System-Theoretic Process Analysis of a Novel Airborne Laser Communication System

by

Brittany E. Bishop

Bachelor of Science in Aeronautical Engineering,
The United States Air Force Academy, 2022

Submitted to the Aeronautics and Astronautics Dept. in Partial Fulfillment of the Requirements For the Degree of

Master of Science in Aeronautics and Astronautics

at the
Massachusetts Institute of Technology

May 2024

Authored by: Brittany E. Bishop
Department of Aeronautics and Astronautics
May 10, 2024

Certified by: Nancy G. Leveson, Ph. D.
J. C. Hunsaker Professor of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: Jonathan P. How
R. C. Maclaurin Professor of Aeronautics and Astronautics
Chair, Graduate Program Committee

Disclaimer

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the United States Air Force.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

System-Theoretic Process Analysis of a Novel Airborne Laser Communication System

by

Brittany E. Bishop

Submitted to the Department of Aeronautics and Astronautics on May 10, 2024
in partial fulfillment of the requirements for the degree of
Master of Science in Aeronautics and Astronautics

Abstract

As the military strives to create a more robust battle network, laser communication offers many advantages such as supporting more secure and efficient data sharing. For this reason, interest has grown in recent years in implementing lasercom as a means for intra-aircraft communication. However, many challenges unique and inherent to lasercom such as stringent line-of-sight and pointing requirements and susceptibility to atmospheric degradation lead to difficulties in implementation. Consequently, establishing and maintaining lasercom links in the dynamic environment of flight will require seamless coordination between aircraft.

The complexity and novelty of such a system warrant a hazard analysis technique that can fully address the associated challenges of collaboration while the system is in an early concept phase of design. System-Theoretic Process Analysis (STPA) is a proactive hazard analysis technique rooted in Systems Theory. While more traditional hazard analysis methods evaluate the safety of system components individually, STPA provides guidance to analyze systems holistically, thus supporting the identification of emergent behaviors that arise due to component interactions.

Recently, STPA has been extended to address hazards specifically associated with collaboration of multiple controllers providing shared control over a physical process. This extension known as STPA-Teaming provides a methodology to analyze unsafe combinations of control actions that may lead to system losses. The method allows for the systematic identification of causal factors related to coordination that are likely to be missed by more traditional hazard analysis techniques. Because this approach relies on abstraction and includes human operators along with software and hardware components, it is well-suited for novel, complex systems.

This thesis applies STPA and its extension, STPA-Teaming, to an early concept airborne lasercom system to identify scenarios in which loss of communication may occur. As a result, it identifies scenarios related not only to individual component failures and unsafe internal control, but also related to flaws in coordination of multiple controllers. The output of the analysis is system recommendations that can support the remainder of the systems engineering process including generation of system requirements, definition of system concept of operations (ConOps) and system architecture, and system validation and verification (V&V). In this way, the results of the analysis provide a baseline level of traceability for future design decisions to manage the emergent behavior of the system and ultimately prevent mission losses.

Thesis Supervisor: Nancy G. Leveson, Ph.D.
Title: J. C. Hunsaker Professor of Aeronautics and Astronautics

Acknowledgements

I am deeply grateful for the abundant blessings in my life, which I attribute to the grace of God. From the unwavering support of my family and the values and education provided throughout my upbringing to the privilege of studying at MIT, every aspect of my journey has been guided by God. As such, it is my heartfelt desire to honor Him in every endeavor, and I hope this thesis reflects that commitment.

"Now all glory to God, who is able, through his mighty power at work within us, to accomplish infinitely more than we might ask or think." Ephesians 3:20

To my parents, words cannot express my gratitude for all you have done for me. Your unwavering support, encouragement, and patience have been the cornerstone of my achievements. You have taught me invaluable lessons in perseverance and positivity, showing me that with hard work and a positive mindset, any challenge can be overcome. Thank you for always pushing me to dream big and believing in me even when I did not believe in myself.

To Professor Nancy Leveson, I extend my deepest appreciation for giving me the opportunity to join your system safety research group and attend MIT. Your methodologies and guidance have profoundly influenced my perspective on systems engineering, leading me to see the world in terms of control-feedback loops. As I move forward in the Air Force, I will carry with me the methods and insights gained under your mentorship. Thank you for your invaluable contributions to my education and professional development.

To Dr. Andrew Kopeikin, thank you for your ongoing mentorship, that extended beyond your time at MIT. Your guidance was instrumental in keeping me focused, disciplined, and decisive when it came time to select a thesis topic. I deeply appreciate your willingness to offer advice and share your expert opinion on STPA-Teaming. The extensions you developed for examining collaborative interactions significantly enhanced the depth and scope of this thesis. Thank you for supporting my development not only as a graduate student, but also as an Air Force officer.

To Dr. John Moores and Group 66 at Lincoln Lab, I extend my sincere gratitude for supporting my studies and research at MIT. Thank you for pushing me to explore unfamiliar subjects and broaden my research horizons, while also being flexible to accommodate my research interests. The concept of an airborne lasercom system proved to be an engaging and rewarding project. Your willingness to share your expert opinion was instrumental in my academic journey.

Finally, I am grateful for the community I found within the Engineering Systems Lab and the broader Aero/Astro department. To Polly Harrington and Rodrigo Rose, your presence in the lab made each day unique and entertaining. You both provided fresh perspectives, motivation to embrace new projects, and invaluable feedback for thesis work. I will truly miss our daily shenanigans of looking for Mario and snagging free food (wherever it may be on campus). Additionally, I appreciate Justin Poh, Alex Hillman, and Michael Schmid for their insightful feedback and stimulating discussions. Finally, to Fluff Gang, thank you for fostering an indispensable sense of community, providing camaraderie and enjoyment in a new city. I cannot wait to see where we all end up after we embark on our respective careers post-MIT.

Table of Contents

Table of Figures

Table of Tables

Chapter 1 Introduction

The modernization of warfare has led to requirements for increasing amounts of raw sensory data and information to be sent over secure links. As such, the United States Air Force (USAF) could benefit from the use of free-space optical communication (FSOC), otherwise known as laser communication (lasercom) for intra-aircraft communication. While lasercom would enable higher data rates, nearly unlimited bandwidth, and significantly increased security for data transmissions, it is heavily limited by stringent pointing requirements and high susceptibility to atmospheric interference. Utilization of lasercom for dynamic airborne platforms would thus require seamless temporal and spatial coordination between aircraft. This thesis applies Nancy Leveson's Systems-Theoretic Process Analysis (STPA) method of hazard analysis to systematically identify potential flaws in collaboration and to generate recommendations to prevent mission losses such as loss in communication and loss of sensitive data.

1.1 Motivation

In recent decades, military strategy has shifted in focus toward information-sharing, calling for more efficient battle networks that better inform and disseminate command and control decisions. In May of 2021, Secretary of Defense Lloyd Austin signed the Joint All Domain Command and Control (JADC2) strategy for the U.S. military establishing a vision for improved joint capabilities and coordination [1]. As its contribution to JADC2, the USAF released its own program known as the Advanced Battle Management System (ABMS) that emphasizes using more efficient methods to collect, share, and process data.

As the modern battle network evolves, increasing amounts of raw sensor data must be collected, and information must be transmitted at greater rates to aid in real-time decision making. Aircraft used for such collection and dissemination currently communicate in the Radio Frequency (RF) spectrum, which is heavily regulated and bandwidth limited. Free-space Optical Communication (FSOC), otherwise known as laser communication (lasercom), overcomes many of these challenges. The optical domain allows for significantly higher data rates, larger bandwidths, increased security and systems of reduced size, weight, and power (SWaP) [2].

Given these advantages, lasercom offers conceivable benefits for military aircraft sharing large amounts of sensitive data at high data rates. Accordingly, interest has grown within the USAF for utilizing airborne laser communications: After several successful airborne lasercom demonstrations by the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL), public affairs out of Kirtland AFB, N.M. released a statement in 2015 that, "Air Combat Command may be able to provide requirements for laser communications applications within the next decade" [3].

Despite its advantages, several challenges have deterred the implementation of lasercom for intra-aircraft communications. Lasercom requires very precise pointing and is highly susceptible to atmospheric interference. These challenges are exacerbated when coupled with the dynamic environment of flight. In order to effectively share data through laser data links, airborne platforms will require seamless coordination between human teams and between humans and automation. This teaming relationship will require cognitive alignment between controllers, dynamic decision-making in the midst of adverse operational conditions, and adequate communication and feedback between controllers regarding the optical signal.

The dynamic and complex environment for airborne lasercom requires a holistic system hazard analysis that not only accounts for hardware failures, but also accounts for software errors, human factors-related issues, design flaws, changes in operational conditions, and the system's emergent behaviors due to coordinating components. While much of the research involving lasercom systems has primarily focused on technologies to mitigate adverse atmospheric effects or execute precise optical pointing [4],[5],[6],[7], little research has investigated the collaboration necessary to maintain links in a dynamic flight environment.

To address this gap, this thesis applies a systematic hazard analysis technique to a conceptual airborne lasercom system to identify causal factors that may lead to loss of communication or other mission losses such as loss of sensitive data. The applied method, known as *STPA-Teaming*, identifies how unsafe combinations of control actions provided by multiple collaborating controllers may occur. STPA-Teaming then facilitates the identification of causal scenarios related to unsafe control, flaws in coordination, and component failures. The results support the generation of requirements and can help guide the systems engineering process starting in the early concept stage of design.

1.2 Thesis Objective

The objective of the thesis is to identify how mission losses may occur due to unsafe internal control or collaborative control using STPA and its extensions. The goal is to then use the identified scenarios to generate requirements for the system while it is in the early concept phase of design. The aim of this thesis is to ultimately answer the following question:

How can system-theoretic processes be applied to identify the risks and challenges associated with coordinating laser communication for intra-aircraft communications? What system recommendations can be generated from the analysis to prevent and mitigate flaws in collaboration?

1.3 Thesis Structure

This thesis is structured as follows: Chapter 2 provides relevant background information regarding laser communication and various safety analysis methods. It includes an overview of STPA-Teaming's theoretical framework and process. Chapter 3 defines the airborne laser communication system and provides a high-level description of how such a system would function within the current structure for Air Force communications. In Chapter 4, STPA-Teaming is applied to the defined system to identify causal scenarios related to both internal control and collaborative control. This chapter also provides recommendations to prevent or reduce the occurrence of scenarios and system losses. Finally, Chapter 5 concludes the thesis with major insights and recommendations for future work as the system is further developed. References are provided in Chapter 6 and appendices follow with the full list of UCCAs, loss scenarios, and recommendations generated in the analysis.

Chapter 2 Background

2.1 Laser Communication

Modern military forces require a battle network that can share larger amounts of data at increasing rates and with more robust security measures. Lasercom is a relatively new method of transmitting data that supports such objectives, and as such, is being considered for use on aircraft. However, there are also many challenges for operational implementation of such a system. This section describes the benefits lasercom offers when compared to traditional radio frequency (RF) transmissions and describes how the same properties that make lasercom advantageous also create challenges that require effective coordination to overcome.

2.1.1 Advantages and Challenges of Lasercom

Radio frequency (RF) communications are ubiquitous for mobile and cross-domain communications. However, they inherently possess weaknesses for communications: they are bandwidth limited because the military must allocate a specific range of frequencies for use in order to avoid interfering with civilian communications [1]. They can be disturbed by natural phenomena and, despite the advent of tactical data links, they are susceptible to jamming and interception from hostile forces who constantly develop new strategies to interfere with communications [1].

Lasercom is a relatively new method of transmitting data that offers many advantages over conventional RF communications. Growing in popularity within the satellite industry, lasercom functions by using narrow lasers as signal carriers. Compared to radio-frequency transmissions, signals within the optical spectrum have a much smaller wavelength and a more narrow beam width, enabling higher power efficiency and higher data rates for transmissions. Furthermore, the direct point-to-point transmissions using narrow beams provides increased security as the probability of interception is reduced [2]. Additionally, the Federal Communications Commission (FCC) does not regulate the optical spectrum requiring FCC licenses or frequency allocations. For this reason, the spectrum is nearly unlimited for use [2]. Because lasercom uses higher frequencies with reduced diffraction loss, lasercom terminals have a reduced aperture size and lower size, weight, and power (SWaP). Consequently, lasercom can be implemented in modular designs that provide enhanced portability and easier integration onto aircraft [2]. Such advantages make lasercom appealing for intra-aircraft communication.

Along with these benefits, the properties of lasercom also lead to several inherent challenges: first, optical links are easily degraded by the turbulent channel of the atmosphere. Transmitted power may fluctuate due to turbulence as well as platform motion and jitter, resulting in a phenomenon known as fading. The boundary layer near the aircraft also may cause the power at the receiver to fluctuate and result in fiber coupling loss. Furthermore, optical signals may be distorted due to atmospheric scattering and absorption of the signal across the channel [4]. Finally, because line-of-sight is required, atmospheric conditions such as clouds, precipitation, dense fog, and smoke can easily block the signal, disrupting the connection. The curvature of the earth, local terrain, and structures of the airframe, such as the wing during a bank, may also cause signal blockage.

An additional limiting challenge to lasercom is its stringent pointing requirements. In order to establish and maintain a lasercom link, connecting terminals must point narrow lasers beams directly at one another and track one another precisely throughout the entire duration of transmissions. This process requires knowledge of a partner terminal's current location, attitude, and velocity as well as its trajectory and future positions. Accurate pointing and tracking can be affected by a variety of factors such as platform motion and jitter, aero-optic effects from the boundary layer surrounding aircraft, near field phase fluctuations, inaccurate position information received by partners, or inaccurate estimations of a partner's future position [8].

2.1.2 Technical Functions of Lasercom

To maintain precise pointing and tracking, lasercom terminals must perform a function known as Pointing, Acquisition, and Tracking (PAT). First, terminals gather data regarding their partner's position and point at their corresponding partner terminal. Next, acquisition is performed. The standard acquisition sequence is as follows: 1) a terminal transmits an acquisition or "beacon" beam (a beam with a wider divergence than the beam used for communications) towards its partner terminal; 2) the partner terminal detects the beacon on its acquisition sensor and directs a narrow communication beam back towards the initiating terminal; and 3) the initiating terminal detects the narrow beam from its partner and transitions to active partner tracking [8]. In the partner tracking stage, the beams are "locked on" in a closed-loop manner and communications may be initiated.

It is important to note that there are a wide range of possible beacon styles and sequences for acquisitions: features such as wavelength, transition states, scan patterns, dwell times, speeds, and entrance/exit criteria are all key architectural decisions that can affect the interoperability of systems. Discussing the technical considerations of the DARPA Space-Based Adaptive Communications Node (Space-BACN), Ulmer, et al. note the various beacon styles and sequences that may be used for lasercom acquisitions: Beacon-based systems can have either symmetric sequences (both terminals scan a beacon) or asymmetric sequences (one terminal scans a beacon and one terminal detects the beacon); systems may complete their sequence synchronously (both progress through the sequence in a deterministic manner) or asynchronously (one terminal may complete the sequence first); and scan patterns, areas, speeds, transition states, and entrance/exit criteria may all vary based on design [9].

Furthermore, systems may be "beaconless" and perform acquisitions by scanning their communications beam, rather than a beacon beam, rapidly over a large area. As a result of different beacon types, detection criteria may also vary: beaconless systems may be configured to detect multiple, short high-power illuminations or beacon-based systems may detect a lower number of scans from a lower power beacon with longer dwell times [9]. Systems may be confined to one sequence and acquisition type or may be able to reconfigure and utilize different types. Whichever type is used, systems must ultimately have compatible acquisition parameters and sequences to successfully acquire one another's signal.

Once systems complete acquisitions, they must continue to track while transmitting data. When lasercom is used for satellite communications, ephemeris data and orbital trajectories allow for temporally and spatially fixed pointing calculations. However, tracking becomes significantly more challenging when coupled with the dynamic environment of flight: lasercom terminals must not only evaluate their own location and attitude, but must also estimate the position and attitude of their partner in a setting where aircraft location and trajectory are subject to frequent and rapid change. To maintain tracking, controllers would need to coordinate flight within adequate ranges of partners, at appropriate airspeeds and altitudes, and at specifically planned times. Because various weather phenomena can degrade communications, planned routes and schedules of aircraft may need to be adapted to avoid atmospheric degradation of links.

After acquisition has been completed and systems are tracking, systems may initiate communications. To effectively transmit and receive data, systems must use compatible wavelengths, modulation schemes, data rates, forward error correction (FEC) schemes, polarization plans, and other technical parameters for communications. They must additionally transmit with adequate power for signals to reach partners. These requirements add to the challenge of lasercom connections where systems may be configured to transmit or receive at various technical parameters.

Complex collaborative interactions will be exhibited at multiple levels of control as higher mission authorities direct pilots, pilots coordinate laterally, and pilots control their own aircraft and lasercom system. Controllers will need to establish, maintain, and, in some scenarios, transfer control responsibilities throughout flights. Control authority, as well as communication channels, and membership in the system may be dynamic as various controllers join and exit the network. Because the optical signal is dictated by these mutually influential interactions, any flaws in coordination could lead to loss in communication.

Several demonstrations have been performed to assess the technical performance of airborne lasercom systems [4], [5], [10], but no research has been dedicated to analyzing the coordination required to maintain links in an operational environment. Because this system is in the conceptual phase of the design, its design and requirements could be positively influenced by such an analysis. This thesis employs a holistic hazard analysis process to identify how collaboration may lead to unsafe system behavior, preventing successful communication. The results of such an analysis can be used to generate system requirements and ultimately support the remainder of the systems engineering process.

2.2 Hazard Analysis Techniques

Hazard analysis techniques serve to systematically identify causal factors that can cause a system to enter a hazardous state and experience losses. Such a process is crucial specifically in the conceptual stages of design to support the remainder of the systems engineering process because the results of a hazard analysis provide guidance from the generation of requirements and system constraints to system design, verification and validation (V&V), and final certification. Despite this foundational role in the systems engineering life cycle, many times hazard analysis techniques are not applied until later in the design of systems [11].

The traditional methods of hazard analysis consider accidents as a linear chain-of-failure-events in which one failure directly causes the next one in a chain [11]. A natural deduction from these models is that elimination of one failure event in the chain will prevent the entire system from failing. However, this assertion does not hold true for the more complex systems under development today. The underlying assumptions of this model omit many potential causes of accidents: the interdependence of components, the emergent behavior of component interactions, systemic factors such as poor organizational or safety culture, and human factors considerations [12].

While the chain-of-failure-events model was useful for simpler systems of the past, the more complex sociotechnical systems of today are dynamic with interdependent components that may cause non-linear failures. For this reason, systems such as the proposed lasercom system require a more holistic analysis that accounts for such emergent system properties. This section outlines the traditional approaches to hazard analysis based on the simple chain-of-failure-events model. Such approaches include Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), and Hazard and Operability Analysis (HAZOP). Other traditional hazard analysis methods not discussed in this section, such as Event Tree Analysis (ETA) and Bow Tie Analysis, have the same limitations. This section highlights the disadvantages of such techniques and offers Systems-Theoretic Accident Model and Processes (STAMP) as a more sophisticated, holistic causality model to appropriately analyze today's complex systems.

2.2.1 Fault Tree Analysis (FTA)

FTA is a top-down hazard analysis method that was developed in the 1960s by Bell Telephone Laboratories to analyze the reliability of the minuteman launch control system [13]. Commonly used in the nuclear, aerospace, and electronic industries, it uses Boolean logic to describe how individual component failures may combine and lead to hazardous conditions. It is performed through four primary steps: (1) system definition, (2) fault tree construction, (3) qualitative analysis, and (4) quantitative analysis [12]. This section provides a brief summary of these steps and describes why they are not sufficient to manage the complexity of a novel airborne lasercom system.

The analysis is initiated by defining the system and its hazards. This step requires analysts to list every component's initial state and existing environmental conditions, as well as create a comprehensive set of top events, or hazards, to be prevented. No guidance is provided on how to identify the hazards themselves. Rather, the technique provides only a method to identify *causes* of hazards [12].

The next step in FTA involves creating a fault tree to illustrate all possible causal events related to the hazard. The analyst assumes a specific system state and a top event and then determines basic events that would be necessary and sufficient to cause the top event to occur [12]. Logic symbols such as AND gates, OR gates, INHIBIT gates, and more are used to represent the relationships between basic events. For example, if two basic events are connected by an AND gate, they must both occur in order for the corresponding top event to occur. For later quantitative analysis, probabilities are assigned to each basic event. Shown below is an example fault tree, representing the loss of an aircraft due to deceleration hazards [12].

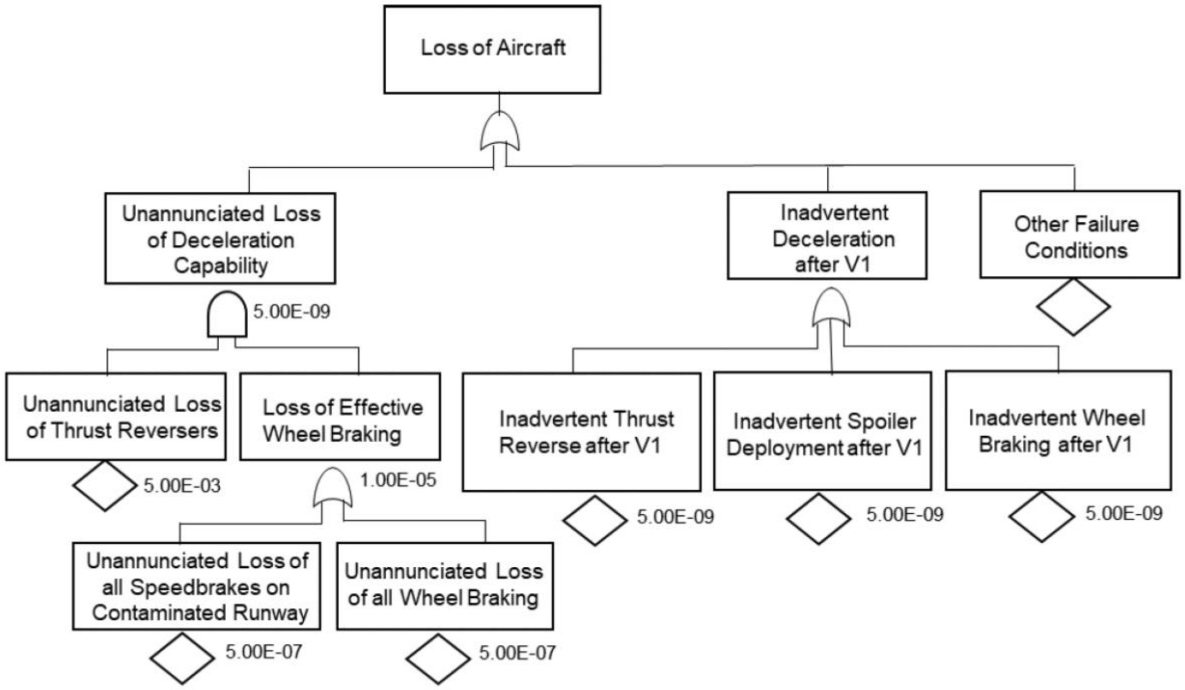

Loss of Aircraft
Unannunciated Loss of Deceleration Capability
5.00E-09
Inadvertent Deceleration after V1
Other Failure Conditions
Unannunciated Loss of Thrust Reversers
5.00E-03
Loss of Effective Wheel Braking
1.00E-05
Inadvertent Thrust Reverse after V1
5.00E-09
Inadvertent Spoiler Deployment after V1
5.00E-09
Inadvertent Wheel Braking after V1
5.00E-09
Unannunciated Loss of all Speedbrakes on Contaminated Runway
5.00E-07
Unannunciated Loss of all Wheel Braking
5.00E-07

Figure 2-1: Example FTA indicating deceleration hazards [from SAE ARP 4761] [12]

Finally, a qualitative and quantitative analysis is performed to identify weaknesses in the system and calculate a probability of the hazard occurring. The qualitative analysis involves first determining the system modes of failure and then the system components that interact such that they may be candidates for common cause failures [13]. *Minimal cut sets*, or groups of basic events that can collectively cause a top event to occur, are identified in this step. In the quantitative analysis, the probabilities of all the cut sets are summed to obtain the probability of the top event occurring (assuming the cut sets are statistically independent, an important assumption that is often untrue for complex systems). The probabilities of each cut set are calculated by multiplying the probability of each basic event within the cut set.

FTA can be useful for helping analysts comprehend the relationships between basic failure events and top events, thus forcing them to develop a more complete understanding of the system. However, there are many issues inherent to FTAs' processes that make it disadvantageous for the analysis of complex systems such as the lasercom system. First, FTA is limited in that it is only useful for analysis of systems with a completed design [12]. In order to generate a fault tree, analysts must have a thorough understanding of the system and its various states. For systems in the early conceptual stage of development, such as the lasercom system, FTA offers no method to model the system and to analyze its behavior.

FTA has additional theoretical limitations in that it is unable to model continuous events. The nodes within a fault tree can only show discrete events, indicating whether an event has occurred or not occurred. In this way, dynamic system behavior is ignored and the analysis often misses hazards such as those due to component degradation or unsafe timing and sequencing of events [13]. The proposed lasercom system will be critically dependent on the proper order and duration of control actions as it must transition between various states to establish and maintain a connection. As such, it requires a hazard analysis technique that can account for continuous. events.

FTA has several other serious weaknesses that make is unsuitable for the lasercom system. Fault tree events focus primarily on hardware failures and largely ignore failures due to human or software interactions. Furthermore, because they emphasize component failure, the analysis omits errors in the design of the system. Finally, attempts to quantify the probability of failure are often based on arbitrary numbers and data that may result in "orders-of-magnitude errors" [12], leading to false confidence in the reliability and safety of the system.

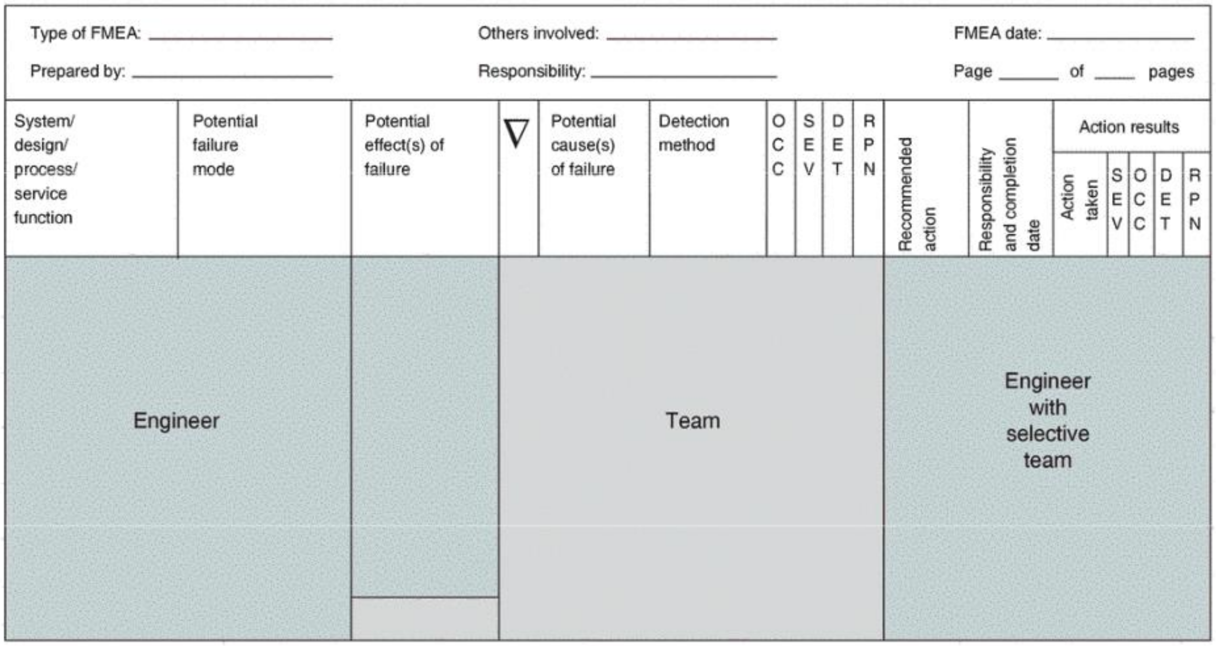
Ultimately, due to its limitations in theory and applications, FTA would miss many influencing factors in the lasercom system such as design faults, interactions between humans and software, and the dynamic collaboration *between* systems necessary to maintain connections. For this reason, it will not be considered as a candidate for analyzing the proposed lasercom system.

2.2.2 Failure Modes and Effects Analysis (FMEA)

FMEA was developed in the 1940s by the U.S. military as a method to estimate hardware reliability in defense systems [14]. Also relying on a linear chain-of-failure events model, it involves an inductive search starting with the failures of individual components and working towards the effects of the failures. Ultimately, the end objective is to calculate the probability that no failures will occur for a specified duration of time [12]. FMEA has since been extended to include an additional analysis of a risk's critically, considering the frequency of failure mode occurrence as well as the failure mode's severity and detectability [15]. This extended method is known as Failure Mode, Effects, and Criticality Analysis (FMECA).

FMEA is initiated by listing all components and their failure modes. Considering each operational state, the analyst then lists all possible causes of the failure mode and the effects on the system or mission. A probability is then assigned to the failure mode using generic failure rates calculated from past experiences, usually provided by hardware manufacturers [12].

In the extended FMECA, a criticality analysis is then performed, assigning a Risk Priority Number (RPN) to failure modes based on their occurrence, severity, and detectability [15]. The effects are then ranked either using numerical scales or categories such as catastrophic, critical, marginal, or minor. Finally, a method to mitigate the causes of the failure mode or reduce the risk is assigned to the failure mode. The results are often documented in a table such as the one shown below in Figure 2-2.



Type of FMEA: ____________ Others involved: ____________ FMEA date: ____________

Prepared by: ____________ Responsibility: ____________ Page ______ of _____ pages

System/ design/ process/ service function	Potential failure mode	Potential effect(s) of failure	∇	Potential cause(s) of failure	Detection method	OCC	SEV	DET	RPN	Recommended action	Responsibility and completion date	Action results				
												Action taken	SEV	OCC	DET	RPN
Engineer			Team							Engineer with selective team						

Figure 2-2: Example FMEA Table [15]

In recent years, FMEA has been applied to assess the reliability and security of military aircraft communication systems [16]. Such analyses highlight several challenges of applying this technique to evaluate military communication systems. First, there is no adequate method to estimate the "occurrence" of a communications system failure when considering information assurance failure modes [16]. In basic FMEAs, the likelihood of hardware failures can at least be obtained from manufactures who test their hardware components and obtain averages of failure. However, as the referenced FMEA emphasizes, many of the failure modes present in a military communication system occur due to factors such as "human actions taken to attack a system, or due to human actions which negligently open vulnerabilities in the system," factors which cannot be tested for or reliably predicted [16].

The analysis results additionally note that "detectability" does not apply to aircraft communication systems as it does in traditional hardware systems. In the case of information assurance in communication systems, if a failure mode is present in one aircraft, it would be present in all aircraft. For example if the modem in a system lacks an exception handling capability and is overwhelmed with void inputs, the failure mode will be present in all aircraft [16]. Thus, the "detectability" factor bares no significance and does not assist in the prioritization of risks.

