An Assessment of STPA as Applied to the Scaled Flight Demonstrator Test Program

Julian McCafferty: julian.mccafferty@nlr.nl / julian.mccafferty.1@us.af.mil
Ryan Bumgardner: ryan.bumgardner@nlr.nl / william.bumgardner.1@us.af.mil
Royal Netherlands Aerospace Centre, The Netherlands

Abstract

Systems Theoretic Process Analysis (STPA) is a methodology for system development and safety assessment which builds on the System-Theoretic Accident Model and Processes (STAMP) causality model which approaches safety as a dynamic control problem. The STPA methodology addresses system analysis and safety assessment for systems that involve complex human interactions and high degrees of coupling. The purpose of this paper is to demonstrate the application of STPA to the remotely piloted Scaled Flight Demonstrator (SFD) aircraft test program, and assess the effectiveness for test planning and risk assessment relative to the traditional Test Hazards Analysis (THA) process. The SFD aircraft is a 1:8.5 scaled model of the Airbus A320 which has been modified into a distributed electric propulsion (DEP) configuration. The aircraft was developed in collaboration with members of the Clean Sky 2 program: The Royal Netherlands Aerospace Centre (NLR), Technische Universiteit Delft (TU Delft), The Office national d'études et de recherches aérospatiales (ONERA), Centro Italiano Ricerche Aerospaziali (CIRA), Airbus, and Orange Aerospace. This effort identifies multiple benefits for flight testers when applying STPA to a highly complex system, including: increased knowledge of the system under test, forced collaboration between the test team and system experts, and identification of risks and mitigations that may otherwise be missed. The team also identifies some drawbacks to applying STPA, including: the time investment required to learn and apply the process, and the challenge in identifying specific hardware or software failure modes. Lessons learned and recommendations are presented to help other flight test professionals determine how and when STPA can best be applied to their programs in the future.

1. BACKGROUND

1.1. STPA Introduction

Systems Theoretic Process Analysis (STPA) is a qualitative hazard analysis technique developed by Professor Nancy Leveson of the Massachusetts Institute of Technology (MIT). STPA builds on the System-Theoretic Accident Model and Processes (STAMP) causality model which expands safety analysis beyond the traditional focus on component and chain of event related failures. STAMP seeks to identify the dynamic control processes and interactions with and within a complex system. STPA is used to identify instances of inadequate control that could lead to a loss and to identify the necessary constraints to prevent them.

Many resources exist to help become familiar with the methodology and learn how to apply the process, including the STPA Handbook [1] and the three-part "STPA for Flight Test Safety" presentation from the 2023 Flight Test Safety workshop [2]. Multiple other STPA resources are available on the MIT PSASS and Flight Test Safety websites.

Traditionally, STPA has been applied by industry to analyze complex interactions among human-integrated system processes, but the flight test community has recently begun to experiment with applying STPA to support the test hazard analysis process. Some notable references for STPA flight test applications are provided in Table 1.

Title	Authors	Date	Ref
Safety Implications of Autonomous Vehicles - STPA Applied to a Neural Network-Controlled Aircraft	Bowers, R. Thomas, J.	Oct, 2023	[3]
STPA as Applied to a Boeing Automated Test Maneuver	Wijayratne, D. D. Stringfield, J. Q. McDonald D. G. Clark, S. S.	Oct, 2022	[4]
STPA Applied to Manned-Unmanned Teaming	Robertson, J.	Feb, 2019	[5]
STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs	Castilho, D. S. Urbina, L. M.S. Andrade, D.	April, 2018	[6]
STAMP safety modelling applied to an aircraft rapid decompression event	Allison, C. K. Revell, K. M. Sears, R. Stanton, N. A.	June, 2017	[7]

Table 1: Applications of STPA in Flight Test

It is worth noting that Causal Analysis based on System Theory (CAST) is another methodology built upon STAMP. CAST is a retroactive analysis method that examines why existing systems and structures did not prevent a loss, whereas STPA is a proactive analysis tool used during the development phase to analyzes potential losses so hazards can be eliminated or controlled [1].

1.2. DEP-SFD Introduction

The Distributed Electric Propulsion (DEP) Scaled Flight Demonstrator (SFD) aircraft is a work package within the Horizon Europe's Clean Sky 2 Joint Undertaking program and was developed jointly by the Royal Netherlands Aerospace Centre (NLR), Technische Universiteit Delft (TU Delft), Office National d'Etudes et de Recherches Aérospatiales (ONERA), Italian Aerospace Research Centre (CIRA), Orange Aerospace, and Airbus [8]. The DEP-SFD objective is to de-risk radical aircraft configurations, such as DEP, meant to reduce emissions in future aircraft.

Figure 1: DEP-SFD Wind Tunnel Tests [8]

The DEP-SFD is a modification of the original SFD, which was a 1:8.5 scaled model of an Airbus A320. The original demonstrator aircraft was built and tested in 2022 as a means to validate predicted Froude scaling effects by using a well-known aircraft configuration, the A320, in flight.

The DEP configuration shares a majority of the components with the original SFD, the most notable exceptions being the replacement of the twin jet engines with an electric propulsion subsystem, which includes: the hexa-engine controller (HEC), six engine speed controllers (ESCs), six electric DC motor driven propellers, and six lithium-polymer batteries. Overall, 106 of the 124 parts from the original SFD configuration were reused [9].

Since the system-under-test (SUT) is a scaled aircraft, it requires remote pilot operation which offers a unique case study for applying STPA. The remote operations, via the Ground Control Station (GCS), result in a diverse and complex set of human-machine interactions for analysis. Operating the DEP-SFD is done via a pilot station with a HOTAS WARTHOG stick and throttle, a custom primary flight display, and a custom heads-up display (HUD) imposed on the tail mounted camera view. The GCS is designed to accommodate a team of four that operate and monitor the aircraft in-flight; however, the operator station is the only position with primary flight controls.

Figure 2: GCS view during aircraft operation

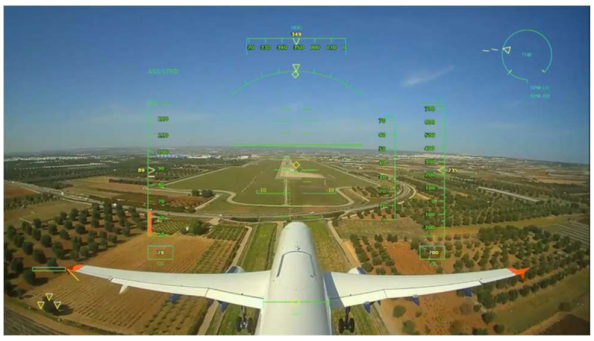

Figure 3: Aircraft HUD Monitor Display

2. STPA APPLICATION

This section outlines how to apply STPA based on the process used for the DEP-SFD system. Leveson and Thomas define four steps in the STPA handbook [1]:

1. Define the purpose of the analysis
2. Model the system control structure
3. Identify unsafe control actions
4. Identify loss scenarios

The STPA process can be used in flight test to identify undesired outcomes and system states, investigate the actions and scenarios that lead to them, and develop appropriate mitigations. This comprehensive analysis can reduce program risk and improve test effectiveness.

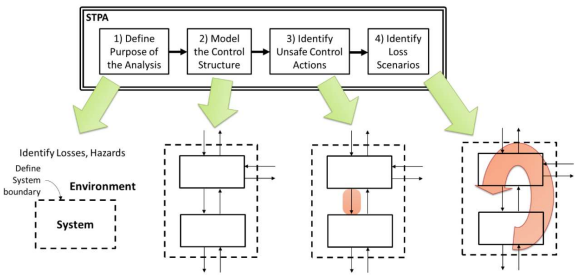

Figure 4: Overview of STPA Steps [1]

2.1. Step 1: Define the Purpose of the Analysis

The STPA handbook outlines four step one tasks:

1. Identify losses
2. Identify system-level hazards
3. Identify system-level constraints
4. Refine hazards (optional)

The first task in defining the purpose of the analysis is to identify possible outcomes that result in a loss. Losses are not only outcomes related to system, personnel, or infrastructure safety but also include any other outcomes undesired by the test team or other stakeholders. A non-safety related example of a loss, that may often be overlooked in a traditional process, is the failure to collect required test data. It may be helpful to think of a loss as what is normally put in the "effect" section of a Threat Hazards Analysis (THA) worksheet.

