Proceedings of ASME Turbo Expo 2020
Turbomachinery Technical Conference and Exposition
GT2020
September 21-25, 2020, Virtual, Online

GT2020-16335

ELECTRIFIED AIRCRAFT PROPULSION SYSTEMS: GAS TURBINE CONTROL CONSIDERATIONS FOR THE MITIGATION OF POTENTIAL FAILURE MODES AND HAZARDS

Donald L. Simon
NASA Glenn Research Center
Cleveland, OH, USA

Joseph W. Connolly
NASA Glenn Research Center
Cleveland, OH, USA

ABSTRACT

This paper provides a high-level review of the potential failure modes and hazards to which electrified aircraft propulsion (EAP) systems are susceptible, along with potential gas turbine control-based strategies to assist in the mitigation of those failures. To introduce the types of failures that an EAP system may experience, a generic EAP system is considered, consisting of gas turbine engines, mechanical drives, electric machines, power electronics and distribution systems, energy storage devices, and motor driven propulsors. The functionality provided by each of these EAP subsystems is discussed, along with their potential failure modes, and possible strategies for mitigating those failures. To further illustrate the role of gas turbine controls in mitigating EAP failure modes, an example based on a simulated EAP concept aircraft proposed by NASA is given. The effects of failures are discussed, along with turbomachinery control strategies, including reversionary control modes, and control limit logic.

NOMENCLATURE

DAL	Development assurance level
EEC	Electronic engine control
EAP	Electrified aircraft propulsion
FHA	Functional hazard assessment
GTF	Geared turbofan
HPC	High pressure compressor
HPX	Horse power extraction
LPC	Low pressure compressor
N1c	Corrected fan speed
N1dot	Fan speed derivative
PLA	Power lever angle
Ps3	High pressure compressor exit static pressure
RU	Ratio unit
SM	Stall margin
STARC-ABL	Single-aisle turboelectric aircraft with aft boundary layer propulsor
T-MATS	Toolbox for the modeling and analysis of thermodynamic systems
VAFN	Variable area fan nozzle
VBV	Variable bleed valve
VSV	Variable stator vane
Wf	Fuel flow rate

INTRODUCTION

Electrified aircraft propulsion (EAP) systems hold great potential for reducing aircraft fuel burn, emissions, and noise. Currently, NASA and other organizations are actively working to identify and mature technologies necessary to bring EAP designs to reality. A requirement for the development of civil aircraft and their systems is to identify and appropriately mitigate any potential hazards in the design to ensure that the system is safe [1,2]. The aircraft development process includes defining aircraft functions, allocating those functions to aircraft systems, developing the system architecture, applying requirements, and implementing the system. As these development steps are conducted, several additional processes integral to ensuring system safety, requirements validation, and process assurance are happening concurrently in a coordinated, iterative fashion. This includes a system safety evaluation that consists of a functional hazard assessment (FHA) conducted to identify all potential failure conditions of each function and classify those failures according to the severity of their effects on the aircraft or its occupants. The more severe a function's failure condition classification, the greater the development assurance level (DAL) required for the function to ensure that the probability of the hazard is acceptably low.

The relationship between the probability of a failure and the consequence of that failure (hazard category) is shown in Figure 1 [3,4]. The required DAL for a function is related to the consequence that a failure in that function will cause—the more severe the hazard, the higher the DAL required to ensure an acceptably low probability of occurrence [4].

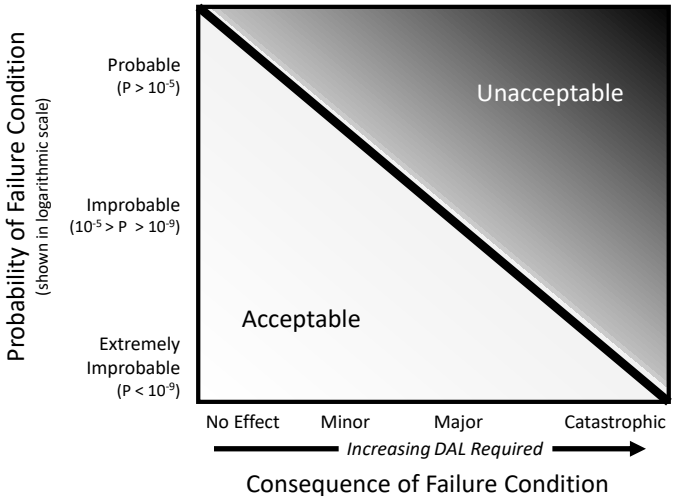


Figure 1. Relationship between Failure Probability and Failure Hazard Category [3]

Typical aircraft propulsion functions considered during the system development and safety assessment process may include thrust modulation, thrust reverser control, communication of engine health and status information to the aircraft, and passenger safety [1]. A combination of protective strategies are applied to ensure that engine functions have safety levels in accordance with their DAL requirements. These strategies may include defined maintenance and overhaul schedules, containment systems to prevent uncontained failures, over-speed protection logic, and fail-safe design concepts leveraging system redundancy. The engine control system plays a significant role in assuring engine fail-safe operation. Typically, an electronic engine control (EEC) is a redundant dual-channel design with built-in test and monitoring capability for potential failures in processors, sensors, and actuators. In the event of a system failure, logic within the EEC is designed to automatically detect and mitigate the anomaly. Mitigation actions may include reverting to physically redundant controls hardware, commanding actuators to fail-safe positions, or transitioning to reversionary control modes that allow the engine to function safely, although perhaps at a reduced performance level.

Today, aircraft engines and their control systems receive type certificate approval as a stand-alone system to signify their airworthiness. However, the complex coupling and distributed nature of EAP designs are expected to place added challenges on the certification of these systems. FHAs are needed to identify and assign DALs to all propulsion system functions. FHAs performed on conceptual EAP systems are provided in Refs. [5,6]. Ref. [5] analyzes the electrical network of a turboelectric distributed propulsion concept while Ref. [6] analyzes the EAP systems of four vertical lift vehicles. In terms of failure mitigation, it is expected that redundancy within the EAP architecture will be required to assure that the propulsion system still delivers propulsive thrust or torque in the event of a failure.

As with conventional engine designs, the EAP control system is expected to play a significant role in assuring that EAP systems comply with the airworthiness standards set forth by regulatory agencies. This includes failure detection [7] and mitigation logic, reversionary control modes, and contingency control modes to respond to EAP system failures. The reconfiguration flexibility of EAP architectures may allow multiple acceptable control mitigation responses for an individual failure, thus enabling optimal control reconfiguration based on current mission objectives.

This document provides an initial high-level review and documentation of the potential failure modes and hazards posed by a generic EAP system. The paper will also provide an example evaluation of the potential failure modes in a concept EAP system proposed by NASA, along with turbomachinery control considerations to assist in the mitigation of those failures.

GENERIC EAP SYSTEM: COMPONENTS AND FAILURE MODES

A high-level diagram of a generic hybrid EAP system architecture is shown in Figure 2. The main subsystems of this architecture are supervisory controls, gas turbine engines, mechanical drive systems, electric machines, power electronics and distribution systems, energy storage devices, and propulsors.

