Application of System-Theoretic Process Analysis (STPA) to a NASA Concept Electric Aircraft Battery System

Matthew P. Huffman, MS; NASA Glenn Research Center, Cleveland, OH, 44135, USA

James M. Green, MS; NASA Glenn Research Center, Cleveland, OH, 44135, USA

Tinicia J. Menifee, BS; Professional Solutions Co Intl, Bay St. Louis, MS, 39520, USA

Keywords: System-Theoretic Process Analysis, Hazard Analysis, Electric Aviation

Abstract

System-Theoretic Process Analysis (STPA) is a systems-based hazard analysis method that identifies unsafe interactions and control deficiencies in complex systems but has been rarely used for NASA programs in favor of more well-established hazard analyses. To evaluate its applicability, a NASA Safety and Mission Assurance (SMA) team applied the STPA method to an early-stage hybrid electrified aircraft concept, focusing on the energy storage system and electric powertrain. Objectives include assessing STPA's value relative to traditional methods and its suitability for early design phases. Activities include team training, system review, detailed STPA execution, and comparison with traditional analyses.

Findings show STPA provides a structured, comprehensive hazard evaluation and can identify additional risks by expanding analysis boundaries. However, traditional methods can yield similar results when applied rigorously, though they typically require more mature designs. Overall, STPA is a valuable addition, particularly for early development, informing safety requirements and supporting preliminary hazard analyses. Further pilot applications are recommended.

Introduction

STPA emerged in the early 2000s as a systems-oriented method for analyzing hazards by examining interactions and identifying deficiencies in system control across complex systems (Levenson, 2018). While widely used in industry, it has seen limited application within NASA, where traditional methods like Failure Modes and Effects Analyses (FMEAs) and Fault Tree Analyses (FTAs) dominate. Unlike these failure-focused approaches, STPA emphasizes system interactions and control structures, enabling identification of hazards beyond component-level failures.

STPA Overview

STPA is a hazard analysis method derived from the System-Theoretic Accident Model and Processes (STAMP) framework, which conceptualizes accidents as the result of inadequate system control rather than solely as consequences of component failures. Within this framework, STPA serves as the analytical technique used to identify hazardous conditions through a structured, top-down evaluation of complex system control structures. By modeling functional interactions among system components, STPA facilitates development of a system-level representation capable of revealing unsafe interactions and control deficiencies throughout the design.

STPA is implemented as an iterative four-step process.

1. **Defining the purpose of the analysis:** Identifies the losses to be prevented
2. **Modeling the control structure:** Development of a control structure block diagram that depicts controllers, control actions, controlled processes, and feedback loops to identify functional relationships and interactions throughout the system
3. **Identifying unsafe control actions:** Identification of unsafe control actions (UCAs) by systematically evaluating each control action within the modeled structure to determine how it could lead to the previously identified hazards. This evaluation considers four general categories: (1) failure to provide a required control action, (2) provision of a control action that leads to a hazard, (3) provision of a control action at an incorrect time or in an improper sequence, and (4) application of a control action for an incorrect duration. The result is a structured set of UCAs, often organized in matrix form.
4. **Identifying loss scenarios:** Identification of loss scenarios by determining the causal factors that could result in each unsafe control action, including deficiencies in the controller, flaws in the control algorithm or process model, communication or feedback failures, and other systemic factors.

Throughout the analysis, identified hazards, unsafe control actions, and loss scenarios may be reformulated as safety constraints. These constraints can be translated into safety requirements of increasing specificity as the design matures, thereby supporting progressive refinement of project-level safety documentation.

The STPA described in this paper was conducted in accordance with the *STPA Handbook*, published in March 2018 by Nancy G. Leveson and John P. Thomas, which provides detailed methodological guidance.

SUSAN Overview

The Subsonic Single Aft eNgine (SUSAN) Electrofan is an advanced hybrid-electric aircraft concept developed to reduce environmental impacts and introduce innovative technologies for next-generation subsonic regional transport. The concept targets a 50% reduction in emissions within the coming decades, with an ultimate objective of achieving net-zero emissions.

The SUSAN concept is designed to accommodate up to 180 passengers with an economic range of approximately 750 miles and a design range of 2,500 miles. A distinguishing feature of the aircraft is its 20-MW electrified propulsion architecture, which enables advanced propulsion–airframe integration to improve overall energy efficiency and reduce fuel consumption. The propulsion system employs a hybrid configuration in which a single aft-mounted turbofan provides primary thrust while also generating electrical power for distributed wing-mounted propulsors. The architecture also incorporates a single-use battery system that provides additional redundancy by supplying electrical power to the aircraft in the event of a primary engine failure. The hybrid-electric propulsion technology utilized by SUSAN aims to drastically reduce fuel consumption and greenhouse gas emissions compared to modern aircrafts while still maintaining safety and reliability. Additionally, the use of an electric motor provides sufficient redundancy to eliminate the need for a second gas turbine engine, making SUSAN unique in maintaining redundancy with a single turbine even in an engine out scenario.

To support the analysis presented in this paper, meetings were conducted with the NASA Glenn Research Center (GRC) SUSAN Project Manager and other technical experts to develop a sufficient technical understanding of the aircraft architecture and propulsion system. In addition, several published research papers describing the SUSAN concept were reviewed. Figure 1, reproduced from these references, provides a schematic overview of the electric powertrain architecture.

Conventional aircraft subsystems, such as hydraulic systems for landing gear and flight control actuation and conventional fuel systems for the gas turbine engine, were considered within the overall system boundary of the analysis, but the detailed hazard analysis focused on the novel aspects of the aircraft, particularly the electrified propulsion (EP) system and associated energy storage system (ESS).