For the analysis of the DEP-SFD, four losses were identified:

1. Loss of life or injury to personnel
2. Loss of/or damage to aircraft
3. Loss of/or damage to infrastructure
4. Loss of mission or data

Unlike most traditional hazard analysis tools, this process begins with identifying the losses rather than ending with it. This focuses the analysis on preventing the undesired outcomes and prevents the analysis from being used to justify why the test plan is safe.

Once the losses are listed, the next task is to identify the system-level hazards by specifying the states or conditions that would result in the defined losses. The hazard identification step is similar to what testers are accustomed to, but in STPA the hazards are not based on a probability of failure in the system. Rather, hazards are system states or conditions to be prevented. Each hazard is attributed to the loss it would result in. If a hazard cannot be traced to a loss, then the item is either not an actual hazard or an additional loss needs to be identified. Since the process is iterative, additional losses and hazards may be identified during subsequent steps.

During the DEP-SFD analysis five initial hazards were identified and traced to losses:

1. Loss of controlled flight [L-1, L-2, L-3, L-4]
2. Aircraft catches on fire [L-1, L-2, L-3, L-4]
3. Aircraft loses structural integrity [L-2, L-4]
4. Aircraft performance is limited [L-2, L-4]
5. Aircraft violates minimum separation distance or boundary
    a. Ground: [L-1, L-2, L-3]
    b. Flight: [L-2, L-3, L-4]

In later iterations, two additional hazards were identified:

6. Data collection failure [L-4]
7. Exposure to high electrical power, RF radiation, and/or moving propellers [L-1]

The next task is to define conditions or behaviors that prevent the system-level hazards from occurring. These constraints can be viewed as procedural or design requirements. Often in flight test, it is too late in the development process to affect the system design, so the test team may need to identify alternative means to prevent the system-level hazards.

Creating system-level constraints can typically be done by rewording the hazards as enforcement statements. For the DEP-SFD seven constraint were created, one for each hazard:

1. Aircraft must remain in controlled flight [H-1]
2. Aircraft must maintain thermal integrity [H-2]
3. Aircraft must maintain structural integrity [H-3]
4. Aircraft power systems must operate within limits [H-4]
5. Aircraft must maintain minimum separation distance from people, aircraft, airspace boundaries, and other objects [H-5]
6. Aircraft must collect mission data [H-6]
7. Personnel must be protected against electrical power, radiation, and moving propellers [H-7]

It is not required to have a one-to-one traceability from constraints to hazards and from hazards to losses. The objective is to sufficiently address each hazard and in turn each loss with a system constraint. Throughout this step, it is important to focus on defining the purpose of the analysis and not outlining specific solutions or implementations.

2.2. Step 2: Model the Control Structure

The next step in the process is to develop a control structure for the system. The control structure is a visual system representation made up of controllers, controlled processes, control actions, and feedback. This provides the targets for analysis when identifying unsafe control actions, loss scenarios, and risk mitigation procedures during the following steps.

It is important to recognize that the control structure is an abstraction of the actual system. This means that the details of the system design will only be modeled to the extent that it is useful for the analysis. As engineers, there is a strong inclination to model every component and linkage within the system design. This would be considered the lowest level of abstraction. While this may be useful as a starting point for building the control structure in STPA, this is not generally recommended. Rather, starting at the highest level of abstraction and then adding detail can help in identifying when the sufficient level of abstraction is achieved for the analysis.

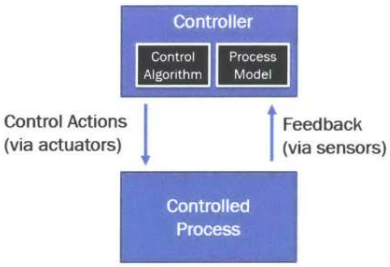

Figure 5: Control Structure Abstraction [5]

The team started building the control structure for the DEP-SFD using the system block diagram given their limited understanding of the system design. The team first identified and removed components that were not part of a control process. This resulted in a control structure that very closely resembled the original system block diagram as shown in Figure 6. (actual components and connections are unimportant; this is simply a visual representation of the team's process).

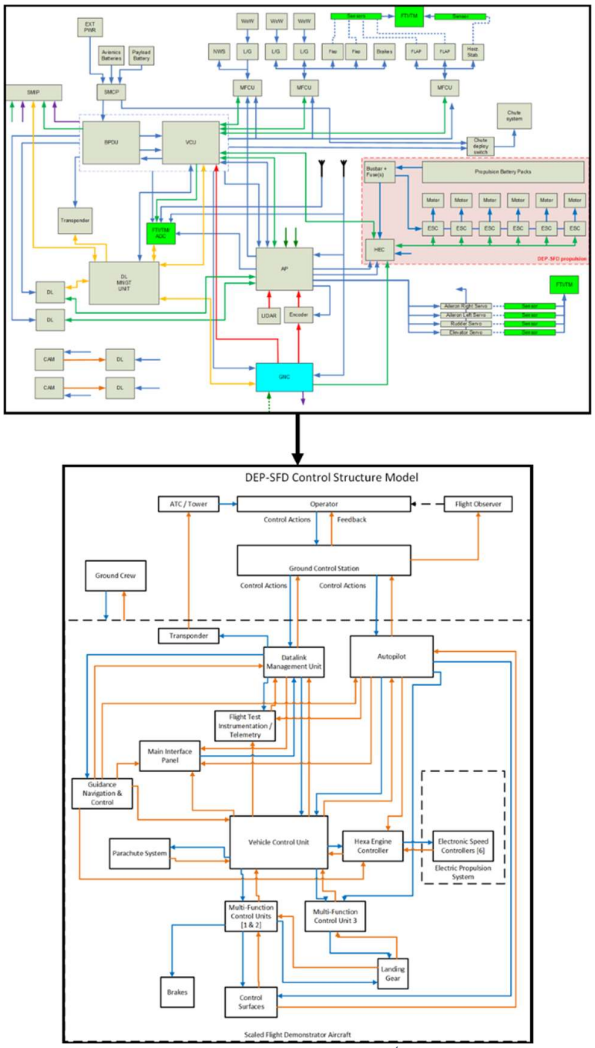

Figure 6: System Block Diagram to 1st Control Structure

An important characteristic of a control structure is that it is hierarchical, meaning controllers of higher levels of authority are positioned on top. In order to develop the system hierarchy, the team annotated the control and feedback paths of each component. Unfortunately, this still closely resembled the linkages of the system block diagram and was unhelpful. What ultimately helped define the system hierarchy was working directly with the system design engineers to review the purpose of each component and how they interacted through a control process. For example, the team assumed the "Datalink Management Unit" was a controller, but instead it was an ethernet switch which was part of a controlled process and could be abstracted out of the model. Following this lesson, the control structure could be further abstracted and a hierarchy emerged for the next iterations.

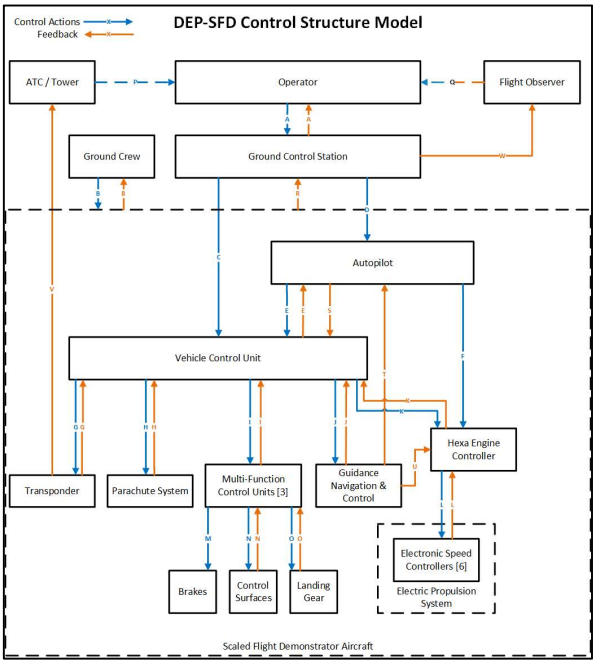

Figure 7: 2nd System Control Structure Iteration

The depth of the control structure is also dependent on the scope and purpose of the analysis. For the DEP-SFD, the scope was limited to the execution of commands from the GCS and ground crew to the aircraft, and crew interactions with Air Traffic Control (ATC) and the airport tower. Internal commands within the control structure and some details about the system were deliberately omitted. This decision was made for three main reasons: first, previous experience and failure analysis was deemed sufficient to limit any redesign; second, the system design was fixed at the current stage in the project; lastly, there was a limited amount of time and budget to apply STPA. These three factors led to a focus on the control actions that the team could most influence.