The architecture shown in Figure 2 is a simple "single string" design in the sense that there is a single path or string that mechanical/electrical power follows as it flows from the gas turbine to the propulsor. In practice, most EAP architectures will include multiple strings to provide protection against single-point failures. Nevertheless, the generic architecture shown in Figure 2 does serve as a basis to consider potential subsystem failures and their coupled effects on other subsystems. This paper focuses on "hard" failure modes that render a subsystem incapable of performing its intended function. "Soft" failures such as in-range sensor measurement errors, deteriorated components, or intermittent behavior where a subsystem can still perform its intended function are not directly considered here but must also be addressed to enable the fielding of EAP systems. Hard failure modes and effects at the subsystem level are further discussed below.

Supervisory Control System

The supervisory control system serves as the interface between the EAP system and the vehicle. In this capacity it receives thrust commands from the vehicle, which it converts to operating commands sent to the various EAP subsystems. In return, the supervisory control receives health and status information from the EAP subsystems, which it analyzes and then communicates back to the vehicle. The supervisory control system plays a key role in coordinating the operation of the underlying EAP subsystems. This includes coordinating the operation of subsystems during transients to ensure system-level

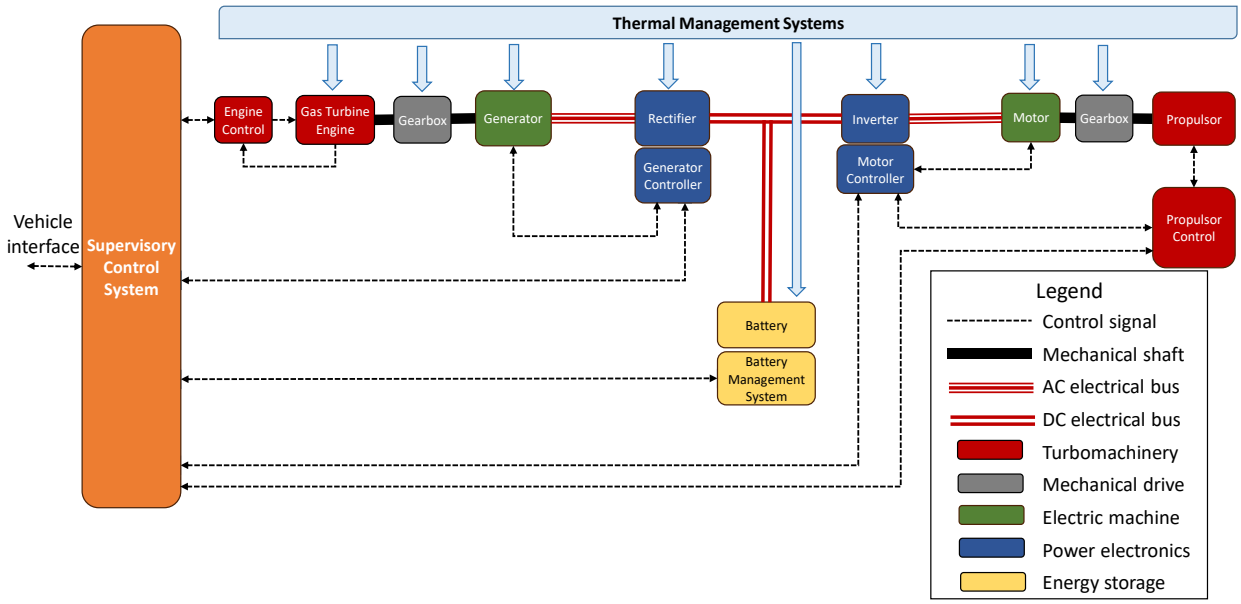


Figure 2. Generic Diagram of EAP System Components

dynamic stability and the control of any active cooling systems to address thermal management requirements. The supervisory control system is considered a flight critical unit as its failure would result in a complete loss of the ability to control and monitor operation of the EAP system. The supervisory control system is thus expected to be a redundant hardware design.

Gas Turbine Engines

Gas turbines convert fuel into mechanical power. Each gas turbine engine has its own control system that communicates directly with the EAP supervisory control system. Gas turbine mechanical offtake power is delivered to a drive shaft and used to generate electrical power. For EAP applications that use turbofan engines, the engine is also used to generate thrust directly. Aircraft gas turbine engines are highly reliable machines, but failures do occur. A historical review of aircraft propulsion system safety-significant propulsion malfunctions is given in Refs. [8,9,10]. A high-level summary of gas turbine engine failure modes and effects is provided in Table 1.

Table 1. Gas Turbine Engine Failure Modes and Effects

Failure Modes	*Failure Effects*
• Fuel exhaustion • Engine Fire • Uncontained failure • Rotor seizure • Engine separation • Engine shutdown (various causes) • Partial power loss (various causes) • Loss of speed control	• Complete loss of engine power and thrust • Partial loss of engine power and thrust

Gearboxes, Transmissions, and Mechanical Drives

Mechanical components are used to transmit mechanical power throughout an EAP system. This includes drive shafts and oil-wetted components such as bearings, gears, and transmissions. These components are designed to operate over a range of rotational speeds and torque levels. They include transmissions and gearboxes that convert shaft speeds to desired levels. These mechanical components will play a critical role in future EAP designs. Insight into the potential failure modes of gearboxes, transmissions, and mechanical drive systems is gained by considering rotorcraft drive system failures [11,12]. A high-level summary of the failure modes and effects of these systems is provided in Table 2.

Table 2. Gearbox, Transmission, Mechanical Drive Failure Modes and Effects

Failure Modes	*Failure Effects*
• Bearing spalling, failure • Gear/Gearbox misalignment, failure • Offtake/drive shaft failure • Loss of oil pump • Loss of oil cooler	• Complete or partial loss of engine mechanical power offtake • Complete or partial loss of the ability to drive electric generators or electric motor driven propulsors

Electric Machines

Electric machines consist of electric generators and electric motors [13]. The former are used to convert mechanical power into electricity and the latter to convert electric power into mechanical power. They directly couple to the mechanical drive systems discussed above. A discussion of the potential failure

modes of these machines is given in Refs. [14,15]. A high-level summary of the failure modes and effects of these systems is provided in Table 3.

Table 3. Electric Machine Failure Modes and Effects

Failure Modes	*Failure Effects*
• Shaft failure • Bearing failure • Stator winding failure • Insulation failure • Broken rotor bar • Air gap eccentricity • Loss of cooling/fire • Power supply faults	• Phase loss • Partial power loss • Complete loss of power

Power Electronics and Power Distribution Systems

Electronics for electric power switching and conversion along with bus hardware for transmitting electric power throughout the system is critical for EAP designs. This includes inverters and rectifiers for power conversion as well as generator and motor controllers. It also includes the cabling (electric bus hardware) to transmit electrical power. A discussion of potential failure modes of these systems can be found in Refs. [15,16,17]. A high-level summary of the failure modes and effects of these systems is provided in Table 4.