Finally, the analysis results emphasize that indirect effects of a failure not be considered in the "severity" of the failure mode in order to "accurately reflect the seriousness of the specific failure in question" [16]. Instead, as FMEA guidance directs, each possible indirect effect is to be considered an entirely new failure mode to assess. In this way, FMEA does not allow for the analysis of multiple failures occurring together and misses common-cause failures. Additionally, it can be almost impossible to list every indirect effect of a failure mode and verify completeness of the analysis. For this reason, FMEA can be extremely costly and time-consuming to complete [12].

While FMEA is advantageous for understanding relatively simple systems that rely primarily on hardware components, it is not suitable for modern systems with unpredictable components such as humans and software. Moreover, the interactions *between* components becomes impossible to accurately predict as systems grow in complexity. The accident investigation board in charge of investigating the Space Shuttle Columbia Accident also cited these weaknesses: “Since the current Failure Mode Effects Analysis/Critical Item List process is designed for bottom-up analysis at the component level, it cannot effectively support the kind of ‘top-down’ hazard analysis that is needed to inform managers on risk trends and identify potentially harmful interactions *between* systems” [17].

In the analysis of the proposed lasercom system, it will be critical to assess the interactions between systems as they attempt to connect. Furthermore, they will exhibit unpredictability at all levels as humans, software, and hardware interact to establish and maintain connections in a dynamic environment. Thus, FMEA is not a suitable candidate for analyzing the system as it would disregard the majority of these interactions and has no viable means of assigning probabilities to identified failure modes.

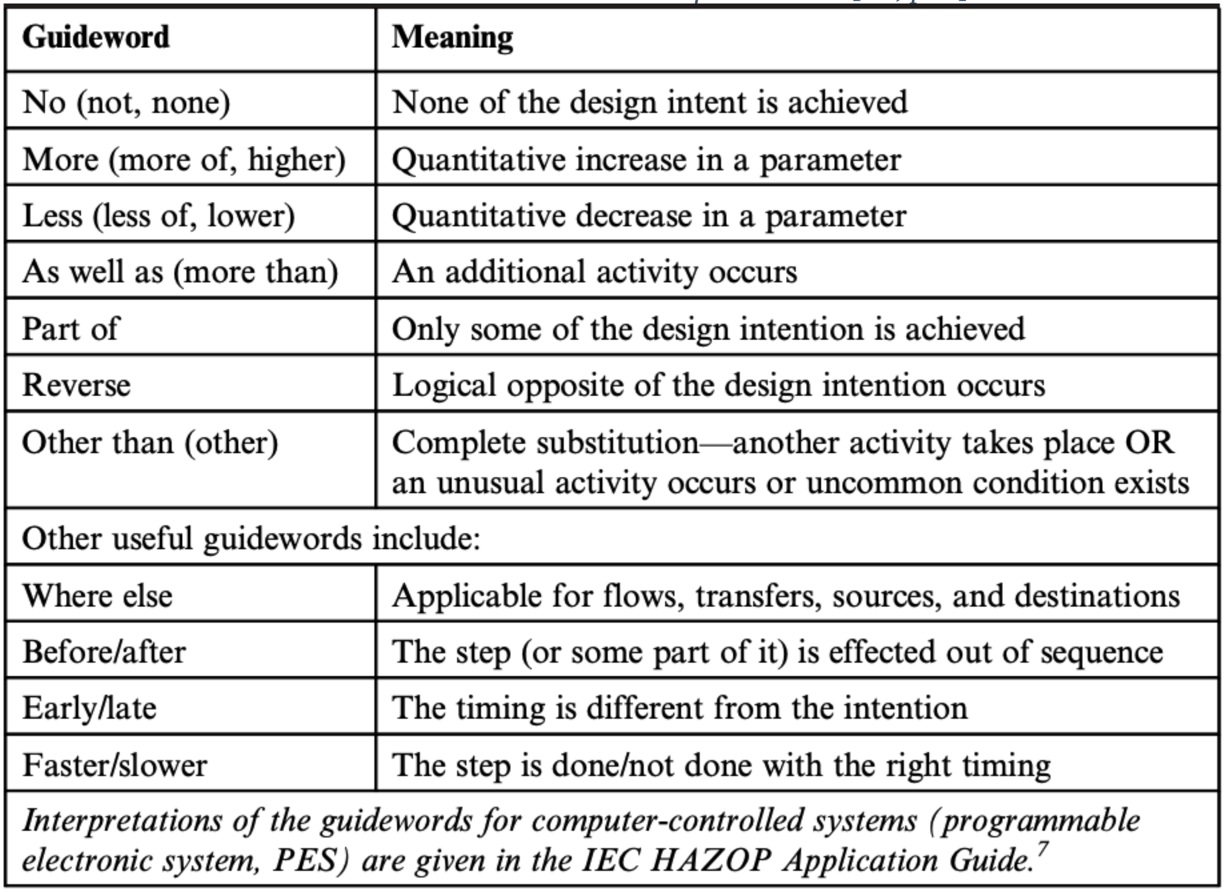
2.2.3 Hazard and Operability Analysis (HAZOP)

HAZOP is a systematic hazard analysis technique that was developed by the Chemical Industries Association (CIA) in the 1960s and has since become the method of choice for various other industries who aim to analyze the design of new processes and operations [18]. Typically conducted by a multidisciplinary team, HAZOPs involve a systematic, yet creative analysis of a system or concept of operations for which detailed design features are readily available. The objective is to ultimately determine how a system or process may deviate from intended operations [12].

To initiate a HAZOP, analysts create a conceptual model of their physical system or operation using provided details of the design or operations. Next, the team states the design intentions of the system and specifies the intended operational range. In this step, analysts may consider intentions for physical equipment, conditions, timing and execution of state transitions, as well as component inputs and outputs. The goal is to clearly connect the design intentions with the generated model of the system [19].

The next step in a HAZOP is to list undesirable deviations from the stated intentions. Specific guidewords, such as those shown below in Table 2-1, are combined with parameters to systematically identify deviations. Parameters refer to the physical activities of the component being analyzed and may include aspects such as flow, speed, monitoring, separation, time, sequencing, signal, phase, control, and communication [19]. Using this process, an example deviation for the lasercom system could be, “Less power is received than intended,” specifying the intended power of signal reception.

Table 2-1: Standard Guidewords for HAZOP [19, p. 3]



Guideword	Meaning
No (not, none)	None of the design intent is achieved
More (more of, higher)	Quantitative increase in a parameter
Less (less of, lower)	Quantitative decrease in a parameter
As well as (more than)	An additional activity occurs
Part of	Only some of the design intention is achieved
Reverse	Logical opposite of the design intention occurs
Other than (other)	Complete substitution—another activity takes place OR an unusual activity occurs or uncommon condition exists
Other useful guidewords include:	
Where else	Applicable for flows, transfers, sources, and destinations
Before/after	The step (or some part of it) is effected out of sequence
Early/late	The timing is different from the intention
Faster/slower	The step is done/not done with the right timing
Interpretations of the guidewords for computer-controlled systems (programmable electronic system, PES) are given in the IEC HAZOP Application Guide.[7]	

After enumerating deviations, the next step is to record the possible causes and consequences of deviations, again assuming a linear chain-of-events. Brainstorming is used to determine as many causes as possible, considering human factors related issues along with hardware failures [20, p. 4]. The effects of the deviations are then evaluated, considering whether they move the system outside of its intended envelope of operation. Both immediate and delayed effects are considered in this step [20, p. 4]. Finally, safeguards already established are evaluated. If the current safeguards are inadequate, new safeguards are implemented or aspects of the design are altered to provide adequate protection against deviations.

There are several properties of HAZOP that make it advantageous. As opposed to the previously mentioned methods, HAZOP includes humans in its considerations of deviations in addition to hardware failure. Furthermore, it is a qualitative method pointing towards design flaws, rather than a quantitative method attempting to establish probabilities of individual component failure. Because the method was designed for new chemical plants with novel design features, it is also useful for evaluating the design of new systems [21]. Its systematic process of identifying deviations in a system using guidewords and its encouragement of multidisciplinary teams helps foster creativity which may lead to the identification of new hazards emerging in new systems.

Despite these advantages, there are also several weaknesses that make HAZOP less fitting for the analysis of a novel lasercom system. HAZOP requires a multidisciplinary team because it requires the judgement of experts in different fields. While this is useful for encouraging creativity in brainstorming, it is also very labor-intensive and can be biased based on the subjectivity of various experts' reasoning [12]. Additionally, HAZOP processes lead to the identification of many hazards related to deviations, but fail to highlight hazards related to information or management systems as the method focuses primarily on proximal events within the linear chain-of-events model [22]. Finally, the method uses physical models of the system. While these system representations may be useful for identifying hazards due to hardware failures and physical connections, they do not adequately capture software [12], a component that is critical to consider in the analysis of complex systems. The method cannot identify anything but unsafe software outputs; there is no way to trace them back through the software and therefore is not useful for deviations related to software causes.

The proposed lasercom system will require an analysis of the software in addition to hardware and human interactions as much of the connection process will be automated. Furthermore, it will be useful to consider the management system and organizational structure implementing the system in addition to lower-level controllers. Due to the complexities of the software and teaming interactions within the lasercom system and HAZOP's limitations, HAZOP will not be considered for the analysis of the system. A more holistic approach that can fully capture the complex interactions within the system is needed.

2.2.4 STAMP and STPA

Systems-Theoretic Accident Model and Processes (STAMP) is a new causality model that is rooted in Systems Theory, a framework that treats systems as a whole, rather than a collection of components to be analyzed individually [12]. In doing so, it views safety, security, and other emergent system behaviors as a control problem rather than a reliability problem. Instead of viewings accidents as linear, STAMP incorporates hierarchical feedback-control loops to model the dynamic interactions between human controllers, software, and hardware. Considering the feedback, hierarchy, and communication within the system, the analysts can better understand the system behavior and generate safety constraints to prevent system losses.

Systems-Theoretic Process Analysis (STPA) is a holistic hazard analysis technique that uses the principles of STAMP as its foundation. Using the control structure to model the feedback-control loops within the system, it provides a method to understand the relationships between components. It is thus useful for large complex systems where losses may occur not only due to individual component failure, but due to the system's *emergent* behavior, that is, the behavior resulting from the interactions between components within the system. Because it uses abstraction in modeling the system, it allows early concept systems to be analyzed, which supports the derivation of safety requirements and architecture design during system development. These attributes make it well-suited to address the challenges associated with the proposed lasercom system.

There are four basic steps to STPA, shown below in Figure 2-3. First, the system and its boundaries are defined, losses and hazards are identified, and system-level safety constraints are derived. In the second step, the system is modeled as a control structure, incorporating feedback-control loops to depict interactions within the system. The third step entails the identification of Unsafe Control Actions (UCAs) which may lead to losses in a specific context. The fourth and final step is to generate causal scenarios that may lead UCAs to occur. These steps will be described in further detail in Chapter 4.

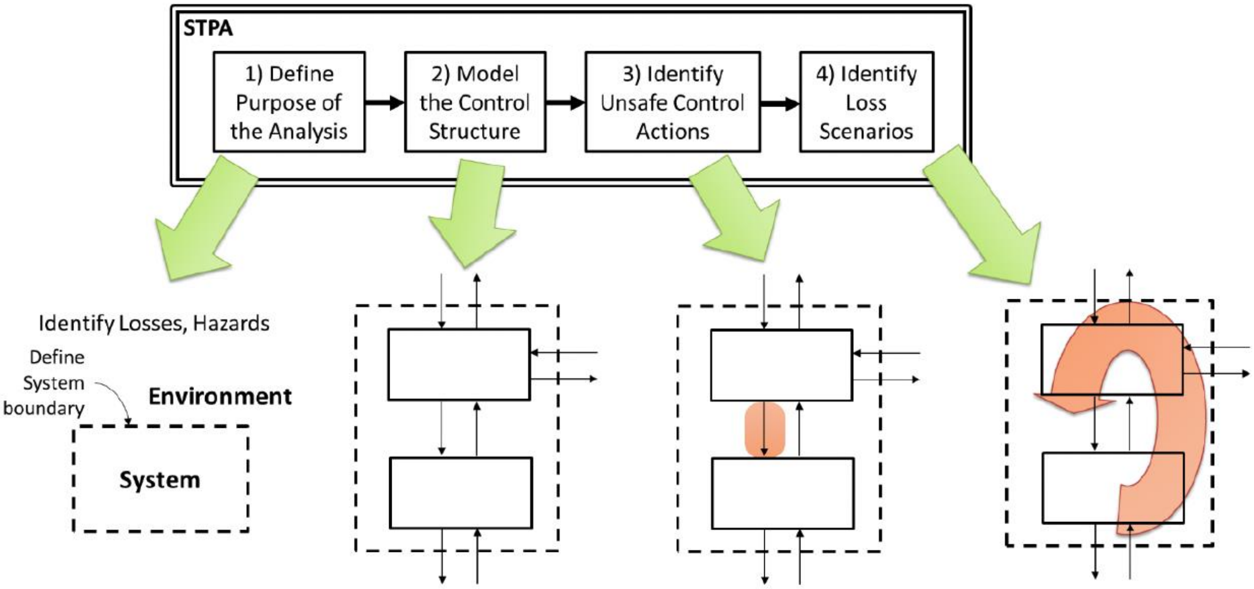

STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

Figure 2-3: Four Basic Steps of STPA [23]

One might question why a hazard analysis technique such as STPA would be useful for the analysis of an early concept communication system, rather than a method designed to assess reliability. Leveson argues that safety and reliability are two separate system properties to be analyzed [11]. A system may be safe, but unreliable if it does not enter hazardous states, but also does not accomplish its intended function. Likewise, it may be reliable, but unsafe if all of the individual components function as designed, but the interactions of the components move the system to a hazardous state.

The previously described analysis techniques all identify scenarios in which systems are unreliable and therefore unsafe. While STPA addresses such scenarios, it additionally identifies scenarios in which systems are unsafe even while being reliable: scenarios in which system components accomplish their intended function, but the system still behaves in a hazardous manner [11]. In the complex design and operation of the proposed lasercom system, analyzing reliability to prevent component failures will not be enough. System designers must understand when the system may enter hazardous states due to component interactions and flawed system design.

Several studies have compared STPA with the traditional hazard analysis techniques based on the linear chain-of-events causality model [23], [24]. In all the investigations, STPA identified the same causal loss scenarios as the other techniques, but also found additional scenarios. Using STAMP as a causality model, STPA is able to find causal scenarios related to software interactions, human factors related issues, or design flaws, and do so in less time and with fewer resources than the other methods [23]. Because of its ability to analyze safety outside of reliability and its consideration of many additional causal factors, STPA is well-suited to address the challenges of developing and operating an airborne lasercom system.

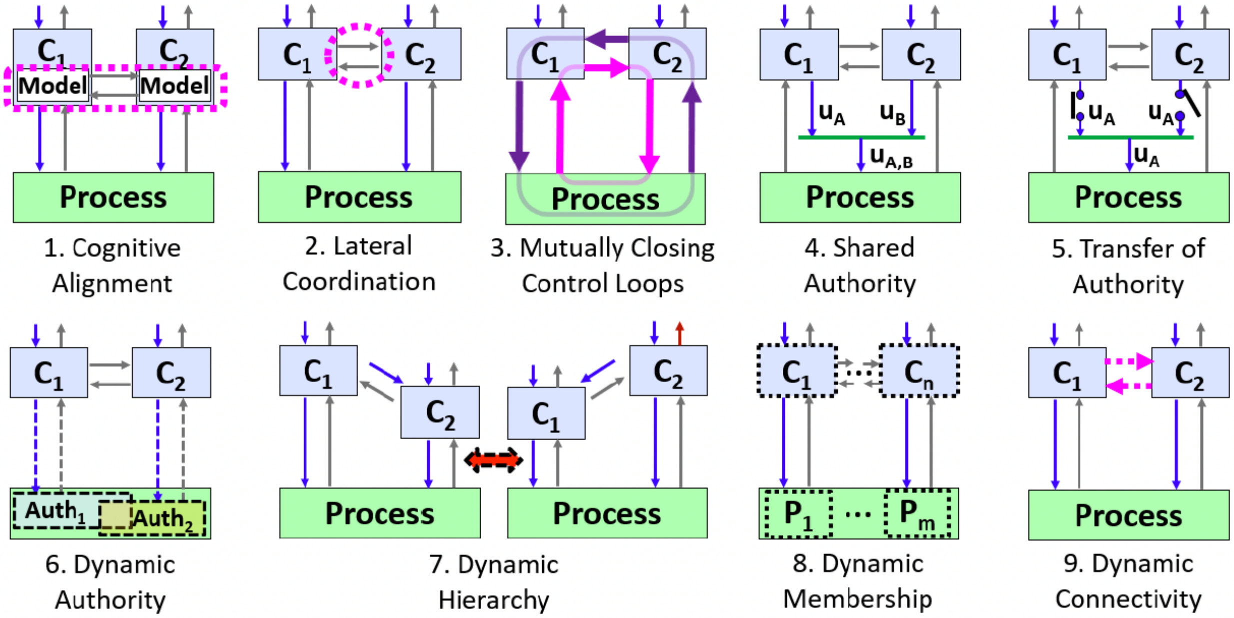
2.3 STPA-Teaming: An Extension of STPA for Systems with Collaborative Control

While traditional STPA provides guidance to analyze the challenges associated with internal control of systems, recent extensions of STPA have been developed to systematically identify challenges associated with *shared control* in collaborative systems. STPA-Teaming is a recent extension that provides a mechanism to analyze coordination in complex teaming systems [25].

2.3.1 A Framework for Collaborative Control

In his MIT dissertation, *System-Theoretic Safety Analysis for Teams of Collaborative Controllers*, Kopeikin creates a framework to describe the interactions between collaborators with shared control [25]. This framework provides a foundation for analyzing unsafe collaborative control actions and ultimately supports the generation of requirements to address the coordination aspects within systems.

Using a system-theoretic approach, Kopeikin introduces nine dynamic behaviors that affect the collaboration and control within teaming systems [26]. These "collaborative control dynamics" shown below in Figure 2-4 highlight concepts of system theory such as hierarchy, control and feedback, and communication. They represent the system's changing hierarchical control and dynamic influences on controller process models. In doing so, they help analysts understand how and why unsafe control may occur.



1. Cognitive Alignment

2. Lateral Coordination

3. Mutually Closing Control Loops

4. Shared Authority

5. Transfer of Authority

6. Dynamic Authority

7. Dynamic Hierarchy

8. Dynamic Membership

9. Dynamic Connectivity

Figure 2-4: Nine Collaborative Control Dynamics for STPA-Teaming; reproduced with permission of author [25]

STPA-Teaming first addresses *Cognitive Alignment*, that is, the consistency of various controllers' process models. Unsafe cognitive alignment may occur if process models and control algorithms are constructed differently, initialized differently, or improperly updated [25]. It additionally addresses *Lateral Coordination*, which is defined by Johnson as "peer interaction where control is not implied" [27]. It refers to how controllers collaborate and share information regarding the state of the controlled process and the state of their own systems. Lateral Coordination can be performed through both direct communications as well as passive observations and predictions that controllers use to maintain situational awareness of the shared process [26].

Mutually-closing Control Loops occur when one controller must "close the loop" providing information about provided control actions or the state of the controlled process—information that the other controller may not otherwise have accessible [25]. There are two ways in which unsafe control may be caused by mutually-closing control loops: 1) Unsafe feedback about the shared process is received from collaborators or 2) Unsafe feedback about collaborator control actions is received from the shared process [25].

Shared Authority may occur when multiple controllers have authority over the same process or interdependent processes [26]. It includes situations in which higher controllers may delegate responsibilities to lower controllers, but intervene and override control actions if necessary. It also includes scenarios in which peer controllers can make inputs into the same process. Authority to provide a common control action may shift between multiple controllers in what is known as *Dynamic Authority*. *Transfer of Authority* occurs when controllers change their division of labor and specifically reallocate responsibilities to other controllers during the physical process [26].

Collaborating controllers may have different capacities to lead given different contexts. *Dynamic Hierarchy* reflects shifts in the hierarchical control structure that occur when controllers switch administrative or leadership roles. In addition, *Dynamic Membership* and *Dynamic Connectivity* consider how system changes over time may lead to unsafe control: Dynamic Membership, refers to the ability of some controllers to leave and join the system over time, while Dynamic Connectivity refers to the changes in communication channels over time. It explores factors such as momentary link outages, delays in information sharing, or the use of unsafe communication channels [25].

2.3.2 STPA-Teaming's Extension to Traditional STPA Processes

These nine collaborative control dynamics provide a framework to analyze the interactions between controllers within a teaming system. STPA-Teaming provides a mechanism to analyze these interactions by extending STPA steps 2-4.

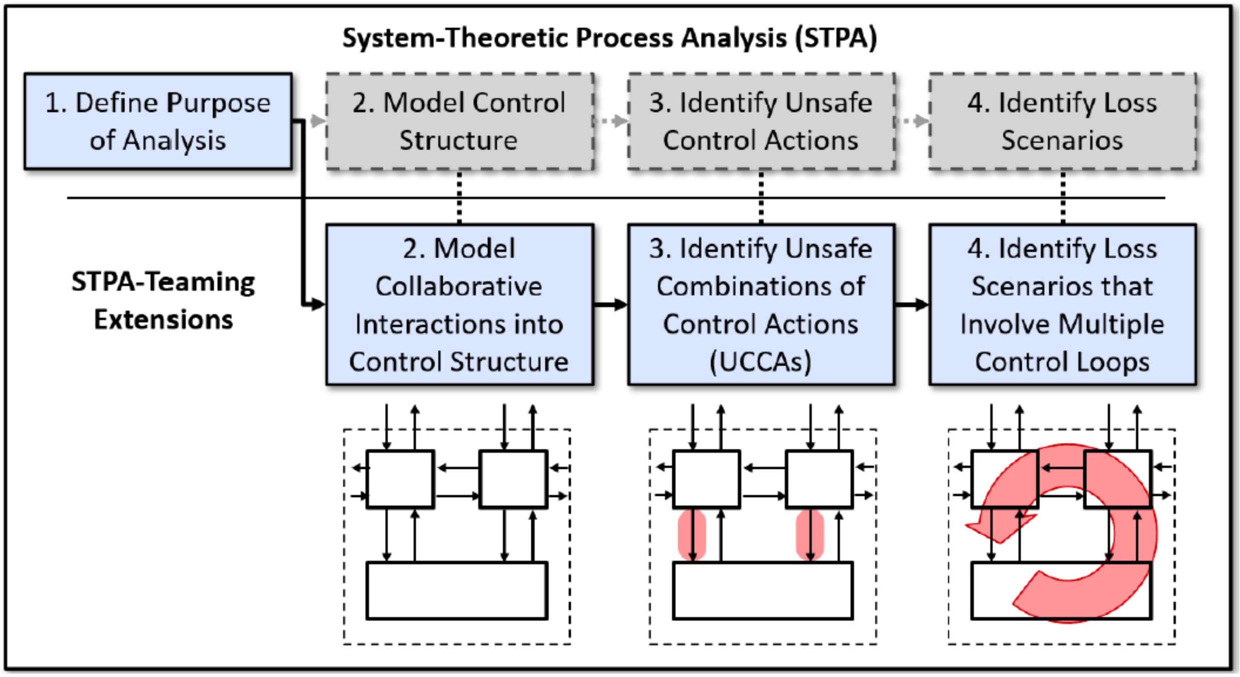

System-Theoretic Process Analysis (STPA)
1. Define Purpose of Analysis
2. Model Control Structure
3. Identify Unsafe Control Actions
4. Identify Loss Scenarios
STPA-Teaming Extensions
2. Model Collaborative Interactions into Control Structure
3. Identify Unsafe Combinations of Control Actions (UCCAs)
4. Identify Loss Scenarios that Involve Multiple Control Loops

Figure 2-5: STPA-Teaming's Extensions to STPA; reproduced with permission of author [25]

First, a *Collaborative Control Structure* is created to depict the systems providing control over a shared process. The goal of the Collaborative Control Structure is to model the dynamic and influential interactions between controllers to understand how they form their process models regarding their own system, other systems, and the shared controlled process [25].

The next step is to identify *Unsafe Combinations of Control Actions (UCCAs)*. In this step, the analysis identifies when combinations of the *same* control action and combinations of *different* control actions may be unsafe, leading to system hazards. STPA-Teaming provides a mechanism to systematically identify such unsafe combinations and recognize when unsafe transfers of control actions may occur [28].

Finally, in the fourth and final step, STPA-Teaming specifically uses the collaborative control dynamics to understand how and why UCCAs may occur. Top-level loss scenarios are generated and then refined to identify contributing collaborative control or internal control factors. The output of the analysis, that is, the identified loss scenarios, are then used to guide the safety-driven design of the system by supporting the generation of safety-constraints.

The proposed lasercom system will most likely exhibit all nine of the collaborative control dynamics defined above. Controllers will need to maintain cognitive alignment and close control loops regarding the state of the optical signal and aircraft within the system. To do so, they will need to coordinate both laterally with partner aircraft and vertically with higher mission authorities, providing information such as aircraft heading and position, acquisition modes, transmission parameters, and more. Furthermore, the system will be subject to frequent change as members enter and exit the network and communication channels change.

Given the applicability of these collaborative control dynamics, STPA-Teaming is well-suited to address the challenges associated with coordinating aircraft for lasercom. As such, this thesis applies STPA-Teaming to identify potential flaws in coordination and generate recommendations for system design and operation. The following chapter describes the proposed system and Chapter 4 details the application of STPA-Teaming to the system along with system recommendations that result from the analysis.

Chapter 3 Defining the System

Before applying STPA, it is necessary to understand the laser communication system and how it may be operated. Moreover, because the purpose of the system is to share data between military platforms, it is necessary to understand the Air Force's system for managing communications and controlling aircraft.

Because this system is in the early conceptual stage of design, the majority of design decisions involving human-computer interfaces, system configurations, and component interactions have not yet been made. Additionally, operating procedures and organizational responsibilities have not yet been established by the Air Force for implementation of the system. For this reason, this section will describe at a high-level how the lasercom system may be controlled by operators and how the Air Force may integrate the lasercom system into its command and control structure, known as a Theater Air Control System (TACS).

Components of the system will include the lasercom systems, human operators, aircraft, and a higher mission authority such as an Air Operations Center (AOC) to guide operations. The system components and typical TACS control of aircraft are described below.

3.1 Air Operations Center (AOC)

The AOC is the senior agency of the TACS and provides command and control (C2) of Air Force air and space assets, while coordinating with other services and allied nations [29]. It consists of both ground-based elements and airborne elements to appropriately plan and manage operations. Responsibilities include tasks such as airspace control, intelligence, surveillance, and reconnaissance (ISR) management, threat warning, battle management, weapons control, combat identification, and strategic communications [29]. The following section details how the AOC provides control throughout the stages of a mission.

Mission Planning
Prior to missions, planners within the AOC develop Information Exchange Requirements (IERs) to support mission objectives. IERs specify communication requirements (who must communicate with who), the systems necessary to enable communications, the data to be shared, and characteristics of communications (throughput of channels, quantity of data, etc.) [30]. Before missions are initiated, the AOC publishes several authoritative documents to provide IERs to operators, as well as to provide general guidance for the mission. These documents are discussed below.

1. Airspace Control Order (ACO): For a specific area of operations, the AOC releases a document known as the Airspace Control Order (ACO) to provide general guidance for airspace control. It includes information regarding airspace deconfliction responsibilities, standard altitudes and routes for various aircraft types and missions, and air refueling procedures. To supplement the ACO, the AOC releases Aircrew Read Files (ARFs) that contain additional rules of engagement (ROEs) and changes to the ACO [31].
2. Air Tasking Orders (ATO): For individual missions, the AOC releases the Air Tasking Orders (ATO), or “frags” every 24 hours. This document contains specific information

regarding flight schedules as well as Special Instructions (SPINS) and the Operational Tasking Data Link (OPTASK LINK) for each mission [32].

a. Special Instructions (SPINS): The SPINS contain pertinent information for in-flight communications with the AOC such as the WORDS for the day. WORDS is a directive or interrogative call for further information or directives relevant to a mission. They are useful for ensuring critical information and commands are relayed when multiple entities are exercising command and control over aircraft in a specific operating area. They contain information such as changes to data packages, changes to the tactical mission network, timing changes, threat updates, and updates regarding weather affecting task execution [33].
b. Operational Tasking Data Link (OPTASK LINK) Message: This document contains detailed procedures on how to establish tactical data link communications and who to establish data links with. It provides tasking information such as the objectives, priorities, and specific duties for communication. It outlines coordinating instructions such as message identification, message schedule, message recipients, unit call signs, and unit locations. Additionally, it provides technical parameters such as cryptography keys, frequencies, waveforms, filter plans, modulation settings, and unit addresses of all participating units in the theater [34].

Control During Missions

During missions, the AOC is responsible for providing airspace control and updating pilots' situational awareness. In many operations, the communication coverage provided by ground elements is not sufficient due to line-of-sight or radio limitations. When these limitations occur, the AOC communicates with aircraft through airborne elements such as an Airborne Warning and Control System (AWACS) or Joint Surveillance Target Attack Radar System (JSTARS). These platforms provide air surveillance, identify airborne objects, and control air operations [29].

Aircraft operators first "check-in" with the AOC before mission execution to establish accountability and ensure critical information is received. During check-in, the AOC conducts several checks to verify aircraft position and identity: it checks for a valid response to the IFF code (i.e. mode 1, 2, 3A, 3, 4, and S), checks precise participant location and identification (PPLI), correlates radar data with the incoming signal, executes authentication procedures, and verifies aircraft adherence to the ACO/briefed sanctuaries [33]. The AOC assigns an air track ID to the aircraft and then provides mission updates to aircrew through the WORDS outlined in the SPINS. It receives feedback from aircrew regarding aircraft/mission status, and it provides weather updates, airspace coordinating measures, and updates regarding other aircraft's location and identities. Finally, the AOC routes the aircraft to its mission area to accomplish the assigned mission or be transferred over to another AOC element controlling a separate area of operations [33].

Post-Mission Reviews

After missions, the AOC and squadrons associated with the mission are responsible for assessing the effectiveness of the communications in the mission. The AOC elements that plan and maintain the data link network are responsible for reviewing the communication system's effectiveness and altering future network plans to address issues experienced in the completed mission. The operators' squadrons are responsible for reviewing the operators' adherence to established ROE's and mission plans and ensuring future mission plans are properly followed by operators.

3.2 Operators

Operators in the context of the lasercom system refer to the pilots controlling both their aircraft and their lasercom system. Operators could be stationed on the ground flying a UAV equipped with a lasercom system, or they could be physically present in the aircraft, conducting manned flight. While the two possibilities may result in different scenarios, both can be modeled and analyzed in the control structure for STPA-Teaming.