Additional technical details on the SUSAN concept are provided in the referenced research papers listed at the end of this paper.

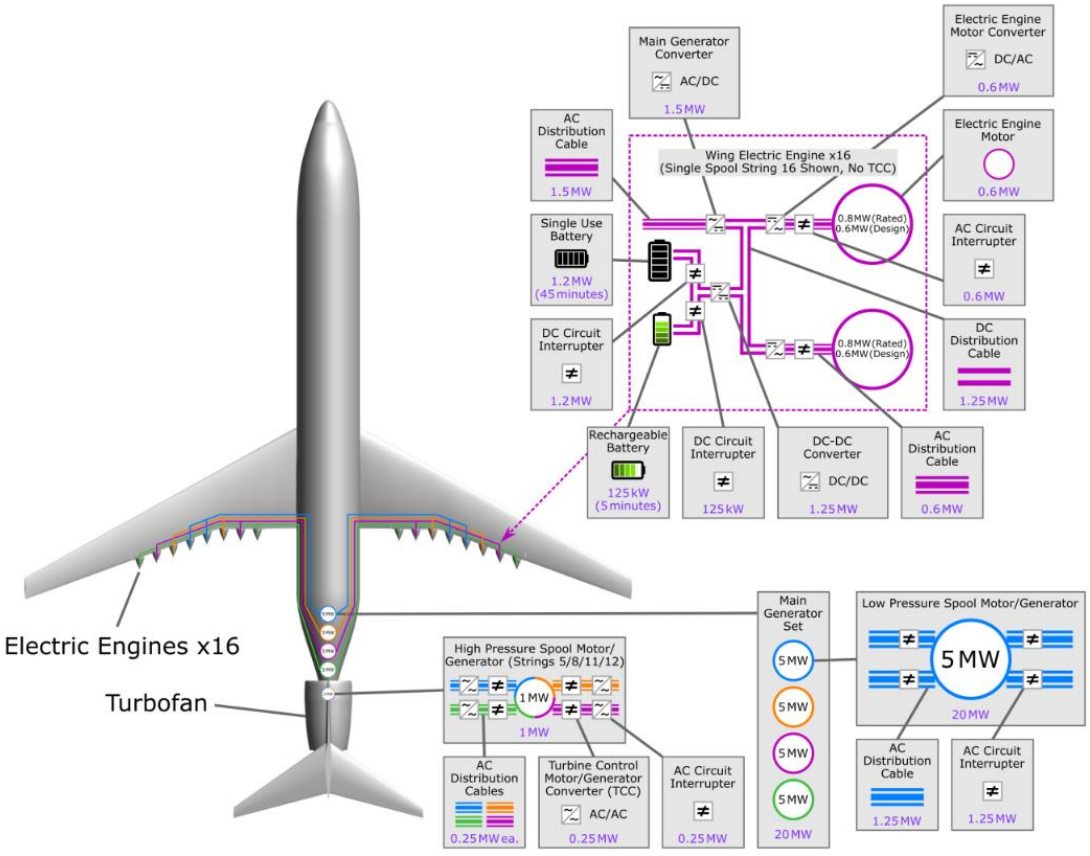

Figure 1—SUSAN Electrofan Power System Diagram [3]

SUSAN STPA

The following section discusses the iterative STPA process that was performed for the SUSAN concept. This serves as a high-level overview of how STPA can be performed on any early concept projects/programs.

Mission Statement.

Before initiating Step 1 of the Systems-Theoretic Process Analysis (STPA), the system mission and relevant stakeholders were identified. The system goal for this analysis was defined as: *"Ensure safe integration, flight, and operation of aviation systems utilizing novel electrical technologies".* Broad stakeholders considered in the analysis included NASA, passengers, flight and ground crew, the electrical aviation industry, airport operators, aircraft manufacturers, and battery/component manufacturers.

Defining the Purpose of the Analysis.

With the scope of the mission statement in mind, Step 1 of STPA could be implemented and is broken down into the four activities identified in Figure 2 below.

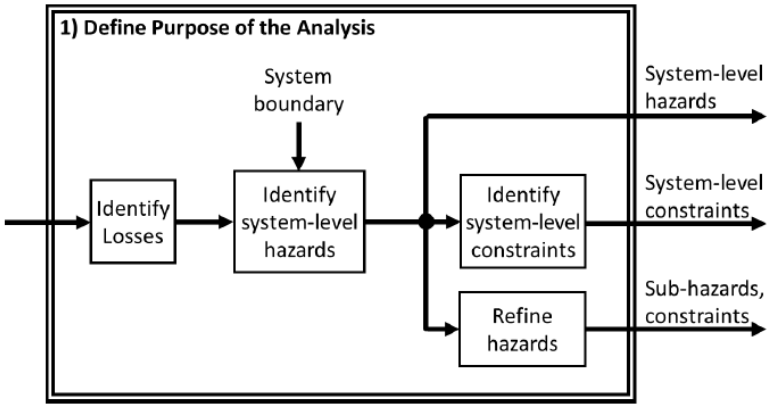

Figure 2—STPA Definition of Analysis Purpose Block Diagram [4]

In STPA, top-level concerns are defined as losses, which broadens the scope beyond traditional hazard analyses that often focuses primarily on component failures or physical injury. While such outcomes remain relevant, STPA also considers broader impacts such as reputational damage or operational disruption. For the SUSAN analysis, the following top-level losses were identified:

- **L-1:** Loss of human life or personnel injury (flight or ground personnel)
- **L-2:** Loss of or damage to aircraft
- **L-3:** Loss of technology credibility or desirability, impacting future adoption
- **L-4:** Loss of aircraft ability to complete intended flight missions

- **L-5:** Loss of system performance (e.g., power, control, thermal systems, turbofan engine, electric propulsors, battery/energy storage system, compressor)
- **L-6:** Damage to ground infrastructure
- **L-7:** Environmental damage
- **L-8:** Loss of ability to complete ground operational missions (e.g., turnaround operations)

Based on these losses, the following system-level hazards were defined. Each system-level hazard is linked to the losses it could produce, and several hazards were refined into sub-hazards following the optional refinement step in STPA Step 1.

