9d] Spacecraft shall not maneuver when total fuel reaches the end of life threshold with buffer.
✓	✓	[H10] Spacecraft actuation strategy causes excessive wear or damage to actuators.	[C10] Spacecraft actuation strategy should conserve actuator use to prevent wear when possible.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

The GS function block includes a ground operator and computer where the satellite owner/operator interacts with the SSN and SC. The GS may request observations of their satellite or objects at risk of colliding with their satellite and send current spacecraft data such as GPS position and velocity to the SSN. The GS human operator provides mission definitions, operations, maneuvers, and commands that are communicated through the ground computer to the spacecraft. The GS has a process model of the global state of space traffic management (database and picture of all the catalog of objects), local state of N satellites in the spacecraft “neighborhood" (which may have multiple definitions such as the N objects with the closest approach distance in a finite time horizon), the state of the spacecraft (including position, velocity, orientation, angular rates, and states subsystems as well as other data like health monitoring), and a model of the spacecraft. For the human ground operator, this is a mental model, while the ground computer may maintain a simulation model of the system. Modeled data and commands may be sent from the GS to the SC. The SC

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

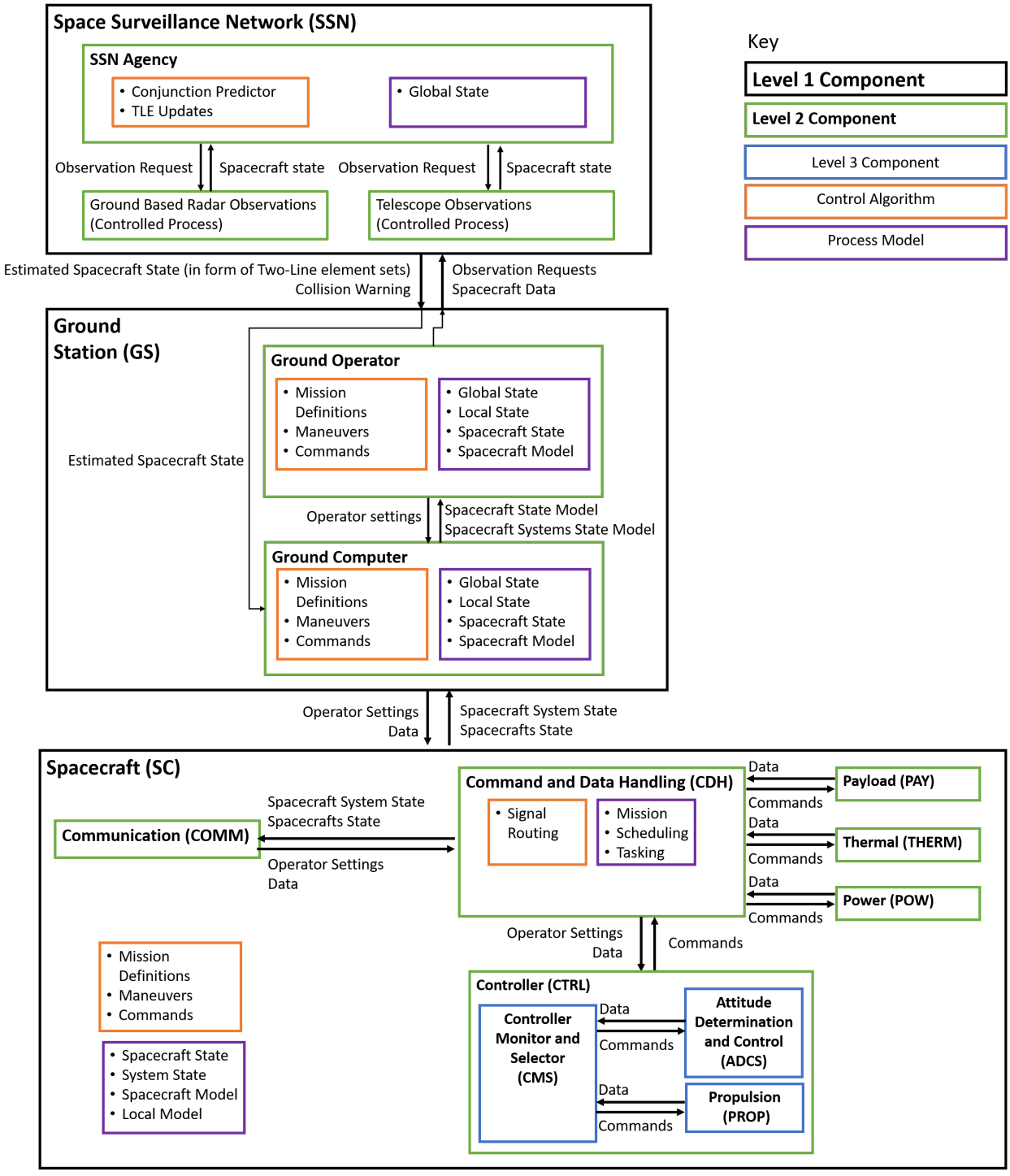


Fig. 2 Multi-layer STAMP model of a hypothetical spacecraft with an automatic maneuver system in the context of a Space Traffic Management System.

provides feedback on the sensed spacecraft, actuator and system states, as well as local state (when capable of sensing or communicating with other objects in the spacecraft "neighborhood," or an echo back of the local state model for verification purposes), and a selected trajectory when a collision avoidance maneuver is activated.

Inside the SC are several subsystems. All data in and out pass through the communication (COMM) subsystem and

then into a central bus called the command and data handling (CDH) subsystem that keeps a model of the mission, schedule, and tasking and then routes data and commands to other subsystems, including the controller (CTRL). The CTRL is anticipated to have a monitor function that evaluates the state of the spacecraft, states of different controllers (which could include translational or rotational control for a variety of tasks, special modes, and degraded operations), incoming commands from operators, and other system information like whether the spacecraft is in communication with the ground, whether it is docked to another spacecraft, whether it is in a special test mode, or if there is a critical operation ongoing that cannot be interrupted.

C. STPA Analysis

For each control action and feedback between systems, STPA analysis was conducted for four possible control action times as described in the Preliminaries section. Two examples of this analysis are provided below, covering the interactions between the Space Surveillance Network (SSN) and the Ground Station (GS) in Table 3, and the Attitude Determination and Control System (ADCS) with the Control Monitor and Selector (CMS) in Table 4. Per the multi-level STAMP Diagram, the former is considered a level 1 analysis, the latter is level 3.

The unsafe control actions identified in this paper tend to fall into the categories of active or passive. *Active* unsafe control actions are those that can only be caused by the spacecraft doing something undesirable, such as running its reaction wheels excessively. *Passive* unsafe control actions are caused by the spacecraft failing to do something desirable, such as failing to actively point at a ground station. Almost no interfaces have the possibility of a “too long" or “too short" duration error. The “too late" unsafe control action type at higher level spacecraft interactions is simply a combination of the “too early” and “not at all” categories. Most current spacecraft communication consists of discrete commands, rather than continuous signals, which renders the “too long" and “too short" error types null. It would certainly be possible for an error to cause a data packet to be too long or too short, but in terms of effect, this is better described as an incorrect or unreadable command. As with active and passive hazards, this assertion breaks down at the lowest levels of communication: those with actual hardware involved. A command to turn on a thruster or ADCS system could certainly run for too long or not long enough. A designer could get around this by having these systems require two discrete commands for “turn on" and “turn off", but this opens up a new set or risks whereupon a thruster or wheel could be left on in the event of a failure. In general, an out-of-control spacecraft would represent a greater hazard than one that with inactive thrusters, if for no other reason that it is easier to predict the latter’s movement. It was observed in this research that the hazards resulting from commands arriving too late are generally equivalent to hazards caused by commands not arriving at all. The sole difference is that “too late” also includes active hazards caused by the (badly-timed) command eventually arriving.

The final observed generalization is that the number of necessary mitigation strategies tends to be far less than the number of possible failures. For example, sending a command multiple times in immediate succession and checking for discrepancies on the receiving end would cost minimal additional bandwidth (unless the command was very large), and would exponentially reduce the chance of random error in the message. This would hypothetically mitigate all errors in the “incorrect" and “unreadable" categories. These generalizations have the potential to significantly simplify automated hazard analysis and traceability.

D. Formalization and Safety Constraint Patterns

Requirements can be sourced from both the safety constraints and unsafe control actions from the STAMP and STPA analysis. The safety constraints are sourced top-down directly from high level accidents and the hazards that could case those accidents. Unsafe control actions are sourced from a bottom-up analysis of signals and information exchanged between different components of the system. A more complete discussion of each of the hazards and safety constraints and an example of the formalization of each safety constraint is found in the Appendix. Safety constraints corresponding directly to the limited set of hazards fell into three general categories: acceleration or velocity limits, pointing and time-bounded pointing constraints, and interlock conditions. Each of these patterns are described in more detail in this section.