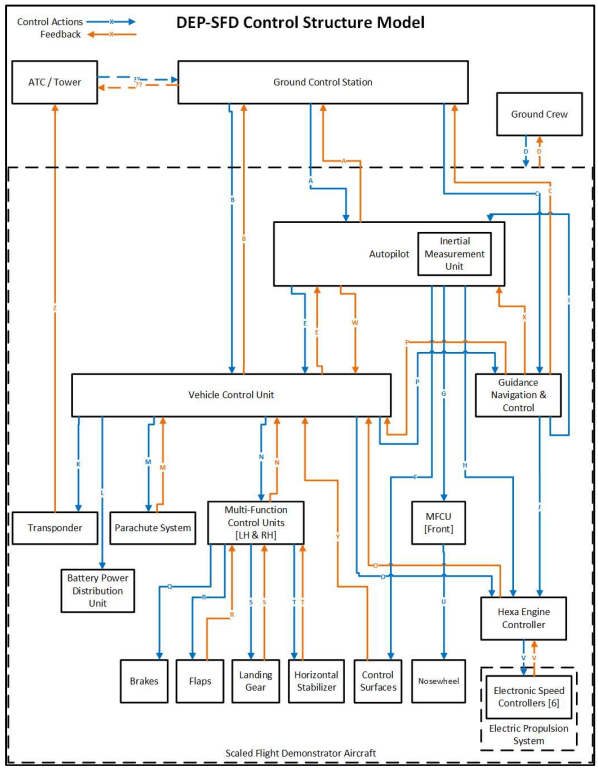

Figure 8: 3rd System Control Structure Iteration

The final iteration of the control structure is shown in Figure 9. Interestingly, the iterations cycled between too much and too little abstraction as the team learned more about the system and what was relevant to the scope of the analysis. One of the most significant lessons which will be discussed in detail in the Lessons Learned section is that the construction of a shared mental model of the SUT is a critical by-product of this step of STPA. As the team asked questions and iterated through this process, many assumptions that various team members had about how the system worked were proven incorrect. This led to a deeper understanding of what needed to be tested and where unknown risks lay in the system design.

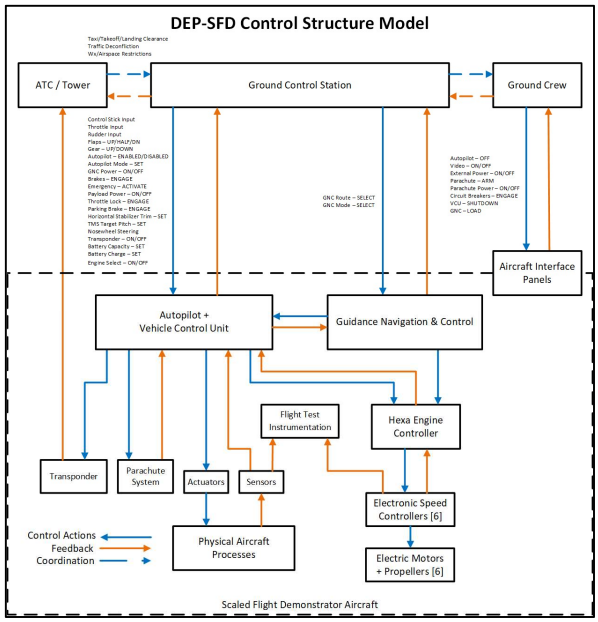

Figure 9: Final DEP-SFD Control Structure

The final control structure also includes the control actions that will be analyzed. Control actions can be divided into two categories: general actions based on system behavior or specific actions describing a physical actuation or software command. For example, a “roll command” is an aircraft behavior that is a result of multiple hardware actuations and software commands, where a “stick input” is a specific action being completed by a controller. The category of control action utilized will be based on the scope of the analysis, but will also determine the focus of the mitigations. If only general control actions are identified, then the team may only be able to develop procedure level mitigations. More specific control actions should allow mitigations to prevent more component level failures. When identifying specific control actions, it is important that the action has a clear traceability through the system to a controlled process. A control action with an unclear traceability would be a “pedal input”, which could result in a nosewheel steering command, a brake command, or a rudder command. The traceability would become dependent on the context provided in the UCA or outlined in a scenario. Utilizing “rudder input” or “nosewheel steering” as control actions creates inherent traceability in the control diagram. By ensuring traceability and focusing on test objectives, the test team will develop more applicable mitigations and will reduce time spent on scenario development.

DEP-SFD Control Actions			
#	CA	From	To
1	Control Stick Input	GCS	AP
2	Throttle Input	GCS	AP
3	Rudder Input	GCS	AP
4	Flaps – UP/HALF/DN	GCS	AP
5	Gear - UP/DOWN	GCS	AP
6	Autopilot – ENABLED/DISABLED	GCS	AP
7	Autopilot Mode – SET	GCS	AP
8	GNC ON/OFF	GCS	AP
9	Brakes	GCS	AP
10	EMERGENCY - Activate	GCS	AP/VCU

Table 2: Sample Control Action List

2.3. Step 3: Identify Unsafe Control Actions

An unsafe control action (UCA) is a control action that in a particular context will lead to a hazard. UCAs are not only actions deemed unsafe in the traditional sense, but any control action that could result in a loss. To assist in identifying the context that makes an action unsafe or undesired, STPA outlines four types of UCAs:

1. The control action is not provided but should have been
2. The control action is provided but should not have been
3. The control action is provided too early, too late, or out of order
4. The control action is stopped too soon or applied too long

Some categories may have multiple UCAs and others may not have any, however every control action requires at least one UCA. If a UCA cannot be identified, then the control action is either too specific or too broad. It is more likely that a broad control action will result in a large number of possibly unrelated UCAs.

Control Action	Not Provided	Provided	Too Early/Late Out of Order	Applied too long/ Stopped too early
Flaps - UP/HALF/DN	UCA-12: GCS does not provide Flaps UP control action during climbout. **H-4**	UCA-14: GCS provides Flaps UP control action during low speed operations. **H-1**	UCA-15: GCS provides Flaps control action too early or too late during takeoff or approach to landing. **H-1/4**	N/A
	UCA-13: GCS does not provide Flaps DN/HALF control action during approach to landing or prior to takeoff. **H-1/4**	UCA-16: GCS provides Flaps DN/HALF during normal operations. **H-4**		

Table 3: Example: UCAs for Flaps

The structure for each UCA should contain the following elements: the controller, the **category of action**, the **control action**, the *context*, and the *hazard number* that it causes. The following is a UCA created for the DEP-SFD "Nosewheel Steering" control action: "The GCS **does not provide** *sufficient* **Nosewheel Steering** *when an obstacle is in the path during ground operations. H-5a*".

When writing UCAs it is important that the context is not dependent on multiple failures or another UCA having to occur first. An example that was originally identified for the Guidance, Navigation, and Control (GNC) of the DEP-SFD is: "The GCS **does not provide GNC Power ON** *prior to setting GNC in control. H-6*". This UCA requires incorrect ground startup and autopilot handover procedures, a lack of prescribed crew communication, and the operator to be hands off, so it was removed from the list. By limiting the UCAs to non-cascading failures, the team is able to apply mitigations specifically to a controller or control action. If a full system analysis is being completed, then layered mitigations should be in place to prevent cascading failures.

For the DEP-SFD, the team analyzed 33 control actions and identified 73 unique UCAs.

2.4. Step 4: Identify Loss Scenarios

A loss scenario is used to identify a chain of events or decisions that can lead to a hazard. They are primarily focused on why an event may occur but they also provide context for when it may occur. Based on the scope outlined for the DEP-SFD, only scenarios involving a controller providing a UCA were identified. For this type of scenario, the STPA handbook provides two factors to consider.