Hazard ID	Hazard Description	Associated Losses	Sub-Hazards / Requirements
H-1	Aircraft has insufficient lift or thrust to meet flight requirements	L-1–L-5	H-1.1: Power to electric propulsion systems is insufficient during any phase of flight H-1.2: Fuel supply to the gas turbine engine is insufficient during any phase of flight
H-2	Aircraft environmental conditions exceed acceptable limits for passengers, crew, or cargo	L-1–L-5	H-2.1: Adequate fresh air is maintained in the cabin under all flight conditions H-2.2: Hazardous gases are safely ventilated in the event of ESS thermal runaway H-2.3: Smoke, fire, and harmful gases are contained and vented during single-cell or module thermal runaway
H-3	Aircraft unable to maintain safe, controlled flight	L-1–L-5	H-3.1: Flight controls and avionics remain functional without electrical interference from electric propulsion systems H-3.2: Electric propulsion configuration provides sufficient redundancy to maintain yaw control during a single failure long enough for safe landing and egress
H-4	Aircraft structure unable to withstand worst-case environmental loading	L-1–L-5	H-4.1: Wing and fuselage structural integrity must be maintained in all loading conditions from electric engine forces, battery, and cable weight for all phases of flight
H-5	Aircraft unable to meet safety and performance requirements following a single hardware or software failure	L-1–L-5	
H-6	Aircraft unable to meet ground operational safety or efficiency requirements	L-6, L-8	H-6.1: Ground infrastructure supporting electric propulsion provides a safe environment for operators and equipment H-6.2: Infrastructure and energy storage systems enable turnaround times compatible with airport operational requirements

The terminology used in STPA differs from traditional NASA hazard analysis language. Many of the hazards listed above may correspond to differently named hazards in conventional analyses, and STPA intentionally avoids defining hazards solely at the component or subsystem level (e.g., "battery short circuit"). This systems-oriented framing is emphasized throughout the STPA methodology to avoid common pitfalls when identifying hazards.

Another key element of Step 1 is the identification of system constraints. These constraints are typically derived by restating hazards as requirements that must always be satisfied. For example, the hazard *"Aircraft has insufficient lift or thrust to meet flight requirements"* corresponds to the constraint *"The aircraft must maintain sufficient lift and thrust to meet all flight requirements."* Such constraints form the basis for deriving safety requirements.

Although the full set of system and subsystem constraints was not developed in this analysis due to time limitations, their development is a critical step in the STPA process. Generating these constraints would support the formulation of safety requirements for project documentation, including contract requests for proposals and top-level program safety specifications. This approach was identified as a main recommendation as it drives the early identification of critical safety requirements and constraints that would likely not emerge until later stages under traditional hazard analysis methods.

With the system losses, hazards, and preliminary constraints defined, the analysis proceeded to development of the system control structure.

Modeling the Control Structure.

Arguably the most fundamental difference between STPA and traditional hazard analysis is STPA's representation of the system as a control structure. The STPA Handbook characterizes a hierarchical control structure as a system model composed of feedback control loops that collectively enforce constraints on system behavior. This concept is illustrated in Figure 3.

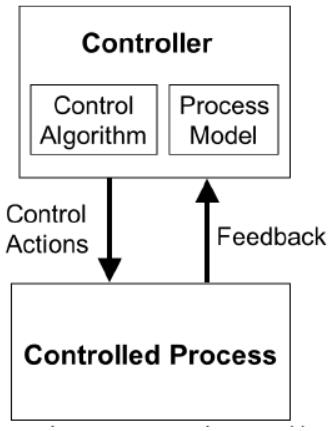

Figure 3—Generic Control Loop [4]

The control structure depicts interactions between system components; however, it is not intended to be a physical model of the system. Importantly, it does not assume perfect execution of control actions, aka "obedience". For example, a control command may not be received, may be

misinterpreted, or may not produce the expected response. This becomes more apparent in later STPA steps when identifying unsafe control actions, which correspond conceptually to traditional hazard definitions used in analyses such as those performed at NASA. Because control structures are central to STPA, the STPA Handbook provides extensive discussion of their development, which is not reiterated here for brevity.

For the SUSAN project, significant early effort was devoted to developing and refining the system control structure. As discussed previously, the analysis examined the Energy Storage System (ESS) and portions of the electric powertrain in greater detail than other subsystems. However, it was also important to represent the overall system—including ground operations—at a high level to ensure that potentially hazardous interactions across the broader system were not overlooked.

The final control structure developed for the SUSAN STPA is shown in Figure 4.

Key aspects of the control structure include:

- Includes a broad set of entities that interact with the aircraft, with color used to indicate areas where the model explores greater subsystem detail. For example, the ESS is modeled down to the individual battery cell level, while traditional flight systems are represented at a higher level.