1. Acceleration and Velocity Constraints

The simplest safety constraint pattern is constraints on the upper limits of translational and rotational accelerations for all time, i.e. the acceleration in any given axis is always smaller than some maximum and larger than some minimum value. These pattern limits are simple enough to be expressed in propositional, first order, or linear temporal logic and

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Table 3 Unsafe control actions between the SSN and GS

Unsafe Control Action	Rationale / Scenario	Requirement	Related Hazard
SSN provides TLE to GS when TLE contains incorrect data.	Incorrect TLE data may prevent GS from recognizing SC collision course, resulting in a collision.	SSN shall ensure or clarify integrity of TLE information before publishing.	H2
	Incorrect TLE data may cause GS to maneuver when a maneuver is unnecessary, resulting in wasted fuel.	(same as above)	H9
SSN does not provide TLE to GS when TLE has been updated.	Outdated TLE data may prevent GS from recognizing SC collision course, resulting in a collision.	SSN shall publish TLE updates as soon as they are available.	H2
	Outdated TLE data may cause GS to maneuver spacecraft unnecessarily, resulting in wasted fuel.	(same as above)	H9
SSN provides TLE to GS too late when TLE has been updated.	Receiving TLE too late may not provide GS sufficient time to alert SC and maneuver to avoid collision, resulting in a collision.	(same as above)	H2
SSN provides CDM to GS when conjunction criteria are not met.	Sending CDMs when conjunction criteria are not met may result in undue analysis burden to GS, mistrust in CDMs, and the possibility that future CDMs are ignored, resulting in a collision.	SSN shall ensure conjunction criteria met before issuing CDMs.	H2
SSN provides CDM to GS when wrong GS.	If the SSN sends a CDM to the wrong GS, then the GS may not be aware of a potential collision, resulting in a collision.	SSN shall ensure that the correct GS is provided with the CDM.	H2
SSN provides CDM to GS when GS is incapable of interpreting data.	If the SSN sends a CDM to a GS that is unable to interpret it, the GS may not be able to act on the information, resulting in a collision.	SSN shall publish information for GS to be able to interpret CDMs.	H2
SSN does not provide CDM to GS when a conjunction is predicted.	If the SSN does not provide a CDM to a GS when a conjunction is predicted, the GS may not be able to act on the information, resulting in a collision.	SSN shall ensure CDMs are issues when criteria are met.	H2
SSN provides CDM to GS too late when GS has insufficient time to act.	If CDM is issued too close to TCA, it may not be possible for the GS or SC to act on the data, resulting in a collision.	SSN shall issue CDMs as far in advance of the TCA as practical.	H2

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

are summarized by Eqs. 1-2, where θ represents any translational or angular position variable. Acceleration constraints prevent damage to the spacecraft and its components such as a structural failure resulting from excessive forces during acceleration, or excessive wear on an actuator that frequently operates near its limits. Velocity limits on the spacecraft help ensure the spacecraft is controllable within a finite time horizon. For instance, it may be difficult or impossible to slow a spacecraft with high angular velocity so that it is able to achieve communication requirements [40].

Table 4 Unsafe control actions between the ADCS and CMS

Unsafe Control Action	Rationale / Scenario	Requirement	Related Hazard
ADCS provides data to CMS when data is unreadable.	If ADCS sends unreadable data back to CMS, CMS will not be able to tell if a maneuver was performed. This could mean an unnecessary correction is performed, or a necessary one is not performed.	The spacecraft shall have a means of verifying its attitude independently of any sensors included in the ADCS subsystem.	H1,H3-H8,H10
ADCS provides data to CMS when data is incorrect.	If ADCS sends incorrect data back to CMS, CMS will not be able to tell if a maneuver was performed. This could mean an unnecessary correction is performed, or a necessary one is not performed.	(same as above)	H1,H3-H8,H10
ADCS does not provide data to CMS when data is needed immediately.	If ADCS does not send data back to CMS, CMS will not be able to tell if a maneuver was performed. This could mean an unnecessary correction is performed, or a necessary one is not performed.	SSN shall publish TLE updates as soon as they are available.	H2,H5-H8
ADCS provides data to CMS too early when a maneuver is imminent.	If data is sent back too early, it could occupy the CMS at a critical moment, preventing a maneuver from happening on time	SSN shall ensure conjunction criteria met before issuing CDMs.	H2,H5-H8
ADCS provides data to CMS too late when data is needed immediately.	If ADCS sends data back to CMS too late, CMS will not be able to tell if a maneuver was performed. This could mean an unnecessary correction is performed, or a necessary one is not performed.	SSN shall ensure that the correct GS is provided with the CDM.	H1,H3-H8,H10

$$\varphi_{acceleration_{limit}} = \square(\ddot{\theta} \leq \ddot{\theta}_{upper_{limit}}) \wedge (\ddot{\theta} \geq \ddot{\theta}_{lower_{limit}}) \tag{1}$$

$$\varphi_{velocity_{limit}} = \square(\dot{\theta} \leq \dot{\theta}_{upper_{limit}}) \wedge (\dot{\theta} \geq \dot{\theta}_{lower_{limit}}) \tag{2}$$

Safety constraint patterns also include time-bounded requirements on spacecraft orientation.

2. Pointing and Time-Bounded Pointing Constraints

Pointing or time-bounded pointing constraints are commonly used to meet spacecraft attitude requirements, such as communications and solar exclusion zones. First, a centerline unit vector $\hat{n}$ of the desired or undesired attitude is defined. This unit vector may be aligned with the boresight of the sensor or antenna or orthogonal to a solar panel or spacecraft surface, depending on the requirement. From this pointing unit vector, all other angles are measured. Second, an angle around this centerline unit vector $\theta_{\hat{n}}$ is defined by variables such as an antenna or sensor's solid angle field of view α, a maximum sun incidence angle for charging, a generalized unsafe angle from the unit vector θ_{US}, and/or a safety buffer angle β. In this simplest cases of this requirement, such as attitude keep out zones or solar panel charging, the angle between $\hat{n}$ and the object of interest (such as the sun) should be less than the desired angle $\theta_{desired}$ or greater than the undesired angle $\theta_{undesired}$:

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

$$\varphi_{attitude_{exclusion}} = \Box\theta_{\hat{n}} \geq \theta_{undesired}, \tag{3}$$

$$\varphi_{attitude_{desired}} = \Box\theta_{\hat{n}} \leq \theta_{desired}. \tag{4}$$

When the pointing requirement is only to be met during some scheduled time, or under some pointing condition $X_{pointing}$ the scope of these constraints may be reduced from always ($\Box$) to during some scheduled time $t_{scheduled}$ in the form:

$$\varphi_{attitude_{desired}} = \Box(X_{pointing} \vee t_{scheduled}) \implies \theta_{\hat{n}} \leq \theta_{desired}. \tag{5}$$

For more complex instances, labeling functions are used to define a line of sight (LOS) and field of view (FOV) property. The LOS property is true when the angle between object of interest and $\hat{n}$, sometimes called the zenith angle θ_s, is less than some max zenith angle $\theta_{s_{max}}$. The FOV property is true when the angle between the centerline unit vector and some desired object (such as a receiving ground station) or undesired object (such as the sun), which is sometimes called the fixation angle θ_R, is within the angle defined by the second step.

$$L(\theta_s, \theta_R) = \begin{cases} \emptyset, & \text{if } \theta_s > \theta_{s_{max}} \text{ and } \theta_R > \theta_{desired} \\ FOV & \text{if } \theta_s > \theta_{s_{max}} \text{ and } \theta_R \leq \theta_{desired} \\ LOS & \text{if } \theta_s \leq \theta_{s_{max}} \text{ and } \theta_R > \theta_{desired} \\ LOS \wedge FOV & \text{if } \theta_s \leq \theta_{s_{max}} \text{ and } \theta_R \leq \theta_{desired}. \end{cases} \tag{6}$$

Then the safety requirement becomes:

$$\varphi_{attitude_{labeled}} = \Box t_{scheduled} \implies (LOS \wedge FOV). \tag{7}$$

3. Interlock Conditions

The third type of safety constraint describes interlock conditions; conditions where it is unsafe to maneuver even when a fault is not present. These conditions were identified as ways to allow a human operator to intervened to prevent excessive fuel or actuator use, by limiting duration of maneuvers or preventing maneuvers when the fuel level f_l below a fuel level threshold f_{l_t} or end of life reserve $f_{l_{EOL}}$ as follows:

$$\varphi_{duration_{limit}} = (\text{condition on time}) \implies i, \text{ or} \tag{8}$$

$$\varphi_{fuel_{limit}} = (f_l \leq f_{l_t}) \vee (f_l \leq f_{l_{EOL}}) \implies i. \tag{9}$$

E. Formal Analysis

Without a specific space system to analyze, analysis in this research is limited to logical consistency, i.e. whether the constraints are free of conflicts. As the system specification becomes less abstract with the inclusion of additional implementation details, the implementation can be analyzed using formal methods such as model checking to determine whether the design specifications meet the safety constraint and unsafe control action-inspired safety requirements.

In this research, the safety constraints were analyzed using the Specification and Analysis of Requirements (SpeAR) tool to ensure logical consistency. The constraints were found to be logically consistent and the specification may be found on GitHub at https://github.com/act3-ace/spacecraftACASRequirements.

IV. Limitations and Recommendations

Two primary challenges were identified in this research, both of which impact the formal specification and analysis of safety requirements derived from the safety constraints and unsafe control actions. These challenges were the choice of the correct formal description and the limitations of the research tools. To understand the challenge of choosing the correct formal description, consider the safety constraint "maintain safe separation with another spacecraft or debris." There are many ways to express this. One approach is to follow traditional collision avoidance procedures by ensuring that the selected spacecraft path maintains a probability of collision P_c greater than some maximum value [6–9]. This

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

approach also captures the complexity of predicting when a collision will occur when uncertainty is present both at observation time and in the space environment until the predicted time of collision. Combined, these uncertainties make collision estimation a non-trivial endeavor. However, in more controlled cases like autonomous rendezvous, proximity operations, and docking (ARPOD), spacecraft may have more precise state awareness of the other object, which enables safety constraints based on relative position and velocity. For instance, a requirement could be to maintain a relative distance from the other object $||\vec{r}||$ greater than some safe minimum distance r_s. Alternatively, a combination of position and velocity could be used to define safety constraints that allow greater velocity at further distances while restricting motion to smaller relative velocities when objects are closer together. The correct formal description will depend not only on the final implementation of the automatic spacecraft maneuver system, but the specific use case of the system. To overcome this limitation, a study could be conducted to develop logic to differentiate between safe, autonomous rendezvous, proximity operations, and docking behavior from unsafe collision behavior. Such work has already been performed to aid collision avoidance in the aircraft domain [41]. The ability to assess both the position and velocity of an incoming object, discussed in Section IV, would be essential in such a system.

The specification of safety requirements is also limited by the analysis capabilities of requirements tools. In this research, requirements are specified and analyzed using SpeAR which calls on external SMT solvers for logical consistency checking. Mature SMT solvers are generally limited to linear dynamics, so systems with linearized relative motion dynamics may be analyzed, but the analysis breaks down for nonlinear orbital mechanics or attitude dynamics. Alternative analysis methods will need to be used in conjunction. The specification of safety requirements will be heavily dependent on the specific system being analyzed (see Section III.E). However, this issue is significantly mitigated by the ability to partially implement a specification (ability to perform minimal analysis on incomplete specifications) this research, i.e. using only the requirements applicable to the system in question. Because it can easily be partially implemented, as opposed to only being applicable to new systems than can utilize it entirely, it is highly applicable to the update of current systems via software update and constellation replenishment.