Operators have the traditional aircraft responsibilities of managing the flight control and propulsion systems, as well as the RF communication and navigation systems. They are responsible for adhering to the AOC's plans and airspace control. Additionally, they must ensure aircraft are positioned within line-of-sight, adequate range, and in viable atmospheric conditions (altitude and weather) for effective optical communications. Controlling the RF communications systems, operators must use appropriate transponder codes and radio frequencies for proper identification and communication with the AOC and other aircraft. During missions, they must effectively communicate their aircraft position, heading, and status with the AOC, and should confirm receipt of AOC updates and commands given changes in plans.

Operators are responsible for controlling their lasercom system such that the correct parameters, partner selection, and operational modes for connection are implemented. To establish a lasercom link, operators must first select a partner for connection. Operators are responsible for verifying partner authorization and ensuring any relevant information such as location, heading, velocity, and intentions is shared with the partner system. To assist in the acquisition process, onboard sensors may be used to locate and track the partner and provide awareness of the host aircraft's trajectory.

Once a partner terminal is selected, operators must select the technical parameters required for communications based on commands from the AOC and/or coordination with partner terminals. These parameters may include, but are not limited to the following:

1. Beacon parameters (if a separate beacon beam is used): wavelength transmitted, modulation format, and data rate
2. Acquisition parameters (if a separate beacon beam is not used): acquisition modulation format on top of communication signal
3. Communications transmitter parameters: wavelength transmitted, modulation format, forward error correction (FEC) type, and data rate
4. Communications receiver parameters: wavelength transmitted, modulation format, FEC type, and data rate

During acquisitions, operators are responsible for ensuring their system either broadcasts a beacon beam or detects a beacon beam until tracking is initiated. Once the systems locate one another and initiate fine-tracking, the operators must monitor transmissions to ensure the entire data set is transmitted and received. If transmission issues occur, operators are responsible for executing built-in tests (BITs) and coordinating with the AOC and partner systems to continue operations.

3.3 The Lasercom System

The lasercom system includes the automation and the optics and modem it controls to provide accurate pointing and signal processing. The lasercom system is responsible for executing the control actions provided by system operators for partner selection, acquisitions, and data sharing through the optical signal. The system automation must provide precise pointing, acquisition, and tracking (PAT) to establish a link. The sequencing of control actions to establish a link is described in detail below.

Pointing & Acquisition

Once the operators command the terminal to establish a connection, the system automation will initiate the acquisition sequence. The goal of the acquisition process is for the two terminal's beams to contact one another and "lock on" for tracking and data sharing. The following section details how a terminal executes acquisitions, searching for its partner terminal, acquiring the partner's beam, and transitioning to communications.

I. Pre-acquisition: Before and during acquisitions, each terminal must process its host aircraft's position and orientation to understand its location in relation to partner aircraft. This information could be provided by inertial navigation system (INS) sensors on the terminal or other navigation and flight control subsystems. The acquisition process is initiated by each terminal transmitting, receiving, and processing information such as global positioning system (GPS) and INS position data to reduce the area of uncertainty. Such information may be shared using existing tactical data link (TDL) communications.

II. Transmitting a beacon: Once systems determine the approximate location and trajectory of one another, systems are responsible for initiating acquisitions by transmitting either 1) a beacon beam (wide, diverged beam used in beacon-based systems) or 2) a synthesized beacon (comms beam used for acquisitions in beaconless systems).

III. Detecting a beacon: The partner system is then responsible for pointing its acquisition sensors in the direction of the incoming beacon such that the beacon is detected. Both systems must be oriented such that the beacon beam is within the detecting system's field of view (FOV) and line-of-sight between terminals is unobstructed.

IV. Open-loop coarse tracking: Once the beacon beam is detected, the detecting system points its beam in the direction of the incoming beacon (towards its partner) in a process known as open-loop coarse tracking. When the initiating terminal detects that beam, it shuts down its acquisition beam to point a more narrow, precise beam towards its partner. Once the two systems' narrow beams point directly at one another, they are able to "lock on" to one another and acquisition has been completed. At this point, the systems can transition to closed-loop fine tracking and can begin sharing data.

Fine Partner Tracking

Systems must maintain precise partner tracking throughout the entire duration of transmissions. Once acquisition is complete and a connection is established, accurate tracking of partner terminals becomes relatively easy. Relying on tracking sensors, both systems utilize a set of nested tracking control loops in which they detect the direction of the incoming optical signal and adjust their pointing direction to maintain tracking. If the received beam moves outside the FOV of the recipient's sensors, the system automation progresses to outer control loops until the beams are locked on again.

In order to maintain tracking in the dynamic environment of flight, the system automation must predict the trajectory of its partner platform so that its beam continues to point at the partner as data is relayed. Algorithms relying on Kalman filters or calculations of Doppler Shift[1] may be used to predict the location of partner platforms based on position data already collected, some uncertainty in position, velocity, and acceleration, and a kinematic model for how the platform is expected to move (motion constraints).

To maintain partner tracking, systems are responsible for link maintenance, that is, ensuring the transmitter and receivers are aligned with the tracking sensors. Atmospheric turbulence and platform jitter can cause such components to become misaligned with the tracking sensors over time, leading to pointing errors. The system automation is responsible for executing functions such as BITs and nutation to check for boresight alignment and maintain accurate tracking.

Communications

Once systems are successfully tracking, they can begin transmitting and receiving data. The automation is responsible for transmitting and receiving data at the technical parameters provided by operators (i.e. wavelength, data rate, modulation, etc.). The system automation is also responsible for adjusting the power used for transmission as altitude and range between terminals could affect the power received.

Systems are responsible for recognizing when the entire data set has been transmitted or when specific packets of data are missing. Similarly, systems are responsible for delivering feedback regarding data received. If inadequate amounts of power are received for some specified duration, the system automation is responsible for detecting the link outage and regressing as needed: The system must stop transmitting or receiving data and transition to acquisitions in an attempt to re-acquire.

As previously mentioned, many components of the lasercom system and aspects of its operations are still undefined. Accordingly, the goal of this chapter was to provide an overview of how the system may operate at a high-level. It described how Air Force command and control elements typically provide mission guidance and it detailed at a more technical level how lasercom systems establish and maintain a connection. In the next chapter, STPA-Teaming is applied to the system to identify causal scenarios that may result in loss of communication as well as other losses that could negatively impact Air Force operations.

[1] Doppler shift is the change in wavelength or change in data clock rate over a given distance. This parameter, provided by the established communications link, can lead to higher accuracy in partner tracking.

Chapter 4 Application of STPA-Teaming to an Airborne Lasercom System

4.1 Step 1: Identifying the Purpose of the Analysis

The first step of STPA is to identify the purpose of the analysis. In this first step, the losses and hazards to be prevented are outlined, and system level safety constraints are derived from the hazards.

4.1.1 System Losses

The system losses are defined as losses involving anything of particular value to stakeholders [23]. Given that the system purpose is to provide a secure, means of communication for military missions, the following losses would be deemed unacceptable.

Table 4-1: System Losses

Loss ID	Loss Description
L-1	Loss of communication
L-2	Loss of sensitive or mission-critical information
L-3	Injury to people
L-4	Damage to aircraft or equipment

4.1.2 System Hazards

The next step in STPA is to define the system hazards, or any "system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to loss" [23]. The following hazards represent such system states or set of conditions that could lead to a loss. Each hazard is linked with its associated loss.

Table 4-2: System Hazards

Hazard ID	Hazard Description	Loss Link
H-1	Systems are unable to establish and maintain a connection	L-1, L-2
H-1.1	Systems exceed maximum separation distance for connection	L-1, L-2
H-1.2	Systems do not point in correct direction	L-1, L-2, L-3, L-4
H-1.3	Systems' communication pathway is blocked by a physical obstruction	L-1, L-2, L-3, L-4
H-2	Systems do not convey intended message	L-1, L-2
H-2.1	Systems do not transmit/receive all necessary information	L-1, L-2
H-2.2	Systems transmit a signal that is distorted	L-1, L-2
H-2.3	Systems transmit a signal that is incompatible with partner system (i.e. parameters such as wavelength, modulation, power, data rate, encryption, etc.)	L-1, L-2
H-3	Systems exceed safe operational limits (i.e. power limits, interference limits, etc.)	L-1, L-2, L-3, L-4

H-4	Systems allow unauthorized/unintended users to receive/transmit data	L-1, L-2, L-3, L-4
H-5	Systems interfere with other operational platforms (other aircraft/spacecraft)	L-1, L-2, L-3, L-4
H-6	Systems expose humans to harmful effects (i.e. burning/blinding lasers)	L-3, L-4

4.1.3 System Level Safety Constraints

The system level constraints can be directly derived from the system hazards. These constraints, or the "system conditions or behavior that need to be satisfied to prevent hazards [23]" are listed below. Associated hazards are linked for ease in traceability.

Table 4-3: System Level Safety Constraints

Constraint ID	Constraint Description	Hazard Link
SC-1	Systems must establish and maintain a connection	H-1
SC-1.1	If systems lose connection, systems must be able to recognize connection has been lost and re-establish connection	H-1
SC-1.2	Systems must not exceed maximum separation distance for connection	H-1.1
SC-1.3	Systems must point at and track partner system's beam	H-1.2
SC-1.4	Systems must avoid physical obstructions to communication pathway	H-1.3
SC-2	Systems must convey intended message	H-2
SC-2.1	Systems must transmit/receive all necessary information	H-2.1
SC-2.2	Systems must avoid signal distortion	H-2.2
SC-2.3	If signal is distorted, systems must detect and report signal distortion	H-2.2
SC-2.3	Systems must transmit a signal that is compatible with partner systems (i.e. wavelength, modulation, power, data rate, encryption, etc.)	H-2.3
SC-3	Systems must not exceed safe operational limits (i.e. power limits, interference limits, etc.)	H-3
SC-4	Systems must prohibit unauthorized/unintended users from connecting	H-4
SC-5	Systems must not interfere with other operational platforms (other aircraft/spacecraft)	H-5
SC-6	Systems must not expose humans to harmful effects (i.e. burning/blinding lasers/compromised position in hostile territory)	H-6
SC-6.1	Systems must deactivate when appropriate (i.e. on the ground/not in use)	H-6.1

This section discussed the purpose of the analysis. In doing so, it defined the system, system losses to be prevented, associated hazards, and system-level safety constraints to prevent the hazards. The next section details the control structure for the analysis.

4.2 Step 2: Generating a Control Structure

In the second step of STPA, the system is modeled as a hierarchical control structure composed of feedback-control loops [23]. As discussed in Chapter 3, the system includes higher mission authorities such as the AOC, operators, aircraft, and lasercom systems. The control structure models the control actions available to these controllers, and the feedback that is necessary to control the physical process.

STPA-Teaming extends the control structure of traditional STPA by including controllers with *shared authority* over a *shared controlled process*. This “Collaborative Control Structure” represents the dynamic collaborative factors within the system with dashed lines [25]. Dashed vertical arrows represent *dynamic authority* of controllers, that is, when controllers may shift the responsibility of providing a control action to other controllers. Dashed lateral arrows between controllers represent *dynamic connectivity,* indicating when controllers cannot always communicate with one another. And dashed lines around a controller symbolize *dynamic membership*, when controllers are not always a part of the system [25]. These dynamic collaborative factors are investigated further in Step 4 of STPA-Teaming.

The collaborative control structure for the airborne FSOC system is shown below in Figure 4-1. The system could contain many aircraft equipped with lasercom capabilities. To account for the similarities of controllers in the network and to model their collaborative interactions, two sets of operators, aircraft, and lasercom systems are depicted. Each set can input identical control actions and can receive identical feedback to control the physical process, which is the optical signal. Additionally, each set interacts with the AOC through the same feedback control loops. Because the system could contain more than two aircraft, the index scheme {1, …, n} controllers is used to represent the variable number of controllers within the system.

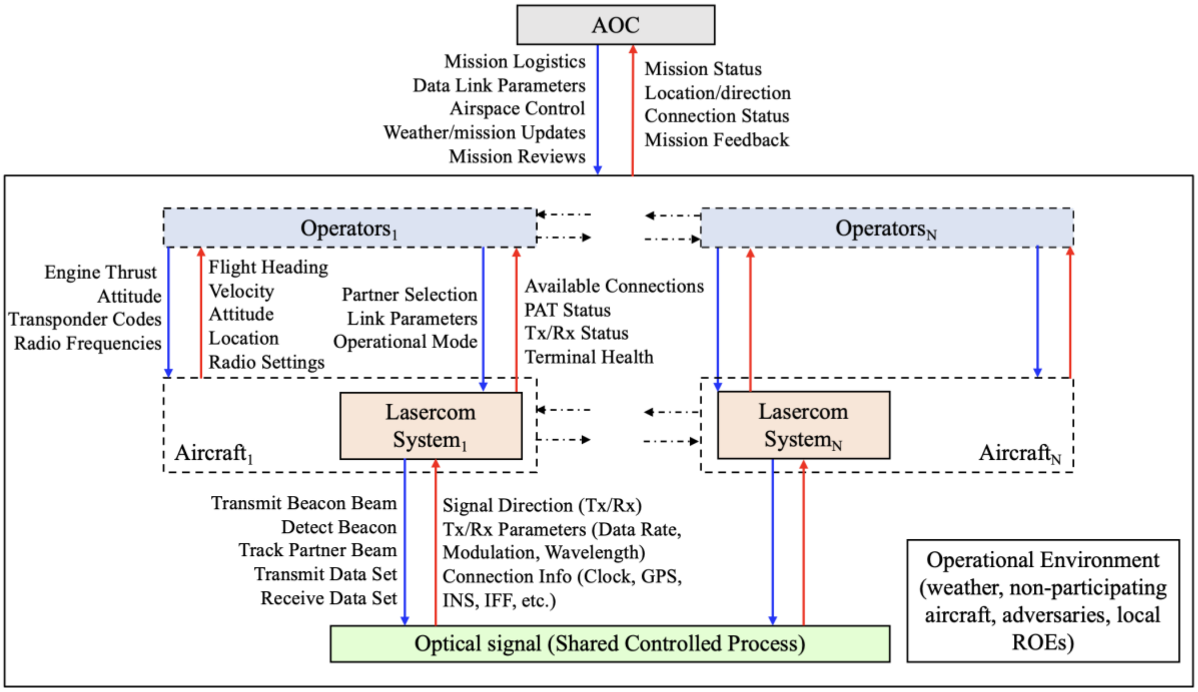


Figure 4-1: Collaborative Control Structure for an Airborne Lasercom System

The responsibilities of each controller are summarized below:

AOC

- Plan mission logistics including flight schedules, routes, and IERs
- Provide data link parameters (i.e. frequencies, modulations, encryption codes, etc.) before and during missions
- Provide airspace control (updates regarding where to fly, when to connect, and who to connect with)
- Update operators regarding status of operations, mission changes, and weather
- Review mission and data link networks after completion of missions

Operators

- Manage engine thrust and attitude to establish appropriate aircraft position and state for connection (location and altitude, heading, attitude, airspeed, etc.)
- Manage communication systems (outside of lasercom) inputting radio frequencies and transponder codes as provided by AOC
- Select partners for connection
- Input necessary technical parameters for acquisitions (frequency, data rate, modulation, etc.)
- Input data link parameters for transmissions (frequency, data rate, modulation, etc.)
- Conduct necessary calibrations and system tests to check for adequate system performance
- Coordinate with connecting operators and AOC to share necessary state information and establish a connection

The Lasercom System

- Transmit beacon beam at input technical parameters (wavelength, modulation, data rate, etc.) for initial acquisitions
- Detect beacon beam for acquisitions using input technical parameters
- Track partner beam throughout duration of connection
- Transmit data at input technical parameters
- Receive data at input technical parameters

This analysis will focus primarily on the five control actions available to the lasercom system with the understanding that control inputs from operators and the AOC will affect how these control actions are executed. Various combinations of these five control actions could lead to unsafe control within the system. These unsafe combinations will be explored in Step 3 of STPA-Teaming. But first, to manage the combinatorial complexity of control actions, STPA-Teaming guides the analyst to abstract the initial control structure.

The approach calls for two different abstractions, shown below in Figure 4-2. Abstraction 1 involves the abstraction of the controllers into one collective team providing various control actions. This abstraction is useful for determining how the combinations of *different* control actions together may be unsafe [25]. Conversely, Abstraction 2 models combinations of controllers providing the same control action, which is useful for identifying when combinations of the *same* control action may be unsafe [25].

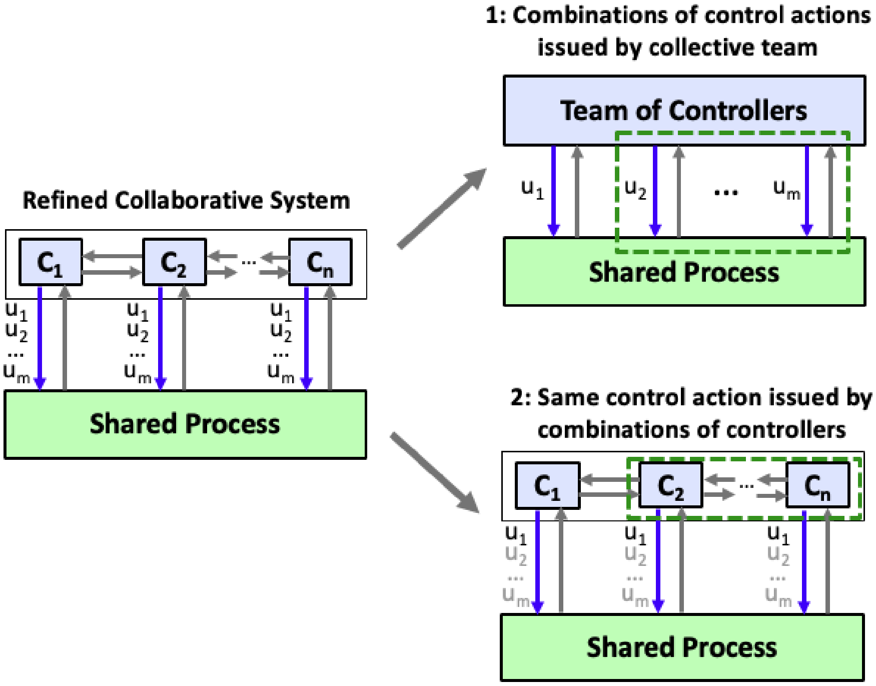

1: Combinations of control actions issued by collective team
Team of Controllers
u_1
u_2
...
u_m
Shared Process
Refined Collaborative System
C_1
C_2
C_n
u_1
u_2
...
u_m
Shared Process
2: Same control action issued by combinations of controllers
C_1
C_2
C_n
u_1
u_2
...
u_m
Shared Process

Figure 4-2: Abstraction of Collaborative Control Structure (adapted from [25])

Following this process, the lasercom system's collaborative control structure is abstracted into two different control structures. The top left control structure in Figure 4-3 depicts Abstraction 1, in which operators and lasercom systems are grouped into teams capable of providing combinations of control actions. The top right control structure shows Abstraction 2 in which a combination of controllers provides the same control actions. Together these control structures are used in Step 3 to determine what combinations of control actions may lead to system hazards.

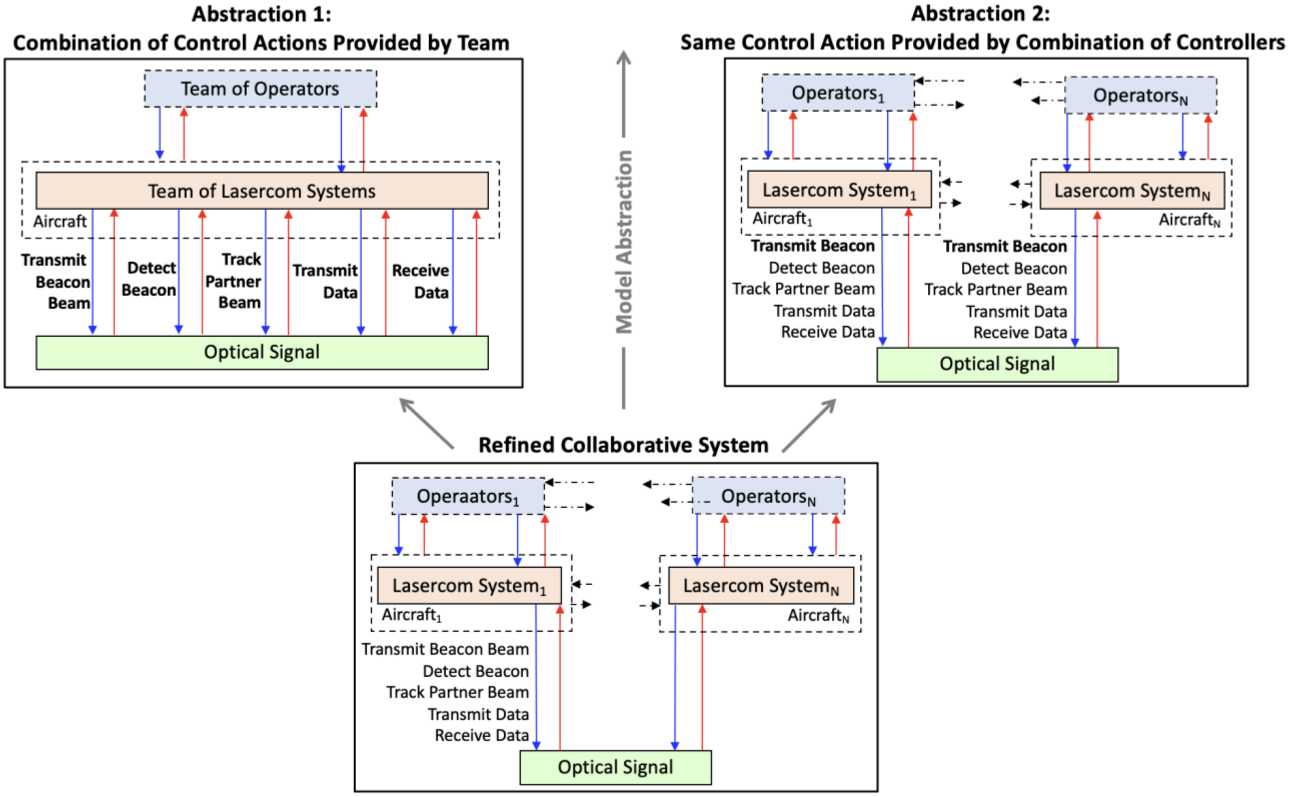


Figure 4-3: Abstractions of Lasercom System to Analyze Combinations of Control Actions

4.3 Step 3: Identifying Unsafe Combinations of Control Actions (UCCAs)

The third step of STPA is to identify Unsafe Control Actions (UCAs), which are “control actions, that in a particular worst-case environment, will lead to a hazard” [23]. There are four ways in which a UCA could occur given one controller, c_i, responsible for providing one control action, u_a:

1) c_i **does not provide** u_a, leading to a hazard
2) c_i **provides** u_a, leading to a hazard
3) c_i **provides** u_a **too early, too late,** or **in the wrong order**, leading to a hazard
4) c_i **provides** u_a for **too long** or **stops too early**, leading to a hazard

STPA-Teaming extends this process by enumerating the *combinations* of control actions that may be unsafe in specific contexts. The abstracted control structures generated in Step 2 are used to systematically identify *Unsafe Combinations of Control Actions* (UCCAs) following the same format of UCAs in traditional STPA [28].

4.3.1 Abstraction 1 UCCAs: Combinations of Control Actions Provided by Collective Team

First, Abstraction 1 is used to identify how combinations of control actions provided by a team of controllers, C_N, may be unsafe. UCCA Types 1-2 follow the same format as UCA Types 1-2 in which a specific control action is provided or not provided. However, the UCCA accounts for more than one control action. In this enumeration, a number of control actions may be abstracted together and compared with one other control action [28]. Abstraction 1 UCCA Types 1-2 are structured as follows:

1) C_N **does not provide** u_1 and **does not provide** $\{u_2$ and/or $u_3\}$ when… [H]
2) C_N **does not provide** u_1 and **provides** $\{u_2$ and/or $u_3\}$ when… [H]
3) C_N **provides** u_1 and **does not provide** $\{u_2$ and/or $u_3\}$ when… [H]
4) C_N **provides** u_1 and **provides** $\{u_2$ and/or $u_3\}$ when… [H]

An example set of these UCCAs are provided below. The logic negation symbol is used to represent a control action not being provided. Context is always provided to explain when the combinations of control actions are unsafe.

Table 4-4: Abstraction 1 UCCAs Types 1-2

#	**Team of Systems**		**Context**
1	¬*Transmit Beacon*	¬{*Detect Beacon, Track Partner Beam*…}	When systems must locate one another to establish a connection [H-1, H-2]
3	¬*Transmit Beacon*	{*Detect Beacon, Track Partner Beam*…}	When system connects with an unintended or unauthorized platform [H-1, H-2, H-4]
5	*Transmit Beacon*	¬{*Detect Beacon, Track Partner Beam* …}	When beacon interferes with partner’s other connections or subsystems [H-1, H-2, H-3]
6	*Transmit Beacon*	{*Detect Beacon, Track Partner Beam* …}	When beacon is transmitted with incorrect parameters for acquisition [H-1, H-2, H-3]

It is important to note that STPA-Teaming purposefully abstracts the controllers into a “Team of Systems” in the first iteration of UCCA-generation. The intention is to later refine the UCCAs to state which specific members of the team provide or do not provide control actions. However, because this analysis focuses on the interactions of one lasercom system with one other lasercom system, it is assumed that “Team of Systems” always refers to one system (including an operator, lasercom system, and aircraft) providing a control action and the connecting system (including coordinating operators, lasercom system, and aircraft) providing the other control action.

UCCAs can also be structured to deal with unsafe timing of control actions. To do so, UCCAs Types 3-4 describe the team of controllers starting or ending control actions before or after other control actions. The structure of this type of UCCA is as follows [28]:

1) C_N **starts to provide** u_1 before it **starts to provide** $\{u_2$ and/or $u_3\}$ when… [H]
2) C_N **starts to provide** u_1 before **ends providing** $\{u_2$ and/or $u_3\}$ when… [H]
3) C_N **ends providing** u_1 before it **starts to provide** $\{u_2$ and/or $u_3\}$ when… [H]
4) C_N **ends providing** u_1 before it **ends providing** $\{u_2$ and/or $u_3\}$ when… [H]

In some cases, combinations of *some*, but not *all* control actions, may be unsafe. For example, it is not unsafe if a system starts *Transmit Data* before its partner system ends *Receive Data*. However, it may be unsafe if a system starts *Transmit Data* before its partner system ends *Detect Beacon*. Accordingly, UCCAs may be refined to eliminate the control actions that do not result in unsafe combinations in a specific context.

A table of the UCCAs Types 3-4 for Abstraction 1 is provided below. **S**{*control action*} represents a controller starting a control action, while **E**{*control action*} represents a controller ending a control action. Only the control actions relevant to the specified context are included.

Table 4-5: Abstraction 1 UCCAs Type 3-4

#	**Any one**	**Before any others**	**Context**
32	**S**{*Transmit Data*}	**S**{*Receive Data*}	When partner system is not prepared to receive data [H-2]
33	**S**{*Transmit Data*}	**E**{*Detect Beacon*}	When acquisition has not been fully completed [H-1, H-2]
34	**E**{*Transmit Data*}	**S**{*Track Partner Beam, Receive Data* }	When acquisition has not been fully completed [H-1, H-2]
35	**E**{*Transmit Data*}	**E**{*Track Partner Beam, Receive Data*}	When entire data set has not yet been transmitted and/or received [H-1, H-2]

This basic process is repeated for each control action to determine all UCCAs for Abstraction 1. A full list of UCCAs can be found in Appendix A. The following section discusses UCCAs for Abstraction 2.

4.3.2 Abstraction 2 UCCAs: Combinations of Controllers Providing the Same Control Action

The generation of UCCAs for Abstraction 2 follows a similar methodology to UCCAs for Abstraction 1. However, instead of describing combinations of different control actions provided by a team of controllers, Abstraction 2 UCCAs focus on combinations of controllers providing the same control action [25]. This UCCA type is structured as follows:

1) c_i **does not provide** u_1 and c_j **does not provide** u_1 when… [H] (*gap*)
2) c_i **does not provide** u_1 and c_j **provides** u_1 when… [H] (*mismatch*)
3) c_i **provides** u_1 and c_j **provides** u_1 when… [H] (*overlap)*

This UCCA type is useful for identifying scenarios in which there may be gaps, mismatches, or undesirable overlaps in provided control actions [25]. For example, one controller may provide a control action in expectation that the other controller will *not* provide the same control action. If that partner system *does* provide the control action, there may be hazardous overlaps resulting in system losses. An example set of these UCCAs for *Transmit Beacon* are provided below.

Table 4-6: Abstraction 2 UCCAs Type 1-2

#	***Transmit Beacon* provided by**		**Context**
39	¬*Any one*	¬*Any of others*	When systems must locate one another to establish a connection for communications [H-1, H-2]
40	¬*Any one*	*Any of others*	When both systems must transmit a beacon to connect (i.e. systems must use a symmetric acquisition sequence) [H-1, H-2]
42	*Any one*	*Any of others*	When transmitting a beacon simultaneously interferes with ability to detect beacon (i.e. systems must use an asymmetric acquisition sequence) [H-1, H-2, H-3]

Finally, UCCAs 3-4 for Abstraction 2 address unsafe timing in a similar manner to Abstraction 1. However, Abstraction 2 is used to specify controllers starting/ending a control action before others start/end the same control action. The format is structured as follows:

1) c_i **starts to provide** u_1 before c_j **starts to provide** u_1 when… [H]
2) c_i **starts to provide** u_1 before c_j **ends providing** u_1 when… [H] (*handoff overlap*)
3) c_i **ends providing** u_1 before c_j **starts to provide** u_1 when… [H] (*handoff gap*)
4) c_i **ends providing** u_1 before c_j **ends providing** u_1 when… [H]

UCCAs 3-4 for Abstraction 2 are particularly useful for identifying issues in handoff overlaps or handoff gaps [25]. Examples of such handoff overlaps and gaps are present in the UCCAs described below.

Table 4-7: Abstraction 2 UCCAs Type 3-4

#	***Transmit Data*** **provided by**		**Context**
58	**S**{*Any one*}	**E**{*Any other*}	When full data set has not yet been transmitted and neither system is full-duplex [H-2, H-3]
59	**E**{*Any one*}	**S**{*Any other*}	When aircraft must relay data [H-2]
60	**E**{*Any one*}	**E**{*Any other*}	When systems are full-duplex and complete data set has not yet been transmitted [H-2]

This UCCA generation process is followed for each control action within both Abstraction 1 and Abstraction 2 control structures and for each UCCA type. The UCCAs are then used in Step 4 of STPA-Teaming to identify the factors that may cause unsafe control to occur.

4.4 Step 4: Identifying Causal Scenarios

The fourth step of STPA involves the identification of loss scenarios, which describe the causal factors that may lead to unsafe control and hazards [23]. The control structure is used to identify control factors that may lead to unsafe controller behavior or unsafe feedback. Such factors include physical failures, unsafe control algorithms, unsafe control input from other controllers, and flawed process models [23]. These causal factors are useful for recognizing why *internal control* of one system may be unsafe, and they help identify many factors that are often missed by other hazard analysis methods [24]. However, in a system with multiple controllers over a shared process, there may be scenarios in which all controllers have adequate internal control, but hazards still occur. In such systems, the *collaborative control* must also be analyzed.