1. Inadequate control algorithm (decision based)
2. Inadequate process models (feedback based)

The handbook recommends starting with a UCA and working backwards to develop a standalone scenario that explains what led to the control action. The team elected instead to list causal factors and system feedback failures for each UCA which could be written out as a scenario. This proved to be more helpful later when identifying mitigation strategies for each scenario since there was a clear delineation between a problem in the control algorithm versus the process model. If causal factors or feedback failures could not be identified, then the UCA was reevaluated or removed.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures
Flaps - UP/HALF/DN	UCA-14: GCS provides Flaps UP control action during low speed operations. **H-1**	Aircraft is moving at a lower speed than the operator realizes.	HUD information (airspeed and/or flap position) is incorrect or not present.
			Lack of indication of flap speeds or stall speed on speed indicator.

Table 4: Example: Loss Scenario for Flaps

2.5. STPA Outputs: Mitigations & Test Points

Where STPA can most benefit flight testers is in using the outputs from the four steps to generate risk mitigations, identify test points, and help develop the test plan. The approach chosen for the DEP-SFD analysis was to add a mitigation column to the

existing scenario table. Mitigations were then developed for each causal factor and feedback failure instead of for the hazards directly. This forced the team to focus on the root causes of hazards that emerged through characteristics of the system design and interactions between the system, personnel, and the environment.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Flaps - UP/HALF/DN	UCA-14: GCS provides Flaps UP control action during low speed operations. **H-1**	Aircraft is moving at a lower speed than the operator realizes.	HUD information (airspeed and/or flap position) is incorrect or not present.	1. Operator and test team need to know the stall speed. 2. Cross check airspeed & altitude with PFD during critical phases of flight. 3. Operator verbalizes control actions prior to execution.
			Lack of indication of flap speeds or stall speed on speed indicator.	

Table 5: Example: Mitigating Procedures for Flaps

After developing the mitigations, the team identified five categories:

1. System Design Recommendations
2. Training Requirements
3. Checklist Items (Including Go/No-Go)
4. General Mitigating Procedures
5. Functionality Verification

The team found it helpful to focus on feasibility of implementing a mitigation during this process. For example, in flight test the aircraft configuration is typically locked down. Most mitigations therefore became procedural, but there were still some small changes to the design that the team could influence such as the instrumentation and updates to the operator displays. Changes to the displays primarily focused on providing clear and critical feedback to the operators. The training requirements focused on ensuring the crew had clear emergency procedures and the operators had practiced scenarios in the simulator. These first two categories focused on mitigating risk prior to execution, whereas checklist items and general mitigating procedures focused on execution. The functionality verification items were considered potential test points and removed from the list of mitigations. The STPA process allows the team to apply mitigations holistically, instead of the traditional execution only approach.

Mitigating Procedures
Battery charge setting should be a start-up checkist item to include verifying a new state of charge in case the batteries were charged or have changed.
Flaps position should be part of prelanding checklist.
Functional tail camera is a Go/No Go item.
GCS must verify mission test points and waypoints are loaded prior to flight operations.
Gear down should be part of the approach checklist.
Ground crew should verify with the GCS that the parking brake is engaged prior to engine checks or shut down.
Operator should verify that parking break is disengaged prior to takeoff and landing.
Pump brakes prior to engine run up for take off.
Routinely check brake performance and brake wear.
The operator should verify that brakes are disengaged prior to landing.
XPDR code setting should be part of statup checklist.
XPDR ON should be part of the pre-taxi checklist.

Table 6: Example Mitigations: Checklist Items

Most flight testers will recognize that there is no mention of risk probability or severity thus far in STPA. While not strictly prohibited in the process, this omission is intentional. The STPA methodology emphasizes the use of non-numerical engineering judgement over numerical values which provide a false sense of accuracy in predicting future events [1]. For the DEP-SFD, setting aside probabilities forced the team to consider each UCA equally. Rather than say “the operator would never do that”, the team could say “the operator might do that under certain circumstances”, and then consider mitigations to prevent that scenario from occurring.

3. LESSONS LEARNED AND RECOMMENDATIONS

3.1. STPA Requires a Shift in Mindset

STPA newcomers may experience that the proper mindset for this type of analysis does not at first come naturally, particularly when building the system control structure and identifying loss scenarios. Engineers know that details are important and it may feel uncomfortable to abstract away deliberate design decisions that make the system work. However, the purpose of abstraction is to represent only the system components necessary for evaluation of complex interactions that may lead to risk. An additional challenge is to recognize that even for a seemingly illogical or impossible unsafe action, the context is important. Many “dumb” control actions can appear logical when placed in a scenario with false or misleading feedback to the pilot or controller. This shift in mindset allows for a more holistic system view and of its interactions from a control perspective. Once the team makes this mindset shift, the value of identifying and preventing loss scenarios becomes apparent.

3.2. STPA is Iterative

When progressing through STPA, the team can easily get trapped in trying to comprehensively

complete each step. A good example is getting stuck building the perfect control structure and identifying every possible control action within the system. It is important for the team to recognize that STPA should be iterative and that it is acceptable to start identifying UCAs with a rough control structure and list of control actions in place. Moving through the process can identify inadequacies or mistakes in previous steps more quickly than trying to get it right the first time. For this reason, it is also important to maintain good documentation and version control of the STPA products. The team found this very helpful throughout the process, especially when multiple people are working at the same time.

3.3. Team Involvement and Documentation

During the STPA process, it is important to involve as much of the test team and design engineers as possible for two main reasons:

First, this brings together diverse experience levels and system insights that are necessary to develop the system control structure and identify effective mitigations; Second, absent team members miss out on building a shared mental model of the system, which is difficult to transfer apart from the collaborative process of developing it. Each step requires different levels of involvement so team member's expertise and responsibilities should be defined early in the process.

Prior to developing the system control structure, it is important to compile and disseminate all available system documentation. Each team member should review as much of this information as possible prior to gathering as a team. During this review, personal assumptions, misunderstandings, and questions should be documented for discussion as a group.

As the team develops the control structure and identifies control actions, team members may disagree about how the system functions. At this point referencing the documentation should provide clarity, but this is not always the case. An anecdote from this analysis involved how a roll command was translated into a flaperon command. Each team member insisted that there was no flap actuation during a roll input. After referencing the document with the team, the engineer who programed the controller acknowledge that the command was present in the code but had been commented out.

Relying on memory inherently adds risk. In the absence of documentation resolving disagreements or removing incorrect assumptions becomes very difficult since a consensus needs to be reached. If the issue is important enough, the team may have to spend valuable time inspecting software code or testing individual components to find the answer.

For the DEP-SFD project, the aircraft utilizes the same control components as the original SFD, giving the team experience with the expected system behaviors. By referencing observations and outcomes from the previous test campaign, the team was able to quickly resolve most confusions without having to dive too deep into documentation or software.

3.4. Defining the Scope

Ideally the team should define the analysis scope prior to starting the process. However, the DEP-SFD team often discovered complexity that would expand the scope beyond the time and resources available. For example, it was found part-way through the process that component failures could also be addressed. This would have taken a large amount time and effort and likely resulted in duplicating already completed work (since a component failure analysis had already been completed), so it was not included. It was also discovered that some of hazards to ground personnel were not fully addressed, so the team expanded the analysis to include ground and lab test events. When determining the scope, the team must also define what types of mitigations are feasible within the project.

3.5. UCA Categorization

It can be difficult to identify which category a UCA belongs in, particularly between "Applied too early/too late or out of order" and "Stopped too soon or Applied too long". One helpful method is to determine if the action is discreet or part of a sequence. Another consideration is whether the outcome would be the same if the action was applied incorrectly or not at all. An example of this is lowering the landing gear prior to landing. If the command is applied too late it is effectively the same as not at all, so this UCA was placed in the "Not Provided" category. The team found it helpful to focus on whether the categorization would affect the follow-on mitigation strategy. If not, then the categorization was less important than ensuring it was documented.

3.6. Formatting of Application Outputs

Formatting of documentation may seem like a trivial topic, but a lot of time was spent finding an efficient way to display information. It is important that the STPA outputs be presented in a manner that allows uninvolved team members to easily apply the findings. For the DEP-SFD analysis, the team used Microsoft Visio for building the control structure and Microsoft Excel for tabulating data. Other suitable software programs exist but the team must ensure availability for everyone in their project.