An additional recommendation for future efforts arises independently of the limitations of the research. Specifically, the specifications in this research lend themselves well to a safety-driven approach to systems engineering applicable to much more than just spacecraft maneuvering. In particular, the safety constraints could have a substantial role in planning the development of automatic communication procedures.

V. Conclusion

This research demonstrates the development of formal requirements for spacecraft maneuvering using STAMP techniques as a baseline. This represents a methodology applicable to virtually all current and future space assets, with a high degree of relevance in an increasingly congested space environment. In this work, it was demonstrated that STAMP and STPA can be used to identify safety constraints and unsafe control actions that can be formally defined in requirements at early notional design stages. The methods in this research enable an effective, safety-oriented method of systems engineering for automatic spacecraft maneuvering systems.

Appendix: Hazards and Safety Constraints Details

Detailed rationale for each hazard and safety constraint are described in this section, and example formal requirements from the safety constraints are explored.

A. Hazards

With the two accidents in mind, *hazards* were identified. MIL-STD-882E, Department of Defense Standard Practice System Safety [42], defines a hazard as “A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment." In STAMP and STPA, a hazard is defined as a system state or set of conditions that will lead to an accident in a worst-case environment. In both definitions, a hazard is a specific condition that could lead to a mishap or accident. Each hazard is traced to the accident(s) they may cause by indicating those accident numbers in parentheses at the end of the hazard. In STAMP and STPA, rationale is provided for each hazard to provide additional context and examples. The hazards are written in priority order, but this priority may be very subjective depending on the spacecraft and mission.

[H1] Spacecraft maneuver causes ground communication loss (A1, A2).

Rationale: A “loss of spacecraft signal" is addressed in a standard fault protection type called “Command Loss

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Response" at JPL [43]. While this communication loss can be caused by a variety of factors, erroneous spacecraft attitude (pointing error) is focused on here, as it can result from incorrect automatic or autonomous control operations. This hazard is listed first because a ground communication loss prevents operator intervention that may be critical to prevent damage or mission loss. This hazard is further scoped to only referring to maneuvers that prevent ground communication that would otherwise be available and scheduled. Many spacecraft missions do not have constant ground communication and may be intentionally out of contact multiple times a day. This could occur because the spacecraft does not have line of sight to a ground station in the operator's network for a portion of its orbit, or communication with that spacecraft is a lower priority than spacecraft that share the same ground station. This hazard only applies in situations where the spacecraft has line of sight to a ground station in the operator's network and has priority to use it over another spacecraft. Communication requires that the ground station is in the field of view of the spacecraft's communication antenna.

[H2] Spacecraft is on a collision course with another spacecraft or debris (A1).

Rationale: Spacecraft collisions are a large concern as they could not only lead to loss of the spacecraft and mission, they could lead to loss of other spacecraft as well as the creation of debris that threatens other space operations. Several examples of collision events may be found in the literature that motivate the importance of this hazard. These include collisions during rendezvous and proximity operations, as well as confirmed random, accidental collisions:

1) 1994: collision of the Soyuz TM-17 ferry spacecraft with the MIR space station, resulting in only minor damage [44];
2) 1997: collision of the Progress M-34 spacecraft with Mir, causing damage to MIR solar panels, radiators, and a hull puncture [45, 46];
3) 2005: collision of DART with MUBLCOM sending MUBLCOM into a higher orbit with no significant damages [47];
4) 23 December 1991: (but not recognized until 2005) collision of a defunct Cosmos navigation satellite with a piece of debris from another Cosmos satellite [48];
5) 24 July 1996: collision of the French Ceris Satellite with a fragment of Ariane-1 H-10 upper rocket stage [49];
6) 2001: an 800kg, 2-meter diameter cylindrical Russian satellite launched in 1998 was struck by Cosmos 926 debris [50];
7) 17 January 2005: collision of a U.S. rocket body with a fragment of the third stage of a Chinese launch vehicle [48, 50];
8) February 2009: Iridium 33 and Cosmos-225 Collision [51]; and
9) 22 January 2013: BLITS retroreflector satellite was impacted by a piece of orbital debris [52].

In addition to the collision events listed here, several suspected but unconfirmed orbital debris collisions have occurred, and are excluded here for brevity; however more details may be found in [50, 53].

[H3] Spacecraft maneuver is aggressive enough to cause damage (A1).

Rationale: An aggressive maneuver is one with high translational or rotational acceleration. It may cause damage to the structure, payload, or appendages of the spacecraft if these accelerations exceed safe limits. An example of this occurred in April 2016 when a combination of a design flaw in reaction wheel rotation direction and bad settings for rocket firings caused the Japanese Hitomi X-ray observatory to spin out of control, shedding portions of its solar panels or deployable telescope as a result [40].

[H4] Spacecraft maneuver leads to uncontrollable state. (A1, A2).

Rationale: It is possible for a maneuver or successive maneuvers to lead to a loss of the ability to control a spacecraft. In the case of the Japanese Hitomi spacecraft, multiple attitude adjustment failures resulted in a spacecraft that was spinning too fast to completely control [40].

[H5] Spacecraft generates insufficient power to maintain operations (A1, A2).

Rationale: In order to generate power, the spacecraft's solar panels must be pointed towards the sun. If a spacecraft is unable to point the solar panels at the sun, or is unable to maintain that attitude, the solar panels may not provide sufficient power to keep batteries charged. This hazard is listed fifth because while it may not directly cause damage or mission loss, many other critical subsystems cannot operate without power. In 1998, a series of attitude anomalies on the Near Earth Asteroid Rendezvous (NEAR) spacecraft nearly caused the loss of the spacecraft, which recovered in a safe mode designed to minimize power usage and maximize solar array output [54]. The Japanese Hitomi attitude failures are an example of this hazard because eventually the spacecraft was spinning too fast for the solar panels to sustain the satellite's battery [40]. This is an excellent example of one

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

hazard causing another hazard.

[H6] Spacecraft loses data transfer with the ground (A2).
Rationale: Data transfer is similar to general communication requirements but features higher bandwidth requirements and often tighter antenna field of view pointing requirements. A loss of data transfer ability could lead to a loss of mission data, this is especially true when onboard memory is often very limited. If the onboard memory fills before the data can be transferred down, new data may not be saved, or older data will have to be deleted before it can be downlinked to the ground for more permanent storage.

[H7] Spacecraft damaged or destroyed by unsafe attitude (A1, A2).
Rationale: Depending on the spacecraft mission or payload, there may be attitudes where it is unsafe to point a spacecraft. The most common example is the solar exclusion angle; where sensitive instruments must not be pointed too close to the sun to avoid damage. This is the motivation behind exclusion zone guidance methods for spacecraft such as that in [55].

[H8] Spacecraft exceeds unsafe attitude duration (A1, A2).
Rationale: This hazard was documented with three specific conditions in mind: the spacecraft attitude causes excessive heating from sun exposure on a particular component (thermal management), the spacecraft's solar panels are pointed away from the sun for long enough to threaten spacecraft power loss (power management), or spacecraft components are left within a solar exclusion angle long enough to cause damage. Development of a safe mode for the Cassini spacecraft included reaching an attitude that enabled the spacecraft to communicate with the ground, was thermally safe for several days, could be maintained without being overwhelmed by aerodynamic forces curing low altitude flybys, and that gave the star tracker a clear field of view [56]. Many spacecraft have a "safe mode" that may do one or more of the following [43]: minimize power by stopping the current operations, powering down all nonessential functions, configuring hardware in safe states, establishing uplink and downlink communications, reconfiguring antenna, and commanding an attitude that achieves thermal safety and solar panel charging.

[H9] Spacecraft expends excess fuel (A1, A2).
Rationale: Fuel is a limited resource on spacecraft and could lead to mission or spacecraft loss when depleted. For example, during the 1998 NEAR spacecraft anomaly, nearly 29 kg of fuel (corresponding to 96 m/s of delta-v) were burned in thousands of thruster fires [54]. After recovering, the spacecraft had barely enough fuel to conduct the original mission, with little to no margin for additional error.

[H10] Spacecraft actuation strategy causes excessive wear or damage to actuators (A1, A2).
Rationale: This hazard was documented with reaction wheel actuators in mind. Reaction wheel actuators control spacecraft attitude by spinning to exchange momentum with the spacecraft. Reaction wheels can become saturated when commanded to their limits and can undergo wear if kept near their limits for extended periods of time. Loss of two reaction wheels occurred in the Kepler Space Telescope mission. After the first wheel was lost, the wheel vendor recommended keeping the wheel speeds below 300 revolutions per minute to preserve functionality of the remaining wheels for as long as possible [57].

B. Safety Constraints

MIL-STD-882E [208.2.1(h)] [42] requires a list of constraints that can be implemented to reduce the risk level of hazards. In the STPA process, a safety constraint is a capability that will prevent a hazard from occurring. The safety constraints corresponding to each of the hazards are listed here. These safety constraints are traced to their corresponding hazards and used to generate formal requirements. Safety constraints here are scoped to only those relating to satellite control.

Each of the formalized safety constraints in this section describe the requirements of the system; they define what property that should be true. Design specifications that describe how the system behaves to achieve those requirements may use a variety of approaches and are left open ended.