STPA-Teaming extends Step 4 of STPA by creating a systematic approach to identify not only flawed internal control factors, but also flawed collaborative control factors. It maintains the same traditional approach for identifying causal factors related to individual unsafe controller behavior, but also provides collaborative control factors that may lead to UCCAs. By considering multiple controllers, it addresses the collaborative dynamics discussed in Chapter 2, many of which may be present in the coordination of an airborne laser communication system.

When generating causal scenarios, it is useful to return to the control structure and analyze how unsafe control inputs, unsafe feedback, or unsafe lateral communication may lead to flawed process models and control algorithms. While the abstracted control structures in Section 4.2

were helpful for generating UCCAs, a more refined control structure could be more useful for identifying scenarios that lead to UCCAs.

The refined control structure shown below in Figure 4.4 depicts in more detail the interactions that inform controllers' process models and the communication channels that allow controllers to share information. For example, subsystems such as the communication and navigation system and the flight control systems may inform the lasercom system of aircraft state information such as location, altitude, airspeed, and heading. The RF communication system will additionally be the primary means of communication to share information with partner aircraft and the AOC.

The control structure below additionally refines the lasercom system controller. In doing so, it depicts the system automation that is responsible for accepting operator inputs and controlling the optics and modem to broadcast the optical signal. It is additionally responsible for providing feedback to system operators on the status of the optics and modem and optical signal. Such interactions must be considered when identifying scenarios related to both internal control and collaborative control.

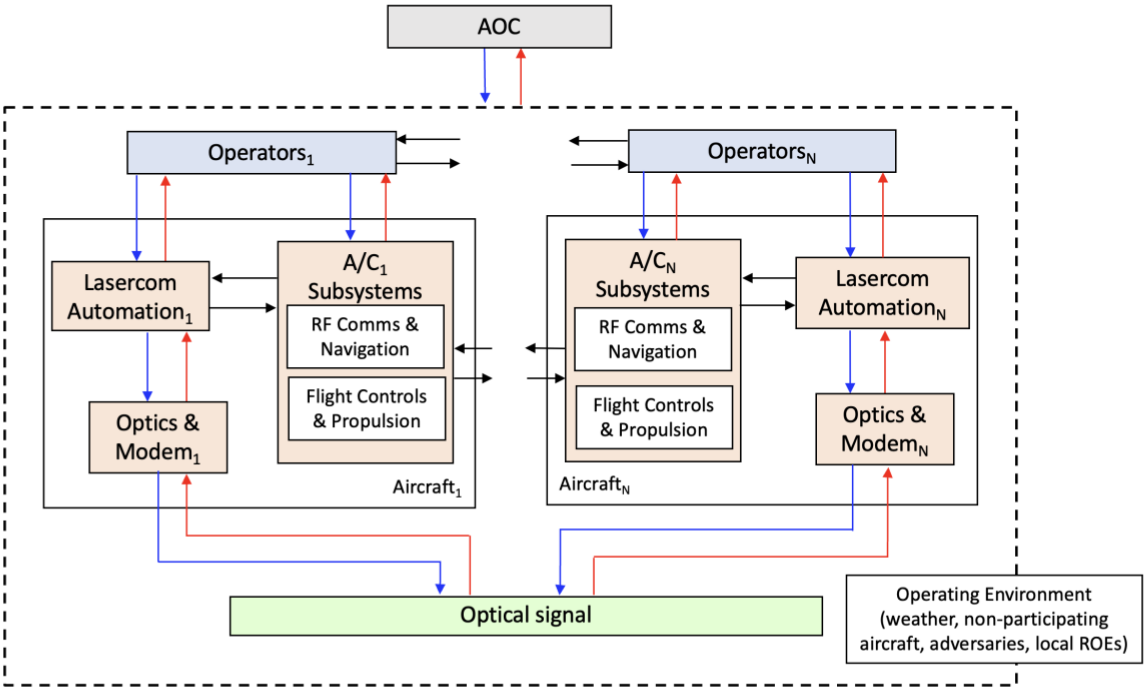


Figure 4-4: Refined Collaborative Control Structure

This control structure is first used to identify *top-level scenarios* that may lead to UCCAs [11]. These top-level scenarios are then refined to identify collaborative control factors and internal control factors contributing to unsafe control. STPA-Teaming provides additional guidance for this refinement process by directing the analyst to identify factors leading to flawed coordination such as unsafe communication, inconsistent control algorithms, or inconsistent decision-making. An overview of this refinement process is shown below in Figure 4-5.

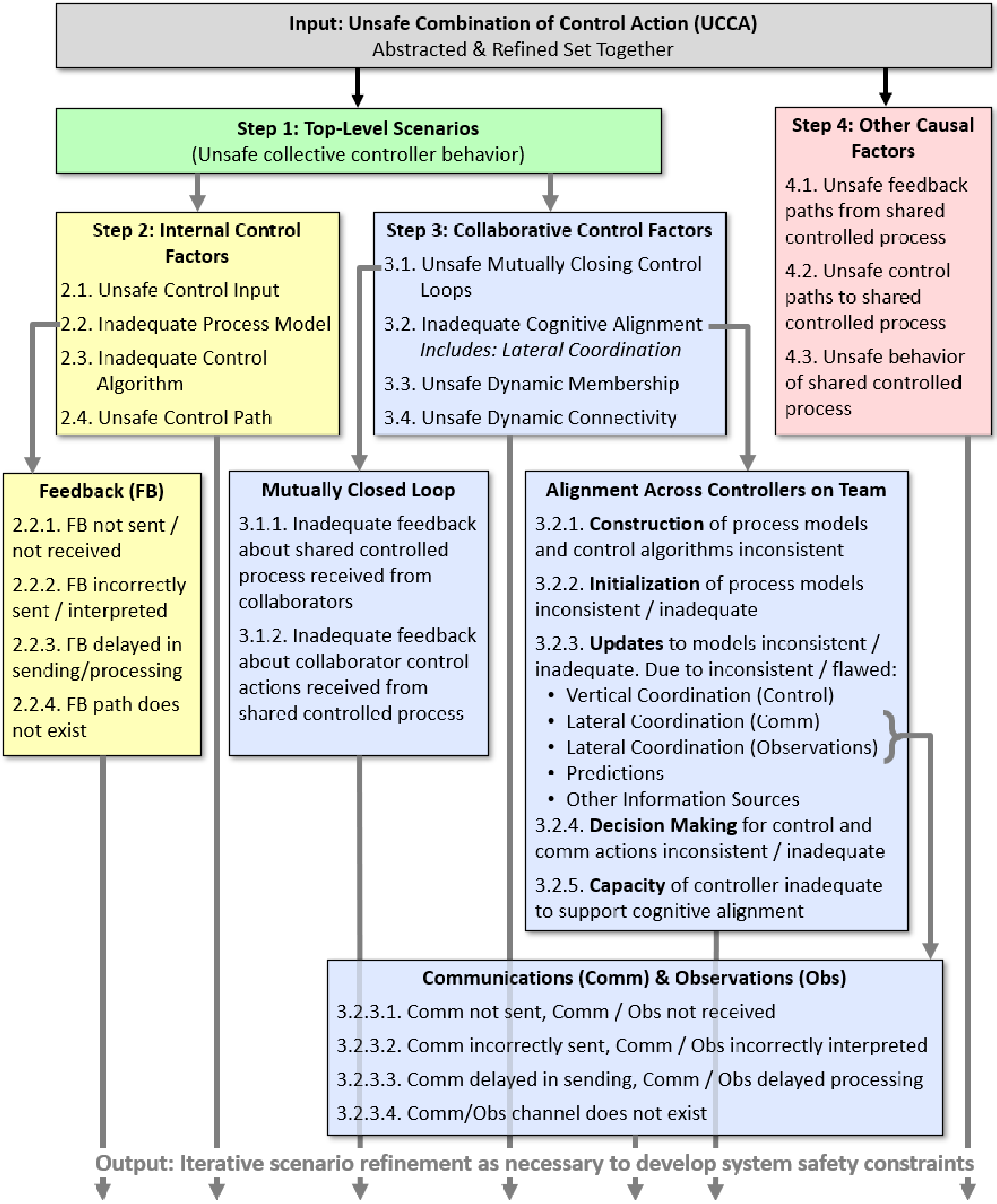

Input: Unsafe Combination of Control Action (UCCA)
Abstracted & Refined Set Together
Step 1: Top-Level Scenarios
(Unsafe collective controller behavior)
Step 4: Other Causal Factors
4.1. Unsafe feedback paths from shared controlled process
4.2. Unsafe control paths to shared controlled process
4.3. Unsafe behavior of shared controlled process
Step 2: Internal Control Factors
2.1. Unsafe Control Input
2.2. Inadequate Process Model
2.3. Inadequate Control Algorithm
2.4. Unsafe Control Path
Step 3: Collaborative Control Factors
3.1. Unsafe Mutually Closing Control Loops
3.2. Inadequate Cognitive Alignment
Includes: Lateral Coordination
3.3. Unsafe Dynamic Membership
3.4. Unsafe Dynamic Connectivity
Feedback (FB)
2.2.1. FB not sent / not received
2.2.2. FB incorrectly sent / interpreted
2.2.3. FB delayed in sending/processing
2.2.4. FB path does not exist
Mutually Closed Loop
3.1.1. Inadequate feedback about shared controlled process received from collaborators
3.1.2. Inadequate feedback about collaborator control actions received from shared controlled process
Alignment Across Controllers on Team
3.2.1. Construction of process models and control algorithms inconsistent
3.2.2. Initialization of process models inconsistent / inadequate
3.2.3. Updates to models inconsistent / inadequate. Due to inconsistent / flawed:
Vertical Coordination (Control)
Lateral Coordination (Comm)
Lateral Coordination (Observations)
Predictions
Other Information Sources
3.2.4. Decision Making for control and comm actions inconsistent / inadequate
3.2.5. Capacity of controller inadequate to support cognitive alignment
Communications (Comm) & Observations (Obs)
3.2.3.1. Comm not sent, Comm / Obs not received
3.2.3.2. Comm incorrectly sent, Comm / Obs incorrectly interpreted
3.2.3.3. Comm delayed in sending, Comm / Obs delayed processing
3.2.3.4. Comm/Obs channel does not exist
Output: Iterative scenario refinement as necessary to develop system safety constraints

Figure 4-5: Template for Refinement of Causal Scenarios [25]; reproduced with permission of author

4.4.1 Top-Level Scenarios

STPA-Teaming defines 5 top-level scenarios for Type 1-2 UCCAs [25]:

1) **Tasks provided (safe) but not executed properly (unsafe):** A controller directs other controllers on the team adequately, but some of those controllers do not execute directions properly, which leads to unsafe collective control.
2) **Tasks not provided (unsafe):** A controller does not direct other controllers on the team as necessary for the team to execute safe collective control of the shared process.
3) **Tasks provided (unsafe):** A controller directs other controllers on the team in a way that leads to unsafe collective control.
4) **Tasks not provided (safe) but executed anyways (unsafe):** A controller adequately does not direct other controllers on the team to provide certain commands, but some of those controllers provide them anyways, which leads to unsafe collective control.
5) **Tasker control actions unsafe with tasks it provides (unsafe**): A controller provides control actions to the shared process that are unsafe in combination with how it directs other controllers on the team.

In a full analysis, these top-level scenarios would be applied to each UCCA Type 1-2. An example set of top-level scenarios for UCCA 4 is provided below:

> **UCCA-4:** System$_1$ provides *Transmit Beacon*, but System$_2$ does not provide *Detect Beacon* when systems must establish a connection for communications. [H-1, H-2]

Top-Level Scenarios for UCCA Types 1-2
S-1: Operators **provide adequate task(s)** to establish a connection, but lasercom systems **do not execute task(s) as directed**. (Context points to systems transmitting/detecting in unintended ways which may be explored in refinement)
S-2: Operators **do not provide some of the tasks** required for lasercom systems to establish a connection. (Context points to scenarios in which operators do not provide some of the required inputs to transmit/detect beacon)
S-3: Operators **provide some of the tasks** to establish a connection **in a way that leads to unsafe collective control**. (Context points to when operators input wrong technical parameters for acquisitions or communications)
S-4: Operators **adequately do not provide certain task(s)**, but some systems **execute them anyways**. (Context points to system not transmitting/detecting properly due to an uncommanded function such an indirect mode transition)
S-5: Operators' **control actions** when establishing a connection **are unsafe in combination with otherwise adequate tasks provided**. (Context points to when operators input flight controls that prevent systems from adequately transmitting/detecting beacon)

In addition to these five top-level scenarios for UCCA Types 1-2, STPA-Teaming defines a separate set of top-level scenarios to address unsafe *timing* of control actions (UCCA Types 3-4):

1) **Tasks as provided lead to unsafe sequencing (unsafe):** A controller directs other controllers on the team in a way that leads to unsafe temporal sequencing.

2) **Tasks provided (safe) but executed in unsafe sequencing (unsafe):** A controller safely directs other controllers on the team, but the way in which those controllers execute the directions leads to unsafe temporal sequencing.
3) **Tasker control actions and tasks provided are unsafe in sequencing (unsafe**): A controller on the team provides control actions to the shared process that are unsafe in temporal sequencing with how it directs other controllers on the team.

Examples of top-level scenarios for UCCA-35 are provided below:

> **UCCA-35:** System$_1$ ends *Transmit Data* before System$_2$ ends *Receive Data* when entire data set has not yet been transmitted and/or received. [H-1, H-2]

Top-Level Scenarios for UCCA Types 3-4
S-6: Operators **provide some of the tasks** to share data **in a way that leads to unsafe sequencing**. (Context points to instances when operators provide tasks to end transmit data before entire data set is received by partner)
S-7: Operators **provide adequate task(s)** to share data, but lasercom systems **execute them in a way that leads to unsafe sequencing**. (Context points to when operators do not command system to end transmit data, but system automation ends transmit data too early)
S-8: Operators' **control actions** and **tasks provided are unsafe in sequencing.** (Context points to scenarios when Operators input aircraft flight controls that disrupt communications)

These scenarios address how UCCAs may occur at a high level. However, they must be refined to reveal the flawed internal control and collaborative control factors that contribute to unsafe behavior. The following section details how these top-level scenarios are refined to generate more specific scenarios.

4.4.2 Refined Scenarios

Refined Scenarios Related to Collaborative Control
STPA-Teaming uses the nine collaborative control dynamics described in Chapter 2 in the refinement of top-level scenarios. In doing so, it identifies scenarios related to unsafe cognitive alignment, lateral coordination, mutually closing control loops, shared authority, transfer of authority, dynamic authority, dynamic hierarchy, dynamic membership, and dynamic connectivity [26]. The following section explores how these scenarios may occur in the airborne lasercom system.

An example is provided below to illustrate the refinement of top-level scenarios using collaborative control factors. The example follows from the top-level scenarios generated for UCCA-4:

UCCA-4: System$_1$ provides *Transmit Beacon*, but System$_2$ does not provide *Detect Beacon* when systems must establish a connection for communications. [H-1, H-2]

Top-level Scenario: **S-1:** Operators provide adequate task(s) for Lasercom Systems to establish a connection, but Lasercom Systems do not execute task(s) as directed.

Refined Scenarios Related to Unsafe Mutually Closing Control Loops

- **S-1.1:** *Unsafe feedback about shared control process is received from collaborators*: Aircraft$_1$ flies through atmosphere with dense cloud coverage when receiving data. As a result, the power of the signal received drops below the min RSSI (Received Signal Strength Indicator) for X amount of time required for fine-tracking. Thus, System$_1$ regresses to open-loop coarse tracking and starts Transmit Beacon to reconnect. System$_1$ does not communicate with System$_2$ that the power of the optical signal received was too low and as a result, System$_2$ does not regress to Detect Beacon as required for re-connection.
- **S-1.2:** *Unsafe feedback about collaborator control actions is received from shared control process*: Lasercom System$_1$ does not notify Lasercom System$_2$ that it is still providing Transmit Beacon: After X amount of time (ex. 60 seconds) of Transmitting Beacon, System$_1$ does not successfully illuminate System$_2$ for beacon detection. As a result of the expired time, System$_2$ automatically stops Detect Beacon. System$_1$ reinitiates Transmit Beacon after expired time but does not communicate to System$_1$ that it has done so. As a result, System$_2$ does not re-initiate Detect Beacon when systems must connect.

Refined Scenarios Related to Inadequate Cognitive Alignment

- **S-1.3:** *Construction of process models/control algorithms unsafe:* It is assumed that all systems operate with the same power and transmission capabilities. However, due to system upgrades, Lasercom System$_1$ has greater power capabilities and thus an extended range. Because Lasercom System$_2$ has a different model of acceptable ranges, it does not believe that Lasercom System$_1$ is within range for connection and does not provide Detect Beacon as commanded.
- **S-1.4:** *Initialization of process models/control algorithms unsafe:* Modulation is used as an additional means of security for acquisition, however, due to unsafe planning (ex. ATO publications), systems are not configured with compatible modulation formats to connect.
- **S-1.5:** *Updates to process models unsafe: C*ontrollers on team receive unsafe updates regarding shared process: Refinement shown below.
    - **S-1.5.1:** *Flawed vertical coordination (control)*: AOC is delayed in providing partner identification or provides wrong identifier for partner terminal. So System$_2$ does not have required information to point its tracking sensor in the correct direction and does not Detect Beacon.
    - **S-1.5.2:** *Flawed lateral coordination (communication)*: Feedback from System$_2$'s GPS, airspeed indicator, attitude indicator, or INS is delayed/inaccurate when sent to System$_1$. So, System$_1$ provides Transmit Beacon in the wrong direction and System$_2$ does not Detect Beacon.
    - **S-1.5.3:** *Inconsistent predictions/decision making:* Aircraft$_2$ banks unexpectantly and Lasercom System$_1$ makes inaccurate predictions regarding Aircraft$_2$'s flightpath. As a result, Lasercom System$_1$ points in the wrong direction while Transmitting Beacon and Lasercom System$_2$ does not Detect Beacon.
    - **S-1.5.4**: *Unsafe observations:* System$_2$ observes that System$_1$ is currently connected with another aircraft (through TDL communications or feedback provided by AOC). System$_2$ thus believes that System$_1$ is unavailable for connection. Aircraft$_1$, however, is equipped with two lasercom terminals and is

capable of simultaneously connecting with two aircraft. Because System$_2$ is unaware of this capability, it does not provide Detect Beacon.

Refined Scenarios Related to Dynamic Membership and Dynamic Connectivity

- **S-1.6:** *Unsafe dynamic membership:* Plans change due to mission needs/weather phenomena, requiring Aircraft$_3$, originally planned for connection, to divert. So, Aircraft$_2$ is sent by AOC as a replacement to establish a connection with Aircraft$_1$. Aircraft$_2$ is not capable of transmitting at a compatible optical frequency for communication with Aircraft$_1$. As a result, it does not Detect Beacon as commanded.
- **S-1.7:** *Dynamic connectivity:* Systems are designed such that their status and availability for acquisition is communicated through an RF link. Systems are unable to communicate due to enemy jamming, interfering terrain, inoperable frequencies, etc.. Therefore System$_2$ is unaware that System$_1$ is prepared to connect and has initiated Transmit Beacon command.
- *See more in Appendix B*

Top-level Scenario: **S-2**: Operators do not provide some of the tasks required for lasercom systems to establish a connection.

Refined Scenarios Related to Unsafe Cognitive Alignment

- **S-2.2:** *Initialization of process models/control algorithms unsafe:* Pre-flight documents such as ACO and ATO do not specify roles in acquisition process for both systems. Operators cannot communicate to establish/verify role in acquisition process so it is unclear which systems will transmit/detect the beacon using an asymmetric acquisition sequence. As a result, both Operators provide the task to Transmit Beacon, and neither provide the task to Detect Beacon.
- **S-2.3:** *Updates to process models unsafe: C*ontrollers on team receive unsafe updates regarding shared process: Refinement shown below.
    - **S-2.3.1:** *Flawed vertical coordination (control)*: Due to incompatible tactical data links, systems cannot share aircraft state information or terminal status updates directly, but must obtain such information through the AOC. The AOC is delayed in sharing System$_1$'s state information and operational mode with System$_2$ so Operators$_2$ are not aware that System$_1$ is positioned appropriately and prepared to connect.
    - **S-2.3.2:** *Flawed lateral coordination (communication)*: System$_2$ experiences a system malfunction that prevents it from Detecting Beacon as originally planned. System$_2$ does not adequately communicate with System$_1$ that it has malfunctioned. So Operators$_1$ continue attempts at acquisitions, while Operators$_2$ do not provide tasks to Detect Beacon.
    - **S-2.3.6:** *Inconsistent predictions/decision making:* Both Systems receive consistent updates regarding weather, but Operators have mismatched understandings of acceptable atmospheric conditions for connection. Due to inconsistent training or guidelines, Operators$_1$ predict that connections will be sustainable in current weather conditions, but Operators$_2$ predict that connections will not be sustainable. As a result of inconsistent decision-making and lack of communication, they decide to not Detect Beacon.
- **S-2.4**: *Capacity:* Due to high task-saturation, Operators$_2$ forget to check in with AOC to receive commands or status updates regarding lasercom connection. As a result,

Operators$_2$ do not receive "WORDs" information including necessary connection parameters with System$_1$. Thus, they do not provide tasks to Detect Beacon.

Refined Scenarios Related to Dynamic Membership and Dynamic Connectivity

- **S-2.5:** *Unsafe dynamic membership:* Aircraft$_1$ enters a new area of operations, requiring a different Identification Friend or Foe (IFF) mode. Operators$_1$ are delayed in changing IFF mode or change to the wrong mode. As a result, Operators$_2$ believe System$_1$ is not authorized to connect and do not provide tasks to Detect Beacon.
- *See more in Appendix B*

Refined Scenarios Related to Internal Control

While STPA-Teaming specifically highlights scenarios related to unsafe collaborative control, it also retains the ability to identify scenarios related to internal control, scenarios that are typically identified in a traditional STPA. The following scenarios demonstrate how unsafe control may occur due to unsafe internal control, using UCCA 38 as an example:

UCCA-38: System$_1$ ends *Receive Data* before System$_2$ ends *Transmit Data* when entire data set has not been transmitted and/or received [H-1, H-2]

Top-level Scenario: **S-14:** Operators provide some of the tasks for the systems to share data in a way that leads to unsafe sequencing.

- **S-14.4:** *Unsafe Control Path (human-human)*: The AOC provides new transmission parameters to both Operators$_1$ and Operators$_2$, but Operators$_2$ do not receive new parameters because the communication channel operation is unsafe (due to fading, jamming from hostile forces, misconfigured TDLs, etc.). As a result, Operators$_2$ do not configure system to receive at frequency transmitted by System$_1$. Because data cannot be appropriately received, System$_1$ ends Receive Data before entire data set is transmitted.

Top-Level Scenario: **S-15**: Operators provide adequate task(s) to share data, but lasercom systems execute them in a way that leads to unsafe sequencing.

- **S-15.6**: *Unsafe control algorithm (machine):* Throughout flight, the alignment between the tracking sensor and transmitter drifts, so feedback of incoming light is misinterpreted. Nutation is used to correct boresight alignment, but the control algorithm for nutation is not configured to adequately correct for the drift. So, the system continues to misinterpret feedback from the tracking sensor, and Transmits Data in the wrong direction. As a result of the lost signal, System$_1$ ends Receive Data.
- **S-15.7:** *Unsafe process model (machine):* Lasercom System$_2$ does not Transmit Data with the correct power because it does not know its host aircraft's altitude. Aircraft$_1$ descends after establishing a link, but feedback from the host aircraft altimeter is delayed or unsafe. As a result of inadequate power, System$_1$ ends Receive Data.

Top-Level Scenario: **S-16**: Operators' control actions when sharing data and tasks provided are unsafe in sequencing.

- **S-16.5:** *Unsafe control input (human-machine):* Operators input flight controls that disrupt their own system's ability to track. Operators bank Aircraft$_1$ such that the wing blocks the line of sight (LOS) between the two terminals. No feedback is provided to operators alerting them to signal disruptions due to aircraft attitude. As a result, operators continue to fly such that LOS is broken and systems are not able to continue partner tracking.

- *See more in Appendix B*

This section provided a few of the scenarios that were generated considering both collaborative control factors and internal control factors. These scenarios can be used to derive safety-constraints and recommendations for system design, which will be especially useful for the system while it is in its early concept phase of design.

4.5 System Recommendations

Following the four steps of STPA-Teaming, analysts are able to provide recommendations to mitigate identified causal scenarios. This section contains the most important takeaways from the generated recommendations. A full list of recommendations can be found in Appendix C.

4.5.1 Recommendations for Collaborative Control Factors

Cognitive Alignment

A recurring theme for the scenarios was the presence of unsafe cognitive alignment regarding plans and protocols for connection (or loss of connection). Systems' control algorithms and process models must be constructed, initialized, and updated consistently to maintain cognitive alignment. Additionally, operators should have consistent processes for decision-making and managing dynamic connectivity/membership of partner systems. This section provides actionable recommendations to maintain cognitive alignment.

RM-1: *Construction of process models/control algorithms (machines)*: System automation for all systems must be configured with consistent control algorithms regarding PAT and transmissions. Many scenarios emerged from the fact that systems may have mismatched control algorithms regarding how to establish and maintain tracking or share data once a connection is established. As such, it is critical that all control systems be constructed with consistent control algorithms regarding the execution of control actions, as well as the sequencing and timing of control actions for processes such as acquisitions, transmissions, regression, and transitioning from/to other TDLs [RM-1.1]. For example, during acquisitions, systems must use consistent acquisition sequences and scan patterns. Additionally, systems should be designed and updated with consistent thresholds for ending/starting control actions. Examples of such parameters that should be consistent across controllers include "time-to-acquire[2]" or minimum RSSI (Received Signal Strength Indicator)[3] such that systems transition at the same time.

It is also recommended that lasercom systems have consistent control algorithms regarding aircraft motion [RM-1.3]. In addition to relying on autopilot information provided by partner systems, systems will use internal control algorithms to process partner state information and predict where partner platforms will be next. Kalman filters, for example, may be used to predict

[2] The time allotted to continue searching for the partner system before ending Transmit/Detect Beacon

[3] The received power determining whether systems regress from active communications to acquisitions

the trajectory of partner platforms based on position data already collected, some uncertainty in position, velocity, and acceleration, and a kinematic model of how the platform is expected to move (motion constraints). When relying on such kinematic models, it is imperative that control algorithms be consistent across systems such that lasercom control systems have consistent expectations of how their own platform will maneuver, as well as how partner aircraft will maneuver.

RM-2: ***Construction of mental models/control algorithms (humans)*****: Operators must be provided consistent training and unambiguous standard operating procedures.** It is also critical that the process models and control algorithms for operators be constructed consistently. This is accomplished through training and unambiguous standard operating procedures. Operators must be properly trained on how to operate their own individual systems [RM-2.1], as well as how to communicate and coordinate responsibilities with partner systems and the AOC. Operators must have consistent models of the responsibilities associated with various roles in the connection process (ex. flying straight and level when receiving data, executing system calibrations before Transmitting Beacon, etc.) [RM-2.3]. It is also critical that operators have congruent understandings of how to transition through warm-up modes, acquisition sequences, transmissions, and regression so that they execute dependent control actions at the correct time [RM-2.4].

Training and guidelines should also specify communication protocols such that operators have consistent understanding of how to interact with partner aircraft and the AOC. This recommendation is discussed in more detail in the vertical and lateral coordination recommendation.

RM-3: ***Initialization of process models/control algorithms (machines)*****: Systems must be consistently initialized when establishing and maintaining a connection.** To effectively establish a laser communication link, it is critical that systems are initialized with consistent parameters for connection. This includes both RF parameters used to coordinate connections (i.e. frequencies and/or IFF modes for authorization) [RM-3.1] as well as technical parameters for the lasercom link (i.e. optical wavelengths, acquisition sequences, modulation, data rates, etc.) [RM-3.2].

Systems must also be synchronized regarding timing and sequencing of control actions [RM-3.3]. For example, during acquisitions, systems must initiate "time-to-acquire" at the same time such that they have alignment regarding when they should stop attempting a connection and transition fully to tactical data links. During transmissions, it is critical that systems initiate their clocks at the same time such that they are synchronized for modulation. Furthermore, if systems regress, they must stop their clocks and reset their clocks at the same time to maintain synchronization upon reconnecting.

RM-4: ***Initialization of mental models/control algorithms (humans)*****: AOC must provide unambiguous, consistent plans for connection to all systems involved.** In order for systems to be consistently initialized, operators must have cognitive alignment regarding required technical parameters, timing, and locations of connections. As such, their mental models and control algorithms must be consistently initialized through plans provided by the AOC. The AOC should provide unambiguous, consistent specifications of the technical parameters required for acquisitions and communications (i.e. frequencies, data rates, modulation, etc.) [RM-4.1, RM-4.6]. Along with parameters, plans should outline what data is to be transmitted [RM-4.3], the timing and location of connections [RM-4.4], and the unique identifiers of connection partners [RM-4.5]. Furthermore, they should specify the responsibilities assigned to each system in the connection process (i.e. Transmit Beacon, Detect Beacon, etc.) [RM-4.2]. Such information could be provided in the Operational Tasking Data Link (OPTASKLINK) and/or other pre-flight documents [34].

Along with baseline plans for operations, the AOC should provide contingency plans for failures to connect as well as loss of connection for lasercom links [RM-4.7]. Contingency plans may include transmitting at different frequencies, transmitting at different altitudes or different times, or communicating through different methods (i.e. other TDLs). Contingency plans should specify how long operators continue attempting to connect before changing plans. They should also specify reporting requirements for failure to connect (to be discussed in further detail in RM-5 and RM-6). It is critical that such plans are consistently provided to ensure operators have cognitive alignment regarding how to coordinate in response to connection failures.

RM-5: ***Updates (Vertical Coordination)*****: The AOC and/or team leadership must be able to provide updates to operators in a consistent, unambiguous, and timely manner.** The operational environment for systems will be extremely dynamic and unpredictable as weather, mission objectives, or aircraft states may quickly change. As such, the AOC must be able to communicate with aircraft and share operational updates in a timely manner. Systems must have sufficient bandwidth in their RF communication links with the AOC to support such updates [RM-5.1].

Training and guidelines should specify how operators communicate and coordinate with the AOC when attempting to establish connections. Communication protocols and plans should specify timing of communication with the AOC and should specify what information operators send and receive from the AOC (such information could be provided through WORDs in the SPINS or other pre-mission documents). This would allow operators to have consistent expectations for how the AOC will provide guidance (i.e. providing aircraft waypoint guidance, connection scheduling, partners for connection, connection parameters, etc.) [RM-2.2].

The AOC should consistently update Operators regarding the operational environment, providing information such as the status of partner aircraft and atmospheric conditions [RM-5.2]. Similarly, systems should send feedback regarding status of operations and health of systems to properly update the AOC’s process model of the operational environment [RM-5.3]. Systems should provide mission updates, status of systems (aircraft position, connection status, terminal health, etc.), and any relevant updates regarding environmental conditions (if they are degrading to laser communication).