3.7. When to Apply STPA

First, teams should recognize that learning and applying STPA comes with a time commitment. While only an estimate, it took about 10-15 hours of reading and watching tutorials before the authors were

comfortable with applying STPA. There is also a steep learning curve when applying it for the first time, although subsequent applications will run much faster. If possible, having at least one team member with STPA experience can make the process significantly more efficient. Overall, the amount of time required to complete the STPA process is significantly more than a traditional THA exercise, but the methodology is likely to identify more risks and create more comprehensive mitigations. However, STPA is very effective for analyzing systems of high complexity. A team must balance these benefits and drawbacks when deciding whether to apply STPA to their program.

One limitation the team encountered is that the analysis did not provide insight as to whether the system was built correctly or if the right system was built. This is the role of verification and validation, which is a different step in the systems engineering development process. This was a common misunderstanding amongst the team when introducing the process. An example of this was the electric propulsion subsystem design. STPA could not identify if the team had selected the correct batteries to power the motors. Rather, the team identified the hazard "Aircraft Performance is Limited". This hazard is an undesired system state that could result from batteries without sufficient capacity to deliver the required mission power levels. This led to a discussion about battery capacity margins and flight test profile requirements, but is not a sufficient substitute for the engineering design process.

4. CONCLUSIONS

This paper provides an overview of the application of STPA to a remotely piloted flight test program. The team identified many benefits and a few drawbacks from applying STPA. Utilizing the STPA methodology drove increased collaboration between the test team and system experts, resulting in a more complete understanding of the system-under-test. This also allowed the team to identify risks and mitigations that may otherwise have been overlooked through alternative processes. The primary drawback was the time investment required to learn and apply the methodology. Additionally, it can be challenging to identify certain failure modes and risks associated with the design through STPA alone. The process and lessons learned from this application are presented along with recommendations to help the flight test community determine how and when STPA may support their missions.

5. References

[1] Leveson, N. G., Thomas, J. P., "STPA Handbook", MIT Partnership for Systems Approaches to Safety and Security (PSASS), 2018

[2] Montes, D., Summers, S., "System-Theoretic Process Analysis for Flight Test Safety", www.flighttestsafety.org, May 2023

[3] Bowers, R., Thomas, J., "Safety Implications of Autonomous Vehicles – Systems Theoretic Process Analysis Applied to a Neural Network-Controlled Aircraft", SFTE, 54th Annual International Symposium, Oct 2023

[4] Wijayratne, D. D., Stringfield, J. Q., McDonald D. G., Clark, S. S., "Systems Theoretic Process Analysis as Applied to a Boeing Automated Test Maneuver", SFTE, 53rd Annual International Symposium, Oct 2022

[5] Robertson, J., "Systems Theoretic Process Analysis Applied to Manned-Unmanned Teaming", Masters of Science Thesis, Massachusetts Institute of Technology, Feb 2019

[6] Castilho, D. S., Urbina, L. M.S., Andrade, D., "STPA for Continuous Controls: A Flight Testing Study of Aircraft Crosswind Takeoffs", Safety Science 108 (2018) 129-139

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

[8] Doll, C., "Distributed Electric Propulsion Scaled Flight Demonstrator", CLEANSKY2 Large Passenger Aircraft, AIAA SciTech Presentation, Jan 2023

[9] Doll, C., Hoogreef, M. F.M., Iannelli, P., Jentink, H., Kierbel, D., "Final Design, Manufacturing and Testing of the Clean Sky 2 Distributed Electric Propulsion Scaled Flight Demonstrator D08 DEP–SFD", AIAA Clean Aviation Special Session: Advanced Engine and Aircraft Configurations, Jan 2024