[C1] Spacecraft shall maintain attitude requirements for communication with ground station (H1). In order to formally specify this constraint as a requirement in ptLTL, first a few definitions are needed. As depicted in Fig. 3, the solid angle field of view (FOV) α is the total angle observable to the sensor/transmitter, the boresight is the centerline of the sensor/transmitter FOV, the target zenith angle θ_s is the angle between the sensor/transmitter and surface normal, and the fixation angle θ_R is the angle between the sensor/transmitter boresight and the receiver.
For communication, a reasonable assumption is that the antenna's solid angle field of view (FOV) α is approximately 70° [58]. Let the atomic proposition $AP = \{LOS_{COMM}, FOV_{COMM}\}$ be the set of events where LOS_{COMM}

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

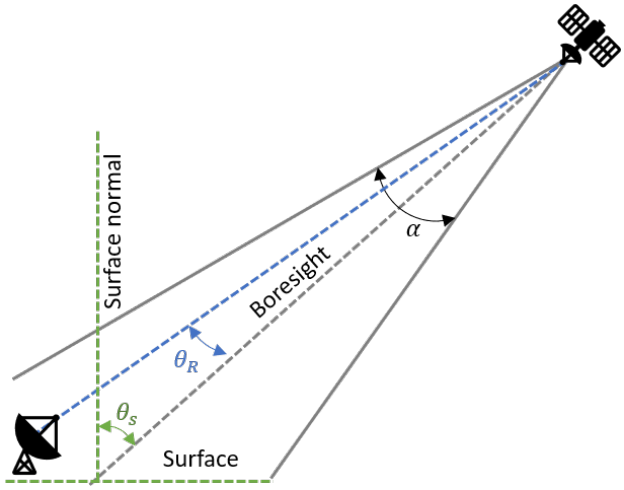


Fig. 3 Diagram of solid angles, boresight, zenith angle, and fixation angle for a satellite communication antenna.

indicates the ground station is in light of sight of the satellite when the zenith angle θ_s is less than or equal to 90° ($\theta_s \leq 90°$), as depicted in Fig. 4a and FOV_{COMM} indicates that the fixation angle θ_R is smaller than half the antenna solid view FOV α ($\theta_R \leq \alpha$) as depicted in 4b. The trace of the system trajectory is then given by the labeling function $L(\theta_s, \theta_R) : \mathbb{R}^2 \rightarrow 2^{AP}$:

$$L(\theta_s, \theta_R) = \begin{cases} \emptyset, & \text{if } \theta_s > \frac{\pi}{2} \text{ and } \theta_R > \frac{\alpha}{2} \\ FOV_{COMM} & \text{if } \theta_s > \frac{\pi}{2} \text{ and } \theta_R \leq \frac{\alpha}{2} \\ LOS_{COMM} & \text{if } \theta_s \leq \frac{\pi}{2} \text{ and } \theta_R > \frac{\alpha}{2} \\ LOS_{COMM} \wedge FOV_{COMM} & \text{if } \theta_s \leq \frac{\pi}{2} \text{ and } \theta_R \leq \frac{\alpha}{2}. \end{cases} \tag{10}$$

Then the safety requirement becomes:

$$\varphi_{C1} = \Box scheduled_{COMM} \implies (LOS_{COMM} \wedge FOV_{COMM}). \tag{11}$$

Further refinements on this requirement might include temporal considerations, such as ensuring proper orientation for some time before the scheduled communication window, to sometime after. A design specification should be created to ensure the spacecraft attitude controller maintains the communication safety constraint requirement φ_{C1}.There is an assumption with this requirement that scheduled communication only takes place when the satellite is within the line of sight of the ground station LOS_{GS}, and in the case of a ground station with a limited field of view receiver, that the satellite is within the ground station's field of view FOV_{GS}. This is a constraint that should be checked on the scheduler.

[C2] Spacecraft maneuvers shall maintain safe separation with another spacecraft or debris (H2).

There are several ways to represent safe separation, including but not limited to the following:

- The spacecraft are safely separated if the probability of collision P_c is less than some maximum $P_{c_{max}}$, such as 10^{-4} used in modern spacecraft collision detection and avoidance approaches [6–9].

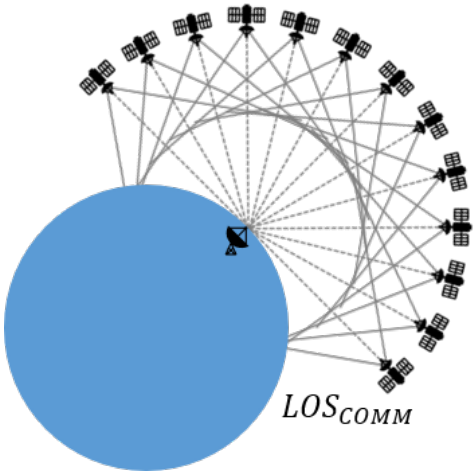
$$\varphi_{C2_{P_c}} = \Box(P_c \leq P_{c_{max}}). \tag{12}$$

- The spacecraft are safely separated if the distance in the relative motion Hill's frame $||\vec{r}_H||$ is greater than some separation distance r_s. This is representative of collision detection systems that warn when the closest simulated miss distance is less than 200 meters, 300 meters, or 1 kilometer (depending on organization) away.

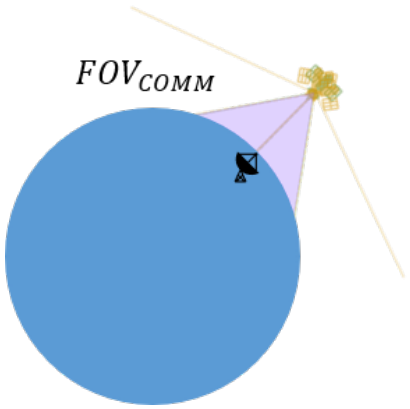
$$\varphi_{C2_{r_s}} = \Box||\vec{r}_H|| > r_s. \tag{13}$$

- The spacecraft are safely separated if the distance in the relative motion Hill's frame $||\vec{r}_H||$ is greater than some separation distance r_s and the relative velocity $||\vec{v}_H||$ is below a threshold v_s, or the spacecraft are

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122



(a) Examples of satellites with line of sight to a ground station, which occurs when the angle between the communication transmitter on the satellite and the surface normal to the Earth's surface where the ground station is located (the zenith angle θ_s) is less than or equal to 90°.



(b) Examples of satellite orientations where the angle between the communication transmitter boresight and the ground station (the fixation angle θ_R) is less than half the antenna solid angle field of view (FOV) α. The two yellow satellites represent extremes of the possible orientations, where the boresight is within the purple shaded region.

Fig. 4 Depictions of satellite communication with line of site or field of view to a ground station.

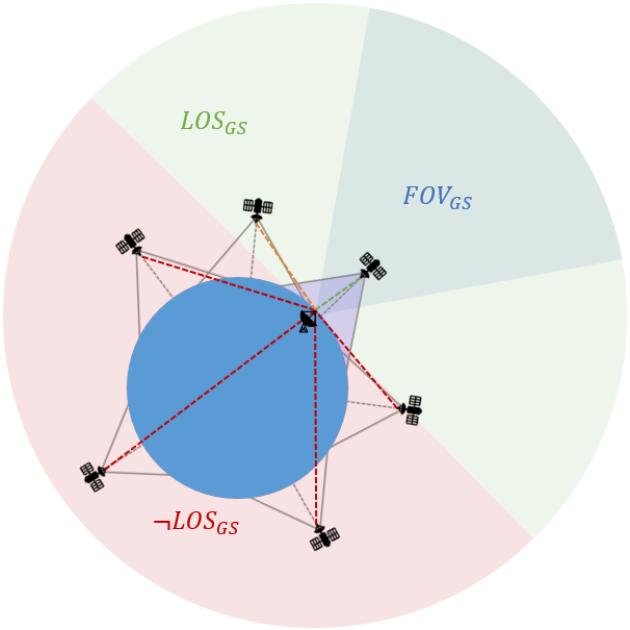


Fig. 5 Notional depiction of regions where the Ground Station's receiver antenna has line of sight to the ground station (LOS_{GS}) , does not have line of sight ($\neg LOS_{COMM}$), and when the satellite's antenna is in field of view of the ground station (FOV).

moving away from one another. Recall that the inner product (or dot product) can indicate relative motion

of the of the spacecraft, as depicted in 6:

$$\vec{v}_H^T \vec{r}_H = \vec{v}_H \cdot \vec{r}_H = ||\vec{v}_H|| ||\vec{r}_H|| \cos\theta = \begin{cases} > 0 \implies \text{moving away} \\ < 0 \implies \text{moving toward} \\ = 0 \implies \text{moving orthogonally.} \end{cases} \tag{14}$$

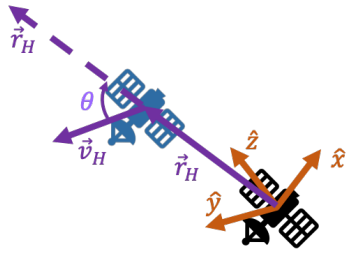


Fig. 6 Relative position and velocity vectors between two objects in Hill's reference frame.

This constraint then becomes:

$$\varphi_{C2_{rv}} = \square(||\vec{r}_H|| > r_s) \wedge \Big((||\vec{v}_H|| < v_s) \vee (\vec{v}_H^T \vec{r}_H \geq 0)\Big). \tag{15}$$

[C2alt] Spacecraft maneuvers shall safely approach spacecraft during autonomous rendezvous, proximity operations and docking (H2). In cases where spacecraft formation flying or a controlled collision (docking) is intended, alternative criteria may be developed. A variation on this constraint changes the magnitude of the acceptable velocity moving towards the spacecraft based on the distance between the spacecraft, where acceptable relative velocity decreases as the spacecraft distance decreases, as depicted in Fig. 7.

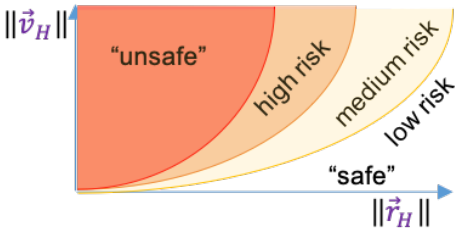


Fig. 7 Notional depiction of a variable safe relative velocity v_s that decreases as the distance between two spacecraft decreases, where a variable risk level setting adjusts the curves to allow higher velocity as the spacecraft approaches.

This concept is also like detecting the difference between aircraft flying in formation and aircraft on a collision course [41]. In the Automatic Air Collision Avoidance System (Auto ACAS) development, a set of formation logic based on range and closure rate as seen in Fig. was used to define whether to inhibit an automatic collision avoidance maneuver. A similar study could be conducted to determine a formation and docking deactivation region for spacecraft.