If systems are incapable of providing any of their assigned control actions that are necessary to establish a connection, systems must report issues to the AOC. Such reasons may include system malfunctions, incorrect directions provided by the AOC, degrading atmospheric effects such as dense cloud coverage or turbulence, or other unexpected changes in the mission. If possible, operators should provide the reasoning for failures to connect such that the AOC can assist in providing solutions and/or alert other operators to unsafe conditions. Such reported issues from operators would allow the AOC to provide additional guidance for continuing operations or for transitioning to alternative means of communication.

RM-6: ***Updates*** **(*Lateral Coordination)*: Connecting systems must be able to coordinate connections and share state information directly in near real-time.** In order to establish and maintain accurate tracking, systems must provide real-time situational updates to partner systems, sharing relevant aircraft state and system status information. Having the AOC monitor aircraft and provide such information to connecting systems is an option, however, as seen in many of the generated scenarios, such a system architecture may lead to delays and inadequacy in shared information.

It is thus critical that systems are capable of communicating directly (through means other than lasercom): Systems should be configured with compatible data links formats [RM-6.1]. Additionally, the RF data links used to support lasercom coordination should have sufficient bandwidth to support lasercom coordination [RM-6.2]. Systems must be able to accurately interpret partner messages. Thus, both human operators and system automation must have semantic alignment regarding exchange of lasercom information and situational updates [RM-6.3, RM-6.4]. Such alignment could be established through standardized message formats and communication protocols.

Standardized communication protocols should specify what information systems share when connecting: Since systems are limited in how many connections they can establish, they should provide updates regarding terminal status and availability for connections [RM-6.5]. Systems should also provide aircraft state information necessary for accurate pointing (i.e. GPS position, aircraft heading, airspeed, terminal attitude, aircraft geometry, etc.) [RM-6.7, RM-6.8].

Communication and coordination protocols should also standardize how systems coordinate sequencing and timing of control actions [RM-6.10]. The recommendations for Mutually Closing Control Loops discusses in more detail how systems should provide updates regarding intentions or initiated/ended control actions.

Finally, if systems are unable to provide any of their expected control actions, communication protocols should standardize how systems report issues to partners [RM-6.12]. If possible, they should provide reasoning for failure to execute control actions (i.e. dysfunctional subsystems, platform jitter, atmospheric effects, etc.). If the system continues to be unable to provide its assigned control actions, systems should coordinate to either transfer responsibilities or alter the mission profile, prioritizing mission objectives appropriately.

RM-7: ***Updates (Predictions)*****: Connecting systems must be able to accurately predict partner aircraft location and motion.** Lasercom connections between military aircraft in an operational environment will be extremely challenging due to the fact that aircraft constantly change location and will also frequently change airspeed and attitude. This challenge is coupled by the fact that connections must be established between *two* moving terminals. Accordingly, connecting systems must be able to predict the future state of partner aircraft.

Estimates of partner systems' relative velocity projection could be provided through Kalman filters as well as algorithms relying on the Doppler Shift of received optical signals once connections are established [RM-7.1]. However, systems should also assist partners in predictions by providing information regarding *future* states of the aircraft in addition to *current* location, attitude, and airspeed [RM-7.2]. One such method of sharing future state information could be transmitting programmed autopilot coordinates. This would allow systems to better predict changes in partner aircraft motion and help reduce pointing errors due to unexpected turns or changes in airspeed.

Additionally, standard operating procedures should establish limits for aircraft angular accelerations (i.e. bank rate and pitch rate) [RM-7.3]. This recommendation would ensure that aircraft do not maneuver in ways that disrupt the internal system's tracking or the partner system's ability to predict aircraft trajectory to maintain tracking. Such limits would also ensure that operators have consistent control algorithms for aircraft control and systems have consistent expectations of aircraft motion when relying on pointing control algorithms such as Kalman filters.

RM-8: *Decision-making*: Collective decision-making of controllers must provide adequate, real-time solutions for connection issues. In some scenarios, the AOC may not be able to provide guidance when systems are unable to establish and maintain a connection. In such scenarios, systems must be able to coordinate decisions amongst themselves regarding how to continue operations. Ideally, plans and protocols established before the mission would provide contingency plans for failed connections (i.e. connect at different altitudes, transmit at different wavelengths, share data through other TDLs). Regardless of established plans, however, systems must be able to coordinate to make decisions together, providing solutions that prioritize the same mission objectives. This requires first that systems consistently decide connectivity is unachievable/unsustainable (given specific environmental factors, aircraft state, or relation between aircraft) [RM-8.1]. It also requires that systems have consistent, accurate models of the mission objectives and ROEs when deciding solutions [RM-8.2].

If systems collectively decide that a connection cannot be established and maintained, they must be able to coordinate and decide whether to postpone the connection [RM-8.3], whether to change location of connection [RM-8.4], or whether to rely on other TDLs for communication [RM-8.5]. Again, such decisions should align with the established mission objectives and ROEs.

Mutually Closing Control Loops

In many cases, partner systems may not have feedback to determine how effective their provided control actions were (i.e. effectively transmitting data, illuminating partner terminals with beacon beams, etc.). In other cases, they may not be aware of what control actions partner systems commanded. In these scenarios, it is critical that partner systems "close-the-loop" and provide feedback that systems would not otherwise have. This section addresses recommendations for mutually closing control loops.

RM-9: *Closing-the-Loop Regarding Control Actions*: Systems must communicate information regarding commanded control action(s) that partner systems would not

otherwise have access to. Partner systems must be able to adequately receive and interpret shared feedback. In many lasercom subprocesses, systems are not able to detect whether their partner is providing (or not providing) a specific control action unless the partner system "closes-the-loop" and informs them. These processes require systems to appropriately update partners when they initiate or end certain control actions.

One such sub-process is acquisitions: To prevent systems from aimlessly searching for beacons when no beacon is being transmitted (or vice-versa), systems should confirm (through established data links) when they start transmitting a beacon or start searching for a beacon [RM-9.1]. Additionally, they should notify partners if they stop transmitting/detecting a beacon due to expired "time-to-acquire" or due to other reasons. If a system stops transmitting/detecting a beacon before transitioning to fine partner tracking as expected, it must inform its partner of its intentions for future attempts at acquisitions (i.e. attempt acquisitions again, attempt connection at different location, etc.).

Another critical subprocess requiring control action updates is regression. As discussed in RM-1, systems should have consistent control algorithms regarding regression should loss of connection occur. These control algorithms would include requirements such as power required to maintain tracking and "time-to-regress" given lack of received power for a specified amount of time. While these consistencies are useful for ensuring systems regress at the same time, systems should also "close-the-loop" regarding regression: If a system stops tracking its partner, stops transmitting/receiving data, and transitions to acquisitions to re-acquire the partner signal, it must notify its partner system and provide any relevant information regarding the state of the regressed terminal [RM-9.2]. The partner system, in return, should confirm that it has received notification of regression and should verify that it is transmitting or detecting a beacon to re-acquire.

In these communications, it is critical that systems not misinterpret partner feedback as a need to provide a control action that is *not* necessary or *not* provide a control action that *is* necessary [RM-9.3]. Again, message formats should be standardized and operators should have semantic alignment such that systems appropriately interpret the feedback regarding control actions.

RM-10: *Closing-the-loop Regarding Controlled Process*: Systems must communicate information regarding the optical signal that partner systems would not otherwise have access to. Partner systems must be able to adequately receive and interpret shared feedback. Atmospheric fading of the optical signal is a major challenge for airborne lasercom: atmospheric conditions may cause the power of the transmitted signal to drop, reducing the Signal-to-noise Ratio (SNR) so low that sensors cannot process what bits were sent. It is thus recommended that systems "close-the-loop" regarding the optical signal received. To do so, systems must first be able to detect if data has been lost or distorted during transmission. Such recognition and feedback could be achieved by encoding redundant bits in the data (i.e. using forward error correction (FEC)[4] and interleaving[5]). Processes such as Automatic Repeat Requests (ARQs) may then be used to provide commands to retransmit data[6]. It is additionally recommended that when ARQ is used, terminals receiving inform the terminals transmitting *which* frames had errors such that transmitters know which frames to retransmit (this style of ARQ was implemented on Lincoln Lab's TBIRD and significantly increased efficiency of transmissions) [37].

If received data continues to have errors, systems should provide feedback to partners and AOC regarding unsafe communications. Systems should coordinate either vertically through the AOC or laterally with partners regarding continued operations, whether that be continued attempts at transmitting/receiving, communicating through other tactical data links, or postponing connections. Again, coordination of future plans should be clear, unambiguous, and confirmed by all controllers involved.

Dynamic Membership & Dynamic Connectivity

In many cases, aircraft will enter or exit areas of operations, requiring connections to be established. The membership of systems in the network may be highly dynamic. Additionally, in the uncertain environment of military operations, the availability and connectivity of communication links may be subject to degradation. This section addresses recommendations for dynamic membership and dynamic connectivity.

RM-11: *Dynamic Membership & Connectivity*: Systems must be able to detect, identify, and track other systems that are available and capable of establishing a lasercom connection. Because the membership of aircraft in the local network will be highly dynamic, controllers must be able to recognize all local systems with which they can establish a connection. Using identifiers, systems must be able to determine if a system is the intended partner so that they do not point their beam in the wrong direction [RM-11.1]. Additionally, systems must be able to determine a system's status and availability before attempting to connect [RM-11.2]. It is thus

[4] FEC creates redundancy in the shared data by allowing terminals to send extra information in addition to the message bits. Redundant symbols, or codewords, are added to the package to make communications more resilient against noise [35]. When codewords reach the partner receiver, the extra symbols allow the receiver to identify how many errors are present in the received codeword. Once the system is aware of the errors in the code, it can correct some number of those errors. The feedback provided by FEC could thus be extremely powerful and lead to several extra dB of link margin.

[5] Because the environment does not behave like ordinary white Gaussian noise (GWN) in which the power spectrum is constant over all frequencies [36], some fade durations are much longer than a typical FEC codeword. To ensure necessary feedback such as FEC codewords is received, systems should use interleaving: Interleaving involves separating the symbols in the codewords by some given amount of time to spread the codeword out over a time period lasting longer than the fade [2]. Thus, one symbol getting lost does not impact the other symbols, and the entire codeword will not get lost in the fade. Once all the symbols reach the receiver, they can all be assembled back together and FEC can be used to correct for any errors. In this way, interleaving provides an additional layer of redundancy to ensure adequate feedback is received.

[6] ARQ is an interactive correction technique that relies on feedback from the decoder to determine whether there are errors present in the received packets (as determined through cording such as FEC). If an error is detected, the terminal receiving uses ARQ over a communication link to command the terminal transmitting to retransmit data [35].

recommended that systems provide updates regarding status and availability for connection. Systems must also be able to determine if a system is capable of transmitting and receiving at compatible parameters (wavelengths, modulations, data rates, etc.) as some systems may have different capabilities [RM-11.3].

Moreover, systems must be able to determine if another system is positioned appropriately for connection: Systems must be able to determine if a local system is within line of sight [RM-11.5] and within range to connect [RM-11.4]. It is recommended that systems be able to determine a partner system's range either through shared state information or through direct detection using sensors such as radar or LADAR (Laser Detection and Ranging). Systems must appropriately assess whether partner aircraft's range is suitable for connection. Guidelines and control algorithms should thus specify maximum ranges for connection.

If systems cannot identify and track systems directly, the AOC should provide information regarding a local system's identity and status (i.e. location, availability, etc.) [RM-11.6]. This requires that the AOC is able to accurately identify and track systems in the network. And it requires that systems provide status updates to the AOC [RM-5.3]. In most operational environments, airborne elements of the AOC, such as AWACs, are capable of monitoring aircraft and providing such updates. Such identification and tracking would ensure systems have adequately updated process models regarding which systems they can connect with.

Summary of Collaborative Control Recommendations

This concludes the safety requirements for collaborative control dynamics. These requirements focused primarily on maintaining consistent control algorithms and process models. In summary the high-level requirements for collaborative control dynamics are:

> **RM-1:** *Construction of process models/control algorithms (machines)*: System automation for all systems must be constructed with consistent control algorithms regarding PAT and transmissions.
>
> **RM-2:** *Construction of mental models/control algorithms (humans)*: Operators must be provided consistent training and unambiguous standard operating procedures.
>
> **RM-3:** *Initialization of process models/control algorithms (machines)*: System automation must be consistently initialized when establishing and maintaining a connection.
>
> **RM-4:** *Initialization of mental models/control algorithms (machines)*: AOC must provide unambiguous, consistent plans for connection to all systems involved.
>
> **RM-5:** *Updates (Vertical Coordination)*: The AOC and/or team leadership must be able to provide updates to operators in a consistent, unambiguous, and timely manner.
>
> **RM-6:** *Updates* (*Lateral Coordination)*: Connecting systems must be able to coordinate connections and share necessary state information directly in near-real time.
>
> **RM-7:** *Updates (Predictions)*: Connecting systems must be able to accurately predict partner aircraft location and motion.
>
> **RM-8:** *Decision-making*: Collective decision-making of controllers must provide adequate, real-time solutions for connection issues.
>
> **RM-9:** *Closing-the-Loop Regarding Control Actions*: Systems must communicate information regarding commanded control action(s) that partner systems would not

otherwise have access to. Partner systems must be able to adequately receive and interpret shared feedback.

RM-10: *Closing-the-loop Regarding Controlled Process*: Systems must communicate information regarding the optical signal that partner systems would not otherwise have access to. Partner systems must be able to adequately receive and interpret shared feedback.

RM-11: *Dynamic Membership*: Systems must be able to detect, identify, and track other systems that are available and capable of establishing a lasercom connection.

4.5.2 Recommendations for Internal Control Factors

While the analysis provided many recommendations for managing collaborative control, it also identified scenarios related to internal control that must be addressed. The following requirements focus on controls and feedback within individual systems to avoid unsafe internal control.

Control Algorithms

System automation must have adequate control algorithms to perform pointing, tracking, and transmission control actions as assigned by operators. Additionally, operators must have adequate control algorithms regarding lasercom system operations, as well as aircraft control limits when connecting. This section addresses recommendations for maintaining adequate control algorithms.

RM-12: System automation must be able to point optics in correct direction to establish and maintain lasercom connections. Systems may receive adequate information from partners regarding location and trajectory, yet not have adequate internal control algorithms to point the optical signal in the correct direction. It is thus necessary that internal control algorithms be configured to accurately command pointing direction. Systems must first be able to detect the direction of the incoming signal [RM-12.1]. The resolution of the sensors on the terminals will be critical in creating speed and efficiency in the acquisitions process. If the sensors have very fine resolution, the terminals will be able to more quickly "acquire" or determine the direction to point their own beams to meet partner terminals. When detecting incoming signals, systems must not misinterpret background light or their own transmitted signal as a signal transmitted by partner aircraft. Systems, thus, must be able to isolate transmitted and received signals from other forms of light. System designers should consider using a bistatic architecture, different wavelengths, narrowband optical filters, and/or various polarization states to provide such means of isolation.

Provided systems are able to detect the incoming signal, systems must be able to accurately calculate pointing direction of optics based on the detected signal [RM-12.2]. Moreover, systems must be able to recognize when a "point-ahead[7]" angle is necessary due to the kinematics of the

[7] Given very high airspeeds, systems may need to execute a form of open-loop tracking in which they do not point directly at their partner, but rather *in front* of their partner. In order to account for the transit time of light, systems may need to aim where the partner terminals *will be* once the light arrives at the given location. This aim point is known as the "point-ahead" angle.

aircraft involved and must be able to calculate the required "point-ahead" angle in time for necessary corrections.

Systems must then be able to accurately command optics to point in intended direction [RM-12.3]. In some scenarios, atmospheric conditions such as atmospheric turbulence and platform jitter or temperature may cause a misalignment between the detector and transmitter/receiver resulting in misinterpreted feedback regarding direction of the optical signal. For this reason, systems must be able to detect the misalignment and perform necessary alignments in flight so that operations may continue. Accordingly, control algorithms involving processes such as nutation or other built-in tests must be configured appropriately to correct such misalignments. While maintenance was not included in the abstracted control structure, maintenance procedures should additionally be implemented to ensure components are appropriately aligned and calibrated before operations such that feedback is adequately interpreted.

RM-13: Controllers must understand necessary and acceptable flight control inputs to achieve mission objectives. Many of the generated loss scenarios emerged from flight control inputs leading to connection disruptions. As such, controllers (whether automated or human) must have adequate control algorithms for acceptable flight maneuvers when connecting. First and foremost, they must not fly aircraft in hazardous ways to achieve a connection (i.e. flying too close to terrain, exceeding range capabilities given fuel on-board, etc.) [RM-13.1].

If controllers can safely establish and maintain a link and mission objectives do not change, controllers must not fly in ways that disrupt tracking [RM-13.2]. Rapid banks or other changes in flight path may disrupt tracking by exceeding the host system's turning rate capabilities, blocking the signal, or by interfering with partner system's ability to accurately predict the aircraft's trajectory. As such, standard operating procedures for humans or control algorithms for automated controllers must provide guidance regarding necessary and acceptable flight control inputs when connecting [RM-13.3]. Guidance should place limits on aircraft angular acceleration (roll rate & pitch rate) as well as aircraft attitude (pitch and bank angle).

RM-14: Systems must be able to detect when host aircraft is not positioned appropriately to establish and maintain a lasercom connection. Controllers establishing a lasercom connection must have an adequate understanding of where aircraft may be positioned to establish a connection. While RM-11 focuses on determining a *partner* system's availability given factors such as aircraft position, this recommendation focuses on determining whether the *host* system is positioned appropriately for connection.

To share adequate information with partners and correctly calculate range, systems must first be able to accurately determine their own location and orientation [RM-14-1]. Because aircraft components such as the wing can block the signal, systems must be able to detect the host aircraft's orientation to verify that lasercom terminals are within unobstructed line-of-sight. Sensors such Inertial Navigation Systems (INSs) or Inertial Measurement Units (IMUs) may be installed to directly determine terminal orientation or aircraft orientation information may be shared from the Attitude and Heading Reference System (AHRS) within the electronic flight instrument system.

Controllers should also be able to determine when aircraft are in unsuitable atmospheric conditions for connection [RM-14.2]. Many atmospheric conditions (fog, dense cloud coverage, turbulence, etc.) may degrade communications. For this reason, guidelines setting limits for cloud coverage, precipitation, or turbulence should be established to ensure operators attempt connections only when conditions are adequate.

Because atmospheric density can affect connections, guidance should also specify limits for aircraft altitude given atmospheric conditions and range of connection. For example, aircraft in communication may need to fly at 40,000 ft or above where atmospheric disturbances do not significantly impact communications. Aircraft should avoid, as much as operationally possible, communicating from low altitude to low altitude where the beam must pass through the thickest part of the atmosphere. However, some operational scenarios may require aircraft to transmit at lower altitudes. For such lower altitude transmissions, aircraft will need to be positioned within a closer range. System requirements thus must also specify limits for range given various altitudes.

To prevent potential lasing and injury of humans, systems should not transmit a laser beam from the ground unless they are undergoing maintenance. Accordingly, systems must be able to detect when they are on the ground [RM-14.3]. Sensors such as a weight-on-wheels sensor (WOW sensors) could be used to prevent the system from lasing when on the ground.

Process Models
To prevent losses in connection, systems and operators must maintain adequate process models of the system, the optical signal, and the operational environment. As such, systems should provide adequate feedback regarding the host system and the optical signal. This section addresses the types of feedback necessary to maintain process models.

RM-15: Systems must provide feedback to Operators regarding status of operations. The lasercom system will most likely feature many modes corresponding to built-in tests as well as various operational modes including initialization, stand-by, and lase modes. It is thus critical that systems clearly indicate to operators the current mode of the system as well as its implications [RM-15.1]. For example, if a system is warming up, it must indicate that it is in "warm-up" mode and indicate the time remaining in "warm-up" mode before it is prepared to lase and able to transition to stand-by mode. Systems should also indicate the availability of other modes and alert operators to any uncommanded changes in modes to avoid mode confusion.

Systems should also indicate status of transmissions and any relevant health metrics [RM-15.2]. Systems should present to operators the status of the connection, indicating whether the system is performing acquisitions or fine-tracking and sharing data. Systems should clearly present the power received and should indicate when the full data set has been transmitted and received. If there are errors in transmissions or complete losses in connection, systems should be able to detect and determine causes (ex. inadequate power received, exceedances in bit-error-rate (BER) platform jitter, need for boresight calibration, etc.). The system should alert operators when it is about to lose a connection (due to reductions in power received) and when the system has fully lost a connection. If possible, the system should indicate the cause in transmission failures such that operators can make real-time decisions to trouble-shoot link outages.

Systems must provide feedback regarding aircraft limitations. For example, the system should clearly indicate any heading limits if its lasercom terminal has a restricted field-of-view and the aircraft must maintain a specific heading to maintain connections. Systems should also alert operators to any exceedances in angular acceleration limits. Systems should clearly indicate the range available for connections and should alert operators if they approach the limits of that range.

Finally, systems should clearly indicate any feedback provided by partner systems [RM-15.6]. To ensure operators select the correct system for connection, systems should clearly present the identity as well as the status and availability of local systems. They should indicate proximity to local systems and verify compatibility with other platforms. In some environments, the workload of pilots may be extremely high, leading to decreased situational awareness. To promote correct partner selection in such highly task-saturated environments, identification and selection of partner terminals could be executed through Heads-up Displays (HUDs) and other flight displays or through alphanumeric identifiers such as a combat IDs.

Summary of Internal Control Recommendations:
This concludes the safety requirements for the internal control factors identified using traditional STPA methods. These requirements focused primarily on maintaining safe internal control algorithms and process models. In summary the high-level requirements for internal control factors are:

> **RM-12:** System automation must be able to point optics in correct direction to establish and maintain lasercom connections.
>
> **RM-13:** Controllers must understand necessary and acceptable flight control inputs to achieve mission objectives.
>
> **RM-14:** Systems must be able to detect when host aircraft is not positioned appropriately to establish and maintain a lasercom connection.
>
> **RM-15:** Systems must provide adequate feedback to Operators regarding status of operations.

4.6 Summary

This chapter presented the four steps of STPA-Teaming applied to an early concept airborne lasercom system. In the first section, the purpose of the analysis (Step 1) was defined. In doing so, the system losses and hazards to be prevented were identified and system-level safety constraints guiding system behavior were derived. The second section modeled the system as a collaborative control structure and further abstracted the control structure to better depict various combinations of control actions (Step 2). In the third section, the unsafe combinations of control actions (UCCAs) were identified (Step 3) describing context that would make each particular UCCA unsafe. Finally, the fourth section detailed the generation of causal loss scenarios (Step 4), first identifying top-level scenarios, and then employing collaborative control dynamics and internal control factors to identify more specific scenarios.

The fifth section provided system recommendations stemming from the identified loss scenarios. In doing so, it showcased how the output of STPA, the scenarios, can be used to generate system requirements to prevent or mitigate hazards while the system is in the early concept phase of design.

Chapter 5 Conclusion

Laser communication offers many advantages for military communications as the Air Force strives to create a more robust, efficient, and secure battle network. However, the inherent challenges of lasercom, such as the need for extremely precise pointing and line-of-sight between terminals, susceptibility to atmospheric degradation, and limited number of connections, lead to a requirement for seamless coordination. This thesis applied STPA and its extension, STPA-Teaming to identify how flaws in coordination between controllers could lead to system losses—primarily loss in communication. In doing so, it identified system recommendations to eliminate or control hazards and design safety into the architecture of the system while the system is still in the early concept stage of development. This chapter discusses the results and major insights of the analysis, as well as recommendations for future work.

5.1 Results and Major Insights of Analysis

Revisiting the objective of this thesis, the goal was to answer the following overarching question:

How can system-theoretic processes be applied to identify the risks and challenges associated with coordinating laser communication for intra-aircraft communications? What system recommendations can be generated from the analysis to prevent and mitigate flaws in collaboration?

STPA assisted in understanding the challenges of airborne lasercom by first providing a method to model the system while in the early concept phase of design. In step 2 of the analysis, the system was abstracted using a Collaborative Control Structure to depict multiple controllers with shared control over the optical signal. By showing the controlled process as a shared process with direct links to and from various controllers, this abstraction more clearly depicted the dynamic interactions between controllers and the types of feedback available to them, allowing for a more systematic analysis of the collaborative dynamics within the system. For example, the dashed lines around controllers and the dashed lateral coordination arrows queued the analyst to consider scenarios in which dynamic membership or dynamic connectivity could lead to unsafe control.

Furthermore, the control structure highlighted certain "mutually-closing control loops" in which controllers would not have direct access to information regarding the optical signal or collaborator control actions. The control structure accordingly emphasized areas in which controllers must "close-the-loop" and provide additional feedback to collaborators regarding the state of the controlled process or input control actions.

Finally, the collaborative control structure was useful for identifying key aspects of lateral coordination and vertical coordination that may have been missed using traditional processes. For example, in traditional STPA, lateral arrows between controllers typically represent communication, while vertical arrows typically represent control inputs and feedback. However, the concept of lateral coordination implies that some controllers may be able to issue commands to collaborating controllers of equal hierarchical status within the control structure. Likewise, vertical coordination implies that higher ranking controllers may send down information that does not only include commands, but also includes updates regarding other controllers or the shared process. This allows the control structure to better represent situations in which the AOC not only passes down commands for connection, but also provides situational updates (and vice-versa for coordinating controllers).

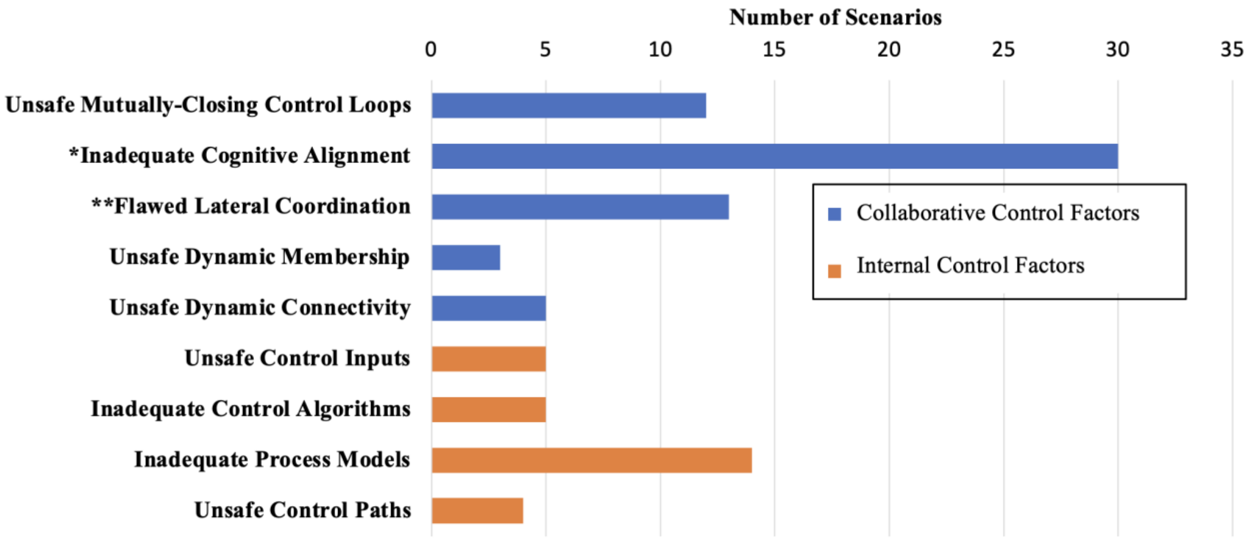
The collaborative control structure was then abstracted into two different control structures, one depicting combinations of *control actions* executed by a *team* of controllers and one illustrating combinations of *controllers* executing the *same* control actions. These abstractions allow the analyst to better understand the combinations of control actions that may be unsafe, assisting in Step 3 of the analysis.

In Step 3, the abstractions were used to generate UCCAs describing the contexts that would make combinations of various control actions unsafe. The process of considering every single combination of the same control action, different control actions, and timing of control actions allows for a rigorous and systematic approach to better identify unsafe control that may occur due to the collaborative design of the system.

One limitation of the technique is that the number of UCCAs exponentially increases as the number of control actions increases. To better manage the combinatorial complexity of the UCCA generation process, it is thus necessary to limit the number of enumerated control actions within the control structure. For this reason, the control actions available to lasercom systems were abstracted into five primary control actions. While more specific control actions such as wavelength, power, pointing direction, etc. could have each been listed in the control structure, these specific control actions were also embodied in the broader control actions such as *Transmit Beacon* or *Track Partner*. The specifics of wavelength, power, pointing direction, etc. are eventually highlighted in the context of UCCAs, when specifying how control actions may be provided in the wrong way. In this way, abstraction is used to manage the combinatorial complexity of the control actions and prevent an exceedingly large number of UCCAs from being generated.

Even after restricting the list of control actions to five primary control actions, however, over 200 UCCAs were generated using the systematic process of identifying unsafe combinations. For ease in manageability, an iterative process was used to refine the list, removing repeated UCCAs and grouping similar UCCAs together. This refinement process led to a total of 62 UCCAs.

Finally, the fourth step of STPA-Teaming involved the identification of causal scenarios that detailed how UCCAs may occur, leading to system losses, such as loss in communication. While the analysis was not an exhaustive search, 91 causal scenarios were identified using the techniques prescribed. In addition to singular component failures, the STPA scenarios included factors ranging from software problems and human factors related issues to unsafe interactions between interacting components such as the aircraft and the lasercom system. Furthermore, the systematic process of STPA-Teaming identified a wide range of scenarios related to collaborative control, highlighting the nine collaborative control dynamics discussed in Chapter 2. Figure 5-1 below compares the number of collaborative and internal control factors represented in the generated scenarios.



*Excludes *Lateral Coordination* scenarios embedded in *Cognitive Alignment*
**Includes scenarios related to *Shared Authority, Transfer of Authority,* & *Dynamic Authority*

Figure 5-1: Comparison of Contributing Collaborative and Internal Control Factors

Using STPA-Teaming to systematically consider collaborative control factors, the analysis identifies a much higher number of scenarios related to unsafe collaborative control rather than internal control. As the chart indicates, unsafe cognitive alignment contributes to the highest percentage of loss scenarios. As such, system designers and operators should particularly focus on maintaining consistent construction, initialization, and updates of control algorithms and process models for controllers. Unsafe mutually-closing control loops, flawed lateral coordination, and unsafe internal process models additionally are high contributors to losses. These leading factors highlight areas of extra importance to be addressed throughout the system's lifecycle from the generation of system requirements to system operations.

Using the generated scenarios, 15 high-level recommendations were identified for the system, from which 74 additional subrequirements were generated. These recommendations address the gaps in collaboration associated with collaborative control dynamics, as well as gaps related to unsafe internal control. Recommendations provide guidance for sequencing and timing of control actions, transitions between control actions, and consistent training/standard operating procedures for operators. Furthermore, the recommendations address the need for clear, unambiguous updates to systems both laterally with other systems and vertically with the AOC. The recommendations also provide guidance to maintain adequate internal control of systems, addressing factors related to adequate sensing, software-related control issues, feedback from/to aircraft flight control systems, and adequate control paths with human operators.