Appendix A: Ground Control Station Analysis

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Brakes	UCA-1: GCS does not provide brake control action when an obstacle is in the path during ground operations. **H-5a**	Operator is unaware that an obstacle is in their path.	The tail camera is not functioning or is unable to see the object in the distance.	1. Functional tail camera is a Go/No Go item. 2. Safety observer provides confirmation of path clearance to the test team.
	UCA-2: GCS does not provide brake control action during landing roll. **H-5a**	Operator is unaware of an overshoot landing.	The tail camera is not functioning. Ground crew does not notify operator of overshoot.	1. Functional tail camera is a Go/No Go item. 2. Safety observer must notify the operator in the event of an overshoot from planned touchdown point.
		Aircraft is moving at a higher speed than the operator realizes.	PFD information is incorrect or not present.	Cross check airspeed & altitude with PFD during critical phases of flight
		Brake performance is inconsistent between actuations	Lack of brake magnitude or engagement status to the operator.	1. Pump brakes prior to engine run up for take off. 2. Routinely check brake performance and brake wear.
	UCA-3: GCS provides excessive brake control action during high speed. **H-4**	Aircraft is moving at a higher speed than the operator realizes.	PFD information is incorrect or not present.	1. Operator should practice aborted takeoff procedures in the simulator and during high speed taxi testing. 2. Takeoff abort procedures should be a memorized emergency procedure in the flight manual.
		There is a nonstandard aborted takeoff procedure.	N/A	
	UCA-4: GCS provides brake control action prior to landing roll. **H-3**	The brake slider can be left in any position.	The operator has no indication of brake engagement other than the slider position which could be outside of an operator's standard crosscheck.	The operator should verify that brakes are disengaged prior to landing.
	UCA-5: GCS stops providing brake control action too early during ground operations. **H-5a**	Brake performance is inconsistent	Lack of brake magnitude or engagement status to the operator.	1. Pump brakes prior to engine run up for take off. 2. Routinely check brake performance and brake wear.
Parking Brake - ENGAGE	UCA-38: GCS does not provide Parking Brake Engage control action prior to engine checks or shut down. **H-5a**	Operator is distracted by other tasks involved in operations.	Brake engagement status is not present.	Ground crew should verify with the GCS that the parking brake is engaged prior to engine checks or shut down.
	UCA-39: GCS provides Parking Brake Engage control action during taxi or prior to landing or takeoff. **H-3/4**	Operator inadvertantly activates the parking break during taxi or prior to landing.	Brake engagement status is not present.	Operator should verify that parking break is disengaged prior to takeoff and landing.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Emergency - ACTIVATE	UCA-6: GCS does not provide Emergency control action when the operator has lost control. **H-5**	Operator is still trying to maintain control of the aircraft.	N/A	1. The test team should practice/train for an Emergency ACTIVATE scenario in the simulator using the Horizon PC. 2. The test team should have Crew Resource Management Training.
		Poor Crew Resource Management within the test team.		
		Horizon PC operator is not prepared to send the Emergency ACTIVATE command so the command is delayed.		
	UCA-9: GCS provides Emergency control action during functional tests with the parachute armed. **H-1**	The test team thougth that the parachute was not armed.	The parachute armed indicator light failed	1. Test team should verify that the parachute arm switch position is correctly set for test points that involve Emergency modes. 2. Test team should verify that no ground crew members are near the aircraft when activating the Emergency controls.
		Ground crew and GCS do not communicate the test procedure and the required configuration of the aircraft.	N/A	
	UCA-10: GCS provides Emergency control action while the aircraft is still recoverable. **H-1**	Operator does not execute proper recovery procedures.		1. Operator should practice recovery procedures in the simulator, with awareness that out of control flight is not modeled correctly in the simulation and so should only focus on the control inputs and not the simulator response. 2. The test team should practice/train for an Emergency ACTIVATE scenario in the simulator using the Horizon PC.
		Operator thinks they are in an unrecoverable condition.	The flight display altitude indications are incorrect.	
		The Horizon PC operator sent the Emergency command while the operator was still recovering the aircraft.	N/A	
Flaps - UP/HALF/DN	UCA-12: GCS does not provide Flaps UP control action during climbout. **H-4**	Operator is distracted by other tasks involved in operations.	N/A	The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits.
	UCA-13: GCS does not provide Flaps DN/HALF control action during approach to landing or prior to takeoff. **H-1/4**			Flaps position should be part of prelanding checklist
	UCA-14: GCS provides Flaps UP control action during low speed operations. **H-1**	Aircraft is moving at a lower speed than the operator realizes.	HUD information (airspeed and/or flap position) is incorrect or not present. Lack of indication of flap speeds or stall speed on speed indicator.	1. Operator and test team need to know the stall speed. 2. Cross check airspeed & altitude with PFD during critical phases of flight. 3. Operator verbalizes control actions prior to execution.
	UCA-16: GCS provides Flaps DN/HALF during normal operations. **H-4**	Operator is not aware of required test conditions due to miscommunication between test team members.	N/A	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Gear - UP/DOWN	UCA-17: GCS does not provide Gear UP control action during climbout. **H-4**	Operator is distracted by other tasks involved in operations.	N/A	The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits.
		Operator leaves gear down on purpose due to any takeoff emergency requiring an immediate return and full-stop landing.		1. Operator should maintain airspeed above gear down stall speed when leaving gear down. 2. Operator should prioritize maintaining control of the aircraft over exceeding climbout turn boundary.
	UCA-18: GCS provides Gear DOWN control action during normal or low speed operations. **H-4**	Operator is not aware of required test conditions due to miscommunication between test team members. Aircraft is moving at a lower speed than the operator realizes.	HUD information (airspeed and/or gear position) is incorrect or not present. Lack of indication of gear speeds or stall speed on speed indicator.	1. Operator and test team need to know the stall speed. 2. Cross check airspeed & altitude with PFD during critical phases of flight 3. Operator verbalizes control actions prior to execution.
	UCA-19: GCS does not provide Gear DOWN prior to landing. **H-3**	Operator is distracted by other tasks involved in operations.	N/A	1. Gear down should be part of the approach checklist. 2. Safety observer should verify that the gear is down visually on approach.
		Operator thinks the gear is down.	Gear indicator is incorrect.	Test team should always verify that the gear is down visually on approach.
Autopilot Mode - SET AUTO	UCA-28: GCS provides Autopilot SET AUTO control action when the current AUTO waypoint is in an undesired location. **H-5b/6**	Waypoints are not reviewed prior to activating AUTO during flight.	N/A	GCS must verify mission test points and waypoints are loaded prior to flight operations.
		Operator is unware of test conditions due to miscommunication between the test team.		1. Prior to mission flights, test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew. 3. Operator verbalizes control action prior to execution.
Autopilot Mode - SET GNC	UCA-29: GCS provides Autopilot SET GNC control action when the GNC is not prepared to take command. **H-1/6**	Operator thinks that the GNC is prepared to take command.	N/A	Operator will conduct mode switching from MANUAL and with the expectation that GNC will NOT take control.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Autopilot Mode - SET ASSISTED	UCA-31: GCS provides Autopilot SET ASSISTED control action while the GNC mode is effectively collecting mission data. **H-6**	The operator thinks that the aircraft is approaching an unsafe/undesired condition.	Aircraft position on the moving map may be incorrect due to a GPS or IMU error.	1. The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits. 2. Loss of or an error in the GPS signal should trigger a warning from the autopilot. 3. In the event of a loss of GPS, utilize compass heading and last known location to avoid borders 4. GCS crew should monitor respective subsystems to ensure that the Operator is receiving proper indications.
			HUD information is incorrect or not present.	
		Operator is unware of test conditions due to miscommunication between the test team.	N/A	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew. 3. Operator verbalizes control action prior to execution.
Autopilot - ENABLED [NOT MANUAL]	UCA-21: GCS does not provide Autopilot ENABLED control action when mission profile requires specific autopilot mode. **H-6**	Operator is unware of test conditions due to miscommunication between the test team.	N/A	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew.
		Operator is closer to the starting point than they think either because the moving map is not in the operators cross-check while setting up for mission profiles or the moving map is incorrect.		1. The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits. 2. Loss of or an error in the GPS signal should trigger a warning from the autopilot. 3. In the event of a loss of GPS, utilize compass heading and last known location to avoid borders
		Operator does not think that the GNC is ready to take control.		Operator monitors GNC light on the PFD to verify it is GREEN prior to setting GNC in control.
	UCA-23: GCS provides Autopilot ENABLED control action prior to setting desired Autopilot Mode setting. **H-1/6**	Operator is unware of test conditions due to miscommunication between the test team. Operator is distracted by other tasks involved in operations.		1. Operator monitors GNC light on the PFD to verify it is GREEN prior to Autopilot ENABLED control action. 2. Need to perform "ground integration checks" of the CIRA developed PFD which provides the GNC status for mode switching. 3. Operator should practice GNC mode switching in the simulator. 4. GCS crew will be prepared to take back command during a GNC mode switch.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Autopilot - DISABLED [MANUAL]	UCA-25: GCS provides Autopilot DISABLED control action when the operator is not prepared to take Manual control. **H-1**	Operator inadvertantly actuates the Autopilot Enable/Disable switch during a seat swap or other GCS activities	N/A	1. Operator seat swap will not occur during flight. 2. Operator will be prepared to take control at all times. 3. Horizon PC Operator should monitor state of Autopilot mode and notify the operator if the control mode unexpectedly changes.
	UCA-26: GCS does not provide Autopilot DISABLED control action when Autopilot mode AUTO or GNC is approaching a hazardous condition. **H-1/5b**	GCS crew isn't aware of the current maneuver being executed, and so doesn't know that a departure is imminent.	N/A	1. All GNC maneuvers will be tested in the simulator 2. All maneuvers will follow a build-up approach in terms of control surface deflections or throttle settings. (Continuation Criteria)
		GNC maneuver fails to execute safely and leads to a departure or limit exceedance.		
	UCA-27: GCS provides Autopilot DISABLED control action when the AUTO or GNC mode is in command and safely collecting mission data. **H-6**	The operator thinks that the aircraft is approaching an unsafe/undesired condition.	Aircraft position on the moving map may be incorrect due to a GPS or IMU error.	1. The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits. 2. Loss of or an error in the GPS signal should trigger a warning from the autopilot. 3. In the event of a loss of GPS, utilize compass heading and last known location to avoid borders.
			HUD, PFD, or SFD information is incorrect or not present.	
		Operator is unware of test conditions due to miscommunication between the test team.	N/A	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew. 3. Operator verbalizes control action prior to execution.
	UCA-89: GCS provides Autopilot DISABLED control action when the throttle has changed positions during GNC mode is in command. **H-1**	Throttle is inadvertently moved during a seat swap or other GCS activities.	There are no throttle position indicators on the throttle or flight displays for mode switches.	1. Operator seat swap will not occur during flight. 2. Operator will note throttle position upon entering GNC mode. 3. GCS crew will actively avoid the throttle during GNC operations.
Engine Select [6] - ON/OFF	UCA-32: GCS provides Engine Select OFF control action while the output of the selected engine(s) are required to maintain safe and controlled flight. **H-1/4**	Operator is unaware of required test conditions due to miscommunication between test team members.	N/A	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew. 3. Operator verbalizes control action prior to execution.
		Operator thinks that an engine must be powered off to prevent an over temp because they think the engine is approaching a temperature limit.	Temperature sensor reading is incorrect or not clearly marked.	1. Temperature readings must be clearly marked for the applicable motor. 2. Test team should practice an engine overheat EP in the simulator.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Payload Power - ON/OFF	UCA-34: GCS provides Payload Power OFF control action after ground set up. **H-6**	Operator inadvertantly actuates the Payload Power switch.	N/A	Payload Power switch should be placed far from other controls done during routine operations and test team should be aware that shutting it off would delete all mission data.
Throttle Lock - ENGAGE	UCA-36: GCS does not provide Throttle Lock Engage control action during ground crew operations. **H-7**	Operator is distracted by other tasks involved in operations.	Throttle lock ENGAGED feedback not present or incorrect on the display.	Ground crew should verify with the GCS that throttle lock is engaged prior to approaching the aircraft when power is applied.
		Operator is unware of test conditions due to miscommunication between the test team.		
	UCA-37: GCS provides Throttle Lock Engage control action during taxi or takeoff roll. **H-4/5a**	Operator inadvertantly activates the throttle lock switch instead of the XPDR switch.	N/A	Test team should ensure XPDR is set prior to taxi so that actuation of the XPDR isn't required during taxi or takeoff.
		Operator thinks that the throttle lock is engaged.	Throttle lock ENGAGED feedback not present or incorrect on the display or switch position because it is a Press-and-Hold switch.	Throttle lock setting should be present on the displays.
Horizontal Stabilizer Trim - SET	UCA-46: GCS provides excessive horizontal stabilizer trim setting control action during takeoff or landing. **H-1/4**	Operator is unaware of required trim setting for proper takeoff/landing procedure.	N/A	Operator should practice relevant flight profiles for the mission in the simulator using the same flight dynamics and stability and control model.
TMS Target Pitch - SET	UCA-47: GCS provides excessive TMS target pitch offset control action prior to takeoff or landing. **H-1/4**	Operator is unaware of required trim setting for proper takeoff/landing procedure.	N/A	Operator should practice relevant flight profiles for the mission in the simulator using the same flight dynamics and stability and control model.
Route - SELECT	UCA-63: GCS provides the incorrect Route SELECT control action while in Autopilot mode. **H-6**	1. The operator is distracted by other tasks involved in operations. 2. Operator is unware of test conditions due to miscommunication between the test team.	Touch screen display provides no haptic or audio feedback to selection.	1. Prior to mission flights test conditions should be briefed to full GCS crew. 2. Prior to mission profile start, required test conditions are verbalized to operator and other GCS crew. 3. Operator verbalizes control action prior to execution.
	UCA-64: GCS provides the desired Route SELECT control action after selecting Autopilot Mode. **H-6**		N/A	