- The Aircraft Controller represents a complex integrated system that could be decomposed further if required. For the scope and timeline of this study, modeling it as a single element was sufficient.

- Single arrows are generally used to represent control or feedback paths, even when multiple signals are involved. The associated labels identify the specific control and feedback signals, which are later analyzed individually during subsequent STPA steps.

As noted in the STPA Handbook, constructing the control structure can reveal hazardous interactions that might not be identified through traditional analyses, particularly during early design phases. For example, depletion of the backup battery if activated prior to required use or potential loss of signal to the emergency battery in an emergency scenario. The control structure provides an organized way to manage increasing system complexity as the analysis evolves, as demonstrated by the treatment of the SUSAN Aircraft Controller.

For these reasons, one of the primary recommendations from this project is to perform STPA as early as possible in the system development process, at minimum through control structure development. Doing so can support the formulation of safety requirements and inform the preliminary hazard analysis.

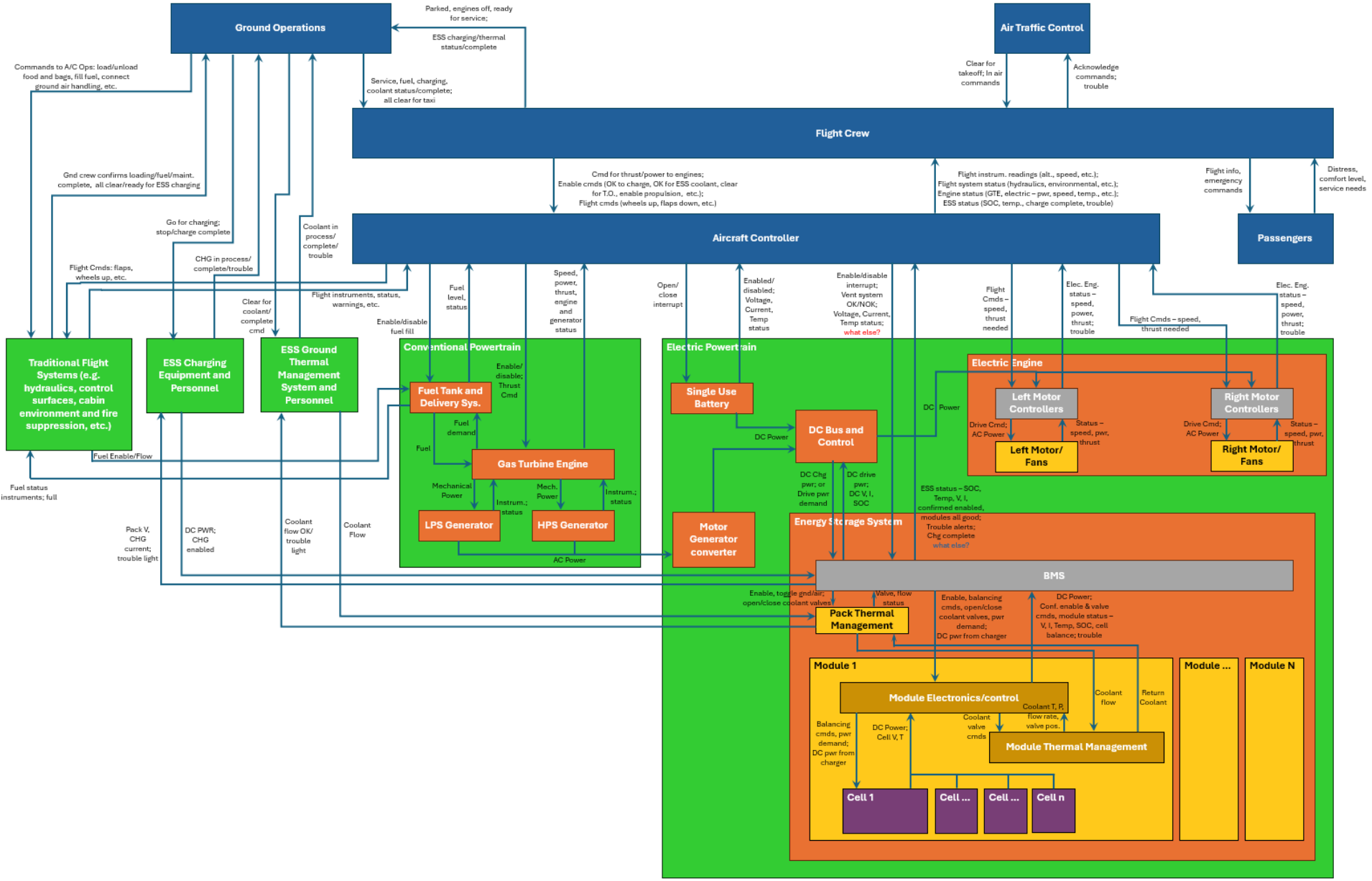

Figure 4—SUSAN STPA Control Structure

Identifying Unsafe Control Actions.

Once the control structure is sufficiently laid out, the next step in the STPA process evaluates each control action identified in the control structure and expands them into Unsafe Control Actions (UCAs) (a control action that, in a particular context and worst-case environment, will lead to a hazard).

STPA identifies four ways in which a control action can be unsafe:

1. Not providing the control action leads to a hazard
2. Providing the control action leads to a hazard
3. Providing a potentially safe control action too early, too late, or in the wrong order leads to a hazard
4. A continuous control action lasts too long or is stopped too soon

To conduct this analysis, the SMA team divided the control structure into three sections: the electrical powertrain, the conventional powertrain, and high-level system interactions. Each team member then developed a detailed spreadsheet listing all control actions within their assigned section and evaluated them for potential UCAs. These entries—as well as the material discussed in the following sections—should be considered preliminary drafts. Current resource limitations prevented more in-depth development of the STPA steps. Future work would focus on more detailed development of the analysis ensuring consistency across the datasets.