This concept is notionally borrowed from the idea of using a temporal rather than distance requirement to avoid collisions in the aircraft domain where the time-to-collision T_c is the separation distance $||\vec{r}_H||$ over closure velocity $||\vec{v}_H||$ [59]:

$$T_c = \frac{||\vec{r}_H||}{||\vec{v}_H||}. \tag{16}$$

However, this function assumes a linear path and in aircraft avoidance maneuver, or in spacecraft relative motion, the path is not linear. A better estimate may be found by the time to collision point T_{cp}, which is

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

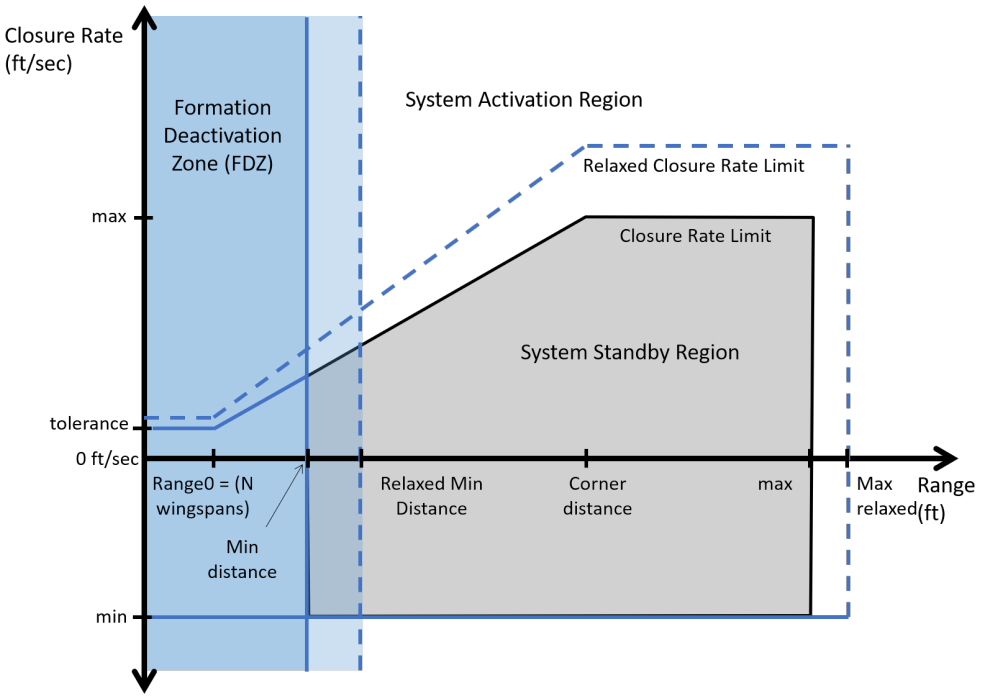


Fig. 8 Formation flight boundary diagram for the Automatic Air Collision Avoidance (Auto ACAS) program [41].

the distance from the present position along the trajectory to the collision point d_{cp}, divided by the speed along the trajectory s_{cp} [59]:

$$T_{cp} = \frac{d_{cp}}{s_{cp}}. \tag{17}$$

Given the development of a finite set of collision avoidance maneuvers, the T_{cp} could be computed for each maneuver option and used in the decision to engage an automatic collision avoidance maneuver. Alternatively, T_c may be a function of the available thrust, spacecraft mass, and distance from the target, where

$$T_c(F_{max}, m_j, ||\vec{r}_H||) = \sqrt{\left(\frac{2m_j}{F_{max}}(||\vec{r}_H||)\right)} \tag{18}$$

The relative velocity of the target spacecraft should be less than the limit defined by a safety factor f_s the following equation:

$$\varphi_{rv} = \square||\vec{v}_H|| \leq v_{H_{max}}, v_{H_{max}} = \frac{(f_s)(||\vec{r}_H||)}{T_c(F_{max}, m_j, ||\vec{r}_H||)} \tag{19}$$

The combination of a linear and time-based velocity limits may be seen in Fig. 9.

[C3] Spacecraft shall maneuver below acceleration threshold to cause damage (H3).

Spacecraft translational and rotational acceleration limits depend on the limits of the structure of the spacecraft (ex. $\ddot{x}_{str}$), the payload that may vary on satellites that otherwise feature the same components (ex. $\ddot{x}_{pay}$), and variations of limits for special states like the use of deployable antennas or booms (ex. $\ddot{x}_{sp}$). For each axis of translational and rotational acceleration, the minimum and maximum accelerations follow the form $\ddot{x}_{min} = -\min(|\ddot{x}_{str}|, |\ddot{x}_{pay}|, |\ddot{x}_{sp}|)$ and $\ddot{x}_{max} = \min(|\ddot{x}_{str}|, |\ddot{x}_{pay}|, |\ddot{x}_{sp}|)$. This is assuming that the acceleration limits are the same in the positive and negative directions. In the case that the limits are not equal and opposite in each direction, the smallest acceleration in either direction (positive or negative) along the axis is the limit for that

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

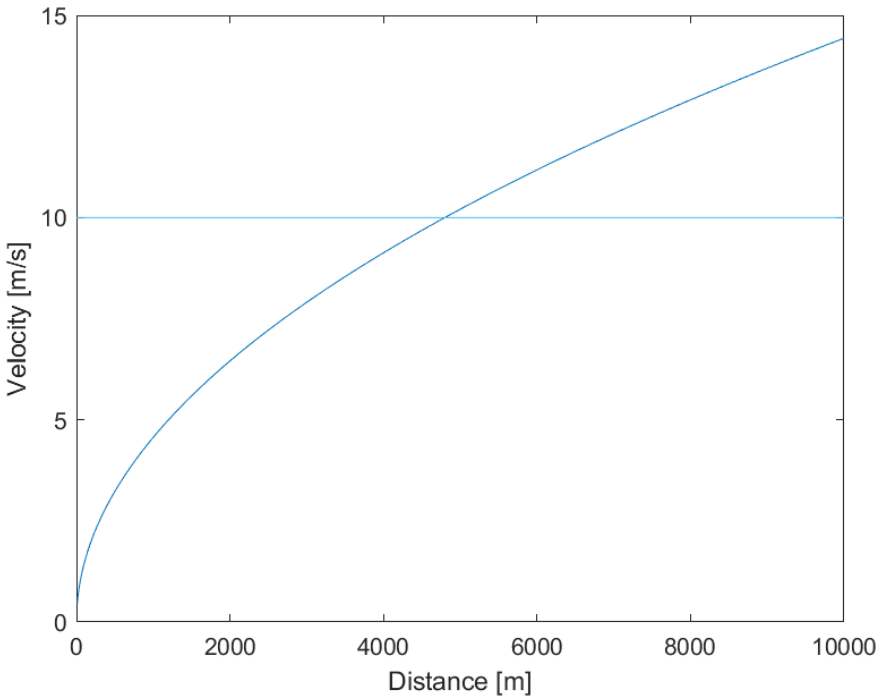


Fig. 9 Maximum velocity versus distance for a constant limit and for a limit allowing for half of maximum deceleration

direction. Then the constraint becomes:

$$\begin{aligned}\varphi_{C3} =& \Box(\ddot{x}_{min} \leq \ddot{x}) \wedge (\ddot{x} \leq \ddot{x}_{max}) \wedge (\ddot{y}_{min} \leq \ddot{y}) \wedge (\ddot{y} \leq \ddot{y}_{max}) \wedge (\ddot{z}_{min} \leq \ddot{z}) \wedge (\ddot{z} \leq \ddot{z}_{max}) \\ & \wedge (\ddot{\theta}_{1_{min}} \leq \ddot{\theta}_1) \wedge (\ddot{\theta}_1 \leq \ddot{\theta}_{1_{max}}) \wedge (\ddot{\theta}_{2_{min}} \leq \ddot{\theta}_2) \wedge (\ddot{\theta}_2 \leq \ddot{\theta}_{2_{max}}) \wedge (\ddot{\theta}_{3_{min}} \leq \ddot{\theta}_3) \wedge (\ddot{\theta}_3 \\ & \leq \ddot{\theta}_{3_{max}}).\end{aligned} \tag{20}$$

[C4] Spacecraft maneuver shall maintain controllability (H4).
In its simplest form, this constraint states that the state of the spacecraft X_{sc} always remains within the set of controllable states:

$$\varphi_{C4} = \Box X_{sc} \in \mathcal{X}_C. \tag{21}$$

Determining the set of controllable states is non-trivial though. A linear time invariant (LTI) system is controllable if for all initial and final states in the state of real numbers ($\forall x_o, x_f \in \mathbb{R}^n$) there exists a control input for a time between 0 and the final time ($\exists u(t), t \in [0, -t_f]$ such that the final state is reached at the final time ($s.t.\ x(t_f) = x_f$). One test for controllability is the controllability matrix: (A, B) is controllable if $C(A, B) = [B, AB, A^2B, ..., A^{n-1}B]$ is full rank (also $C(A, b)$ is invertible).
The relative translational motion of a “chaser" (or “deputy") spacecraft to a target (or chief) spacecraft, in linearized Clohessy-Wiltshire dynamics in Hill’s frame are:

$$\begin{aligned}\ddot{x} &= 2n\dot{y} + 3n^2x + \frac{F_x}{m_c} \\ \ddot{y} &= -2n\dot{x} + \frac{F_y}{m_c} \\ \ddot{z} &= -n^2z + \frac{F_z}{m_c}\end{aligned} \tag{22}$$

In state space form ($\dot{X} = AX + BU$), the equations may be described as:

$$\dot{X} = \begin{bmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \\ \ddot{x} \\ \ddot{y} \\ \ddot{z} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 3n^2 & 0 & 0 & 0 & 2n & 0 \\ 0 & 0 & 0 & -2n & 0 & 0 \\ 0 & 0 & -n^2 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ \dot{x} \\ \dot{y} \\ \dot{z} \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1/m_c & 0 & 0 \\ 0 & 1/m_c & 0 \\ 0 & 0 & 1/m_c \end{bmatrix} \begin{bmatrix} F_x \\ F_y \\ F_z \end{bmatrix} \tag{23}$$

As can be found from the equations, the controllability matrix $C(A, B) = [B, AB, A^2B, ..., A^{n-1}B]$ is full rank, indicating that it is controllable. In addition, the in-plane dynamics (x and y) are decoupled from the out-of-plane dynamics (z). While the dynamics are controllable, the in-plane dynamics are unstable with two eigenvalues at the origin and two at $\pm nj$. The out-of-plane dynamics are stable with two eigenvalues at $\pm nj$. The in-plane dynamics are completely controllable from F_y but not controllable from F_x, and the out of plane dynamics are controllable from F_z.