Returning to the thesis objective, it is clear that STPA-Teaming provides a systematic mechanism to identify the challenges associated with coordination for lasercom links for aircraft-to-aircraft communications. By identifying loss scenarios related to collaborative control dynamics as well as internal control factors, this analysis allowed a wide range of system recommendations to be generated. The identified recommendations can ultimately support the remainder of the systems engineering process, ensuring that safety, security, and reliability are designed into the system while it is in an early conceptual stage of development.

5.2 Future Work

System architecture can largely affect the emergent behavior of a system. While several assumptions were made regarding the system architecture in this initial analysis, it is recommended that STPA be applied to future architectures as the system is further refined. For example, this analysis only considered the use of lasercom for aircraft-to-aircraft communications. However, there are also possibilities of using such a system to connect aircraft to ground stations or aircraft to satellites. The implications of such an architecture could be highlighted in iterated control structures that help identify new causal scenarios.

An additional architecture decision that should be further investigated is the degree of automation and human supervision within the system. Kharsanksy demonstrated how STPA can be used to compare architectures and found that STPA assisted in evaluating tradeoffs between automation, safety, and reliability [38]. In his comparison of architectures, Kharsanksy specifically evaluated levels of automation: automation is a continuum that can be ranked from the lowest level of fully manual to the highest level of fully automated [39]. There are many possible options for levels of automation within the proposed lasercom system from partner selection, acquisitions, and terminal maintenance to control of flight. In the same way Kharsansky used STPA in an architecture trade-off study, STPA-Teaming could be used to compare architectures with varying levels of autonomy for the lasercom system. Such an analysis could provide more insight into how much control software and human operators should be allotted without inducing task saturation or complacency due to lack of involvement.

As the system is further refined and the military selects an aircraft for system integration, it is recommended that a more detailed STPA be conducted using the specific technical information of the aircraft and details regarding integration. Because this thesis was applied at a high-level, the control structure used a generic aircraft with no assumptions regarding aircraft type, configuration, or capability. The technical aspects of aircraft type and details regarding system integration will lead to more specific scenarios, with more specific traceable safety-constraints. For example, aspects such as whether the aircraft is manned or unmanned will lead to vastly different scenarios as major sources of feedback and control for operators are altered. As such, STPA should continue to be used as systematic analysis tool throughout the system's development.

This thesis also assumed a generic Air Operations Center for its higher-level mission authority. As the system is developed and operationalized in specific squadrons, more details will emerge regarding entities within the AOC and how they interact with operators in a given area. Local rules of engagement (ROEs) and standard operating procedures may vary squadron to squadron. As a result, assumptions made in this initial analysis regarding AOC vertical control may be invalidated. An STPA should thus be performed again on operationalized systems to not only identify more specific scenarios, but to reassess prior assumptions and correct the system design, integration, operating procedures, or organizational structure if assumptions are invalidated. In this way, STPA can be used to identify and constrain unsafe system behavior throughout the system's lifecycle from early concept development to the operational and maintenance phase.

This thesis specifically focused on the early concept phase, applying STPA to identify and mitigate the major challenges that arise from collaborative interactions within the lasercom system. The analysis made clear that to fully capture the behavior emerging from teaming interactions, the system needs a holistic, top-down approach based on systems thinking, rather than an approach using decomposition or based on a linear chain-of-events model. Thus, it is ultimately recommended that STPA-Teaming be applied at all stages of the system's development to generate additional requirements and to ensure traceability as specific system information emerges throughout the system's lifecycle. In this way, losses in communication or mission may continue to be mitigated as the system changes such that the system may continue to support the resilient battle network intended for military forces.

Chapter 6 References

[1] T. Harrison, “Battle Networks and the Future Force. Part 1: A Framework for Debate,” *Cent. Strateg. Int. Stud. CSIS Briefs*, Aug. 2021, [Online]. Available: www.csis.org

[2] A. K. Majumdar and J. C. Ricklin, Eds., *Free-Space Laser Communications: Principles and Advances*. in Optical and Fiber Communications Reports, no. 2. New York, NY: Springer, 2008.

[3] Rebecca Grant, “Comms Through the Aerial Layer,” *J. Air Force Assoc. Air Force Mag.*, vol. 98, no. 12, pp. 54–58, Dec. 2015.

[4] F. G. Walther, S. Michael, R. R. Parenti, and J. A. Taylor, “Air-to-ground lasercom system demonstration design overview and results summary,” presented at the SPIE Optical Engineering + Applications, A. K. Majumdar and C. C. Davis, Eds., San Diego, California, United States, Aug. 2010, p. 78140Y. doi: 10.1117/12.864262.

[5] R. J. Feldmann and R. A. Gill, “Development of laser crosslink for airborne operations,” in *IEEE Military Communications Conference. Proceedings. MILCOM 98 (Cat. No.98CH36201)*, Boston, MA, USA: IEEE, 1998, pp. 633–637. doi: 10.1109/MILCOM.1998.722203.

[6] R. A. Conrad, R. J. Murphy, T. H. Williams, W. E. Wilcox, S. Michael, and J. M. Roth, “Experimental comparison of tracking algorithms in the presence of aircraft boundary-layer distortions for emulated free-space laser communication links,” *Appl. Opt.*, vol. 48, no. 1, p. A98, Jan. 2009, doi: 10.1364/AO.48.000A98.

[7] H. Kaushal and G. Kaddoum, “Optical Communication in Space: Challenges and Mitigation Techniques,” *IEEE Commun. Surv. Tutor.*, vol. 19, no. 1, pp. 57–96, 2017, doi: 10.1109/COMST.2016.2603518.

[8] S. A. Hamilton *et al.*, “Long-Haul Atmospheric Laser Communication Systems§,” in *Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011*, Los Angeles, California: OSA, 2011, p. OWX2. doi: 10.1364/OFC.2011.OWX2.

[9] T. Ulmer *et al.*, “Generalized spatial acquisition for a space-based adaptive communications node optical terminal,” in *Free-Space Laser Communications XXXV*, H. Hemmati and B. S. Robinson, Eds., San Francisco, United States: SPIE, Sep. 2023, p. 12. doi: 10.1117/12.2652012.

[10] F. Moll *et al.*, “Demonstration of High-Rate Laser Communications From a Fast Airborne Platform,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1985–1995, Sep. 2015, doi: 10.1109/JSAC.2015.2433054.

[11] N. Leveson, *Engineering a safer world: systems thinking applied to safety*. in Engineering systems. Cambridge, Mass: MIT Press, 2011.

[12] N. G. Leveson, *An Introduction to System Safety Engineering*. Cambridge, MA: MIT Press, 2023.

[13] J. B. Fussell, “A Review of Fault Tree Analysis with Emphasis on Limitations,” *IFAC Proc. Vol.*, vol. 8, no. 1, pp. 552–557, Aug. 1975, doi: 10.1016/S1474-6670(17)67596-7.

[14] “Procedures for Performing a Failure Mode Effect and Criticality Analysis.” Department of Defense, 1949.

[15] D. Stamatis, *Failure Mode Effect Analysis: FMEA from Theory to Execution*. Milwaukee: Quality Press.

[16] C. J. Middleton, “Risk Assessment Planning for Airborne Systems: An Information Assurance Failure Mode, Effects and Criticality Analysis Methodology," Masters Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, 2012.

[17] *Columbia Accident Investigation Report*, vol. 1. Columbia Accident Investigation Board, 2003.

[18] F. Crawley and B. Tyler, “Chapter 1 - Introduction,” in *HAZOP: Guide to Best Practice (Third Edition)*, F. Crawley and B. Tyler, Eds., Elsevier, 2015, pp. 1–3. doi: 10.1016/B978-0-323-39460-4.00001-3.

[19] F. Crawley and B. Tyler, “Chapter 3 - The HAZOP Study Method,” in *HAZOP: Guide to Best Practice (Third Edition)*, F. Crawley and B. Tyler, Eds., Elsevier, 2015, pp. 10–12. doi: 10.1016/B978-0-323-39460-4.00003-7.

[20] F. Crawley and B. Tyler, “Chapter 4 - The Detailed HAZOP Study Procedure,” in *HAZOP: Guide to Best Practice (Third Edition)*, F. Crawley and B. Tyler, Eds., Elsevier, 2015, pp. 13–28. doi: 10.1016/B978-0-323-39460-4.00004-9.

[21] T. Van de Putte, “Purpose and Framework for a Safety Study in the Process Industry,” in *Hazard Prevention*, 1983, pp. 18–21.

[22] Juoko Suokas and Veikko Rouhiainen, “Quality Control in Safety and Risk Analysis,” *J. Loss Prev. Process Ind.*, vol. 2, pp. 67–77, Apr. 1989.

[23] N. G. Leveson and Thomas, John P., *STPA Handbook*. 2018.

[24] John P Thomas, “Empirical Evaluations of STPA in the Aviation Industry,” presented at the STAMP Workshop, Massachusetts Institute of Technology, Cambridge MA, Jun. 2023.

[25] A. N. Kopeikin, “System-Theoretic Safety Analysis for Teams of Collaborative Controllers,” PhD Dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2024.

[26] Andrew N. Kopeikin, Nancy G. Leveson, and Natasha A. Neogi, “Defining Collaborative Control Interactions Using Systems Theory,” *INCOSE Int. Symp.*, vol. 33, no. 1, pp. 895–909, 2023.

[27] K. E. Johnson, “Systems-Theoretic Safety Analyses Extended for Coordination," PhD Dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2017.

[28] A. N. Kopeikin, N. G. Leveson, and N. A. Neogi, “System-Theoretic Analysis of Unsafe Collaborative Control in Teaming Systems,” *AIAA SciTech*, 2024.

[29] “Air Force Doctrine Publication (AFDP) 3-03 Counterland Operations Theater Air Control System.” Curtis E. Lemay Center for Doctrine Development and Education, Oct. 21, 2020. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-03/3-03-D23-TACS.pdf

[30] “Joint Publication 6-0 Joint Communications System.” Chairman of the Joint Chiefs of Staff (CJCS), Oct. 04, 2019.

[31] “Joint Publications 3-30 Joint Air Operations.” Joint Chiefs of Staff, Sep. 17, 2021.

[32] M. Conner, M. Lambertson, and M. Roberson, “Analyzing the Air Operations Center (AOC) Air Tasking Order (ATO) Process Using Theory of Constraints (TOC)”.

[33] “Multi-service Tactics, Techniques, and Procedures for Air Control Communication.” Air Land Sea Applications (ALSA) Center, Sep. 2021. [Online]. Available: https://www.alsa.mil/

[34] “Introduction to Tactical Digital Information Link J and Quick Reference Guide (TADIL J).” HQ TRADOC Attn: ATDO-A Fort Monroe, VA, Jun. 2000.

[35] D. R. Bull and F. Zhang, "Communicating pictures: delivery across networks," in *Intelligent Image and Video Compression*, Elsevier, 2021, pp. 385–434. doi: 10.1016/B978-0-12-820353-8.00020-7.

[36] "Appendix II: Gaussian White Noise," in *Nonlinear Dynamic Modeling of Physiological Systems*, John Wiley & Sons, Ltd, 2004, pp. 499–501. doi: 10.1002/9780471679370.app2.

[37] "Communications system achieves fastest laser link from space yet | MIT Lincoln Laboratory." Accessed: Apr. 24, 2024. [Online]. Available: https://www.ll.mit.edu/news/communications-system-achieves-fastest-laser-link-space-yet

[38] A. Kharsansky, "A Systemic Approach Toward Scalable, Reliable and Safe Satellite Constellations," Masters Thesis, Massachusetts Institute of Technology, Cambridge, MA, 2020.

[39] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A Model for Types and Levels of Human Interaction with Automation," *IEEE Trans. Syst. Man Cybern. - Part Syst. Hum.*, vol. 30, no. 3, pp. 286–297, May 2000, doi: 10.1109/3468.844354.

Appendix A: Unsafe Combinations of Control Actions (UCCAs)

Table A-1: Abstraction 1 UCCAs Types 1-2

Team of Lasercom System Controllers		**Context**
¬Transmit Beacon	¬{Detect Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 1 When systems must locate one another to establish a connection for communications [H-1, H-2]
¬Transmit Beacon	{Detect Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 2 When systems must establish a connection for communications [H-1, H-2]
		UCCA 3 When system connects with an unintended or unauthorized platform [H-1, H-2, H-4]
Transmit Beacon	¬{Detect Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 4 When systems must establish a connection for communications [H-1, H-2]
		UCCA 5 When beacon interferes with partner's other connections or subsystems [H-1, H-2, H-3]
Transmit Beacon	{Detect Beacon, ~~Track Partner Beam, Transmit Data, Receive Data~~}	UCCA 6 When systems must establish a connection for communications and system does not transmit beacon correctly (i.e. points in incorrect direction, transmits with incompatible technical parameters or sequences, transmits using incompatible optical terminal, etc.) [H-1, H-2, H-3, H-4, H-5, H-6]
		UCCA 7 When systems must establish a connection and aircraft transmitting beacon is not positioned appropriately (i.e. not within LOS, not at appropriate altitude, not within adequate range, on the ground, in adverse atmospheric conditions, in a vulnerable/compromised position, etc.) [H-1, H-2, H-3, H-4, H-5, H-6]
Detect Beacon	¬{Transmit Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 8 When hostile forces are attempting to connect with system [H-4]
Detect Beacon	{Transmit Beacon, ~~Track Partner Beam, Transmit Data, Receive Data~~}	UCCA 9 When systems must establish a connection for communications and system does not correctly scan for and detect beacon (i.e. points in incorrect direction, scans using incompatible technical parameters or sequences, detects using incompatible optical terminal, etc.) [H-1, H-2, H-3, H-4, H-5, H-6]
		UCCA 10 When systems must establish a connection and aircraft detecting beacon is not positioned appropriately [H-1, H-2, H-3, H-4, H-5, H-6]

¬Track Partner Beam	{Transmit Beacon, Detect Beacon, ~~Transmit Data, Receive Data~~}	UCCA 11 When systems must maintain a connection for communications [H-1, H-2]
Track Partner Beam	¬{~~Transmit Beacon, Detect Beacon~~, Transmit Data, Receive Data}	UCCA 12 When systems have established a connection and systems must share data for mission purposes [H-1, H-2]
Track Partner Beam	{Transmit Beacon, Detect Beacon, Transmit Data, Receive Data}	UCCA 13 When systems must share data and partner beam is not tracked correctly (i.e. incompatible optical terminal provides tracking or tracking beam is pointed in incorrect direction) [H-1, H-2, H-3, H-4. H-5, H-6]
		UCCA 14 When systems must share data and aircraft is not positioned to maintain accurate partner tracking (i.e. not within LOS, not at appropriate altitude, not within adequate range, on the ground, in adverse atmospheric conditions, in a vulnerable/compromised position, etc.) [H-1, H-2, H-3, H-4. H-5, H-6]
Transmit Data	¬{~~Transmit Beacon, Detect Beacon, Track Partner Beam~~, Receive Data}	UCCA 15 When system must transmit data for mission purposes and transmits in incorrect manner (i.e. transmits using incompatible optical terminal, incompatible technical parameters, etc.) [H-1, H-2, H-4. H-5]
		UCCA 16 When transmitting data will interfere with other aircraft functions (i.e. RF communications) [H-1, H-2, H-3, H-6]
Transmit Data	{Transmit Beacon, Detect Beacon, Track Partner Beam, Receive Data}	UCCA 17 When systems are not intended to connect and share data [H-4]
		UCCA 18 When system must also receive data, and transmitting data simultaneously interferes with ability to receive [H-1, H-2]
Receive Data	¬{Transmit Beacon, Detect Beacon, Track Partner Beam, Transmit Data}	UCCA 19 When system must receive data for mission purposes [H-1, H-2]
		UCCA 20 When data is not intended to be received (i.e. system’s own transmissions interfere with receiver) [H-1, H-2, H-3]
Receive Data	{Transmit Beacon, Detect Beacon, Track Partner Beam, Transmit Data}	UCCA 21 When systems must share data and system receives data in incorrect manner (i.e. incompatible optical terminal, incompatible technical parameters, etc.) ([H-1, H-2, H-3, H-4, H-6]

Table A-2: Abstraction 1 UCCAs Types 3-4

Team of Lasercom System Controllers		**Context**
Starts Transmit Beacon	*Before Starts* {Detect Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 22 When connecting system is unaware/not prepared to receive an optical signal and optical signal may interfere with other aircraft subsystems [H-1, H-2, H-3, H-5, H-6]
Starts Transmit Beacon	*Before Ends*{~~Detect Beacon~~, Track Partner Beam, Transmit Data, Receive Data}	UCCA 23 When partner terminal is still transmitting with another system and transmitting a beacon will interfere with established connection [H-1, H-2, H-3, H-5]
Ends Transmit Beacon	*Before Starts*{~~Detect Beacon~~, Track Partner Beam, ~~Transmit Data, Receive Data~~}	UCCA 24 When systems must establish a connection for mission purposes [H-1, H-2]
Ends Transmit Beacon	*Before Ends* {Detect Beacon, ~~Track Partner Beam, Transmit Data, Receive Data~~}	UCCA 25 When system is still attempting to locate partner terminal's position for acquisition [H-1, H-2]
Starts Detect Beacon	*Before Starts* {Transmit Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 26 When scanning for a beacon will expose system to jamming/intercepting threats [H-1, H-2, H-3, H-4]
Ends Detect Beacon	*Before Starts*{Transmit Beacon, Track Partner Beam, Transmit Data, Receive Data}	UCCA 27 When systems must establish a connection for mission purposes [H-1, H-2]
Ends Detect Beacon	*Before Ends*{Transmit Beacon, ~~Track Partner Beam, Transmit Data, Receive Data~~}	UCCA 28 When systems must connect and system transmitting beacon has not yet located partner terminal to complete acquisition and initiate tracking [H-1, H-2]
Ends Track Partner Beam	*Before Starts*{~~Transmit Beacon, Detect Beacon Beam~~, Transmit Data, Receive Data}	UCCA 29 When systems must maintain tracking to transmit/receive data for mission purposes [H-1, H-2]
Ends Track Partner Beam	*Before Ends*{~~Transmit Beacon, Detect Beacon Beam~~, Transmit Data, Receive Data}	UCCA 30 When entire data set has not been transmitted and received [H-1, H-2]
Starts Transmit Data	*Before Starts* {~~Transmit Beacon, Detect Beacon Beam,~~ Track Partner Terminal, Receive Data}	UCCA 31 When terminals have not yet established a connection and must determine each other's location to initiate tracking [H-2]

Starts Transmit Data	*Before Starts* {~~Transmit Beacon,~~ ~~Detect Beacon Beam~~, ~~Track Partner Terminal~~, Receive Data}	UCCA 32 When partner system is not prepared to receive data [H-2]
Starts Transmit Data	*Before Ends*{Transmit Beacon, Detect Beacon ~~Beam, Track Partner Terminal, Receive Data}~~	UCCA 33 When acquisition has not been fully completed [H-1, H-2]
Ends Transmit Data	*Before Starts*{~~Transmit Beacon,~~ ~~Detect Beacon Beam~~, Track Partner Terminal, Receive Data}	UCCA 34 When acquisition has not been fully completed [H-1, H-2]
Ends Transmit Data	*Before Ends*{~~Transmit Beacon,~~ ~~Detect Beacon Beam~~, Track Partner Terminal, Receive Data}	UCCA 35 When entire data set has not yet been transmitted and/or received [H-1, H-2]
Starts Receive Data	*Before Starts* {Transmit Beacon, Detect Beacon Beam, Track Partner Terminal, Transmit Data}	UCCA 36 When data received is from an unintended partner [H-1, H-2, H-4]
Ends Receive Data	*Before Starts*{~~Transmit Beacon,~~ ~~Detect Beacon Beam, Track Partner Terminal~~, Transmit Data}}	UCCA 37 When systems must transmit/receive data for mission purposes [H-1, H-2]
Ends Receive Data	*Before Ends*{~~Transmit Beacon,~~ ~~Detect Beacon Beam, Track Partner Terminal,~~ Transmit Data}	UCCA 38 When entire data set has not yet been transmitted and/or received [H-1, H-2]

Table A-3: Abstraction 2 UCCAs Types 1-2

Transmit beacon provided by		**Context**
¬Any one	¬Any of others	UCCA 39 When systems must locate one another to establish a connection for communications [H-1, H-2]
¬Any one	Any of others	UCCA 40 When both systems must transmit a beacon to connect (i.e. systems must use an asymmetric acquisition sequence) [H-1, H-2]
¬Any one	Any of others	UCCA 41 When tasked terminal is not capable of transmitting beacon, but another one is [H-1, H-2, H-3, H-5]
Any one	Any of others	UCCA 42 When transmitting a beacon simultaneously interferes with ability to detect beacon (i.e. systems must use a symmetric acquisition sequence) [H-1, H-2, H-3]

Detect beacon provided by		**Context**
¬Any one	¬Any of others	UCCA 43 When systems must locate one another to establish a connection for communications [H-1, H-2]
¬Any one	Any of others	UCCA 44 When tasked terminal is not capable of detecting beacon, but another one is [H-1, H-2]
Track partner beam provided by		**Context**
¬Any one	¬Any of others	UCCA 45 When both systems must track one another to maintain a connection for communications [H-1, H-2]
¬Any one	Any of others	UCCA 46 When both systems must track one another to maintain a connection for communications [H-1, H-2]
Any one	Any of others	UCCA 47 When systems track unintended partners [H-1, H-2, H-4]
Transmit data provided by		**Context**
¬Any one	¬Any of others	UCCA 48 When systems must transmit/receive data for mission purposes [H-1, H-2]
¬Any one	Any of others	UCCA 49 When both systems must transmit data and have the ability to do so simultaneously [H-1, H-2]
Any one	Any of others	UCCA 50 When systems cannot transmit and receive simultaneously and doing so will interfere with comms [H-1, H-2]
Receive data provided by		**Context**
¬Any one	¬Any of others	UCCA 51 When systems must transmit/receive data for mission purposes [H-1, H-2]
¬Any one	Any of others	UCCA 52 When both systems must receive information and have the ability to do so simultaneously [H-2]
Any one	Any of others	UCCA 53 When only one system is transmitting data [H-1, H-2]

Table A-4: Abstraction 2 UCCAs Types 3-4

Transmit beacon by	**Before transmit beacon by**	**Context**
Any one *starts*	Any of others *end*	UCCA 54 When system is attempting to connect with a different system and simultaneously transmitting a beacon will interfere with beacon acquisition for another connection [H-1, H-2, H-3]
Detect Beacon by	**Detect Beacon by**	**Context**
Any one *starts*	Any of others *end*	UCCA 55 When partner system's return beam for acquisitions has not yet illuminated initiating terminal and system must continue to transmit beacon [H-1, H-2, H-3]
Track partner beam by	**Track partner beam by**	**Context**
Any one *ends*	Any of others *start*	UCCA 56 When a connection must be established and data must be shared for mission purposes [H-1, H-2]
Any one *ends*	Any of others *end*	UCCA 57 When complete data set has not yet been transmitted/received [H-1, H-2]

Transmit data by	**Transmit data by**	**Context**
Any one *starts*	Any of others *end*	UCCA 58 When full data set has not yet been transmitted and neither system is full-duplex [H-2, H-3]
Any one *ends*	Any of others *start*	UCCA 59 When aircraft must relay data [H-2]
Any one *ends*	Any of others *end*	UCCA 60 When systems are full-duplex and complete data set has not yet been transmitted [H-2]
Receive data by	**Receive data by**	**Context**
Any one *starts*	Any of others *end*	UCCA 61 When neither system is full-duplex and data is still being transmitted by partner [H-2]
Any one *ends*	Any of others *end*	UCCA 62 When both systems are transmitting data and entire data set has not yet been transmitted [H-2]

Appendix B: Loss Scenarios

Table B-1: Top-level Scenarios and Refined Scenarios

Loss Scenario	Related UCCAs
S-1 *Top-level:* Operators provide adequate task(s) to establish a connection, but Lasercom Systems do not execute task(s) as directed. **S-1.1** *Unsafe feedback about shared control process is received from collaborators*: Aircraft$_1$ flies through atmosphere with dense cloud coverage when receiving data. As a result, the power of the signal received drops below the min RSSI (Received Signal Strength Indicator) for X amount of time required for fine-tracking. Thus, System$_1$ regresses to open-loop coarse tracking and starts Transmit Beacon to reconnect. System$_1$ does not communicate with System$_2$ that the power of the optical signal received was too low and as a result, System$_2$ does not regress to Detect Beacon as required for re-connection. **S-1.2** *Unsafe feedback about collaborator control actions is received from shared control process*: Lasercom System$_1$ does not notify Lasercom System$_2$ that it is providing Transmit Beacon: After X amount of time (ex. 60 seconds) of Transmitting Beacon, System$_1$ does not successfully illuminate System$_2$ for beacon detection. As a result of the expired time, System$_2$ automatically stops Detect Beacon. System$_1$ reinitiates Transmit Beacon after expired time but does not communicate to System$_1$ that it has done so. As a result, System$_2$ does not re-initiate Detect Beacon when systems must connect. **S-1.3** *Construction of process models/control algorithms inadequate:* It is assumed that all systems operate with the same power and transmission capabilities. However, due to system upgrades, Lasercom System$_1$ has greater power capabilities and thus an extended range. Because Lasercom System$_2$ has a different model of acceptable ranges, it does not believe that Lasercom System$_1$ is within range for connection and does not provide Detect Beacon as commanded. **S-1.4** *Initialization of process models/control algorithms inadequate:* In pre-flight mission documents (ex. ATO publications), operators are not provided consistent and compatible technical parameters for connection. As a result, they configure systems to connect using different modulation formats, frequencies, or data rates. **S-1.5** *Updates to process models inadequate:* Controllers on team receive inadequate updates regarding shared process: Refinement shown below. **S-1.5.1** *Flawed vertical coordination (control)*: AOC provides incorrect/delayed identification of tracks from radar. So System$_2$ points its tracking sensor in the incorrect direction to establish a connection and does not Detect Beacon. **S-1.5.2** *Flawed lateral coordination (communication)*: Feedback from System$_2$'s GPS, INS, or flight control system is delayed/inaccurate when sent to System. So, System$_1$ provides Transmit Beacon in the wrong direction and System$_2$ does not Detect Beacon. **S-1.5.3** *Inconsistent predictions/decision making:* Lasercom System$_1$ relies on Kalman filter for trajectory prediction, but Aircraft$_2$ banks unexpectantly. As a result, Lasercom System$_1$ makes inaccurate predictions regarding Aircraft$_2$'s flightpath and points in the wrong direction while Transmitting Beacon. Lasercom System$_2$ thus does not Detect Beacon.	UCCA 1 UCCA 4 UCCA 11 UCCA 23 UCCA 31 UCCA 32 UCCA 33 UCCA 39 UCCA 43 UCCA 45 UCCA 46 UCCA 48 UCCA 51 UCCA 52 UCCA 56 UCCA 57 UCCA 60 UCCA 62

S-1.5.4 *Unsafe observations:* System$_2$ observes that System$_1$ is currently connected with another aircraft (through TDL communications or feedback provided by AOC). System$_2$ thus believes that System$_1$ is unavailable for connection. Aircraft$_1$, however, is equipped with two lasercom terminals and is capable of simultaneously connecting with two aircraft. Because System$_2$ is unaware of this capability, it does not provide Detect Beacon. **S-1.6** *Unsafe dynamic membership:* Plans change due to mission needs/weather phenomena, requiring Aircraft$_3$, originally planned for connection, to divert. So, Aircraft$_2$ is sent by AOC as a replacement to establish a connection with Aircraft$_1$. Aircraft$_2$ is not capable of transmitting at a compatible optical frequency for communication with Aircraft$_1$. As a result, it does not Detect Beacon as commanded. **S-1.7** *Dynamic connectivity:* Systems are designed such that their status and availability for acquisition is communicated through an RF link. Systems are unable to communicate due to enemy jamming, interfering terrain, inoperable frequencies, etc. So System$_2$ is unaware that System$_1$ is prepared to connect and has initiated Transmit Beacon command.	
S-2 *Top-level**:*** Operators do not provide some of the tasks required for lasercom systems to establish a connection. **S-2.1** *Unsafe feedback about collaborator control actions received from collaborators**:*** Operators$_2$ do not confirm when they reach waypoint designated in ATO for transmissions. As a result, Operators$_1$ do not know Aircraft$_2$ is positioned appropriately to begin acquisitions, so they do not provide tasks to Detect Beacon or Transmit Beacon. **S-2.2** *Initialization of process models/control algorithms unsafe:* Pre-flight documents provided by the AOC (i.e. ACO and ATO) do not specify roles in acquisition process for both systems. Operators cannot communicate to establish/verify role in acquisition process so it is unclear which systems will Transmit/Detect Beacon. As a result, both Operators provide tasks to Transmit Beacon, and neither provide tasks to Detect Beacon. **S-2.3** *Updates to process models inadequate: C*ontrollers on team receive inadequate updates regarding shared process: Refinement shown below. **S-2.3.1** *Flawed vertical coordination (control)*: Due to incompatible tactical data links, systems cannot share aircraft state information or terminal status updates directly, but must obtain such information from the AOC. The AOC is delayed/unable to share state information so Operators$_2$ are not aware that System$_1$ is positioned appropriately and prepared to connect. **S-2.3.2** *Flawed vertical coordination (control)*: Weather information from AOC is inaccurate/delayed so operators do not have an accurate mental model of turbulence/weather phenomena in a certain location. As a result, operators believe weather/atmosphere would block signal and do not provide task(s) to establish a link. **S-2.3.3** *Flawed lateral coordination (communication)*: System$_2$ experiences a system malfunction that prevents it from Detecting Beacon as originally planned. System$_2$ does not adequately communicate with System$_1$ that it has malfunctioned. So Operators$_1$ continue attempts at acquisitions, while Operators$_2$ do not provide tasks to Detect Beacon. **S-2.3.4** *Flawed lateral coordination (communication)*: Partner flies through mountainous terrain to rendezvous with host system, but GPS data is delayed/inadequate, so host system automation indicates to operators that partner is not within line of sight or it fully prohibits Transmit/Detect Beacon command.	UCCA 1 UCCA 2 UCCA 3 UCCA 4 UCCA 11 UCCA 23 UCCA 25 UCCA 26 UCCA 28 UCCA 40 UCCA 43 UCCA 45