Examples of several UCAs identified during the analysis are shown in Table 1. Terms are abbreviated for brevity.

Table 1—Examples of Unsafe Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
UCA-AC3: Ground Ops Commands ground crew Go for ESS charging	UCA-AC3.1: Gnd Ops does not provide Cmd to gnd crew to begin ESS charging when needed during ground operations	UCA-AC3.2: Gnd Ops provides Cmd to gnd crew to begin ESS charging when ESS does not require charge	UCA-AC3.3a: Gnd Ops provides Cmd to gnd crew to begin ESS charging at a time in the process that conflicts with fuel filling operational safety requirements;	N/A. Discrete command
Enable vent system from aircraft controller to BMS	**UCA-AC-005.1:** Aircraft controller does not enable vent system to Battery Management System when system is overheating or a fire occurs	**UCA-AC-005.2:** Aircraft controller enables vent system to Battery Management System in low temperature environments	**Too early:** N/A **Too late: UCA-AC-005.3:** Aircraft controller enables vent system to Battery Management System too late in a fire/loss of cabing pressure/ emergency scenario **Out of order:** N/A	Enabling is an on/off scenario, not too long/too soon application

As shown in the UCA tables, many control actions are binary in nature (on/off, apply/do not apply, provide/don't provide command, etc). For binary actions, the final column of the UCA table is not applicable. While such actions may occur too early or too late, they cannot be applied for too long or stopped too soon, since they represent discrete on/off commands similar to operating a power switch. The tables also illustrate that multiple UCAs may be associated with a single control action. For example, a hazard may arise if an action occurs either too early or too late.

Due to time constraints, the UCAs developed in this analysis were not explicitly linked to higher-level hazards. Although this linkage is a routine step in the STPA process, it was not performed during this preliminary analysis due to being lower priority. Once a UCA is identified, they can be used to derive controller constraints. These constraints typically restate UCAs in a form that can be translated into more detailed safety requirements, analogous to the higher-level constraints discussed earlier. For example, the UCA "*Aircraft controller does not enable vent system to Battery Management System when system is overheating or a fire occurs"* could be written as the constraint *"Aircraft controller shall provide proper environmental ventilation when an overtemperature or fire occurs (i.e. Fire Detection and Suppression Systems)".*

At this stage of the analysis, the focus remains on identifying unsafe control actions rather than examining their causes or consequences, which would be more typical of traditional hazard analyses. The next step in the STPA process is to develop loss scenarios, which explore the potential causal paths leading to the identified UCAs.

Identifying Loss Scenarios.

In the context of STPA, a loss scenario encompasses the causal factors that may result in unsafe control actions and associated hazards. Developing loss scenarios is a rigorous, iterative process that systematically examines all pathways within the control structure, as depicted in Figure 5, to identify potential failures in control actions or feedback mechanisms. For example, the Aircraft Controller (controller) provides power to the Single Use Battery in an emergency (Controlled Process) via a voltage gate (Actuator), which in turn provides a feedback command back to the Aircraft Controller to notify power demands (Feedback) via a voltage sensor (Sensor). The loss scenario exercise examines methods in which all these methods can individually experience failure.

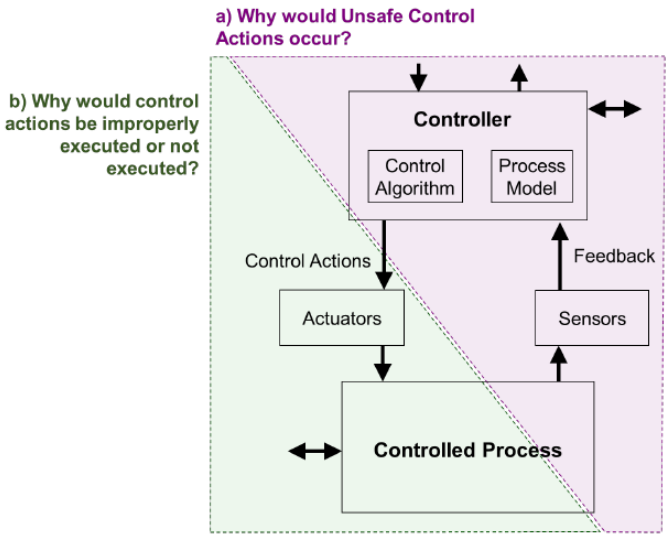

Figure 5—STPA Loss Scenarios Block Diagram [4]

Up to this stage, the STPA method focused primarily on the relationships between controllers and controlled processes rather than the physical mechanisms used to implement control or feedback. In the loss scenario step, actuators and sensors are introduced to represent how control actions are executed and how feedback is returned to the controller. These elements may represent physical hardware or conceptual/virtual signals.

Evaluating the interactions shown in Figure 5 leads to four general categories of causes for unsafe control actions, as illustrated in Figure 6.