Table 4. Power Electronics and Power Distribution Systems Failure Modes and Effects

Failure Modes	*Failure Effects*
• Supply line or voltage failures • Electronics failure • Transformer failure • Loss of cooling • Controller failures • Bus failures (short or open circuit, corona discharge, arcing)	• Voltage sag, high current levels • Degraded power quality (voltage ripple, power instabilities) • Low power • Complete loss of power

Energy Storage (Battery) Systems

Systems for the storage of electrical energy in EAP systems include batteries and supercapacitors. These devices supply electrical power to the EAP system when being discharged and can absorb excess electrical power when being charged. Aircraft have experienced battery failure issues in the past, including failures of the Boeing 787 Dreamliner lithium-ion batteries [18]. A discussion of potential battery failure modes within the automotive industry is provided in Ref. [19]. A summary of the failure modes and effects of these systems is provided in Table 5.

Table 5. Energy Storage (Battery) Failure Modes and Effects

Failure Modes	*Failure Effects*
• Thermal runaway / fire • Aging and internal mechanical stress • Energy density degradation • Depleted state of charge • Battery management system faults • External short/open circuit	• Reduction in energy storage capacity • Reduction in discharge/charge rate • Complete loss of functionality

Propulsors

The motor driven fans or propellers are used to generate thrust and are considered analogous to aircraft propellers or rotorcraft rotors. Propeller failure modes are discussed in Ref. [20]. A summary of potential failure modes and effects is provided in Table 6.

Table 6. Propulsor Failure Modes and Effects

Failure Modes	*Failure Effects*
• Seizure • Shaft failure • Bearing failure • Blade damage/failure • Foreign object damage • Loss of speed control	• Loss of propulsor thrust • Reduction in propulsor thrust • Loss of propulsor pitch control

Thermal Management Systems

EAP system developers face significant thermal management design challenges [21]. The need for increased levels of energy and power supplied by smaller and lighter components are factors contributing to increased thermal loads. Thermal management systems are overarching in the EAP architecture shown in Figure 2 as they are integral to the operation of all subsystems. As such, failure modes within the thermal management system may lead to the need to shut down affected subsystems or run them at reduced operating levels.

EAP DESIGN CONSIDERATIONS FOR FAILURE MITIGATION

Robust, fail-safe design and operating practices are necessary to ensure that any safety hazards posed by EAP system failures are properly mitigated. Much of this involves engineering and life cycle management practices to minimize the probability of failure in flight. Examples include robust design of parts through structural design and analysis, following specified maintenance, repair, and overhaul schedules, and reliance on health and usage monitoring systems for the detection of incipient failures. In addition to life-management practices to reduce the probability of failure, design

consideration must also be given to strategies for mitigating failures occurring in flight.

Fail-safe design approaches are needed such that if an in-flight failure does occur, it happens gracefully without catastrophic impact to the system. This includes fast-acting electrical system protection equipment such as circuit breakers, current limiters, and power electronics [22,23]. Design for failure mitigation is also expected to include hardware redundancy and reconfiguration capabilities within the system. This may necessitate overdesigning the system for short durations of increased "contingency" power output in the presence of a failure.

AN EXAMPLE OF TURBOMACHINERY CONTROL CONSIDERATIONS FOR THE MITIGATION OF EAP SYSTEM FAILURES

While certainly not the only mitigation strategy that will be necessary for the design and certification of EAP systems, turbomachinery control logic is expected to play a key role in the mitigation of potential EAP system failures. To help illustrate the role of turbomachinery controls in mitigating EAP failures, an example is given based on the Single-aisle Turboelectric AiRCraft with Aft Boundary Layer propulsor (STARC-ABL) concept aircraft proposed by NASA [24]. The STARC-ABL, shown in Figure 3, consists of two wing-mounted engines and an electric motor driven tailfan propulsor. Although the STARC-ABL applies geared turbofan (GTF) engines, the work presented in this study is also applicable to EAP architectures that apply conventional turbofan engine designs. Figure 4 shows a block diagram of the STARC-ABL propulsion architecture assumed in this study. Power lever angle (PLA) commands specify the requested thrust output from the GTFs and the tailfan. In addition to producing thrust, the two GTFs also supply mechanical offtake power from their low pressure shaft, which is delivered to generators to produce electricity needed to drive the tailfan. Alternating current electricity from the generators travels through rectifiers to transport the power over direct current buses. Motor controllers command inverters that deliver the

Figure 3. STARC-ABL NASA EAP Concept Aircraft

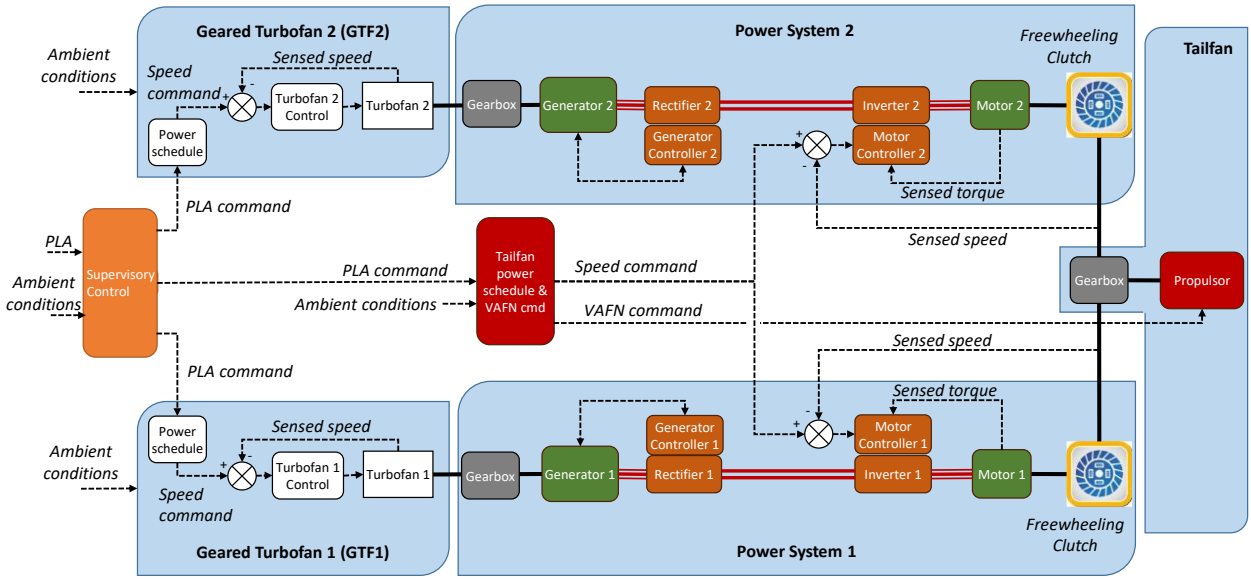


Figure 4. Example STARC-ABL Propulsion System Architecture. Note that the gearboxes contained in the Power System blocks are distinct from those in the GTFs.

necessary electrical power to the tail fan motors, which are connected to the tailfan through a common gearbox.

STARC-ABL Subsystem Failure Modes

From a high-level, the following three major subsystem failure modes exist in the STARC-ABL:

1) Failure of a GTF
2) Failure of a power system (assumed to include failures in a gearbox, generator, power electronics, electric bus, or electric motor)
3) Failure of the tailfan (due to a tailfan gearbox or tailfan turbomachinery failure)

Figure 5 presents a Failure Modes and Effects matrix listing potential STARC-ABL subsystem failures (columns), and the effects of those failures on other subsystems (rows). While partial failure of a subsystem may be possible, this table only reflects complete failures, which are considered "worst case" scenarios. Furthermore, it is assumed that the two parallel power systems are completely isolated from each other with no capability of power grid reconfiguration for the rerouting of electrical power from one power system to the other. It is also assumed that if a failure occurs in either a GTF or a power system, the parallel GTF and power system will experience increased horse power extraction (HPX) demands and electrical power levels, respectively, in an attempt to recover the tailfan thrust loss due to the failure.