The spacecraft attitude dynamics are nonlinear and cannot be evaluated using a traditional controllability matrix test. More details on the spacecraft attitude dynamics were described previously by the authors in [17, 18].

While the system is completely controllable, it is possible for the translational or angular velocity to be so high that it exceeds reasonable capabilities of the actuators. One way to deal with this is to place limits on the maximum angular velocity, much like the acceleration limits in constraint 3. Then the constraint becomes:

$$\varphi_{C4} = \square(\dot{x} \leq \dot{x}_{max}) \wedge (\dot{y} \leq \dot{y}_{max}) \wedge (\dot{z} \leq \dot{z}_{max}) \wedge (\dot{\theta}_1 \leq \dot{\theta}_{1_{max}}) \wedge (\dot{\theta}_2 \leq \dot{\theta}_{2_{max}}) \wedge (\dot{\theta}_3 \leq \dot{\theta}_{3_{max}}). \tag{24}$$

[C5] Spacecraft shall maintain attitude requirements for sufficient power generation (H5).

The use of solar panels to provide power to spacecraft is ubiquitous. Since these panels must face the sun to function, power generation is inherently tied to attitude in most spacecraft. Solar panel charging may be triggered in multiple ways. One way is by scheduling charging attitudes based on projections of orbital locations and power usage. Let $scheduled_{CHRG}$ be an atomic proposition indicating that charging is scheduled at the present time. Another way to trigger charging is to monitor the depth of discharge DOD of the batteries. When above a threshold DOD_{max}, a sun safe mode is activated that minimizes power usage and maximizes charging [54] until some charge level is achieved.

In order to generate power, the solar panels must have a sun incidence angle that is within a range required for charging. The power P generated by the solar panels is described by

$$P = P_I I_d \cos\theta_{SI}, \tag{25}$$

where P_I is the ideal performance (maximum power that can be generated in watts per square meter), I_d is inherent degradation (nominally 0.677, generally $\in [0.49, 0.88]$), and θ_{SI} is the sun incidence angle (angle between the surface normal $\hat{n}_{SP}$ and sun incident $\hat{r}_{SI}$ unit vectors [58]. The cosine of the sun incidence angle is the cosine loss of power generated compared to a sun pointed normal to the solar panels. The geometry for charging is depicted in Fig. 10.

The constraint then becomes that when the depth of discharge is above the max threshold, or when charging is scheduled, the spacecraft should have a sun incidence angle smaller than the angle required for charging:

$$\varphi_{C5} = \square((DOD > DOD_{max}) \vee scheduled_{CHRG}) \implies (\theta_{SI} \leq \theta_{CHRG}). \tag{26}$$

[C6] Spacecraft shall maintain attitude requirements for data transfer with ground station (H6).

This constraint is very similar [C1], except that the antenna's solid angle FOV for data transfer α_{DATA} is usually tighter than that required for communications, necessitating a separate constraint. For data transfer, a reasonable assumption is that α_{DATA} is approximately 40° [58]. Let the atomic proposition $AP = \{LOS_{DATA}, FOV_{DATA}\}$ be the set of events where LOS_{DATA} indicates the ground station is in line of sight of the satellite when the zenith angle θ_s is less than or equal to 90° ($\theta_s \leq 90°$), and FOV_{DATA} indicates that the fixation angle θ_R is smaller than half α_{DATA} ($\theta_R \leq \frac{\alpha_{DATA}}{2}$). The trace of the system trajectory is then given by the labeling function $L(\theta_s, \theta_R) : \mathbb{R}^2 \rightarrow 2^{AP}$:

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

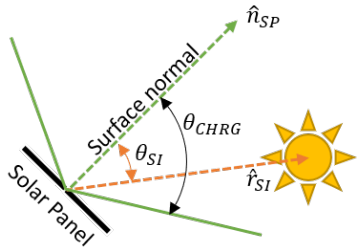


Fig. 10 Relative position and velocity vectors between two objects in Hill's reference frame.

$$L(\theta_s, \theta_R) = \begin{cases} \emptyset, & \text{if } \theta_s > \frac{\pi}{2} \text{ and } \theta_R > \frac{\alpha_{DATA}}{2} \\ FOV_{DATA} & \text{if } \theta_s > \frac{\pi}{2} \text{ and } \theta_R \leq \frac{\alpha_{DATA}}{2} \\ LOS_{DATA} & \text{if } \theta_s \leq \frac{\pi}{2} \text{ and } \theta_R > \frac{\alpha_{DATA}}{2} \\ LOS_{DATA} \wedge FOV_{DATA} & \text{if } \theta_s \leq \frac{\pi}{2} \text{ and } \theta_R \leq \frac{\alpha_{DATA}}{2}. \end{cases} \tag{27}$$

Then the safety requirement becomes:

$$\varphi_{C6} = \Box scheduled_{DATA} \implies (LOS_{DATA} \wedge FOV_{DATA}). \tag{28}$$

Like [C1], several possible refinements may be made on this constraint.

[C7] Spacecraft shall adhere to attitude keep out zone geometries (H7).

The spacecraft adheres to attitude exclusion zone geometries when the angle between the sensor boresight and the direction of exclusion $\hat{r}$, denoted θ_{EZ} is less than half the sensor field of view α plus a safety buffer angle β, as depicted in Fig.11. Then the safety requirement becomes:

$$\varphi_{C7} = \Box \theta_{EZ} > \frac{\alpha}{2} + \beta \tag{29}$$

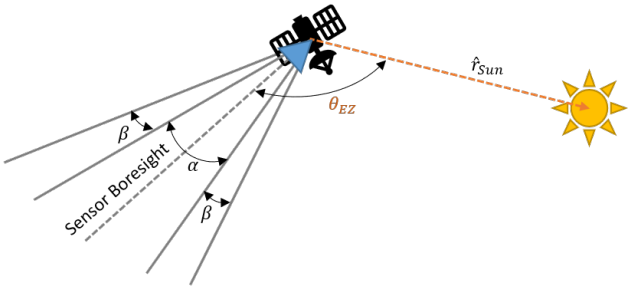


Fig. 11 Notional depiction of attitude keep out (or exclusion) zone geometry.

[C8] Spacecraft shall limit duration of unfavorable attitudes (H8).

The primary difference between [C7] and [C8] is that in [C7] it is never safe to point in an exclusion zone direction, while in [C8] it is acceptable to point in an exclusion zone direction as long as it is for a limited duration. Let $AP = \{LOS_S, T_S\}$ be the set of events where LOS_S indicates that the spacecraft is in a favorable and safe attitude, and T_S indicates that if the system has been pointing in an unfavorable duration, it has been for a safe duration. One way to define the safe line of sight is using the method in [C7]. Another way to define the safe line of sight is with a vector X_{US} aligned with the sensitive spacecraft directions and the vector to the unfavorable attitude $\hat{r}$. In this case, θ_R is the angle between the sensitive spacecraft component and the unsafe attitude direction, and θ_{US} is some buffer angle around the sensitive spacecraft component that shouldn't be exposed to the unsafe attitude for a long duration of time. In the case where one face of the spacecraft is sensitive to an exclusion zone, θ_{US} might be 90°. The line of sight is safe (LOS_S is true) when $\theta_R > \theta_{US}$, as pictured in Fig. 12. The pointing duration is safe

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

(T_S is true) when the amount of time that the system has had an unfavorable attitude t_{US} is less than the duration safety limit T_{SL}. These conditions are captured by the labeling function $L(LOS_S, T_S) : \mathbb{R}^2 \rightarrow 2^{AP}$:

$$L(LOS_S, T_S) = f(\theta_R, t_{US}) = \begin{cases} \neg LOS_S \wedge \neg T_S & \text{if } \theta_R \leq \theta_{US} \text{ and } t_{US} \geq T_{SL} \\ \neg LOS_S \wedge T_S & \text{if } \theta_R \leq \theta_{US} \text{ and } t_{US} < T_{SL} \\ LOS_S \wedge \neg T_S & \text{if } \theta_R > \theta_{US} \text{ and } t_{US} \geq T_{SL} \\ LOS_S \wedge T_S & \text{if } \theta_R > \theta_{US} \text{ and } t_{US} < T_{SL}. \end{cases} \tag{30}$$

Then the safety requirement becomes:

$$\varphi_{C8} = (LOS_S \wedge T_S) \vee (LOS_S \wedge \neg T_S) \vee (\neg LOS_S \wedge T_S) \tag{31}$$

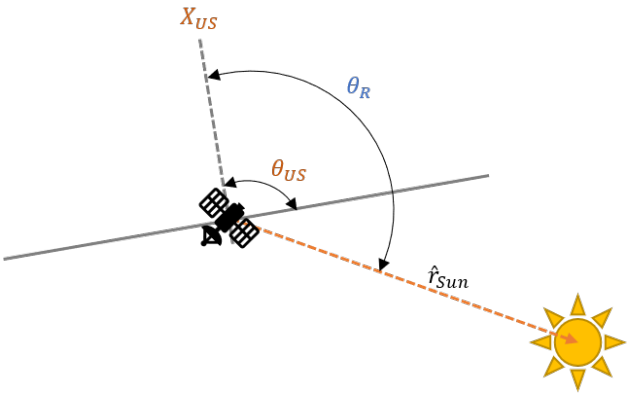


Fig. 12 Notional depiction of attitude keep out (or exclusion) zone geometry.

[C9] Hazard 9 is divided into 4 different safety constraints, each one of which corresponds to an interlock condition. An interlock condition occurs when two events are mutually exclusive. In the case of [C9], each constraint represents a condition that would prevent an autonomous system from maneuvering as a safety measure to prevent excessive fuel use. Interlock conditions should be used sparingly and analyzed for conflicts with other requirements. For example, the Mars Polar Lander included a requirement to go into a sleep mode to conserve batteries after 24 hours without receiving a command, which conflicted with a requirement to test alternative communication methods after 24 hours without a command [60].