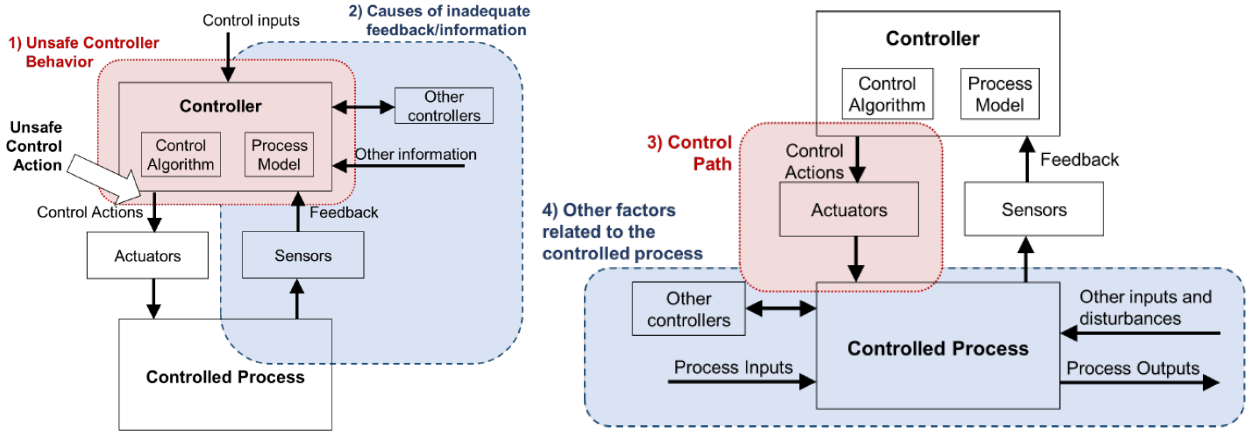

Figure 6—Categories of Loss Scenarios [4]

The STPA Handbook provides extensive guidance for this step, which is typically the most time-consuming portion of the analysis. For the SUSAN project, a representative set of loss scenario tables was developed, although additional time would have been required to fully complete and refine them. Appendix B provides an example of a loss scenario developed based on a UCA from the electric powertrain, which was the primary focus of the project.

Several observations emerged from performing the loss scenario analysis:

Scale and rigor of the process: Evaluating approximately 180 UCAs across roughly ten loss-scenario categories results in a very large analysis matrix. This approach has both advantages and limitations.

- *Advantages*
  - The process encourages a highly rigorous examination of the system, including interactions that may not be considered in traditional hazard analyses
  - Potential hazards can be evaluated even before detailed interface designs are finalized
  - The process can be iterative. In some cases, analysis shows that an identified item is not actually a UCA, while in other cases it reveals previously unidentified UCAs
- *Limitations*
  - The STPA Handbook provides general guidance, but practical application often requires experience or additional training
  - Distinguishing between the various loss scenario categories can be challenging, as their perspectives are closely related
  - Identification of loss scenarios may vary among analysts depending on their background and expertise
  - The method does not explicitly incorporate likelihood-versus-consequence prioritization, and the treatment of existing mitigations is not always clear.
  - Attempting to populate the entire matrix may produce scenarios of limited practical value (for example, simple human availability issues). Greater experience with the method can

help streamline the analysis by de-prioritizing low-value combinations earlier in the process

Insights from the loss scenario analysis: Despite these challenges, the process revealed several noteworthy scenarios that might not have been identified using traditional hazard analysis approaches:

- External influences—such as personnel actions or environmental conditions—can be readily incorporated into the analysis.

- Communication failures between hardware, software, or personnel may reduce system fault tolerance. For example, independent verbal checks by ground personnel could verify that aircraft charging has begun successfully if onboard notifications fail.

- One scenario of broader relevance to electric aircraft operations involved the UCA: *"Air Traffic Control (ATC) provides routing or flight commands when the aircraft does not have sufficient energy to execute them."* This highlights the potential need for ATC awareness of aircraft energy state. Conventional aircraft typically maintain large fuel reserves, reducing the need for ATC to consider fuel status when assigning holding patterns. For electric or hybrid aircraft, however, even a short delay—such as a 10–15 minute hold—could significantly affect the ability to land safely or perform a go-around.

- Another scenario involved the UCA: *"Flight crew commands the aircraft controller that charging is permissible while ESS power is still required for aircraft operations."* This suggests a potential need for additional interlocks between ground operations and the aircraft. In efforts to begin charging quickly during turnaround, hazards could arise if the aircraft appears parked but still requires power for shutdown or other functions. Such interactions may not have been identified through traditional hazard analysis methods.

Completion of the loss scenario analysis represents the final major step in the STPA process. The results are intended to inform design engineers and support collaborative refinement of the system design as it evolves. The analysis can also be used to further develop safety constraints and translate them into detailed safety requirements.

The STPA Handbook does not provide direct guidance on how to complete the transition from analysis results to finalized requirements. However, based on the experience of the team, our interpretation would be that the system safety requirements would be generated to prevent the casual scenarios (UCAs) identified by STPA. For example, the loss scenario: *Actuator opens the gate to send power to the Single Use Battery but isn't properly executed at the Single Use Battery due to electrical failure* can be used to develop the requirement *Electrical connections and wiring shall be designed with insulation and shielding to prevent circuit failure*.

Traditional Hazard Analysis and Comparison to STPA

A key claim made by proponents of the STPA method is that it can be applied early in the concept phase of a design and can identify hazards that may be overlooked by traditional hazard analysis methods. This advantage is attributed primarily to STPA's broader system perspective, including explicit consideration of software, control systems, and complex interactions between system elements.