This matrix shows that a failure in either GTF will cause a loss of electrical power in the power system that interfaces with the failed GTF. It also causes increased HPX demands on the opposite GTF, increased electrical power in the opposite power system, and a reduction in electrical power available to the tailfan. A power system failure will result in the elimination of HPX from the interfacing GTF, increased HPX on the opposite GTF, increased electrical power in the opposite power system, and likely a reduction in electrical power available to the tailfan. A tailfan failure will result in the elimination of HPX from both GTFs and elimination of electrical power in both power systems.

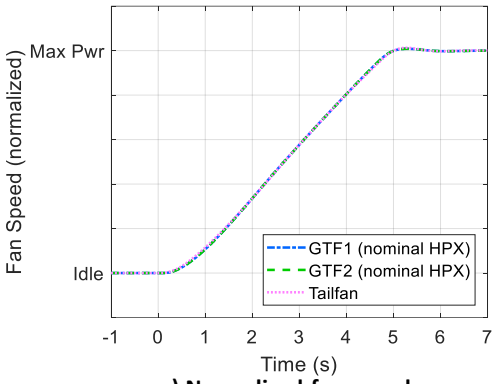
		Failed Subsystem				
		GTF1 Failed	GTF2 Failed	Power System 1 Failed	Power System 2 Failed	Tailfan Failed
Coupled Failure Effects on Other Subsystems	GTF1	*Failed*	*Increased HPX*	*No HPX*	*Increased HPX*	*No HPX*
	GTF2	*Increased HPX*	*Failed*	*Increased HPX*	*No HPX*	*No HPX*
	Power System 1	*No Electric Power*	*Increased Electric Power*	*Failed*	*Increased Electric Power*	*No Electric Power*
	Power System 2	*Increased Electric Power*	*No Electric Power*	*Increased Electric Power*	*Failed*	*No Electric Power*
	Tailfan	*Reduced Electric Power*	*Reduced Electric Power*	*Reduced Electric Power*	*Reduced Electric Power*	*Failed*

Figure 5. STARC-ABL Failure Modes and Effects

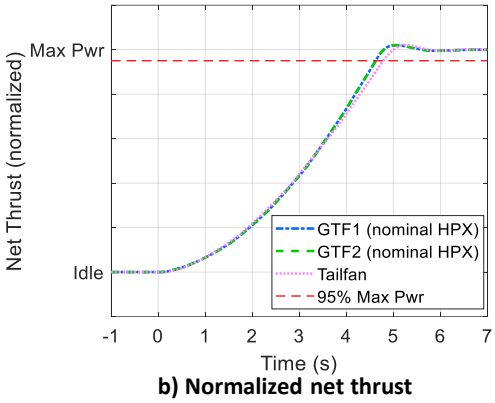
STARC-ABL Propulsion System Simulation

A computer simulation of the STARC-ABL propulsion system was created to enable initial failure management studies, including the ability to insert subsystem failures and evaluate the system-level effects of those failures. In this simulation, turbomachinery components are modeled using the NASA-developed Toolbox for the Modeling and Analysis of Thermodynamic Systems (T-MATS) [25], which is coded in MATLAB® Simulink® (The MathWorks, Natick, MA), while electrical system components are modeled using a power flow modeling approach [26]. Power flow is a steady-state technique commonly applied for the modeling of electrical systems through an architecture of interconnected nodes representing the generation, distribution, and consumption of electrical power in the system. The simulation includes separate controllers for each GTF and the tailfan, enabling transient operation of the system. The GTF control system includes fuel control logic plus control schedules for variable area fan nozzle (VAFN) and variable area bleed valve (VBV) actuators included in the GTF [27]. The GTF simulation used in this study does not directly include variable stator vane (VSV) hardware typically found on most turbofan engines. Instead, the compressor modules implemented within the GTF are modeled assuming that any VSV actuators are always operating "on-schedule." In the future, the inclusion of VSV actuators to more fully evaluate the effects of operating VSV's "off-schedule" will be explored. The tailfan controller includes motor control logic plus a control schedule for a VAFN actuator included in the tailfan. The GTF fuel controller and the tailfan motor controller include a combination of set point controllers, transient control schedules, and limit logic [28]. The STARC-ABL electrical system consisting of generators, motors, rectifiers, inverters, and power buses is simulated using a power flow modeling approach mentioned above.

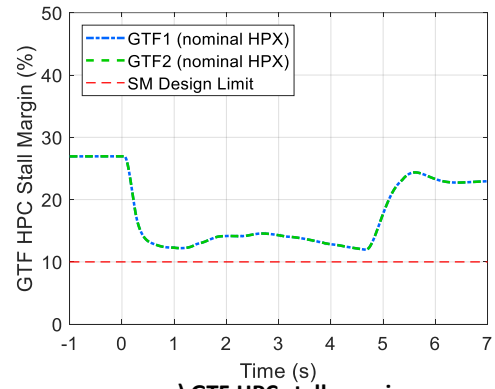
Nominal System Response. Figure 6 shows a STARC-ABL propulsion system simulation acceleration response due to a throttle step command from idle to maximum PLA performed at the 25k feet, Mach 0.6 flight condition. The throttle step command occurs at time 0 seconds; the engine with the baseline control system is operating nominally (no failures) with nominal levels of GTF HPX. The acceleration schedules included in the baseline control are designed to provide matching (symmetric) transient response in normalized fan speed between the two GTFs and the tailfan (see Figure 6a), and to transition from idle to 95% of the maximum net thrust output in less than 5 seconds (see Figure 6b). The GTF acceleration schedule is based on a fuel ratio unit (RU) versus corrected fan speed (N1c) schedule, where RU = fuel flow rate (Wf) divided by compressor exit static pressure (Ps3), or Wf/Ps3. The tailfan acceleration schedule applies a fan speed derivative (N1dot) versus tailfan N1c schedule. The results show that with no failures present, the two normalized GTF response plots lie atop one another, with the