[C9a] Spacecraft shall not maneuver if an insufficient amount of time has passed since the last maneuver (H9).
Restricting the minimum time between maneuvers provides an opportunity for a human or computer monitor to detect a fault between firings and prevents a fault from triggering multiple successive firings that deplete fuel reserves. This translates to an interlock condition i being true when the time since the last maneuver T_{s_m} is less than or equal to some minimum time between maneuvers $T_{s_{m_{min}}}$, written as:

$$\varphi_{C9a} = T_{s_m} \leq T_{s_{m_{min}}} \implies i \tag{32}$$

[C9b] Spacecraft shall not maneuver if the cumulative maneuver time within a past time frame exceeds a threshold total time (H9).
Restricting the maximum amount of time that a system can maneuver (i.e. expend fuel) within a time window is a second fault tolerance approach. In this case, if the cumulative maneuver time T_{c_m} exceeds a maximum cumulative maneuver time $T_{c_{m_{max}}}$, an interlock condition i is present.

$$\varphi_{C9b} = T_{c_m} > T_{c_{m_{max}}} \implies i \tag{33}$$

[C9c] Spacecraft shall not maneuver if the fuel level is below an operator-specified threshold (H9).
This constraint allows a human operator to specify a fuel level that an automated maneuver cannot operate under as an additional fault tolerant approach. For this constraint, if the fuel level f_l goes below the operator specified threshold, f_{lt}, then an interlock condition i is present.

$$\varphi_{C9c} = f_l \leq f_{lt} \implies i \tag{34}$$

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

[C9d] Spacecraft shall not maneuver when total fuel reaches the end of life threshold with buffer (H9).
Anticipated to be far below the operator's safety threshold, another fault tolerant measure is to ensure faulty automatic maneuvers do not deplete the fuel required to deorbit or reorbit a satellite at the end of its life. Similarly to [C9c], this is written formally as:

$$\varphi_{C9d} = f_l \leq f_{lEOL} \implies i. \tag{35}$$

[C10] Spacecraft actuation strategy should conserve actuator use to prevent wear when possible (H10).
As discussed in [18], this constraint is like the acceleration and velocity constraints of [C3] and [C4]. Accelerating uses fuel or can cause excessive wear to actuators like reaction wheels and excessive velocity on internal actuators over an extended period can have the same effect. While there may be other factors, for a first cut, acceleration and velocity limits are used here, assuming the limits are the same in the positive and negative direction, which may not be the case for all situations.

$$\begin{aligned}\varphi_{C3} =& \square(||\ddot{x}|| \leq \ddot{x}_{wear}) \wedge (||\ddot{y}|| \leq \ddot{y}_{wear}) \wedge (||\ddot{z}|| \leq \ddot{z}_{max}) \wedge (||\ddot{\theta}_1|| \leq \ddot{\theta}_{1_{wear}}) \wedge (\ddot{\theta}_{|}|2|| \leq \ddot{\theta}_{2_{wear}}) \\ & \wedge (||\ddot{\theta}_3|| \leq \ddot{\theta}_{3_{wear}}) \wedge (||\dot{x}|| \leq \dot{x}_{wear}) \wedge (||\dot{y}|| \leq \dot{y}_{wear}) \wedge (||\dot{z}|| \leq \dot{z}_{wear}) \wedge (||\dot{\theta}_1|| \leq \dot{\theta}_{1_{wear}}) \\ & \wedge (||\dot{\theta}_2|| \leq \dot{\theta}_{2_{wear}}) \wedge (||\dot{\theta}_3|| \leq \dot{\theta}_{3_{wear}}).\end{aligned} \tag{36}$$

A summary of the safety constraint formalization is presented in Table 5.

Table 5 Summary of formalized safety constraints in ptLTL.

Requirement	ptLTL
φ_{C1}	$\square scheduled_{COMM} \implies (LOS_{COMM} \wedge FOV_{COMM})$
$\varphi_{C2_{P_c}}$	$\square(P_c \leq P_{c_{max}})$.
$\varphi_{C2_{r_s}}$	$\square\|\|\vec{r}_H\|\| > r_s$.
$\varphi_{C2_{rv}}$	$\square(\|\|\vec{r}_H\|\| > r_s) \wedge \left((\|\|\vec{v}_H\|\| < v_s) \vee (\vec{v}_H^T \vec{r}_H \geq 0)\right)$
φ_{C3}	$\square(\ddot{x}_{min} \leq \ddot{x}) \wedge (\ddot{x} \leq \ddot{x}_{max}) \wedge (\ddot{y}_{min} \leq \ddot{y}) \wedge (\ddot{y} \leq \ddot{y}_{max})$ $\wedge(\ddot{z}_{min} \leq \ddot{z}) \wedge (\ddot{z} \leq \ddot{z}_{max}) \wedge (\ddot{\theta}_{1_{min}} \leq \ddot{\theta}_1)$ $\wedge(\ddot{\theta}_1 \leq \ddot{\theta}_{1_{max}}) \wedge (\ddot{\theta}_{2_{min}} \leq \ddot{\theta}_2) \wedge (\ddot{\theta}_2 \leq \ddot{\theta}_{2_{max}})$ $\wedge(\ddot{\theta}_{3_{min}} \leq \ddot{\theta}_3) \wedge (\ddot{\theta}_3 \leq \ddot{\theta}_{3_{max}})$.
$\varphi_{C4_{set}}$	$\square X_{sc} \in \mathcal{X}_C$
φ_{C4}	$\square(\dot{x} \leq \dot{x}_{max}) \wedge (\dot{y} \leq \dot{y}_{max}) \wedge (\dot{z} \leq \dot{z}_{max})$ $\wedge(\dot{\theta}_1 \leq \dot{\theta}_{1_{max}}) \wedge (\dot{\theta}_2 \leq \dot{\theta}_{2_{max}}) \wedge (\dot{\theta}_3 \leq \dot{\theta}_{3_{max}})$
φ_{C5}	$\square((DOD > DOD_{max}) \vee scheduled_{CHRG})$ $\implies (\theta_{SI} \leq \theta_{CHRG})$.
φ_{C6}	$\square scheduled_{DATA} \implies (LOS_{DATA} \wedge FOV_{DATA})$
φ_{C7}	$\square\theta_{EZ} > \frac{\alpha}{2} + \beta$
φ_{C8}	$(LOS_S \wedge T_S) \vee (LOS_S \wedge \neg T_S) \vee (\neg LOS_S \wedge T_S)$
φ_{C9a}	$T_{s_m} \leq T_{s_{m_{min}}} \implies i$
φ_{C9b}	$T_{c_m} > T_{c_{m_{max}}} \implies i$
φ_{C9c}	$f_l \leq f_{lt} \implies i$
φ_{C9d}	$f_l \leq f_{lEOL} \implies i$
φ_{C10}	$\square(\|\|\ddot{x}\|\| \leq \ddot{x}_{wear}) \wedge (\|\|\ddot{y}\|\| \leq \ddot{y}_{wear}) \wedge (\|\|\ddot{z}\|\| \leq \ddot{z}_{wear})$ $\wedge(\|\|\ddot{\theta}_1\|\| \leq \ddot{\theta}_{1_{wear}}) \wedge (\ddot{\theta}_2\|\| \leq \ddot{\theta}_{2_{wear}}) \wedge(\|\|\ddot{\theta}_3\|\| \leq \ddot{\theta}_{3_{wear}})$ $\wedge(\|\|\dot{x}\|\| \leq \dot{x}_{wear}) \wedge (\|\|\dot{y}\|\| \leq \dot{y}_{wear}) \wedge (\|\|\dot{z}\|\| \leq \dot{z}_{wear})$ $\wedge(\|\|\dot{\theta}_1\|\| \leq \dot{\theta}_{1_{wear}}) \wedge (\|\|\dot{\theta}_2\|\| \leq \dot{\theta}_{2_{wear}}) \wedge (\|\|\dot{\theta}_3\|\| \leq \dot{\theta}_{3_{wear}})$.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

Acknowledgments

The authors would like to thank Dr. Chris "Chrispy" Petersen, Dr. Sean Phillips, Dr. R. Scott Erwin, Dr. Kendra Lang, Ms. Michelle Simon, and Dr. Daren McKnight for feedback and opportunities to present this information to others in the spacecraft community for feedback.

References

[1] Smith, M., "ESA Urges Automated Satellite Collision Avoidance Systems After Aeolus/Starlink Maneuver," , 2019. URL https://spacepolicyonline.com/news/esa-urges-automated-satellite-collision-avoidance-systems-after-aeolus-starlink-maneuver/.

[2] *Space Policy Directive-3, National Space Traffic Management Policy*, 2018. Presidential Memoranda.

[3] Jah, M., Greiman, D., Sengupta, M., Magnus, S., Melroy, P., Helms, S., and Brown, M., "Space Traffic Management (STM): Balancing Safety, Innovation, and Growth ," An Institute Position Paper, American Institute of Aeronautics and Astronautics, Inc, Reston, VA, November 2017.

[4] Council, N. R., *Continuing Kepler's Quest: Assessing Air Force Space Command's Astrodynamics Standards*, National Academies Press, 2012.

[5] Klinkrad, H., "On-orbit Risk Reduction - Collision Avoidance," *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, Vol. 221, No. 6, 2007, pp. 955–962.

[6] Symonds, K. G., Flohrer, T., Mardle, N., Fornarelli, D., Marc, X., and Ormston, T., "Operational Reality of Collision Avoidance Manoeuvres," *SpaceOps 2014 Conference*, 2014, p. 1746.

[7] Flohrer, T., Krag, H., and Klinkrad, H., "ESA's Process for the Identification and Assessment of High-risk Conjunction Events," *Advances in Space Research*, Vol. 44, No. 3, 2009, pp. 355–363.

[8] Flohrer, T., Klinkrad, H., Krag, H., Bastida Virgili, B., and Merz, K., "Operational Collision Avoidance for LEO Satellites at ESA," *Proceedings of the 28th International Symposium on Space Technology and Science (ISTS), Okinawa, Japan*, 2011.

[9] Flohrer, T., Krag, H., Lemmens, S., Bastida Virgili, B., Merz, K., and Klinkrad, H., "Statistical Look on ESA's Conjunction Event Predictions," *Proc. of the 6th Europ. Conf. on Space Debris, Darmstadt, Germany ESA SP-723*, 2013.