To evaluate this claim, the intent of the assessment was to perform a relatively comprehensive independent hazard analysis using traditional methods, led by experienced system safety personnel who were not involved in the STPA effort. Due to resource restrictions, the project concluded earlier than anticipated, resulting in only a limited independent hazard analysis being completed. The following list of high-level hazards was identified by the external system safety team:

Identified hazards:

- Vehicle loses control in flight
- Battery chemical exposure
- Short circuit
- Propulsion fan failure
- Unknown battery state of charge (off-nominal condition)
- Thermal runaway

This list illustrates a common characteristic of traditional hazard analyses: the process typically begins with high-level hazards and progressively expands as system design matures. Analysts then examine each subsystem in greater detail to identify additional hazards, consequences, controls, and verification methods. Although the abbreviated analysis performed here did not reach that level of detail, prior experience with similar projects provides useful context for comparison with the STPA results. One final thought is that if traditional hazard analysis techniques were to broaden their system boundary scope, they may be able to achieve similar results captured in the STPA analysis as the largest benefit of STPA is its rigorous process.

This discussion provides context for the central question of this study: does STPA offer significant advantages compared with traditional NASA hazard analysis approaches? This question is addressed further in the Conclusion section.

Conclusions and Recommendations

STPA offers several advantages, particularly its ability to be applied during early concept development and its emphasis on evaluating system-wide interactions in addition to its extensive built-in level of rigor. For this reason, the authors recommend prioritizing the use of STPA during the pre-award and concept phases of projects. At these stages, STPA can support the development of safety requirements for procurements and augment the traditional Preliminary Hazard Analysis (PHA). Applying STPA early may help identify system interactions and potential loss scenarios that can be incorporated into contract requirements or considered during early design development.

Traditional hazard analysis methods can also be strengthened by incorporating STPA principles, including expanding system boundaries and applying more structured, interaction-focused evaluations. This integration can broaden hazard identification and produce a more comprehensive safety assessment. Regardless of method, analytical rigor remains essential.

Established NASA safety processes retain key strengths, including their structured progression from hazard identification through verification and their ability to prioritize risk using likelihood-consequence frameworks. This study did not find sufficient evidence that STPA can fully replace these prioritization and verification approaches.

NASA should continue evaluating how SMA interacts with engineering, production, testing, and acquisition organizations throughout project lifecycles. Earlier engagement may present challenges related to maintaining SMA independence, but it may also create opportunities to apply safety expertise and tools earlier in project development. Because STPA emphasizes system interactions and control structures, its greatest benefit may occur when it is integrated with systems engineering processes rather

than applied solely as a standalone safety analysis, allowing additional benefits that extend beyond just SMA.

Outside of hazard analysis the STPA Handbook discusses applications of its method to workplace safety programs, leading indicators for mishaps, safety management systems, and how STPA concepts might inform organizational safety improvement. Future work could evaluate these topics as potential adoption/application benefits within the SMA organization.

It is the recommendation of this team that established system safety and reliability tools such as traditional hazard analysis, Fault Tree Analysis (FTA), or Failure Modes and Effects Analysis (FMEA) should continue to be used.

Acknowledgements

The authors would like to thank our SMA Management for funding and staffing this project, the SUSAN technical team, particularly project leader Ralph Jansen, and our SMA colleagues Abigail Rodriguez, Ian Milray, and Darcy DeAngelis for helping with hazards analysis and reviewing materials along the way.

Appendix A – Acronym List

ATC	Air Traffic Control
ConOps	Concept of Operations
EPFD	Electrified Powertrain Flight Demonstrator
ESS	Energy Storage System
FAA	Federal Aviation Administration
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HPS	High Pressure Spool
IA	Independent Analysis
LPS	Low Pressure Spool
LxC	Likelihood x Consequence
MAI TAI	Mitigating Arc Inception via Transformational Array Instrumentation
PHA	Preliminary Hazard Analysis
STAMP	System-Theoretic Accident Model and Process
STPA	System-Theoretic Process Analysis
SUB	Single Use Battery
SUSAN	Subsonic Single Aft eNgine
UCA	Unsafe Control Action

Appendix B – Loss Scenarios Examples

	Failures Related to the Controller (for physical controllers)	Inadequate Control Algorithm	Unsafe Control Input	Inadequate Process Model
Unsafe Controller Action	STPA Examples: - Physical failure of the controller itself - Power Failure - Etc.	STPA Examples: - Flawed implementation of the specified algorithm -Algorithm is flawed -Algorithm becomes inadequate (i.e. degradation, time, etc.)	STPA Examples: - UCA received from another controller (already addressed when considering UCAs from other controllers)	STPA Examples: Controller: -Receives incorrect feedback/information - Receives correct F/I but interprets incorrectly or ignores it -Does not receive F/I when needed (i.e. delayed or never) - Necessary controller F/I does not exist
UCA-AC-001.1: Aircraft controller does not enable power to single use battery in emergency situation	The A/C physical controller to the single use battery fails during emergency scenarios resulting in the inability of the aircraft to power engines/provide backup power in the event of engine/power failure Causes of physical failures: - Short/open circuit in component/wire - Connector failure	An emergency scenario occurs but the software in the A/C fails to enable the single use battery	Pointers to other related UCAs	Aircraft controller does not enable power to single use battery in emergency situation because it receives incorrect feedback/information that the aircraft is in nominal state Aircraft controller does not enable power to single use battery in emergency situation because software misinterprets input or provides inaccurate output Aircraft controller does not enable power to single use battery in emergency situation because it does not receives/gets delayed feedback/information that the aircraft is in emergency state (no communication that engines have failed, external power sources have failed, etc.) There is no feedback/information that identifies that the aircraft is in an emergency scenario (i.e. required single use battery power)