S-2.3.5 *Flawed lateral coordination (communication):* Standard communication procedures involve confirming completion of checklists before connection (i.e. boresight alignment, inputting necessary parameters, etc.). Operators become task-saturated, so they do not send necessary verbal/digital communications to verify that they are ready for connection. **S-2.3.6** *Inconsistent predictions/decision making:* Both Systems receive consistent updates regarding weather, but Operators have mismatched understandings of acceptable atmospheric conditions for connection. Due to inconsistent training or guidelines, Operators$_1$ predict that connections will be sustainable in current weather conditions, but Operators$_2$ predict that connections will not be sustainable. As a result, they decide to not Detect Beacon. **S-2.4** *Capacity:* Due to high task-saturation, Operators$_2$ forget to check in with AOC to receive commands or status updates regarding lasercom connection. As a result, Operators$_2$ do not receive "WORDs" information including necessary connection parameters with System$_1$. Thus, they do not provide tasks to Detect Beacon. **S-2.5** *Unsafe dynamic membership:* Aircraft$_1$ enters a new area of operations, requiring a different Identification Friend or Foe (IFF) mode. Operators$_1$ are delayed in changing IFF mode or change to the wrong mode. As a result, Operators$_2$ believe System$_1$ is not authorized to connect and do not provide tasks to Detect Beacon. **S-2.6** *Unsafe dynamic connectivity:* AOC attempts to send commands for a specific laser link configuration to be established, but commands are not received due to enemy jamming, inadequate comms frequency settings, TDL network issues/latencies, interfering terrain, etc. **S-2.7** *Unsafe internal control due to unsafe control path:* Configuration files containing state information are altered on the ground, but are not uploaded properly once system is powered on in flight. Thus, the system cannot change from inactive mode to subsequent operational modes. For this reason, Operators are unable to provide Transmit/Detect Beacon command. **S-2.8** *Unsafe internal process model:* Operators do not command system to Transmit/Detect Beacon because they are not aware partner system is within range and line-of-sight to connect. System adequately receives information regarding partner system location and proximity but is delayed in processing data to determine range and pointing direction.	
S-3 *Top-level***:** Operators provide some of the tasks to establish a connection in a way that leads to unsafe collective control. **S-3.1** *Unsafe feedback received regarding collaborator control actions:* System$_1$ is responsible for assigning control actions, Transmit Beacon and Detect Beacon. Their assignment of control actions is unclear/ambiguous so System$_2$ is unsure of its role in the acquisition process. Neither system communicates to confirm whether they are Transmitting/Detecting Beacon so both provide the same control action (Transmit vs. Detect Beacon) and neither provide the necessary corresponding control action. **S-3.2** *Initialization of control algorithms inadequate:* Plans deviate from the ACO resulting in new timing, waypoints, technical parameters, or partners to connect. Before takeoff, Operator$_2$ do not receive Aircrew Read Files (ARF) indicating changes to the ACO. As a result, they provide task(s) to connect at wrong time or location. **S-3.3** *Updates to process models inadequate: C*ontrollers on team receive inadequate updates regarding shared process. **S-3.3.1** *Flawed lateral coordination (communication):* Controllers on team do not have semantic alignment regarding communications during transmissions. As a result, Operators$_2$ misinterpret Operators$_1$ updates as a request to connect at X	UCCA 1 UCCA 2 UCCA 4 UCCA 23 UCCA 28 UCCA 40 UCCA 42 UCCA 43 UCCA 45 UCCA 48 UCCA 54

technical parameter (wavelength, modulation, data rate, etc.). As a result, they provide task(s) to establish a connection at incompatible parameters. **S-3.4** *Unsafe predictions/observations:* Operators attempt to connect at incompatible technical parameters because they assume that their partner system has the same capabilities and/or will use the same technical parameters. Systems do not communicate capabilities or intended parameters so are not aware that partner system will use different parameters. So, systems cannot appropriately acquire each other's beams. **S-3.5** *Unsafe dynamic membership*: Commonly accepted practices evolve where one system routinely performs acquisition role (i.e. Transmit Beacon vs. Detect Beacon) based on its location, airframe type, Combat ID #, transmitting/receiving role, or some other mechanism. However, a change in personnel/squadrons/military branches/allied forces occurs where the commonly accepted roles are not in place or are reversed. For this reason, operators misunderstand their role in the acquisition process and both system's Operators command Transmit Beacon, while neither provide Detect Beacon. **S-3.6** *Unsafe internal process model:* Operators$_1$ provide task to Transmit Beacon in incorrect direction because System does not clearly indicate local operating aircraft. Feedback regarding aircraft identity is inadequate, confusing, or missing so Operators select wrong aircraft for connection. **S-3.7** *Unsafe internal control algorithm:* Due to inadequate training or procedural updates, Operators do not know how to properly power on subsystems of lasercom automation. For example, Operators may attempt to power on controller electronics before space switching unit (SSU), leading to errors in power up. For this reason, Operators are shown errors to which they do not know how to respond and thus do not provide Transmit/Detect Beacon command.	UCCA 55
S-4 *Top-level:* Operators adequately do not provide certain task(s) when establishing a connection, but Systems execute them anyways. **S-4.1** *Unsafe dynamic connectivity:* Means of partner verification are inadequate. As a result, hostile forces are able to interfere with the command link in RF comms. They send false position, velocity, or timing information to disrupt acquisition or direct optical signal to their own aircraft. **S-4.2** *Unsafe internal process model:* A fault is detected causing an inadvertent mode change to occur. The system switches from "standby" mode (in which it is ready to connect) to "fiber loopback" mode designed for system calibration and testing. No feedback is provided regarding mode change or mode status so Operators are unaware modes have changed and do not understand how to respond to establish a connection.	UCCA 1 UCCA 2 UCCA 3 UCCA 4 UCCA 11 UCCA 17 UCCA 18 UCCA 21 UCCA 23 UCCA 27 UCCA 28 UCCA 40 UCCA 41 UCCA 43 UCCA 44

	UCCA 45 UCCA 47
S-5 *Top-level:* Operators' control actions when establishing a connection are unsafe in combination with otherwise adequate tasks provided. **S-5.1** *Inconsistent construction of control algorithms:* Operators attempt to establish a connection when the partner aircraft is out of range. Due to inconsistent training, guidelines, or feedback from host system regarding power capabilities, Operators have a misunderstanding of range capabilities for their system and their partner system given altitude and atmospheric conditions. **S-5.2** *Inconsistent initialization of control algorithms:* Pre-flight mission documents provide GPS waypoints for connection that position aircraft out of range. As a result of these plans and inadequate feedback provided by systems, Operators provide adequate task(s) to command acquisitions, but attempt the connection when they are too far from connecting systems. **S-5.3** *Updates to process models inadequate: C*ontrollers on team receive inadequate updates regarding shared process. **S-5.3.1** *Flawed vertical coordination:* Atmospheric conditions change, requiring aircraft to connect at a different altitude. Communication from AOC to Operators is delayed, inadequate, or missing so Operators fly at an unsuitable altitude when Transmitting/Detecting Beacon. **S-5.4** *Unsafe internal process model:* Operators provide task to Transmit/Detect Beacon in correct direction, but Lasercom System does not execute as tasked because System is not capable of pointing in intended direction: Commanded steering direction is not within field of regard of System given current aircraft heading. No feedback is implemented to communicate to Operators that aircraft is not oriented properly to position connecting terminal within field of regard for steering.	UCCA 4 UCCA 6 UCCA 7 UCCA 9 UCCA 10 UCCA 13 UCCA 14 UCCA 22 UCCA 24 UCCA 25 UCCA 27 UCCA 28 UCCA 39 UCCA 40 UCCA 41 UCCA 43 UCCA 44 UCCA 45 UCCA 46 UCCA 55
S-6 *Top-level:* Operators provide some of the tasks to establish a connection in a way that leads to unsafe sequencing. **S-6.1** *Updates to process models inadequate: C*ontrollers on team receive unsafe updates regarding shared process. **S-6.1.1** *Flawed vertical & lateral coordination:* Operators$_1$ experience a beacon failure and notify AOC of malfunction. They assume that the AOC will notify System$_2$ of operational errors during acquisition and deconflict acquisition roles. However, AOC does not deconflict acquisition roles due to prioritized mission needs or assumptions that aircraft will laterally coordinate. **S-6.2** *Unsafe feedback received from collaborators regarding control actions:* Aircraft$_2$, which is planned for connection, experiences an in-flight emergency/prioritized mission need that diverts Operators$_2$' attention away from establishing a connection. There is no feedback to alert System$_1$ that System$_2$ is not attempting to establish a connection. Thus, System$_1$ continues to Detect Beacon before System$_2$ starts Transmitting Beacon.	UCCA 1 UCCA 2 UCCA 4 UCCA 6 UCCA 9 UCCA 11 UCCA 22 UCCA 24 UCCA 27 UCCA 39 UCCA 40

	UCCA 41 UCCA 43 UCCA 44
<u>S-7</u> *Top-level:* Operators provide adequate task(s) to establish a connection, but Lasercom Sßystems execute them in a way that leads to unsafe sequencing. **<u>S-7.1</u>** *Unsafe feedback received from collaborators regarding control actions:* System$_1$ is configured to wait for X (ex. 3) scans of partner beacon before transmitting a return beam. System$_2$ is configured to scan beacon around cone of uncertainty X times (ex. 5) for acquisitions. System$_1$ detects 2 out of the 5 scans, but does not detect 3rd scan due to atmospheric effects or vibrations. After accomplishing all scans, System$_2$ ends Transmit Beacon in expectation for System$_1$ to transmit a return beam. System$_1$ does not communicate that it has not detected all 3 scans, and System$_2$ does not communicate that is has completed all 5 scans. As a result, System$_2$ ends Transmit Beacon before System$_1$ ends Detect Beacon and before systems start tracking. **<u>S-7.2</u>** *Unsafe feedback received from collaborators regarding controlled process*: System$_1$ Detects Beacon but feedback regarding partner location is inadequate/delayed due to delayed internal processing. As a result, System$_1$ is delayed in transitioning to partner tracking and does not immediately point a return beam towards System$_2$. System$_1$ does not communicate to System$_2$ that it has been illuminated but is experiencing system delays so System$_2$ stops attempting to connect before partner tracking has been initiated. **<u>S-7.3</u>** *Unsafe decision-making:* Systems are designed such that role in acquisition process is determined automatically by connecting lasercom systems. Operators must only provide command to initiate acquisition. Using a pre-determined algorithm/data base of beacon transmitters vs beacon detectors, System Automation$_1$ automatically decides its role in the acquisition process is to Detect Beacon. System$_2$ however has a non-functioning beacon and does not have the capability to Transmit Beacon. System$_2$ does not communicate that it cannot Transmit Beacon so both systems attempt to Detect Beacon and neither Transmit Beacon. **<u>S-7.4</u>** *Dynamic connectivity*: Systems are designed such that their role in the acquisition process or their acquisition sequence type (i.e. symmetric vs. asymmetric sequence) is determined automatically through an RF link and "handshake" protocol. Systems are unable to communicate due to enemy jamming, interfering terrain, inoperable frequencies, etc. so systems do not know role in acquisition process or are unclear regarding acquisition sequence type. Both assume role is to Transmit Beacon. As a result, System$_1$ starts Transmit Beacon before System$_2$ ends Transmit Beacon or starts Detect Beacon and systems do not acquire each other's signal. **<u>S-7.5</u>** *Unsafe internal process model (Machine):* Lasercom System does not point in the correct direction because it does not know its host aircraft's position/orientation/velocity. Host aircraft telemetry data (i.e. INS/GPS/airspeed indicator) is delayed, inadequate, or misinterpreted. Misinterpretation may occur if the INS axis is not appropriately aligned with the host terminal or if subsystems use inconsistent units. As a result, systems do not appropriately point transmitter/receivers when a connection must be established and maintained. **<u>S-7.6</u>** *Unsafe internal process model (Machine):* Lasercom System does not point in the correct direction because it does not know its host aircraft's location/trajectory. Feedback from auto-pilot system is delayed, incorrect, or misinterpreted. Delays may occur if the aircraft diverges unexpectedly from a programmed auto-pilot route.	UCCA 4 UCCA 6 UCCA 9 UCCA 10 UCCA 11 UCCA 24 UCCA 25 UCCA 27 UCCA 28 UCCA 39 UCCA 41 UCCA 42 UCCA 43 UCCA 45

S-8 *Top-level:* Operators' control actions to establish a connection and tasks provided are unsafe in sequencing. **S-8.1** *Unsafe initialization of process models*: Operators do not command System to establish a connection at designated time of connection because Operators cannot adequately identify partner system. Lasercom System identifies partners by having partner terminal send an ID/position beacon that positively identifies them. Systems' identifiers are changed, and the AOC provides inadequate/outdated ID information. As a result, Operators are not able to confirm ID of partner to connect. **S-8.2** *Updates to process models inadequate: C*ontrollers on team receive inadequate updates regarding shared process. **S-8.2.1** *Flawed vertical & lateral coordination:* Systems share inadequate/delayed feedback regarding aircraft route: In first RF transmission, Aircraft$_2$ shares initial autopilot waypoint coordinates. However, Aircraft$_2$ is directed by AOC to deviate from established route, resulting in delays to intended point of connection. System$_2$ and AOC do not communicate changes in route, so System$_1$ starts Transmitting Beacon before System$_2$ is within range to start Detecting Beacon. **S-8.2.2** *Flawed lateral coordination:* Once in area of operations, Systems do not communicate operational status or current mode due to security reasons/mission requirements for brevity on radios. Operators notify partners when they initiate mode changes (i.e. command "warm-up" mode), but do not notify partners when their system fully transitions to intended mode (i.e. standby mode ready for lasing). System$_1$ takes longer than System$_2$ to "warm-up." As a result of varying transition times and lack of communication, Operators$_2$ assume System$_1$ is ready to lase before it is. As a result, they attempt to Detect Beacon before System$_1$ is ready to Transmit Beacon. **S-8.3** *Unsafe internal control due to unsafe control inputs:* Aircraft banks while receiving and establishes a heading/attitude where the angle of arrival of solar waves produces maximum noise at the detector (i.e. the detector is blinded by incoming sunlight). As a result, the system cannot distinguish the transmitted signal from the background light and does not have feedback to detect partner terminal's transmitted beacon (or transmitted comms beam). System thus stops Detecting Beacon (or Tracking and Receiving) before its partner system stops Transmitting Beacon (or Transmitting Data). Operators are provided inadequate feedback regard the LOS sun angle so are unaware that the turn will disrupt data sharing.	UCCA 1 UCCA 2 UCCA 2 UCCA 4 UCCA 7 UCCA 9 UCCA 10 UCCA 11 UCCA 13 UCCA 14 UCCA 22 UCCA 24 UCCA 25 UCCA 28 UCCA 29 UCCA 30 UCCA 35 UCCA 38 UCCA 39 UCCA 40 UCCA 43 UCCA 45 UCCA 46
S-9 *Top-level:* Operators provide adequate task(s) to share data, but Lasercom Systems do not execute task(s) as directed. **S-9.1** *Unsafe feedback received from collaborators regarding shared process:* Operators$_2$ fly at too low of an altitude given the current atmospheric conditions to establish a connection. Operators$_1$ fly at an appropriate altitude to maintain a connection, but the atmospheric density at Aircraft$_2$'s altitude blocks the signal and prevents Aircraft$_2$ from receiving. Aircraft$_1$ has no feedback to recognize that Aircraft$_2$ is not receiving due to atmospheric blockages so continues to transmit even though Aircraft$_2$ does not receive. **S-9.2** *Inconsistent initialization of control algorithms/process models:* Systems do not have congruent clock settings because initialization of clock settings is inconsistent: Regression occurs due to momentary link outage, and systems successfully re-acquire. Upon re-acquiring System$_1$ resets its clock, but System$_2$ does not reset its clock from the initial connection. Thus, the two systems are	UCCA 11 UCCA 12 UCCA 13 UCCA 14 UCCA 15 UCCA 21 UCCA 29 UCCA 30 UCCA 35 UCCA 37

misaligned for their clock recovery settings and do not have time synchronization. As a result, they do not properly Transmit/Receive Data. **S-9.3** *Updates to process models inadequate: C*ontrollers on team receive unsafe updates regarding shared process. **S-9.3.1** *Flawed lateral coordination:* Aircraft enters slightly turbulent air and platform motion/vibration causes pointing and tracking errors that prevent accurate partner tracking. Rate disturbance sensors adequately detect platform jitter and alert Operators, but system does not notify its partner system that it is experiencing disrupting turbulence. As a result, the partner system is unaware that its partner is not appropriately Receiving Data and/or it does not know cause of link outage. The partner system is thus unaware of necessary control actions to re-establish connection or transmit through other means. **S-9.4** *Unsafe predictions/observations:* Systems relies on programmed autopilot waypoints to determine direction for pointing. Aircraft$_2$ broadcasts its programmed GPS waypoints to Aircraft$_1$ to assist in pointing estimations during changes in aircraft attitude and route. However, shared autopilot coordinates are inadequate because operators input flight controls manually and/or GPS is delayed. As a result, Lasercom System$_1$ does not accurately predict Aircraft$_1$'s location and tracks in the wrong direction. **S-9.5** *Unsafe internal process model:* System Automation has incorrect feedback regarding where to point because its tracking sensors (i.e. camera, detector array, etc.) sense LOS errors incorrectly, or sense LOS errors correctly, but are delayed in sending feedback to system automation. As a result of inadequate feedback, System Automation generates incorrect rate commands, leading to inaccurate pointing a reduction in delivered power. **S-9.5.1** *No feedback received:* This may occur if no additional fine-tuning loop such as nutation is implemented to provide feedback on alignment and correct for free drift. **S-9.5.2** *Incorrect feedback received:* This may occur if hostile forces intentionally "blind" the system. **S-9.5.3** *Feedback is misinterpreted:* This may occur is the system uses a bistatic architecture and only one tracking sensor is utilized to provide guidance for pointing the receiver and the transmitter. If the tracking sensor is mounted adjacent to the receiver and separate from the transmitter, feedback may be adequate for the receiver, but not the transmitter. **S-9.6** *Unsafe internal control due to unsafe control inputs:* System Automation receives adequate feedback from tracking sensors and flight control system, but its control inputs to control mechanisms (mirrors, gimbals, or other actuators) are inadequate or delayed. Thus, System does not point in correct direction to maintain partner tracking. **S-9.7** *Unsafe internal control algorithms:* Aircraft$_1$ flies through atmosphere in which it is susceptible to turbulence-induced fading, or scintillation. System$_1$ uses error control coding to mitigate the effects of turbulence-induced fading. However, deterministic models do not accurately predict fading in atmosphere so fading is more severe than expected. As a result, codewords embedded for forward error correction (FEC) are lost in one fade and system does not adequately Receive Data.	UCCA 38 UCCA 45 UCCA 46 UCCA 48 UCCA 49 UCCA 51 UCCA 57 UCCA 62
S-10 *Top-level:* Operators do not provide some of the tasks required for Lasercom Systems to share data. **S-10.1** *Unsafe internal control due to unsafe control path:* Operators$_1$ assume boresight alignment only needs to be accomplished once after takeoff and thus do not check boresight alignment before initiating a new connection. Methods of stabilization (i.e. stabilization loop bandwidth, mounting of angular rate sensors, dampening etc.) do not adequately isolate the sensor and laser from jitter during	UCCA 1 UCCA 2 UCCA 4 UCCA 6

flight. As a result, platform jitter (due to platform maneuvers or external loads such as wind and air-stream induced torque) cause boresight to become misaligned. Feedback to detect jitter and/or alert Operators to misalignment is inadequate. As a result, System does not execute necessary BITs to recalibrate and System cannot appropriately Detect Beacon, Transmit Beacon, and Track Partner terminal. **S-10.2** *Unsafe internal process model:* Rate disturbance sensors erroneously send signals to System Automation indicating platform jitter. As a result,Ssystem notifies Operators that aircraft is flying through turbulent air which would prevent adequate tracking. Operators are flying a UAV so cannot physically feel turbulence. As a result, they do not provide commands to Transmit/Detect Beacon or Transmit/Receive Data when data must be shared for mission purposes and atmosphere is suitable for connections.	UCCA 9 UCCA 11 UCCA 13 UCCA 19 UCCA 22 UCCA 30 UCCA 38 UCCA 57
S-11 *Top-level:* Operators provide some of the tasks to share data in a way that leads to unsafe collective control. **S-11.1** *Inconsistent construction of mental models/process models:* It is assumed in the initial network design that all Systems will operate with the same data rates. However, a partner nation's system or a new system has the capability to operate at various data rates. As a result of established procedures based on the initial assumption, Systems do not communicate their intended transmission parameters and Operators command System to Transmit/Receive at different data rates. **S-11.2** *Unsafe internal control algorithm:* System uses a bistatic architecture to provide isolation between the transmitted and received signals. Due to inadequate training/guidelines/feedback, Operators provide command to boresight the transmitter, but not the receiver. As a result, the tracking sensor is not properly aligned with the receiver and the System points in the correct direction to Transmit Data, but does not point in the correct direction to Receive Data.	UCCA 11 UCCA 12 UCCA 13 UCCA 15 UCCA 29 UCCA 38 UCCA 51 UCCA 59 UCCA 62
S-12 *Top-level:* Operators adequately do not provide certain task(s) when attempting to share data, but some Systems execute them anyways. **S-12.1** *Unsafe initialization of control algorithms/process models:* Operators do not provide command to Transmit/Receive Data at X parameter, but System automatically selects parameter because it believes the partner terminal will use that parameter based on a provided database. The database, however, is outdated so system Transmits/Receives Data at incompatible parameters and Systems do not appropriately share data. **S-12.2** *Updates to process models inadequate:* Operators on team receive inadequate updates regarding shared process. **S-12.2.1** *Flawed lateral coordination:* System automatically initiates boresight alignment due to timing specifications or detection of misalignment. System uses built-in retroreflector to check boresight alignment, so communications are interrupted when built-in test is initiated. There are no procedures/warnings to alert connected systems of BIT processes, so Operators$_1$ do not alert Operators$_2$ or AOC that boresight alignment has been initiated. Thus, Operators$_2$ do not know cause of link outage. **S-12.3** *Unsafe internal control algorithm (machine):* Operators do not command system to establish a connection and share data with a specific system. However, hostile forces broadcast an acquisition beam in an attempt to jam/intercept communications. System automatically detect acquisition beam so attempts to initiate a connection. System design does not include sufficient authorization protocols (i.e. IFF, modulation, etc.) for acquisitions so there is inadequate feedback regarding authorization of connecting terminal. For this reason, the System believes the hostile acquisition beam is transmitted from friendly forces and establishes a connection.	UCCA 8 UCCA 11 UCCA 17 UCCA 19 UCCA 20 UCCA 21 UCCA 29 UCCA 30 UCCA 37 UCCA 38 UCCA 47 UCCA 53 UCCA 56 UCCA 59 UCCA 60 UCCA 62

S-12.4 *Unsafe internal control due to unsafe control path:* Lasercom System$_1$ Receives Data when Operators$_1$ did not provide command to Receive Data and Operators$_2$ did not provide command to Transmit Data. System$_1$ utilizes a monostatic architecture with an aperture that supports both the transmitter and receiver. Aircraft$_1$ flies into clouds that reflect Lasercom System$_1$'s transmitted signal back into its aperture. Because the System has an inadequate means of isolation, it interprets the reflected signal as a signal transmitted from its partner rather than from its own terminal. Thus, the signal is not fully transmitted to the System$_2$ and Operators$_1$ believe they are Receiving Data from Lasercom System$_2$ when it did not Transmit Data.	
S-13 *Top-level:* Operators' control actions when sharing data are unsafe in combination with otherwise adequate tasks provided. **S-13.1** *Unsafe initialization of process models/control algorithms:* Airspace Control Order (ACO) does not provide adequate altitude guidance for designated mission. For this reason, Operators$_2$ fly at too low of an altitude given the current atmospheric conditions to appropriately Transmit/Receive Data. **S-13.2** *Updates to process models unsafe:* Operators on team receive unsafe updates regarding shared process. **S-13.2.1** *Flawed lateral coordination:* Operators exceed connection range when sharing data. Operators misinterpret shared waypoints from partner system: Format for communicating aircraft intentions when connecting is not standardized across AF squadrons, operational areas, military branches, or national allies. For this reason, operators do not know correct waypoints to fly to not exceed range limitations. **S-13.3** *Unsafe observations/predictions:* Due to atmospheric effects or turbulence, the optical link is broken. Systems rely on Kalman filter for trajectory prediction in cases of link outage. Kinematic models assume that aircraft will maintain constant trajectory during connection. Aircraft$_2$ however banks or makes an unexpected maneuver during time of outage so System points in the wrong direction when attempting to re-establish the link. **S-13.4** *Unsafe internal process model (human):* Operators exceed connection range when sharing data because they misinterpret the feedback provided by their own system. Aircraft$_1$ approaches maximum range for connection given transmission power. Power constraints are set too tightly on warning system so Operators$_1$ are frequently alerted that System is approaching power limits and they frequently ignore alarms. As a result, they accidently exceed the maximum range on a day with higher atmospheric density. **S-13.5** *Unsafe internal control due to unsafe control input:* Operators$_2$ are given instruction by the AOC to descend to an altitude 1000 ft lower. Due to the increase in range combined with the higher atmospheric density, System$_1$'s power received is reduced to a level below acceptable limits for connection. The connection is thus broken and Lasercom System$_1$ cannot Receive Data.	UCCA 11 UCCA 13 UCCA 14 UCCA 19 UCCA 29 UCCA 30 UCCA 32 UCCA 33 UCCA 37 UCCA 38 UCCA 45 UCCA 46 UCCA 48 UCCA 49 UCCA 51 UCCA 52 UCCA 57 UCCA 60 UCCA 62
S-14 *Top-level:* Operators provide some of the tasks to share data in a way that leads to unsafe sequencing. **S-14.1** *Inconsistent initialization of control algorithms:* Due to inadequate information provided in pre-flight mission documents and inadequate feedback sent from partner systems, Operators are unaware that their partner system is not full duplex (cannot Transmit and Receive Data at the same time). As a result, Operators command Transmit Data while their partner system is Transmitting Data and their partner system does not Receive Data. **S-14.2** *Updates to process models inadequate: C*ontrollers on team receive inadequate updates regarding shared process.	UCCA 15 UCCA 18 UCCA 20 UCCA 21 UCCA 35 UCCA 37 UCCA 38

S-14.2.1 *Flawed lateral & vertical coordination (communication):* Lasercom System$_1$ has a bistatic design and has the ability to Transmit/Receive Data at the same modulation, while Lasercom System$_2$ has a monostatic design and must Transmit/Receive Data at different frequencies. Connecting Operators and/or AOC does not communicate that System$_2$ is monostatic. Operators$_1$ thus assume their partner system has the same capabilities, so they use the same modulation for transmission/reception. Thus, System$_2$ does not Receive Data when the same modulation is used. **S-14.3** *Flawed observations*: Operators$_2$ send specific data over RF links to conduct required system tests. Operators$_1$ misinterpret Operators$_2$ actions as a cue to end laser communications entirely and transmit solely through RF links. Operators do not adequately communicate intentions for continuing laser communications so Operators$_1$ transition to RF communications entirely and end data sharing before full data set is shared. **S-14.4** *Dynamic connectivity:* The AOC provides new transmission parameters to both Operators$_1$ and Operators$_2$, but Operators$_2$ do not receive new parameters because the communication channel is inadequate (due to fading, jamming from hostile forces, misconfigured TDLs, etc.). As a result, Operators$_2$ do not configure System to Receive Data at frequency transmitted by System$_1$. Because data cannot be appropriately received, System$_1$ ends Receive Data before entire data set is transmitted. **S-14.5** *Unsafe control due to unsafe control input:* System is designed with a monostatic architecture and utilizes modulation to isolate transmitted and received signals when transmitting and receiving simultaneously. System$_2$ is configured by Operators$_2$ to transmit and receive at the same modulation so it cannot isolate its transmitted signal from the received signal. Operators are not provided adequate training/feedback regarding requirements for modulation. As a result, system does not receive data.	UCCA 50 UCCA 51 UCCA 58 UCCA 61 UCCA 62
S-15 *Top-level:* Operators provide adequate task(s) to share data, but Lasercom Systems execute them in a way that leads to unsafe sequencing. **S-15.1** *Unsafe feedback received from collaborators regarding shared process:* A short outage occurs causing several packets of data to be lost. Systems are consistently configured for FEC and interleaving. System$_1$ thus detects that data is missing. However, System$_1$ does not request a packet retransmission from System$_2$ because Systems are not able to communicate directly through RF links (incompatible links, enemy jamming, etc.). **S-15.2** *Unsafe feedback received from collaborators regarding control actions:* System is designed with a monostatic architecture and utilizes polarization-multiplexing to isolate transmitted and received signals. Systems do not communicate intentions for polarization when Transmitting/Receiving Data. As a result, Systems use wrong polarization and do not Transmit/Receive Data properly. **S-15.3** *Inconsistent initialization of control algorithms:* A short outage occurs causing several packets of data to be lost. Feedback regarding transmitted data is missing/inadequate because Systems are not configured consistently for FEC or interleaving (i.e. feedback regarding transmitted data is missing/inadequate). This may occur if System$_1$ is not configured to use interleaving at the same time period intervals as System$_2$. Thus, System$_2$ does not appropriately Receive Data and stops Receiving Data. **S-15.4** *Updates to process models inadequate: C*ontrollers on team receive unsafe updates regarding shared process. **S-15.4.1** *Flawed lateral coordination:* Lasercom System does not know where to point because its partner does not adequately communicate its INS/GPS data: The partner system transmits its raw INS and GPS data through the optical link once connection	UCCA 11 UCCA 15 UCCA 29 UCCA 30 UCCA 35 UCCA 38 UCCA 45 UCCA 46 UCCA 48 UCCA 49 UCCA 51 UCCA 52 UCCA 57 UCCA 58 UCCA 60 UCCA 61

is established. Due to atmospheric effects or turbulence, the optical link is broken. The partner system does not appropriately transition to RF to share INS and GPS data to re-establish a link so systems cannot transition to acquisitions. **S-15.5** *Unsafe observations/predictions*: Aircraft establish a heading and velocity such that a point-ahead angle and open-loop tracking is required. System Automation does not adequately recognize that point-ahead angle is required so does not appropriately transition to open-loop tracking. Or System does not accurately calculate required point-ahead angle. As a result, System points in the incorrect direction and ends Partner Tracking before entire data set is shared. **S-15.6** *Unsafe internal control algorithm (Machine):* Throughout flight, the alignment between the tracking sensor and communication receiver drifts, so feedback of incoming light in misinterpreted. Wideband nutation is used to correct co-alignment, but the control algorithm for nutation is not configured to adequately correct for the drift. This may occur if the nutation tracker is not able to appropriately calculate received power due to atmospheric scintillation. As a result of the misalignment, System continues to misinterpret feedback from the tracking sensor, and Transmits Data in the wrong direction. **S-15.7** *Unsafe internal process model (Machine):* Lasercom System does not Transmit Data with the correct power because it does not know its host aircraft's altitude. Aircraft descends after establishing a link, but feedback from the host aircraft altimeter is delayed or inadequate. As a result of inadequate power, System ends Receive Data. **S-15.8** *Unsafe internal process model (Machine):* Lasercom systems end Transmit/Detect Beacon or Transmit/Receive Data because System believes host aircraft is on the ground. Feedback from Weight on Wheels (WOW) Sensor is erroneously sent after takeoff. So Lasercom System Automation prohibits laser beaming to avoid physical harm to personnel.	UCCA 62
S-16 *Top-level:* Operators' control actions when sharing data and tasks provided are unsafe in sequencing. **S-16.1** *Unsafe feedback received from collaborators regarding controlled process*: System Automation$_1$ is not designed to handle the Doppler Shift experienced due to the heading and velocities of the two aircraft. For this reason, System Automation$_1$ believes the connection has been lost when it does not receive a wavelength within a given range. It thus regresses and ends Receive Data. System$_1$ does not inform System$_2$ that it has stopped receiving due to unexpected wavelength so System$_2$ continues to Transmit Data in a futile effort. **S-16.2** *Inconsistent construction of control algorithms:* Kinematic models used for pointing are configured with different assumptions regarding how aircraft will fly (angular/linear accelerations). Operators$_1$ perform a maneuver that disrupts their partner's ability to track. They believe their partner's PAT system can handle such a maneuver because their own PAT system can account for such maneuvers and there is no system indication that such a maneuver will disrupt tracking. There is also no standardization in training across operational platforms with different lasercom systems, so Operators$_1$ are not aware that such maneuvers will disrupt tracking for partner systems. **S-16.3** *Updates to process models inadequate: C*ontrollers on team receive unsafe updates regarding shared process. **S-16.3.1** *Flawed lateral coordination (communication)*: Operators bank aircraft such that the connection is broken due to exceedances in maximum steering rate, inadequate terminal field of regard, or wing blockage. Operators are adequately alerted to exceedance and broken connection but do not adequately communicate to partner system reasoning for connection disruption. As	UCCA 11 UCCA 12 UCCA 13 UCCA 14 UCCA 15 UCCA 16 UCCA 19 UCCA 21 UCCA 29 UCCA 30 UCCA 31 UCCA 35 UCCA 37 UCCA 38 UCCA 45 UCCA 46

a result, partner system Operators does not know why connection has been broken and do not input appropriate commands to reconnect. **S-16.3.2** *Flawed lateral coordination (communication)*: Operators bank aircraft to establish a new heading. INS/GPS data is delayed/inadequate so System$_2$ does not know where to point to maintain connection. **S-16.4** *Unsafe internal control due to inadequate control algorithm (human-machine):* Operators input flight controls that disrupt their own system's ability to track: System$_1$ does not have capability to maintain tracking under specific angular rate/accelerations due to physical limitations or processing power limitations. Operators are not aware of these angular rate/acceleration limits due to inadequate training or guidelines. As a result, Operators bank aircraft such that the Lasercom System's maximum steering rate is exceeded and System does not Transmit Data in the correct direction. **S-16.5** *Unsafe internal control due to unsafe control input:* Operators are not aware of angular rate/acceleration limits due to inadequate feedback provided by System. As a result, Operators bank aircraft such that the Lasercom System's maximum steering rate is exceeded and System does not Transmit Data in the correct direction. System does not alert Operators that connection has been broken due to exceedances in turning limits, so Operators do not know why connection has been broken. **S-16.6** *Unsafe internal process model:* Operators input flight controls that disrupt their own System's ability to track. Operators bank Aircraft$_1$ such that the wing blocks the line of sight (LOS) between the two terminals. No feedback is provided to Operators alerting them to signal disruptions due to aircraft attitude. As a result, Operators continue to fly such that LOS is broken and Systems are not able to continue Partner Tracking. **S-16.7** *Unsafe internal control due to unsafe control path:* Operators$_1$ provide command to stop Transmitting Data before Lasercom System$_2$ receives full data set because Operators$_1$ believe data is not being transmitted appropriately. Communications are being adequately transmitted, but alert for boresight alignment is set to appear every X amount of time. Operators$_1$ receive message that boresight alignment needs to be checked, and assume communications are not being transmitted properly or are complete. Thus, Operators$_1$ enable built-in tests to check boresight alignment. System uses built-in retroreflector to check boresight alignment, so communications are interrupted when built-in tests are initiated.	UCCA 48 UCCA 49 UCCA 51 UCCA 52 UCCA 56 UCCA 57 UCCA 58 UCCA 59 UCCA 60 UCCA 62

Appendix C: System Recommendations

Listed in the table below are the recommendations generated from the analysis. Each recommendation is associated with a collaborative control dynamic or internal control factor, as designated by the acronyms below.