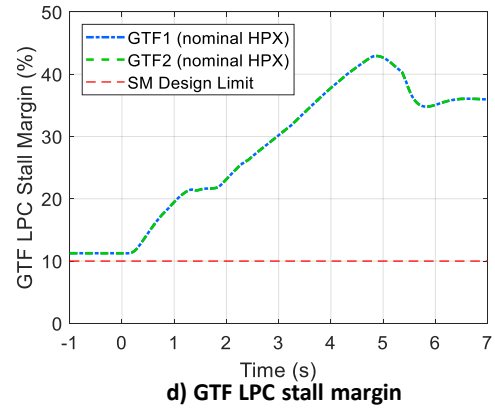
a) Normalized fan speed



b) Normalized net thrust

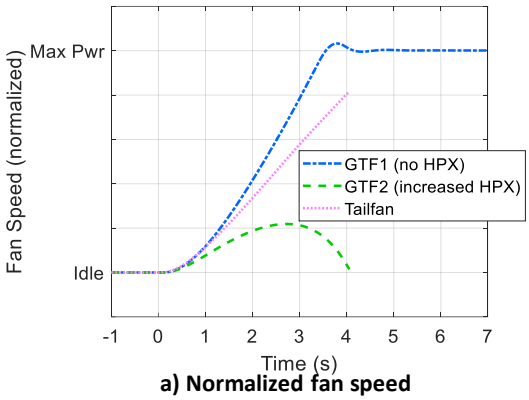


c) GTF HPC stall margin

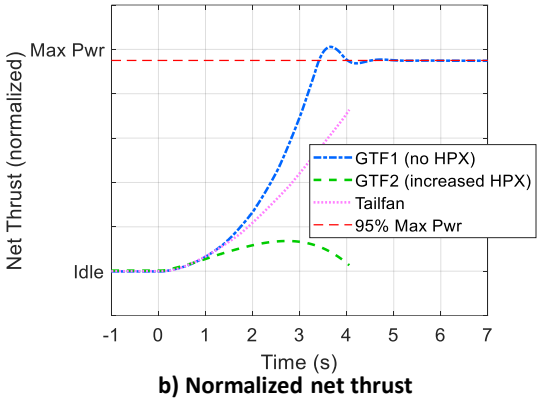


d) GTF LPC stall margin

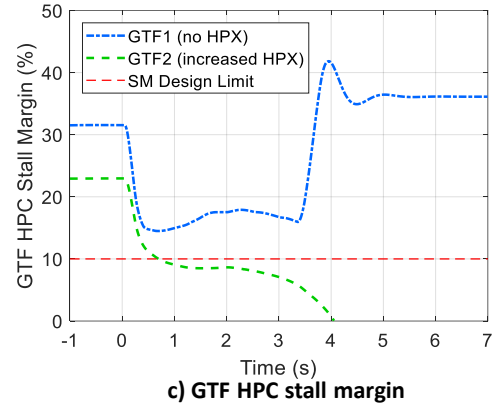
Figure 6. STARC-ABL Acceleration Response under Nominal Operating Conditions with Baseline Control



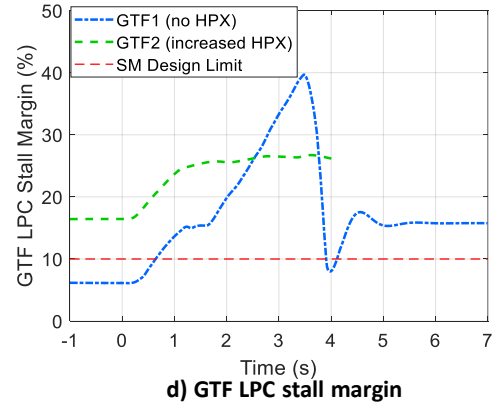
a) Normalized fan speed



b) Normalized net thrust



c) GTF HPC stall margin



d) GTF LPC stall margin

Figure 7. STARC-ABL Acceleration Response under Power System 1 Failure with Baseline Control

normalized tailfan speed response in close agreement. Normalized thrust responses also match well and reach the 95% maximum thrust threshold within 5 seconds. The two GTFs reach this threshold in 4.6 seconds while the tailfan reaches this threshold in 4.8 seconds. Net thrust of each GTF slightly leads that of the tailfan due to the fact that the GTF's high pressure spool (core spool) leads the fan spool during acceleration transients. Once the GTFs reach steady-state, their core thrust and fan bypass thrust stabilize to their maximum values. Net thrust shown in the figure is normalized to illustrate symmetry in the thrust responses. However, as a point of reference, each GTF contributes 36.3% of the propulsion system's total maximum net thrust output at this flight condition, while the tailfan contributes 27.3% of the net thrust.

The other constraint applied in designing the transient control system for the STARC-ABL is that a minimum of 10% stall margin (SM) must be maintained in GTF high pressure compressor (HPC) and low pressure compressor (LPC) modules at all times. From Figure 6c and Figure 6d, it is observed that these SM design limits are indeed maintained by the baseline control under this scenario.

Unmitigated Failure Response. Next, the simulation is used to evaluate the effects of a failure within the STARC-ABL propulsion architecture. Here, the simulation is updated to emulate a failure within power system 1 connected to GTF1 (see Figure 4). This scenario, which could be due to the failure of any individual component within power system 1 (i.e., generator, inverter, bus, motor, etc.), is assumed to result in gearbox disengagement and elimination of all HPX from GTF1. Under such a scenario, the baseline control system will attempt to extract 100% of the power needed to drive the tailfan from GTF2.

Figure 7 shows simulation results under this condition for the same transient acceleration scenario presented in Figure 6. In this case, the simulation begins with the failure having already occurred and the simulation stabilized at the idle condition with the failure present. As a PLA step change is introduced, the tailfan controller attempts to operate the tailfan on its target fan speed acceleration schedule, requesting all necessary power from GTF2. However, GTF2 is not capable of supplying this HPX demand. GTF2's fan speed and thrust exhibit sluggish initial response followed by a roll back in these parameters commencing around 3 seconds after the start of the transient (see Figure 7a and Figure 7b). As HPX demands on GTF2 continue to increase, GTF2 HPC SM eventually reaches zero at time 4 seconds (see Figure 7c). At this point, GTF2 and the tailfan are assumed to experience shutdowns, and are no longer capable of producing thrust.

GTF1, which experiences an elimination of all HPX under this failure scenario, is able to continue to operate and produce thrust throughout the transient. In fact, the baseline control Wf3/Ps3 versus N1c acceleration schedule will result in GTF1 fan speed and net thrust accelerations faster than during the nominal case (see Figure 7a and Figure 7b). Here, GTF1 reaches the 95% maximum net thrust output level in only 3.4 seconds compared to 4.6 seconds in the nominal case. While the acceleration rate is faster, the final steady-state net thrust output produced by GTF1 is about 5% less than that under nominal HPX levels. This is due to a reduction in GTF core speed and core thrust with the elimination of HPX.

Overall, given the slight reduction in GTF1 thrust output and the total loss of GTF2 and tailfan thrust output, the system only produces 34.6% of the total maximum net thrust achieved under nominal operating conditions. Such a drastic reduction in thrust output is likely to be a catastrophic hazard for the STARC-ABL.

Figure 7 also illustrates how changes in GTF HPX levels result in a shift in compressor SM relative to the nominal case. Figure 7c shows that HPC SM increases when power extraction is eliminated (GTF1) and reduces when power extraction is increased (GTF2). The opposite trend holds for LPC SM as shown in Figure 7d. Here, LPC SM reduces with the elimination of HPX (GTF1) and increases when HPX is increased (GTF2). In fact, GTF1 LPC SM is below the 10% SM design limit during various portions of the scenario shown in Figure 7d, putting GTF1 at increased risk of an LPC stall. The combined risks posed by an unmitigated STARC-ABL power system failure (i.e., one engine at higher risk of an HPC stall and the opposite engine at higher risk of an LPC stall) places the vehicle in jeopardy of experiencing a multi-engine shutdown event.