Unsafe Control Action	Feedback or information not received	Inadequate feedback is received
	Examples: - F/I sent by sensor(s) but not received by controller - F/I is not sent by sensor(s) but is received or applied to sensor(s) - F/I is not received or applied to sensor(s) - F/I does not exist in control structure of sensor(s) do not exist	Examples: - Sensor(s) respond adequately but controller receives inadequate F/I - Sensor(s) respond inadequately to F/I that is received or applied to sensor(s) - Sensor(s) are not capable or not designed to provide necessary F/I
UCA-AC-001.1: Aircraft controller does not enable power to single use battery in emergency situation	Feedback/Information is not sent by the BMS to the Aircraft Controller telling it to turn on the Single Use Battery (i.e. identified emergency scenario)	Inadequate Feedback/ Information is sent by the Single Use Battery voltage sensor(s) to the Aircraft Controller incorrectly telling the A/C that it is powered on, resulting in the A/C assuming the Single Use Battery is already powered on and making the decision not to turn it on - Sensor(s) respond inadequately to F/I that is received or applied to sensor(s) - Sensor(s) are not capable or not designed to provide necessary F/I

Unsafe Control Action	Control Action is not executed	Control Action improperly executed
	Examples: - Control action is sent by controller but not received by actuator(s) - Control action is received by actuator(s) but actuator(s) do not respond -Actuator(s) responds but the control action is not applied to or received by the controlled process	Examples: - Control action is sent by controller but received improperly by actuator(s) - Control action is received correctly by actuator(s) by actuator(s) respond inadequately - Actuator(s) respond adequately, but the control action is applied or received improperly at the controlled process - Control action is not sent by controller, but actuators or other elements respond as if it had been sent

UCA-AC-001.1: Aircraft controller does not enable power to single use battery in emergency situation	A/C sends command to send power to the Single Use Battery, but the command is not executed due to: - Faulty Actuator/Switch - Wire breaks - Bad connectors Which results in the Single Use Battery not receiving power (turning on) when needed (i.e. in emergency scenario)	A/C sends command to send power to the Single Use Battery, but the command is not executed due to: - Malfunction in the line out from the Aircraft Controller misinterprets information sent to actuator - Actuator receives input but does not respond to send power to SUB or send insufficient power - Actuator opens the gate to send power to the SUB but isn't properly executed at the SUB due to leakage current

Unsafe Control Action	<u>Control Action not executed</u>	<u>Control action improperly executed</u>
	Examples: - Control action is applied or received by the controlled process but the controlled process does not respond	Examples: - Control action is applied or received by the controlled process but the controlled process responds improperly - Control action is not applied or received by the controlled process but the process responds as if the control action had been applied or received
UCA-AC-001.1: Aircraft controller does not enable power to single use battery in emergency situation	Power is sent from Aircraft Controller to SUB but the SUB does not respond due to: - SUB is depleted (dead battery) - Internal SUB failures (wire shortages, chemical leakage, overheated, electrical component failure)	Power is sent from Aircraft Controller to SUB but the SUB responds improperly via: - Not providing sufficient power back to system

References

[1] Bowman, A. (2021). *SUSAN Electrofan* [Review of *SUSAN Electrofan*]. Electrified Aircraft Propulsion; NASA Glenn Research Center. https://www.nasa.gov/eap-aircraft-concepts/susan-electrofan/

[2] Chapman, J., Kratz, J., Dever, T., Mirhashemi, A., Heersema, N., & Jansen, R. (2023). *SUSAN Concept Vehicle Power and Propulsion System Study* [Review of *SUSAN Concept Vehicle Power and Propulsion System Study*]. https://doi.org/10.2514/6.2023-1749

[3] Chau, T., & Duensing, J. (2024). *Conceptual Design of the Hybrid-Electric Subsonic Single Aft Engine (SUSAN) Electrofan Transport Aircraft* [Review of *Conceptual Design of the Hybrid-Electric Subsonic Single Aft Engine (SUSAN) Electrofan Transport Aircraft*]. https://doi.org/10.2514/6.2024-1326

[4] Leveson, N., & Thomas, J. (2018). *STPA Handbook*. MIT. https://www.flighttestsafety.org/images/STPA_Handbook.pdfNASA SUSAN project details: https://www.nasa.gov/eap-aircraft-concepts/susan-electrofan/

[5] Litt, J., Kratz, J., Biano, S., Sachs-Wetstone, J., Dever, T., Buescher, H., Ogden, N., Valdez, F., Budolak, D., Boucher, M., Patterson, A., & Jansen, R. (2023). *Control Architecture for a Concept Aircraft with a Series/Parallel Partial Hybrid Powertrain and Distributed Electric Propulsion* [Review of *Control Architecture for a Concept Aircraft with a Series/Parallel Partial Hybrid Powertrain and Distributed Electric Propulsion*]. https://doi.org/10.2514/6.2023-1750

[6] *MIT Partnership for Systems Approaches to Safety and Security (PSASS)*. (2025). Mit.edu. https://psas.scripts.mit.edu/home/

[7] Sachs-Wetstone, J., Buescher, H., & Horning, M. (2024). *SUbsonic Single Aft eNgine (SUSAN) Power/Propulsion System Hardware-in-the-Loop Test Results* [Review of *SUbsonic Single Aft eNgine (SUSAN) Power/Propulsion System Hardware-in-the-Loop Test Results*]. https://doi.org/10.2514/6.2024-3823 System Health Management for a Series-Parallel Partial Hybrid Powertrain with Distributed Electric Propulsion – Jlitt