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Control Stick Input	UCA-40: GCS does not provide control stick input when Autopilot modes AUTO or GNC are not set. **H-5b**	Operator is unaware that they are in control because the GNC control has failed and control has been transferred back to ASSISTED.	Control mode indication on the Operator displays is incorrect or not clearly visible.	1. The GNC engineer should notify the test team if the GNC fails during operations. 2. Horizon PC should play an audible tone when the control mode changes to ASSISTED mode. 3. Horizon PC Operator should monitor state of Autopilot mode and notify the operator if the control mode unexpectedly changes.
			GNC indicator displays the GNC health and that it should be capable of taking control, but does not indicate whether or not the GNC is in control.	
		Operator commands GNC in control and GNC does not take control (either due to flight conditions or GNC failure).	GNC indicator displays the GNC health and that it should be capable of taking control, but does not indicate whether or not the GNC is in control.	Operator will conduct mode switching from MANUAL and with the expectation that GNC will NOT take control.
	UCA-41: GCS provides unexpected control stick input during ground crew operations. **H-7**	Operator is unaware of ground crew proximity to the aircraft.	N/A	Ground crew should always notify the GCS when they are approaching the aircraft.
	UCA-43: GCS provides insufficient control stick input while in MANUAL or ASSISTED modes to avoid a boundary or hazard. **H-5/6**	Operator is unfamiliar with the aircraft handling qualities.	N/A	Operator should practice relevant flight profiles for the mission in the simulator using the measured moments of inertia, center of gravity, and stability and control model.
		Operator is closer to an obstacle or boundary than they think either because the moving map is not in the operators cross-check during critical phases of flight or the moving map is incorrect.	Aircraft position on the moving map may be incorrect due to a GPS or IMU error.	1. The GCS crew should practice good CRM to ensure the Operator is aware of hazards, boundaries, and aircraft and subsystem limits. 2. Loss of or an error in the GPS signal should trigger a warning from the autopilot. 3. In the event of a loss of GPS, utilize compass heading and last known location to avoid borders
	UCA-44: GCS provides excessive control stick input while in MANUAL or ASSISTED modes. **H-1/5/6**	Operator is unfamiliar with aircraft handling qualities.	N/A	Operator should practice relevant flight profiles for the mission in the simulator using the measured moments of inertia, center of gravity, and stability and control model.
		Operator is trying to recover the aircraft from an unsafe condition.	No g-force reading on the displays to the GCS.	1. When executing recovery procedures, the operator should first place the throttle to IDLE. 2. Operator should practice border or obstacle avoidance maneuvers within aircraft limits. 3. Operator should practice landing procedures with excessive or too little speed (that may require excessive control inputs for a safe landing).

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Throttle Input	UCA-48: GCS does not provide sufficient throttle control action to safely manoeuvre, climb, avoid an obstacle, or land. **H-5**	Throttle control process could be over or under sensitive to throttle movement.	N/A	1. A suitable "throttle control curve" should be implemented between the throttle lever angle and the command to the motors. 2. The operator should practice all flight profiles with the defined throttle control curve.
		Throttle control process may have changed with insufficient practice prior to flight test.		Test team should not change the throttle control process after taxi testing.
		Thrust response to throttle input will change during the flight profile based on the battery state of charge, as well as atmospheric density.		1. The simulator model should reflect the loss of achievable RPM due to battery state of charge. 2. Operator should practice takeoff and landings in the simulator at a variety of battery states of charge and atmospheric densities.
	UCA-49: GCS provides throttle control action when engines are powered and enabled during ground crew operations. **H-7**	Throttle Lock is thought to be ENGAGED or has failed.		Throttle lock setting should be present on the displays.
		Throttle is inadvertently moved during a seat swap or other GCS activities.		1. Engage throttle lock at all times when the motors are not in use. 2. Operator seat swap will not occur while the motors are powered. 3. Operator should carefully guard the throttle during ground operations.
	UCA-50: GCS provides throttle control action prior to desired engine select control action. **H-7**	The operator is distracted by other tasks involved in operations.		Operator should practice flight profiles in the simulator involving testing various configurations of the distributed electric propulsion system engine selections.
		Operator is unware of test conditions due to miscommunication between the test team.		Test team must maintain discipline following and between test points regarding aircraft configuration for recovery and transitions between waypoints.
	UCA-51: GCS provides throttle control action too long during landing roll or ground operations. **H-5a**	Throttle control process could be over or under sensitive to throttle movement.		1. A suitable "throttle control curve" should be implemented between the throttle lever angle and the command to the motors. 2. The operator should practice all flight profiles with the defined throttle control curve.
	UCA-52: GCS provides throttle control action too long when approaching a critical subsystem temperature limit. **H-2/4**	The aircraft is too far from the runway to safely recover without maintaining high motor power.		Test team should maintain proximity to the runway such that the aircraft can recover with minimum time at high motor power.
		The operator is unaware that an engine or critical component is approaching a temperature limit.	Internal temperature measurements are incorrect, not present, or in the wrong locations.	1. Temperature sensor readings must be verified in ground tests using a secondary source (such as FLIR camera). 2. Temperature readings must be clearly marked for the applicable motor or component.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Nosewheel Steering	UCA-55: GCS does not provide sufficient Nosewheel Steering control action when an obstacle is in the path during ground operations or during takeoff roll. **H-5a**	Operator is unaware that an obstacle is in their path.	N/A	1. Safety observer provides confirmation of path clearance to the test team. 2. Ground crew should remain behind the aircraft during operations to the maximum extent possible.
		The aircraft is moving at a faster speed then the operator realizes resulting in less NWS control than expected.		1. If avoiding an obstacle on the ground the operator should first reduce speed while attempting nosewheel steering. 2. Operator should practice takeoffs in the simulator starting and veering off of centerline.
	UCA-56: GCS provides excessive Nosewheel Steering control action during ground operations or during takeoff roll. **H-3/5a**	The aircraft is moving at a slower speed then the operator realizes resulting in greater NWS control than expected.		Operator should practice nosewheel steering during low-speed and high-speed taxi testing.
Transponder - ON/OFF	UCA-57: GCS does not provide XPDR ON control action prior to takeoff or after ATC direction. **H-5a**	The operator is distracted by other tasks involved in operations or delays XPDR power on due to extended ground operations and does not complete a secondary check.	N/A	1. XPDR ON should be part of the pre-taxi checklist. 2. Test team should maintain good checklist dicipline.
	UCA-58: GCS provides XPDR ON control action when the incorrect XPDR code is set. **H-5a**	The operator is unaware of the programmed XPDR code.	The operator has no indication of XPDR code.	1. XPDR code setting should be part of statup checklist. 2. The XPDR code should be verified with tower prior to taxing.
Battery Capacity - SET (Ah)	UCA-59: GCS provides the incorrect (too high or too low) Battery Capacity control action. **H-2/4**	The test team is unaware of what the actual battery capacity.	Battery tester and check device do not account for degradation of battery performance	An extra set of batteries not used in operation should be maintained and tested to characterize degredation of capacity from usage.
Battery Charge - SET (Ah)	UCA-60: GCS does not provide the Battery Charge setting control action after aircraft batteries have been recharged. **H-2/4**	The horizon PC operator is distracted by other tasks involved in operations.	There is no accurate real time measurement system for the battery charge.	1. Battery charge setting should be a start-up checkist items to include verifying a new state of charge in case the batteries were charged or have changed. 2. Test team should maintain good checklist discipline including redoing start-up checklists following extended ground operations.
	UCA-61: GCS provides the incorrect (too high or too low) Battery Charge setting control action. **H-2/4**		The reading from the battery check device gives a battery status that doesn't match the real battery state or the instrumentation reading.	Method for measuring battery state of charge should be verified in ground testing using a secondary source and for all batteries.
	UCA-62: GCS provides the Battery Charge setting control action too early prior to operating the battery such that the capacity has reduced from the measured state. **H-2/4**	Operations were delayed after the batteries were removed from the charger.	There is no accurate real time measurement system for the battery charge.	Battery charge should be re-tested and inputted prior operations to account for passive discharge.