STARC-ABL Simulation Updates to Include Reversionary Control Logic

To assist in the mitigation of STARC-ABL subsystem failure scenarios, the inclusion of reversionary modes within the control system is considered. These control modes are designed to be invoked by a supervisory controller for the mitigation of subsystem failures upon their occurrence. While such technology will require associated real-time logic for the diagnosis of system failures, this paper only addresses the control mitigation aspects of the overall failure diagnosis and mitigation problem. The reversionary control modes are designed to adhere to the constraints of maintaining minimum GTF HPC and LPC SM of 10% and accelerating from idle to 95% of available maximum thrust in less than 5 seconds. Additionally, the reversionary control modes are designed to maximize total available system thrust output. Exact specification of the permissible amount of failure-induced thrust loss in an EAP architecture such as the STARC-ABL is not possible at this time. This would require detailed knowledge of the vehicle's aerodynamic characteristics as well as regulatory airworthiness standards for transport category airplanes equipped with EAP systems. Given the current lack of such information, this study assumed that for any single subsystem

failure the maximum available vehicle thrust output should be no less than 50% of the maximum thrust output under nominal operating conditions. This constraint is analogous to a two engine commercial aircraft with one engine inoperative. Designing the reversionary control modes to simultaneously satisfy all of the design constraints is a manual and iterative process, which required updates to both the GTF and tailfan control logic.

Tailfan Reversionary Control Logic. The tailfan reversionary control logic includes two changes relative to the baseline control design. First, the tailfan's acceleration schedule is updated to follow a slower acceleration transient. Additionally, a maximum power demand limit is placed on the tailfan controller restricting the amount of electrical power that it can request. These two revisions result in the tailfan accelerating more slowly and peaking at a lower fan speed and net thrust output than nominal when a failure occurs in one of the GTFs or one of the power systems.

GTF Reversionary Control Logic. For the GTF controller, different reversionary control modes are defined for the cases in which the engine is experiencing either the elimination of or increase in requested HPX. Changes relative to the baseline GTF control design include revisions to the VBV schedule, the fuel control Wf/Ps3 versus N1c acceleration schedule, and the fuel control set point controllers.

The GTF VBV, which is installed at the LPC exit, serves to maintain a suitable amount of stall margin in the engine's LPC. As this valve opens, it causes airflow to be bled off the GTF core and transferred to its bypass duct. The control system schedules VBV position as a function of N1c as shown in Figure 8a. The schedule commands VBV to be fully closed at high N1c, and then to open as N1c is reduced. Under nominal operating scenarios, the baseline VBV schedule will maintain an appropriate amount of LPC stall margin. However, a power system failure will eliminate the HPX load placed on the GTF low pressure shaft. This causes a shift in the LPC operating line, which in turn affects the amount of LPC SM. This is seen in Figure 8b showing the GTF LPC map with the machine's nominal steady-state operating line, plus the cases with increased and decreased levels of HPX. For the increased HPX case (shown in green), the operating line is shifted downward. This increases the amount of SM and may result in the engine operating less efficiently. More concerning, from an LPC operability standpoint, is the case were HPX is completely eliminated (shown in blue). Here, the operating line is shifted upwards reaching the stall line at certain operating speeds and placing the LPC at risk of stall. To address this, reversionary VBV control schedules are implemented as shown in Figure 8c. For the increased HPX case, the valve begins opening at a lower N1c and opens a smaller amount compared to the nominal schedule. For the case where HPX is eliminated, the valve is scheduled to begin opening at a higher N1c and opens a larger overall amount for a given N1c. The resulting STARC-ABL GTF

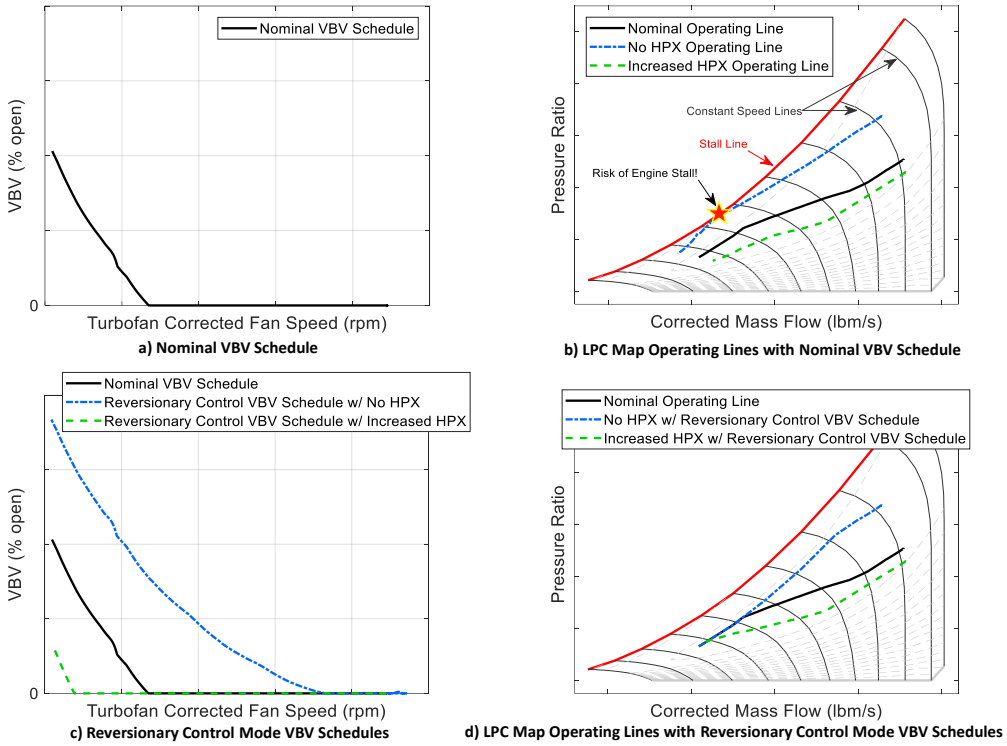


Figure 8. Application of Reversionary VBV Control Schedules for HPX Failure Mitigation

LPC operating lines with revised VBV control schedules are shown in Figure 8d. As desired, the operating line with increased HPX is shifted upward, and the operating line with decreased HPX is shifted downward, maintaining suitable levels of LPC SM over all operating speeds.

The reversionary control modes for failure mitigation also include adjustments to the GTF fuel control logic. First, adjustments to the Wf/Ps3 versus N1c acceleration schedule are performed to achieve GTF accelerations from idle to full power following the same fan speed trajectory as in the nominal case. Additionally, revised set point fuel control gains are applied to produce a comparable closed-loop dynamic response of the GTF for small perturbations (i.e., near the beginning and end of the acceleration transient when not operating on the acceleration schedule). This modification is necessary, as the dynamic response of the engine is dependent on the amount of HPX placed on the low pressure shaft.