CA: Cognitive Alignment
MC: Mutually Closing Loops
LC: Lateral Coordination

DH: Dynamic Hierarchy
DA: Dynamic Authority
SA: Shared Authority
IC: Internal Control

DM: Dynamic Membership
DC: Dynamic Connectivity
TA: Transfer of Authority

Table C-1: System Recommendations

Rec. ID	Recommendation	Control Dynamic
SC-1	***Construction of process models/control algorithms:*** **System automation for all systems must be configured with consistent control algorithms regarding PAT and transmissions.**	CA, DM, MC, DA, DC, LC, SA, TA
SC-1.1	System automation must be constructed with consistent control algorithms regarding sequencing and timing of control actions including acquisitions, regression, transmissions, and transitioning from/to other RF TDLs.	CA, TA, LC, SA, DA
SC-1.1.1	Systems must be constructed with consistent acquisition sequences and scan patterns.	CA, LC, DA, SA, TA
SC-1.1.2	Systems must have matching acquisition control algorithms (i.e. thresholds for time to acquire) so that both end Transmit/Detect Beacon command at the same time if tracking has not been initiated after specified amount of time.	CA, LC, DA, SA, TA
SC-1.1.3	System commanded to Detect Beacon must transmit a return tracking beam towards direction of incoming beacon beam once beacon beam has been detected (initiate open-loop coarse tracking).	CA, LC, TA
SC-1.1.4	Systems must appropriately transition from open-loop coarse tracking to fine-tracking once beacon beam has been detected and return tracking beam has been detected.	CA, LC, TA
SC-1.1.5	Systems must appropriately initiate Transmit/Receive Data once connection is established and Partner Tracking has been initiated.	CA, LC, TA, SA, DA
SC-1.1.6	Systems must appropriately end Transmit/Receive Data once full data set has been transmitted and received.	CA, DM, DC, LC
SC-1.1.7	If connection is lost and power received drops below specified threshold for specified amount of time, both systems must appropriately regress from fine-tracking to open-loop coarse tracking to re-acquire and re-establish connection.	CA, MC, DC, LC, SA
SC-1.1.8	Systems must have matching thresholds for power received and duration of outage to initiate regression.	CA, DC, LC, SA

SC-1.2	System automation must be constructed with consistent control algorithms regarding requirements for shared state/status information.	CA, DM, MC, LC
SC-1.3	System automation must be constructed with consistent kinematic models for aircraft motion.	CA, LC
SC-1.4	Process models regarding partner transmission capabilities must be consistent across all systems.	CA, DM, MC, LC
SC-1.4.1	Process models regarding partner range capabilities must be consistent across all systems.	CA, DM, DA, LC
SC-1.5	Systems must be configured with consistent control algorithms for boresight calibration (ex. use of flip-in retroreflectors vs. nutation).	CA, DM, MC, DA, LC,
SC-2	***Construction of process models/control algorithms:* Operators must be provided consistent training and standard operating procedures.**	CA, DH, DM, MC, DA, DC, SA, TA, IC
SC-2.1	Operators must be provided consisting training and standard operating procedures for controlling individual Systems.	CA, IC
SC-2.1.1	Operators must understand how to input necessary control actions including pre-flight calibrations and other functions of Systems.	CA, IC
SC-2.1.2	Operators must be able to interpret and appropriately respond to feedback provided by Lasercom Systems.	CA, IC
SC-2.2	Operators must have consistent expectations for how the AOC will provide guidance (i.e. providing aircraft waypoint guidance, connection scheduling, partners for connection, connection parameters, etc.).	CA, DM, IC
SC-2.3	Operators must have consistent understandings of responsibilities associated with specified roles in the connection process.	CA, DH, DM, MC, DA, LC, SA, TA
SC-2.4	Operators must have consistent understandings of sequencing and timing control actions including acquisitions, regression, and transitioning from/to other RF TDLs.	CA, LC, SA
SC-2.5	Operators must have consistent control algorithms for acceptable/expected flight maneuvers during connection.	CA, MC, DC, LC, SA, IC
SC-2.6	Operators must have consistent communication/coordination protocols.	CA, DM, MC, DC, LC
SC-2.6.1	Coordination protocols should specify timing and content of communications.	CA, DM, MC, LC
SC-2.6.2	Coordination protocols should specify necessary “check-ins” to verify system state and intentions.	CA, DM, MC, LC
SC-2.6.3	Coordination protocols should specify necessary feedback Systems must provide to partners when expected control actions cannot be performed.	CA, DM, MC, DC, LC
SC-3	***Initialization of process models/control algorithms (machines):* Systems must be consistently initialized when establishing and maintaining a connection.**	CA, DM, MC, DC, LC, SA, TA, IC
SC-3.1	Communication systems, other than lasercom, must be initialized with consistent frequencies and authorization protocols (i.e. IFF, modulations types, etc.).	CA, DM, MC, DC, LC, SA

SC-3.2	Systems must be initialized with matching technical parameters for acquisition and optical communication links (frequencies, data rates, modulation, etc.).	CA, DM, MC, DC, LC, SA
SC-3.3	Systems must be synchronized regarding timing and sequencing of control actions.	CA, MC, DC, LC
SC-3.3.1	“Time-to-acquire” must be initialized consistently across systems once systems initiate acquisitions.	CA, MC, DC, LC
SC-3.3.2	System clocks must be initialized consistently such that they are synchronized during transmissions.	CA, MC, DC, LC
SC-3.3.3	System clocks must be initialized consistently after regression.	CA, MC, DC, LC
SC-4	***Initialization of process models/control algorithms (humans):*** **AOC must provide unambiguous, consistent plans for connection to all systems involved.**	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-4.1	Plans must specify technical parameters for acquisition and optical communication links (frequencies, data rates, modulation, etc.).	CA, DM, MC, LC, SA
SC-4.1.1	The AOC must not direct a system to establish a connection that is not capable of providing necessary parameters to connect with a partner system.	DM, DA, DC, TA
SC-4.1.2	The AOC must not provide technical parameters that a system is not capable of providing if the system is capable of providing other technical parameters that would allow for connection with a partner system.	DM, DA, DC, TA
SC-4.2	Plans must specify various roles in acquisition and communications processes.	CA, DH, DM, DA, LC, SA, TA
SC-4.2.1	Plans must direct one system to Transmit Beacon and one system to Detect Beacon at the same acquisition parameters if systems require an asymmetric acquisition sequence.	CA, DM, DA, DC, LC
SC-4.2.2	Plans must direct both systems to Transmit Beacon at the same acquisition parameters if systems require a symmetric acquisition sequence.	CA, DM, DA, DC, LC, SA
SC-4.3	Plans must specify data to be transmitted/received.	CA, DM, LC
SC-4.4	Plans must specify location and timing of connections.	CA, DM, LC, SA
SC-4.5	Plans must specify identifiers for connection partners.	CA, DM, DC, LC
SC-4.6	Plans must specify technical parameters for other RF links used to share state/status information.	CA, DM, DC, LC
SC-4.7	Plans must specify protocols to manage failures to connect or losses of connection for optical links.	CA, DM, MC, DC, LC, SA
SC-4.7.1	Plans must specify duration of time operators continue operations before transitioning to contingency plans.	CA, DA, DC, LC, SA
SC-4.7.2	Plans must specify alternative tactical data links to use for connection.	CA, DC, LC, SA
SC-4.7.3	Plans must specify reporting requirements for failures to connect or losses of connection.	CA, MC, DC, LC, SA
SC-4.8	Plans must specify protocols to manage losses of connection for RF links.	CA, DH, DC, MC, LC

SC-4.8.1	Protocols must specify alternate communication methods for data to be transmitted (other TDLs, data relays through other systems, etc.).	CA, MC, DC, LC, SA
SC-5	***Updates (Vertical Coordination):*** **The AOC and/or team leadership must be able to provide updates to operators in a consistent, unambiguous, and timely manner.**	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-5.1	Systems must have sufficient bandwidth in RF comms with AOC to support lasercom connections.	CA, DM, MC, DC
SC-5.2	The AOC and/or team leadership must provide commands or operational updates in a consistent, unambiguous, and timely manner that leads to safe execution of mission objectives.	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-5.2.1	AOC must consistently provide information regarding operational environment (status of other aircraft, atmospheric conditions, status of operations, etc.).	CA, DC, LC, SA, TA, IC
SC-5.2.2	The AOC must command operators to provide control actions achieving higher priority mission objectives (i.e. flying at a specific altitude and speed to reach a target location) before commanding control actions to achieve lower priority objectives (i.e. flying at a specific altitude and speed to establish and maintain a lasercom link).	CA, DC, DA, LC, SA, TA
SC-5.2.3	The AOC must not command operators to provide control actions achieving lower priority objectives (i.e. flying a route to establish and maintain a lasercom link) if they conflict with them providing control actions to achieve higher priority objectives (i.e. maintaining safe flight, reaching a target location, etc.).	CA, DC, DA, LC, SA, TA
SC-5.2.4	The AOC must not direct a system to establish a lasercom connection that is not capable of providing the necessary control actions to connect if other means of communications (TDLs, data relays through other systems, etc.) are viable and acceptable.	CA, DM, DA, DC, LC, SA, TA, IC
SC-5.3	Systems must provide feedback to AOC regarding status of operations and health of systems.	CA, MC, DA, DC, IC
SC-5.3.1	Systems must consistently provide feedback to AOC regarding status of systems (i.e. aircraft position, connection status, terminal health, etc.).	CA, MC, DA, DC, IC
SC-5.4	Operators must provide feedback to higher ranking controller or AOC if the commands they receive are not appropriately specified or directed.	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-5.4.1	Operators must provide feedback if their systems are incapable of providing control actions at specified technical parameters.	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-5.4.2	Operators must provide feedback if the atmospheric conditions prevent the control actions from effectively being provided.	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-5.4.3	Operators must provide feedback if the direction in which they are directed to point is incorrect/infeasible.	CA, MC, DA, LC
SC-5.4.4	Operators must provide feedback if connections are unable to be established with commands provided due to unknown reasons.	CA, MC, DA, DC, LC, SA, TA, IC
SC-5.5	Systems must consistently provide feedback to AOC regarding operational environment (i.e. atmospheric conditions, status of operations, etc.) upon request by AOC.	CA, MC, DA, DC, LC, SA, TA, IC

SC-6	***Updates (Lateral Coordination):* Connecting systems must be able to coordinate connections and share necessary state information directly in near-real time.**	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-6.1	Systems' tactical data links must be configured in compatible manners such that partner systems are capable of communicating directly.	CA, DH, DM, MC, DA, DC, LC, SA, TA
SC-6.1.1	If systems RF/TDL systems are unable to connect or maintain connection, system operators must report communication issues to AOC.	CA, DM, DC, LC, SA
SC-6.2	Communication channels used to support coordination of lasercom connections must have sufficient bandwidth to support coordination messages.	CA, DM, MC, DC, LC, SA, TA
SC-6.3	Communication channels used to support coordination of lasercom connections must be able to overcome atmospheric degradation (i.e. fading and interference).	CA, DM, MC, DC, LC, SA, TA
SC-6.4	Communication channels used to support coordination of lasercom connections must be resilient against interception.	CA, DM, MC, DC, LC, SA, TA
SC-6.5	Operators must have semantic alignment regarding exchange of lasercom information and control action updates.	CA, DH, DM, MC, DA, LC, SA, TA
SC-6.6	Lasercom systems automatically transmitting updates must have semantic alignment regarding exchange of lasercom information and control action updates.	CA, DH, DM, MC, DA, LC, SA, TA
SC-6.6.1	Systems must have standardized message formats for communicating critical lasercom state information.	CA, DM, MC, LC
SC-6.6.2	Systems must not misinterpret shared INS/IMU data or GPS data.	CA, DM, MC, LC
SC-6.7	Operators responsible for allocating control actions to other operators in the system must be consistent in how tasks are assigned and prioritized by commanded aircraft.	CA, DH, DM, MC, DA, LC, SA, TA
SC-6.7.1	Operators responsible for allocating control actions for acquisition must unambiguously assign aircraft to Transmit/Detect Beacon.	CA, DH, DM, MC, DA, LC, SA, TA
SC-6.8	Systems' must be able to determine if aircraft geometry will block signal.	CA, LC, SA, TA, IC
SC-6.8.1	Systems must share relevant information regarding aircraft geometry or changes in aircraft geometry.	CA, MC, LC, SA
SC-6.9	Systems must share relevant information regarding aircraft state (position, attitude, heading, airspeed, etc.) in time to establish and maintain tracking.	CA, DM, MC, DA, DC, LC, SA, TA
SC-6.9.1	Systems must be able to determine partner aircraft's position and state from shared data.	CA, DM, MC, LC
SC-6.9.2	Systems must be able to determine partner aircraft's range from shared data.	CA, DM, MC, LC
SC-6.9.3	Systems must be able to adjust transmitted power based on partner aircraft's range.	CA, MC, LC, IC
SC-6.9.4	Systems must be able to determine if environment between aircraft will block signal (i.e. terrain, atmosphere, etc.).	CA, MC, DA, DC, LC, SA, TA, IC
SC-6.9.5	If state information provided is unsafe (delayed, incorrect, incomplete, etc.), systems must be able to recognize unsafe information and report it to provider.	CA, DM, MC, DA, DC, LC, SA

SC-6.10	Systems must coordinate such that they are positioned within unobstructed line-of-sight.	CA, DM, MC, LC
SC-6.11	Systems must coordinate sequencing and timing of acquisitions.	CA, MC, LC, SA, TA
SC-6.11.1	Multiple systems must not provide the same control action (Transmit Beacon vs. Detect Beacon, Transmit Data vs. Receive Data) if that leads to ineffective acquisitions/communications.	CA, MC, DA, DC, LC, SA, TA
SC-6.11.2	Systems must provide updates when they arrive at specified location for connection.	CA, MC, LC, SA
SC-6.12	Systems must be capable of detecting and analyzing optical signal transmitted by partner system to establish and maintain partner tracking.	CA, DM, MC, DC, LC, SA, TA
SC-6.13	If one of the systems is unable to provide its planned control actions, it must inform its partner system such that its partner does not provide its dependent control actions.	CA, MC, DA, DC, LC, SA, TA, IC
SC-6.13.1	Systems must report any dysfunctional subsystems to their partner system.	CA, MC, LC, IC
SC-6.13.2	If all subsystems are functioning as designed and system can detect reasoning for failed control action execution (i.e. inaccurate pointing, platform jitter, atmospheric distortions), systems must report reasoning to partner system.	CA, MC, DC, LC, IC
SC-6.13.3	If a system continues to be unable to provide its assigned control actions, systems should coordinate to either transfer responsibilities or alter the mission profile, prioritizing mission objectives appropriately.	CA, DH, MC, DA, DC, LC, SA, TA
SC-7	***Updates (Predictions)*: Connecting systems must be able to accurately predict partner aircraft location and motion.**	CA, DM, MC, DC, LC
SC-7.1	Systems must be able to detect partner's relative velocity projection. *Consider:* Use Doppler Shift of optical signal to estimate partner's relative velocity projection.	CA, LC
SC-7.2	Systems must share information that assists partner systems in predictions of aircraft state.	CA, DM, MC, LC
SC-7.2.1	*Consider*: Share programmed autopilot coordinates to assist in predictions of aircraft trajectory.	CA, DM, MC, LC
SC-7.3	Limits must be established for aircraft maneuvers (i.e. linear and angular accelerations) during connection.	CA, DM, LC, SA, IC
SC-7.4	Pointing estimation algorithms must provide accurate calculations of partner aircraft trajectory.	CA, SA, IC
SC-8	***Decision-making:* Collective decision-making of controllers must provide adequate, real-time solutions for connection issues.**	CA, DH, MC, DA, DC, LC, SA, TA, IC
SC-8.1	Systems must consistently decide when connectivity will be unachievable/unsustainable given specific environmental factors, aircraft states, or relation between aircraft.	CA, DH, MC, DA, DC, LC, SA, TA, IC
SC-8.2	Systems must have consistent models of mission objectives and ROEs when deciding solutions.	CA, DC, LC, SA
SC-8.3	Systems must be able to coordinate and decide when to postpone lasercom connections.	CA, MC, DC, LC
SC-8.4	Systems must be able to coordinate and decide when to change location of connection.	CA, MC, DC, LC
SC-8.5	Systems must be able to coordinate and decide when to rely on other TDLs for communication.	CA, MC, DC, LC
SC-9	***Closing-the-loop Regarding Control Actions:* Systems must communicate information regarding commanded control action(s) that partner systems would not otherwise have access to (i.e.**	CA, MC, DA, DC, LC, SA, TA

	acquisition, regression, status of transmissions, etc.). Partner systems must be able to adequately receive and interpret shared feedback.	
SC-9.1	Systems must provide feedback to partner system regarding input control actions for acquisitions.	CA, MC, LC, SA
SC-9.1.1	System providing Transmit Beacon must inform partner system that it has initiated acquisitions so that partner system has consistent process model regarding time-to-acquire.	CA, MC, LC
SC-9.1.2	System providing Detect Beacon must verify with partner system that it has initiated Detect Beacon.	CA, MC, LC
SC-9.1.3	If a system ends Transmit/Detect Beacon before time to acquire expires and before connection has been established, it must communicate to partner system that it has stopped providing expected control action.	CA, MC, LC
SC-9.2	Systems must provide feedback to partner system regarding regression.	CA, MC, LC, SA, TA
SC-9.2.1	If a system stops Tracking Partner and regresses to Transmit/Detect Beacon, it must inform its partner.	CA, MC, LC, SA
SC-9.2.2	If a system regresses, it must provide any information relevant to the state of the regressed terminal.	CA, MC, LC, SA
SC-9.2.3	Systems connecting to a regressed system should acknowledge notification of regression and should regress to transmit/detect beacon as necessary to re-aqcuire.	CA, MC, LC, SA
SC-9.3	Systems must not misinterpret feedback provided by a partner system as a need to provide a control action that is not necessary or to *not* provide a control action that *is* necessary (i.e. Transmitting Beacon vs. Detecting Beacon, not provide Transmit or Receive data command, etc.).	CA, MC, DA, DC, LC, SA, TA
SC-10	***Closing-the-loop Regarding Controlled Process:* Systems must communicate information regarding the optical signal that partner systems would not otherwise have access to. Partner systems must be able to adequately receive and interpret shared feedback.**	CA, MC, DA, DC, LC, SA, TA, IC
SC-10.1	System Transmitting Data must provide feedback to system Receiving Data once full data set has been transmitted.	CA, MC, LC, SA
SC-10.2	System Receiving Data must provide feedback to system Transmitting Data once full data set has been received.	CA, MC, LC, SA
SC-10.3	Systems must be able to detect when data has been lost or distorted during transmission: Redundancy must be added to encoded data to provide feedback regarding errors present in transmissions (i.e. FEC & Interleaving).	CA, MC, DC, LC, SA, IC
SC-10.3.1	Systems Receiving Data must communicate to system Transmitting Data when data has been lost or distorted.	CA, MC, DC, LC, SA
SC-11	***Dynamic Membership & Connectivity:* Systems must be able to detect, identify, and track other systems that are available and capable of establishing a lasercom connection.**	CA, DH, DM, MC, DA, DC, LC, SA
SC-11.1	Systems must not allow unintended or unauthorized partners to connect.	CA, DM, DC, LC
SC-11.1.1	Systems must be able to determine if another system is the intended partner using provided identifiers.	CA, DM, DC, LC
SC-11.1.2	Systems must be able to determine if another system is authorized to connect.	CA, DM, DC, LC

	Consider: Use authentication protocols such as IFF modes, encryption, or specific modulation schemes to verify authorization.	
SC-11.2	Systems must be able to determine another system’s status and availability before connecting.	DM, MC, DC, LC
SC-11.2.1	Systems must provide updates to other systems regarding terminal status and availability for connections.	CA, DM, MC, LC
SC-11.3	Systems must be able to determine if another system is capable of Transmitting/Receiving Data at compatible parameters.	CA, DM, DC, LC, SA, TA
SC-11.4	Systems must be able to determine if another system is within range to connect.	CA, DM, MC, LC
SC-11.4.1	Standard operating procedures/control algorithms must specify maximum ranges for connection given atmospheric conditions.	CA, DM, MC, LC
SC-11.4.2	Systems must be able to directly detect if a partner system is within range. *Consider:* Equip systems with radar/LADAR sensors to detect partner systems’ range and direction.	CA, DM, IC
SC-11.5	Systems must be able to determine if a partner system is within unobstructed line-of-sight.	CA, DM, DC, LC
SC-11.5.1	Systems must be able to determine if the environment between the terminals (i.e. terrain, atmosphere, etc.) will block the signal.	CA, DM, DC, LC
SC-11.6	If systems cannot identify and track systems directly in the network, AOC must provide information regarding identity and status of local systems.	CA, DM, DC
SC-11.6.1	The AOC must be able to provide updates regarding location and availability of partner systems.	CA, DM, DC
SC-11.6.2	The AOC must be able to provide information regarding capabilities of local systems.	CA, DM, DC
SC-11.6.3	AOC must be able to accurately identify and track systems in the network or attempting to join the network.	CA, DM, DC
SC-11.6.4	AOC must assign unique identifier to each aircraft in the system.	CA, DM, DC
SC-12	**System automation must be able to point optics in correct direction to establish and maintain lasercom connections.**	CA, DM, MC, DA, DC, LC, SA, TA, IC
SC-12.1	System must be able to detect direction of incoming signal.	IC
SC-12.1.1	Sensors must have resolution fine enough to determine precise direction of incoming signal.	IC
SC-12.1.2	Systems must be able to isolate transmitted & received signal from other forms of light (i.e. not mistake background light or own transmitted signal as signal transmitted by partners). *Consider:* Use bistatic architecture, different wavelengths, narrowband optical filter, or different polarization states as means of isolation.	IC
SC-12.2	System must be able to accurately calculate pointing direction of optics based on detected signal and information shared by partner.	MC, LC, SA, IC
SC-12.2.1	System must be able to recognize when a “point-ahead” angle is necessary to maintain a connection.	MC, LC, SA, IC
SC-12.3	System must be able to point optics in direction intended by automated controller.	IC

SC-12.3.1	Atmospheric environment (i.e. temperature, turbulence & platform jitter) must not degrade systems' ability to point in correct direction. Systems must be able to withstand shock, vibration, and thermal variations of operational environment.	IC
SC-12.3.2	Systems must be able to detect if receiver and transmitter are not aligned with detector (i.e. boresight alignment is needed).	IC
SC-12.3.3	Systems must be able to correct any misalignments and perform any other necessary calibrations in flight. *Consider:* Use built-in tests (bits) and/or nutation to provide boresight alignment in flight.	IC
SC-12.3.4	Maintenance protocols should provide routine inspections and calibrations to ensure boresight alignment before operations.	IC
SC-13	**Controllers must understand necessary and acceptable flight control inputs to achieve mission objectives.**	CA, DM, MC, DA, DC, LC, SA, IC
SC-13.1	Operators must not fly aircraft in hazardous ways in order to achieve objective of establishing and maintaining a lasercom link.	CA, LC, SA, IC
SC-13.2	Operators must not fly aircraft in ways that disrupt tracking unless higher objectives compel them to (mission objectives, maintaining safe flight, environmental factors, etc.).	CA, DM, LC, SA, IC
SC-13.3	Standard operating procedures/control algorithms must provide guidance on necessary and/or acceptable flight control inputs when establishing and maintaining connection.	CA, DM, SA, IC
SC-13.3.1	Standard operating procedures/control algorithms must specify limits for aircraft attitude (pitch and bank angle).	CA, DM, SA, IC
SC-13.3.2	Standard operating procedures/control algorithms must specify limits for aircraft angular acceleration (i.e. roll rate & pitch rate).	CA, DM, SA, IC
SC-14	**Systems must be able to detect when host aircraft is not positioned appropriately to establish and maintain a lasercom connection.**	CA, MC, DC, LC, SA, IC
SC-14.1	Systems must be able to determine host aircraft's location and orientation.	IC
SC-14.2	Systems must be able to detect when atmospheric conditions are unsuitable for connections.	CA, MC, LC, SA, IC
SC-14.2.1	Standard operating procedures/control algorithms must specify minimum altitude given atmospheric conditions and range of connection.	CA, LC, SA, IC
SC-14.2.2	Standard operating procedures/control algorithms must specify minimum ranges given specific altitude for connection.	CA, LC, SA, IC
SC-14.2.3	Standard operating procedures must specify acceptable atmospheric conditions (precipitation, turbulence, cloud coverage, etc.) for connections.	CA, MC, SA, IC
SC-14.3	Systems must be able to detect when aircraft are on the ground.	IC
SC-15	**Systems must provide adequate feedback to operators regarding status of operations.**	CA, MC, LC, IC

SC-15.1	Systems must indicate mode and provide relevant information regarding mode.	IC
SC-15.1.1	Systems must indicate time necessary to “warm-up” before transitioning to stand-by mode.	IC
SC-15.1.2	If a system is programmed to transition modes, it must indicate future modes.	IC
SC-15.1.3	If a system performs an uncommanded mode change, it must alert operators to change.	IC
SC-15.1.4	System must clearly indicate required inputs to change a mode.	IC
SC-15.1.5	System must clearly indicate available modes.	IC
SC-15.2	Systems must provide adequate feedback to operators regarding status of transmissions and health of system.	CA, MC, LC, IC
SC-15.2.1	Systems must clearly indicate the status of the connection (i.e. performing acquisitions vs fine-tracking & transmitting data).	IC
SC-15.2.2	Systems must clearly indicate the power of the optical signal received.	IC
SC-15.2.3	Systems must clearly indicate when full data set has been transmitted and received.	CA, IC
SC-15.3	The alert system must be appropriately configured to alert human operators when system connection is about to be lost (power received is approaching threshold for connection outage).	CA, MC, DC, LC, IC
SC-15.3.1	The timing and intensity of system automation feedback to human operators must not be misinterpreted such that they provide unnecessary control actions (ex. Transmit Beacon when connection is still established) or do *not* provide *necessary* control actions (ex. Transmit Beacon when connection has been lost).	IC
SC-15.3.2	System must alert operators if it must halt transmissions to conduct BITs for boresight alignment.	IC
SC-15.4	Systems must alert human operators when there are errors in transmissions.	CA, MC, DC, LC, IC
SC-15.4.1	Systems must be able to detect errors in transmissions.	CA, MC, DC, LC, IC
SC-15.4.2	Systems must be able to determine causes of errors in transmissions (ex. inadequate power received, exceedances in bit-error-rate (BER), platform jitter, need for boresight calibration, etc.).	CA, MC, DC, LC, IC
SC-15.4.3	Systems must indicate causes of transmission errors to operators.	IC
SC-15.5	Systems must provide adequate feedback to operators regarding aircraft limitations.	CA, LC, IC
SC-15.5.1	Systems must indicate heading limits if lasercom terminal has a restricted field-of-view.	CA, LC, IC
SC-15.5.2	Systems must alert operators to exceedances in angular acceleration limits.	IC
SC-15.5.3	Systems must indicate range limits for connection with partner aircraft.	IC
SC-15.6	Systems must clearly present to operators the feedback or commands provided by partner systems.	CA, DA, MC, LC, IC
SC-15.6.1	Systems must clearly present identity of local systems.	CA, DM, LC, IC
SC-15.6.2	Systems must clearly present status and availability of local systems.	CA, DM, DC, LC, IC
SC-15.6.3	Systems must clearly present proximity of local systems.	CA, DM, DC, LC, IC

SC-15.6.4	Systems must clearly present compatibility with local systems.	CA, DM, DC, LC, IC