Appendix B: Air Traffic Control and Tower Analysis

Control Actions	Unsafe Control Actions	Causal Factors	Feedback Failures	Mitigating Procedures
Taxi/Takeoff/Landing Clearance	UCA-85: Tower does not provide Clearance control action as needed for operations. **H-6**	Tower was not informed that aircraft is ready to taxi/takeoff, or scheduled to fly that day.	Test Team may not receive any positive acknowledgement from the Tower that they received the flight plan or request for clearance.	1. Call Tower during ground ops to provide an Est. Departure Time and verify that they have the flight plan 2. Invite Ops personnel (tower/flight ops) to the hangar and/or setup area to introduce them to the aircraft and mission
		Tower does not receive a radio call from the Test Team indicating that the aircraft is on approach for landing.	N/A	
		Tower does not receive the signal from the transponder indicating that the aircraft is on approach for landing.	Test Team may not have any feedback as to whether the transponder is functioning correctly.	
	UCA-86: Tower provides Clearance control action when an obstacle or debris is present on taxiway or runway. **H-5**	Tower is unaware of an obstacle or debris on the runway/taxiway at time of operations.	N/A	Test team completes FOD check prior to operations.
Weather/ Airspace Restrictions	UCA-87: Tower does not provide Weather notification when conditions in the airspace or at the airfield change. **H-1**	Tower is not aware that the test team is testing, that the weather was requested, or the test specific weather concerns.	N/A	1. Test team should brief the weather forecast for each day of testing to identify potentially limiting weather conditions to the DEP-SFD. 2. Test team should have a mechanism to monitor real-time ground weather conditions such as calling Tower to make determinations whether or not to takeoff prior to each sortie.
Traffic Deconfliction	UCA-88: ATC does not provide Traffic Deconfliction control action when traffic enters the airspace. **H-5b**	ATC in Italy doesn't have any direct way to communicate with the test team, particularly in the event of traffic entering the mission airspace	N/A	Consider getting Flight Aware software or another means to monitor air traffic for ourselves in real-time

Appendix C: Ground Crew Analysis

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Autopilot - OFF	UCA-69: GND Crew provides Autopilot OFF control action when preparing or during GCS operations. **H-6**	Ground crew is unaware that the GCS is utilizing or has already initialized the autopilot.	N/A	The Autopilot OFF switch, which resets the Autopilot, should only be actuated when called for by the Horizon PC operator.
Video - ON/OFF	UCA-71: GND Crew provides the Video ON control action during extended ground crew operations. **H-7**	Ground crew provides Video ON control action with the intention of utilizing the Video feed, but extenuating circumstances or test objectives delays or negates use of the GCS and need for the Video.	No Video ON indicator exists on the aircraft other than the switch position. If GCS is not in use or monitor is off, then ground crew may be unaware that the Video link is ON.	Ground crew should be concious of extended RF exposure risk and periodically verify that power to the video link is OFF during extended ground operations.
External Power ON/OFF	UCA-72: GND Crew provides an External Power ON control action while the external power is plugged in and external power circuit breaker is engaged when crew members are manipulating electrical components. **H-7**	GND Crew purposefully provides External Power ON control action but does not verify that other personnel are clear of electrical components because they are in a rush or unaware of the risk to ground personnel.	N/A	Ground crew should verify that personnel are clear of electrical components when providing the External Power ON control action.
	UCA-73: GND Crew provides the External Power ON control action prior to connecting the external power with the external power breaker engaged. **H-7**	GND Crew misinterprets the external power circuit breaker indicator light, thinking that the light OFF means the breaker is disengaged. (The circuit breaker collar is the indicator that the breaker is disengaged).	External power circuit breaker indicator light is ON when circuit breaker is engaged, regardless of external power switch setting.	SMCP should have a label "DISENGAGE BREAKERS PRIOR TO CONNECTING POWER"
		GND Crew member is unaware of the correct ground power control action order.	External power circuit breaker and indicator light are unlabled.	The external power circuit breaker and indicator light should be labeled.
Parachute - ARM	UCA-74: GND Crew does not provide the Parachute ARM control action prior to flight. **H-5b**	GND Crew is in a rush during ground procedures and inadvertantly skips arming the parachute.	N/A	1. GND Crew should verbalize mission critical actions to test team. 2. Test team should maintain good checklist discipline including redoing start-up checklists following extended ground operations.
		GND Crew delays arming of parachute because of extended ground operations and does not return to arm the parachute before flight operations.		
	UCA-75: GND Crew provides the Parachute ARM control action when the parachute system is being handled by ground crew and parachute power is ON. **H-7**	GND Crew does not verify that other personnel are clear of parachute system because they are in a rush or unaware of the risk to ground personnel.		GND Crew should verify that personnel are clear of the parachute system prior to arming.

Control Action	Unsafe Control Action	Causal Factors	Feedback Failures	Mitigating Procedures
Parachute Power ON/OFF	UCA-76: GND Crew does not provide the Parachute Power ON control action prior to flight. **H-5b**	GND Crew is in a rush during ground procedures and inadvertantly skips powering the parachute.	N/A	1. GND Crew should verbalize mission critical actions to test team. 2. GND Crew should complete preflight check immediately prior to taxiing for flight
		GND Crew delays powering of parachute because of extended ground operations and does not return to power the parachute before flight operations.		
	UCA-77: GND Crew provides the Parachute Power ON control action when the parachute system is being handled by ground crew. **H-7**	GND Crew does not verify that other personnel are clear of parachute system because they are in a rush or unaware of the risk to ground personnel.		GND Crew should verify that personnel are clear of the parachute system prior to arming.
Circuit Breakers ENGAGE [Bat 1/2/PL/EP]	UCA-78: GND Crew does not provide the Battery 1, Battery 2, and/or Payload Circuit Breaker(s) ENGAGE control action prior to operations. **H-6**	GND Crew is in a rush during ground procedures and inadvertantly skips the procedure.	N/A	1. GND Crew should verbalize mission critical actions to test team. 2. GND Crew should complete preflight check immediately prior to taxiing for flight
		GND Crew delays powering of parachute because of externanl power operations and does not return to power the parachute before battery operations.		
	UCA-79: GND Crew provides the Battery 1, Battery 2, and/or Payload Circuit Breaker(s) ENGAGE control action when subsystems are being handled by ground crew. **H-7**	GND Crew engages circuit breaker(s) but does not verify that other personnel are clear of electrical components because they are in a rush or unaware of the risk to ground personnel.		GND Crew should verify that personnel are clear of the parachute system prior to arming.
	UCA-80: GND Crew provides the Circuit Breaker(s) ENGAGE control action prior to connecting the power source(s). **H-7**	GND Crew is unaware of the correct procedure to power up the aircraft or is in a rush to complete the procedure.		SMCP should have a label "DISENGAGE BREAKERS PRIOR TO CONNECTING POWER"
VCU - SHUTDOWN [VCU Power - OFF]	UCA-81: GND Crew provides a VCU SHUTDOWN control action during GCS ground operations. **H-6**	Ground crew is unaware that the GCS is utilizing or has already initialized the VCU.	N/A	VCU shutdown should only be completed after verifying with the Horizon PC operator.
	UCA-82: GND Crew does not provide the VCU SHUTDOWN control action prior to removing power. **H-6**	GND Crew is unware of correct shutdown procedure or are in a rush.		GND Crew should verbalize shutdown actions to test team prior to completion.