Reversionary Control Logic Simulation Results. The resulting acceleration response of the STARC-ABL propulsion system in the presence of a power system 1 failure with the reversionary control logic applied is shown in Figure 9. Once again, this is for a failure in power system 1 at the 25k, 0.6 Mach flight condition. Fan speed responses are shown in Figure 9a. (Note that the plots in Figure 9a and Figure 9b are normalized with respect to their counterparts in Figure 6.) The two GTFs follow fan speed acceleration responses matching those of the nominal case shown in Figure 6a. The tailfan accelerates more slowly, and its maximum value settles at a lower level compared to the nominal case. This is due to the adjustments made to the tailfan acceleration schedule and the maximum electrical power demand limit placed on the tailfan. Net thrust responses are shown in Figure 9b. Here, the dashed horizontal line reflects the 95% maximum thrust level of the nominal failure-free case. Maximum net thrust output of GTF2 is 100.3% that of the GTF under the nominal case, with the slight increase attributed to an increase in core thrust. GTF1's maximum thrust output is 95.3% that of the nominal case due to a reduction in core thrust. Tailfan maximum net thrust output is 55.6% of that produced by the tailfan under the nominal case due to the control limit placed on the tailfan electrical power demand. Collectively, the STARC-ABL propulsion system produces 86.3% of the maximum net thrust produced under nominal operating conditions, but it continues to run, unlike the faulted case with nominal control shown in Figure 7.

HPC and LPC SM results are shown in Figure 9c and Figure 9d, respectively. GTF1 HPC SM operates above the 10% SM design limit over the entire transient, while GTF2 HPC SM rides on the SM design limit during most of the transient. LPC SM for both GTF1 and GTF2 remains above the 10% SM design limit over the entire transient, unlike in the unmitigated failure case

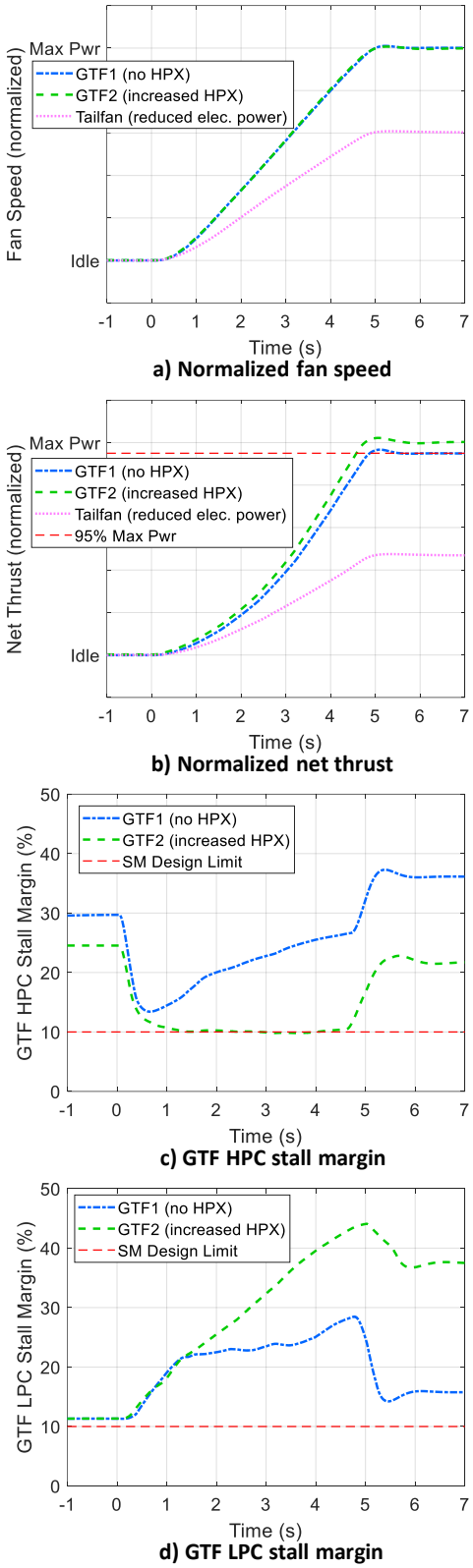


Figure 9. STARC-ABL Acceleration Response with Power System 1 Failure and Reversionary Control

where GTF1 LPC SM dropped below the design limit (see Figure 7d).

Discussion of Reversionary Control Mode Design Decisions

There are several nuances pertaining to subsystem coupling that factor into the design of the reversionary control logic that warrant additional discussion. As shown in Figure 9, with the reversionary control logic the system was able to satisfy the 5 second thrust acceleration response and the ≥ 50% of nominal maximum thrust design constraints while also adhering to the 10% HPC SM design limit in the presence of a failure. Furthermore, the fan speed acceleration response transient of both GTFs was able to be designed to match that of the nominal case. However, meeting these design goals required coordinated adjustments to the maximum electrical power demand limit placed on the tailfan (set to 54.4% of maximum electrical power under nominal conditions) as well as to the acceleration schedules applied to the tailfan and the GTF supplying additional HPX (i.e., GTF2 in the Figure 9 example). Total system maximum net thrust output, which is 86.3% of nominal for the presented failure example, could be increased by increasing the tailfan power demand limit, but this will come at the expense of violating one or more of the design constraints. For example, increased maximum thrust output would require allowing HPC SM to drop below 10%, allowing GTF2 and the tailfan to accelerate more slowly, or sacrificing the ability to maintain symmetric fan speed acceleration profiles matching those of the nominal case. Such design choices were not considered in this study, but illustrate some of the complexities facing the designers of an EAP system such as the STARC-ABL.

Given the simulation results presented above, using the reversionary control mode to mitigate faults, an analysis of the maximum net thrust output of the STARC-ABL propulsion system under nominal and mitigated failure conditions at the 25k 0.6 Mach flight condition are provided in Table 7. Here, the same potential STARC-ABL subsystem failure modes presented in Figure 5 are considered. All entries are shown as a percentage of the total maximum net thrust output of the STARC-ABL propulsion system when operating nominally (failure-free). This table shows that maximum net thrust is most limited for the case of a GTF failure (51.6% of nominal thrust), followed by a tailfan failure (69.3% of nominal thrust), and a power system failure (86.3% of nominal thrust). In each case, 10% compressor stall margin limits, 5 second acceleration transient response rate, and ≥ 50% of nominal maximum thrust design constraints were all met. Additional analysis would be necessary to extend these results to other flight conditions, and to assess whether or not sufficient thrust is available to safely mitigate these subsystem failures throughout the vehicle's entire operating envelope.

It should be emphasized that the results presented in this paper only cover an initial high level analysis of STARC-ABL

subsystem failure effects and potential turbomachinery control mitigation strategies conducted at one flight condition. Furthermore, the development of reliable failure detection strategies and supervisory control logic to coordinate turbomachinery control mitigation strategies with other failure mitigation strategies in the system is necessary. Any developed failure mitigation strategies also need to be robust to the speed at which a failure may occur (abrupt or gradual), as well as a subsystem failure recovery, if that possibility exists.