[10] Mattis, J., "Summary of the National Defense Strategy of the United States of America," *Washington, DC*, 2018, pp. 1–11.

[11] *Satellite Communications*, 2010. 47 CFR §25.

[12] *Update to Parts 2 and 25 Concerning Non-Geostationary, Fixed-Satellite Service Systems and Related Matters*, 2016. IB Docket No. 16-408.

[13] Federal Aviation Administration's Office of Commercial Space Transportation (FAA AST), "The Annual Compendium of Commercial Space Transportation: 2018," Tech. rep., Federal Aviation Administration, 800 Independence Avenue SW, Washington, DC, 20591, 1 2018. https://www.faa.gov/about/office_org/headquarters_offices/ast/ media/2018_AST_Compendium.pdf.

[14] Consultative Committee for Space Data Systems, "All Active Publications," https://public.ccsds.org/Publications/AllPubs.aspx, 2017. Accessed: 26 August 2019.

[15] NASA, "NASA Systems Engineering Handbook," NASA/SP-2007-6105 Rev1, 2007.

[16] U.S. Air Force Space & Missile Systems Center, "SMC Systems Engineering Primer & Handbook," 2nd Edition, 2004.

[17] Gross, K. H., "Evaluation of Verification Approaches Applied to Nonlinear System Control," Master's thesis, Air Force Institute of Technology, March 2016.

[18] Gross, K. H., Clark, M. A., Hoffman, J. A., Swenson, E. D., and Fifarek, A. W., "Run-time Assurance and Formal Methods Analysis Applied to Nonlinear System Control," *Journal of Aerospace Information Systems*, Vol. 14, No. 4, 2017, pp. 232–246.

[19] Hobbs, K. L., Perez, I., Fifarek, A., and Feron, E. M., "Formal Verification of System States for Spacecraft Automatic Maneuvering," *AIAA Scitech Forum*, 2019.

[20] Leveson, N. G., "Role of Software in Spacecraft Accidents," *Journal of Spacecraft and Rockets*, Vol. 41, No. 4, 2004, pp. 564–575.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

[21] Leveson, N. G., "A Systems-Theoretic Approach to Safety in Software-Intensive Systems," *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 1, 2004, pp. 66–86.

[22] Leveson, N. G., "Software Challenges in Achieving Space Safety," 2009.

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

[24] Allison, C. K., Revell, K. M., Sears, R., and Stanton, N. A., "Systems Theoretic Accident Model and Process (STAMP) Safety Modelling Applied to an Aircraft Rapid Decompression Event," *Safety Science*, Vol. 98, 2017, pp. 159–166.

[25] Rising, J. M., and Leveson, N. G., "Systems-Theoretic Process Analysis of Space Launch Vehicles," *Journal of Space Safety Engineering*, Vol. 5, No. 3-4, 2018, pp. 153–183.

[26] Johnson, K., and Leveson, N. G., "Investigating Safety and Cybersecurity Design Tradespace for Manned-Unmanned Aerial Systems Integration Using Systems Theoretic Process Analysis." *GI-Jahrestagung*, 2014, pp. 643–647.

[27] Fleming, C. H., Spencer, M., Thomas, J., Leveson, N., and Wilkinson, C., "Safety Assurance in NextGen and Complex Transportation Systems," *Safety science*, Vol. 55, 2013, pp. 173–187.

[28] Harkleroad, E., Vela, A., and Kuchar, J., "Review of Tystems-Theoretic Process Analysis (STPA) Method and Results to Support NextGen Concept Assessment and Validation," *Lexington, MA: Massachusetts Institute of Technology*, 2013.

[29] Hobbs, K. L., Cargal, C., Feron, E., and Burns, R. S., "Early Safety Analysis of Manned-Unmanned Team System," *AIAA Information Systems-AIAA Infotech@ Aerospace*, 2018.

[30] Robertson, J. J. R., "Systems Theoretic Process Analysis Applied to Manned-Unmanned Teaming," Master's thesis, Massachusetts Institute of Technology, 2019.

[31] Chen, J., Zhang, S., Lu, Y., and Tang, P., "STPA-based Hazard Analysis of a Complex UAV System in Take-off," *2015 International Conference on Transportation Information and Safety (ICTIS)*, IEEE, 2015, pp. 774–779.

[32] Leveson, N. G., "Intent Specifications: An Approach to Building Human-Centered Specifications," *IEEE Transactions on software engineering*, Vol. 26, No. 1, 2000, pp. 15–35.

[33] Weiss, K. A., Dulac, N., Chiesi, S., Daouk, M., Zipkin, D., and Leveson, N., "Engineering Spacecraft Mission Software Using a Model-based and Safety-driven Design Methodology," *Journal of Aerospace Computing, Information, and Communication*, Vol. 3, No. 11, 2006, pp. 562–586.

[34] Leveson, N., *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT press, 2011.

[35] Peled, D. A., *Software reliability methods*, Springer Science & Business Media, 2013.

[36] Clarke, E. M., and Emerson, E. A., "Design and synthesis of synchronization skeletons using branching time temporal logic," *Workshop on Logic of Programs*, Springer, 1981, pp. 52–71.

[37] Koymans, R., "Specifying Real-time Properties with Metric Temporal Logic," *Real-time systems*, Vol. 2, No. 4, 1990, pp. 255–299.

[38] Baier, C., Katoen, J., and Larsen, K., *Principles of Model Checking*, MIT Press, 2008.

[39] Formal Systems Laboratory of the Department of Computer Science at the University of Illinois at Urbana-Champaign, "Past Time Linear Temporal Logic," , 2008. URL `http://fsl.cs.illinois.edu/index.php/Past_Time_Linear_Temporal_Logic`, accessed 15 April 2019.

[40] Clark, S., "Attitude Control Failures led to Break-up of Japanese Astronomy Satellite," , April 2016. URL `https://spaceflightnow.com/2016/04/18/spinning-japanese-astronomy-satellite-may-be-beyond-saving/`.

[41] Turner, R., Lehmann, R., Wadley, J., Kidd, D., Swihart, D., Bier, J., and Hobbs, K., "Automatic Aircraft Collision Avoidance algorithm Design for Fighter Aircraft," *Asia-Pacific International Symposium on Aerospace Technology*, 2012.

[42] MIL-STD-882E, "MIL-STD-882E: System Safety," Standard Practice, Department of Defense, May 2012.

[43] Morgan, P. S., "Fault Protection Techniques in JPL Spacecraft," 2005.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122

[44] Evans, B., "Dawn of a New Era," *Partnership in Space*, Springer, 2014, pp. 453–482.

[45] Holland, D., "6.4. 1 A Case Study of the Near-Catastrophic Mir-Progress 234 Collision with Emphasis on the Human Factors/Systems-Level Issues Surrounding this Mishap," *INCOSE International Symposium*, Vol. 12, Wiley Online Library, 2002, pp. 820–827.

[46] Oberg, J., "Shuttle-Mir's Lessons for the International Space Station," *IEEE Spectrum*, Vol. 35, No. 6, 1998, pp. 28–37.

[47] Thomas, L. D., "Selected Systems Engineering Process Deificiencies and Their Consequences," Tech. rep., National Aeronautics and Space Administration George C. Marshall Space Flight Center, 2007.

[48] Office, N. O. D. P., "Accidental Collisions of Cataloged Satellites Identified," *The Orbital Debris Quarterly News*, Vol. 9, No. 2, 2005, pp. 1–2.

[49] Alby, F., Lansard, E., and Michal, T., "Collision of Cerise with Space Debris," *Second European Conference on Space Debris*, Vol. 393, 1997, p. 589.

[50] Johnson, N. L., Stansbery, E., Whitlock, D. O., Abercromby, K. J., and Shoots, D., "History of On-orbit satellite Fragmentations," 2008. URL `https://orbitaldebris.jsc.nasa.gov/library/satellitefraghistory/tm-2008-214779.pdf`.

[51] Wang, T., "Analysis of Debris from the Collision of the Cosmos 2251 and the Iridium 33 Satellites," *Science & Global Security*, Vol. 18, No. 2, 2010, pp. 87–118.

[52] Kelso, T., Parkhomenko, N., Shargorodsky, V., Vasiliev, V., Yurasov, V., Nazarenko, A., Tanygin, S., and Hiles, R., "What Happened to Blits? An Analysis of the 2013 Jan 22 event," *Proceedings of the Advanced Maui Optical and Space Surveillance Technologies Conference*, Vol. 4, 2013.

[53] Portree, D. S. F., and Loftus, J. P., "Orbital Debris: A Chronology," Tech. rep., NASA Technical Report, 1999.

[54] Hoffman, E. J., Ebert, W., Femiano, M., Freeman, H., Gay, C., Jones, C., Luers, P., and Palmer, J., "The NEAR Rendezvous Burn Anomaly of December 1998," *Applied Physics Laboratory, Johns Hopkins University, Tech. Rep*, 1999.

[55] Koenig, J. D., "Exclusion Zone Guidance Method for Spacecraft," , Sep. 14 2010. US Patent 7,795,566.

[56] Burk, T., "Managing Cassini Safe Mode Attitude at Saturn," *AIAA Guidance, Navigation, and Control Conference*, 2010, p. 7558.

[57] Larson, K. A., McCalmont, K. M., Peterson, C. A., and Ross, S. E., "Kepler Mission Operations Response to Wheel Anomalies," *SpaceOps 2014 Conference*, 2014, p. 1882.

[58] Wertz, J. R., and Larson, W. J., *Space Mission Analysis and Design, Third Edition*, Microcosm, 1999.

[59] Barfield, F., "Autonomous Collision Avoidance: the Technical Requirements," *National Aerospace and Electronics Conference, 2000. NAECON 2000. Proceedings of the IEEE 2000*, IEEE, 2000, pp. 808–813.

[60] Johnson, C. W., "The Natural History of Bugs: Using Formal Methods to Analyse Software Related Failures in Space Missions," *International Symposium on Formal Methods*, Springer, 2005, pp. 9–25.

Downloaded by KING ABDULLA UNIV OF SCIENCE & TECHNOLOGY on February 23, 2021 | http://arc.aiaa.org | DOI: 10.2514/6.2021-1122