Table 7. Maximum Net Thrust Contribution of STARC-ABL GTFs and Tailfan under Nominal and Mitigated Failure Conditions

	System Status					
Thrust source	All Nominal	GTF1 Failed	GTF2 Failed	Power Sys1 Failed	Power Sys2 Failed	Tailfan Failed
GTF1	36.3%	0.0%	36.5%	34.6%	36.5%	34.6%
GTF2	36.3%	36.5%	0.0%	36.5%	34.6%	34.6%
Tailfan	27.3%	15.2%	15.2%	15.2%	15.2%	0.0%
Total	**100.0%**	**51.6%**	**51.6%**	**86.3%**	**86.3%**	**69.3%**

SUMMARY

Due to their increased complexity and integrated nature, electrified aircraft propulsion (EAP) systems present additional failure modes and hazards not found in conventional aircraft propulsion designs. Mitigation of these EAP failures will require a system-level design and analysis approach. This document provides a high-level review of the potential failure modes of an EAP system along with potential strategies for the mitigation of those failures. Also presented was an example of a power system failure in the simulated STARC-ABL EAP system along with a turbomachinery control strategy to assist in the mitigation of that failure. This control mitigation strategy can be extended to other potential subsystem failures as well. This example illustrated the complex integrated nature of EAP system designs, and the need to approach failure mitigation from a system-level perspective.

ACKNOWLEDGMENTS

This work was conducted under the NASA Advanced Air Vehicles Program, Advanced Air Transport Technology Project, Electrified Aircraft Powertrain Technologies Subproject.

REFERENCES

[1] SAE International Aerospace Recommended Practice, (2010), "Guidelines for Development of Civil Aircraft and Systems," SAE Standard ARP4754A, December 2010.

[2] SAE International Aerospace Recommended Practice, (1996), "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," SAE Standard ARP4761, December 1996.

[3] Hayhurst, K.J., Maddalon, J.M., Miner, P.S., Szatkowski, G.N., Ulrey, M.L., DeWalt, M.P., Spitzer, C.R., (2007), "Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems," NASA/TM-2007-214539, February.

[4] Federal Aviation Administration, "Advisory Circular (AC) 25.1309-1A System Design and Analysis," June 21, 1988.

[5] Shaw, J.C., Fletcher, S., Norman, P., Galloway, S., Burt, G., (2015), "Failure Analysis of a Turboelectric Distributed Propulsion Aircraft Electrical Network: A Case Study," SAE Technical Paper 2015-01-2403.

[6] Darmstadt, P.R., Catanese, R., Beiderman, A., Dones, F., Chen, E., Mistry, M.P., Babie, B., Beckman, M., Preator, R., (2019), "Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems," NASA Contractor Report NASA-CR-2019-220217, June 2019.

[7] Sebastian, R.K., Perinpinayagamb, S., Choudharyb, R., (2016), "Health Management Design Considerations for an All Electric Aircraft," The 5th International Conference on Through-life Engineering Services (TESConf 2016).

[8] Federal Aviation Administration and Aerospace Industries Association, (1999), "Technical Report on Propulsion System and Auxiliary Power Unit (APU) Related Aircraft Safety Hazards," October 25, 1999.

[9] Federal Aviation Administration and Aerospace Industries Association, (2005), "2nd Technical Report on Propulsion System and Auxiliary Power Unit (APU) Related Aircraft Safety Hazards," January 31, 2005.

[10] Federal Aviation Administration and Aerospace Industries Association, (2017), "3rd Technical Report on Propulsion System and Auxiliary Power Unit (APU) Related Aircraft Safety Hazards," March 30, 2017.

[11] Astridge, D.G., (1989), "Helicopter Transmissions-Design for Safety and Reliability," Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering, Vol 203, Issue 2, July 1989.

[12] Davies, D.P., Jenkins, S.L., Belben, F.R., (2013), "Survey of Fatigue Failures in Helicopter Components and Some Lessons Learnt," Engineering Failure Analysis, Volume 32, September 2013, Pages 134-151.

[13] Ganev, E., (2014), "Selecting the Best Electric Machines for Electrical Power-Generation Systems," *IEEE Electrification Magazine*, December 2014, pgs 13-22.

[14] Karmakar, S., Chattopadhyay, S., Mitra, M., Sengupta, S., (2016), "*Induction Motor Fault Diagnosis – Approach Through Current Signature Analysis*," Singapore, Springer.
[15] Armstrong, M., Ross, C., Phillips, D., Blackwelder, M., (2013), "Stability, Transient Response, Control, and Safety of a High-Power Electric Grid for Turboelectric Propulsion of Aircraft," NASA/CR—2013-217865, June 2013.
[16] Kastha, D., Bose, B.K., (1994), "Investigation of Fault Modes of Voltage-Fed Inverter System for Induction Motor Drive," IEEE Transactions on Industry Applications, Vol. 30, No. 4, July/August 1994.
[17] Zhang, W., Xu, D., Enjeti, P.N., Li, H., Hawke, J.T., Krishnamoorthy, H.S., (2014), "Survey on Fault-Tolerant Techniques for Power Electronic Converters," IEEE Transactions on Power Electronics, Vol. 29, No. 12, December 2014.
[18] Williard, N., He, W., Hendricks, C., and Pecht, M., (2013), "Lessons Learned from the 787 Dreamliner Issue on Lithium-Ion Battery Reliability," *Energies 2013*, Issue 6, pgs. 4682-4695.
[19] U.S. Department of Transportation National Highway Traffic Safety Administration, "Lithium-ion Battery Safety Issues for Electric and Plug-in Hybrid Vehicles," DOT HS 812 418.
[20] The Commercial Aviation Safety Team (CAST), "Propeller Operation and Malfunctions Basic Familiarization for Flight Crews", SKYbrary Bookshelf, 2011, Retrieved from https://skybrary.aero/bookshelf/books/3703.pdf, 16 pgs.
[21] National Academies of Sciences, Engineering, and Medicine. 2016. Commercial Aircraft Propulsion and Energy Systems Research: Reducing Global Carbon Emissions. Washington, DC: The National Academies Press. https://doi.org/10.17226/23490.
[22] Flynn, M.C., Jones, C.E., Rakhra, P., Norman, P.J., Galloway, S.J., (2017), "Impact of Key Design Constraints on Fault Management Strategies for Distributed Electrical Propulsion Aircraft," AIAA-2017-5034, AIAA Propulsion and Energy Forum, Atlanta, GA, July 10-12.
[23] Kostakis, T., Norman, P.J., Galloway, S.J., Burt, G.M, (2017), "Demonstration of Fast-Acting Protection as a Key Enabler for More-Electric Aircraft Interconnected Architectures," IET Electrical Systems in Transportation, Vol. 7, No. 2, pp. 170-178, May 2017.
[24] Welstead, J.R., Felder, J.L., (2016), "Conceptual Design of a Single-Aisle Turboelectric Commercial Transport with Fuselage Boundary Layer Ingestion," AIAA 2016-1027, AIAA SciTech Forum, 54th AIAA Aerospace Sciences Meeting, San Diego, CA, January 4-8.
[25] Chapman, J.W., Lavelle, T.M., May, R.D., Litt, J.S., Guo, T-H., (2014), "Toolbox for the Modeling and Analysis of Thermodynamic Systems (T-MATS) User's Guide," NASA/TM-2014-216638, January.
[26] Chapman, J.W., Litt, J.S., (2018), "An Approach for Utilizing Power Flow Modeling for Simulations of Hybrid Electric Propulsion Systems," AIAA-2018-5018, AIAA Propulsion and Energy Forum, Cincinnati, OH, July 9-11.
[27] Chapman, J. W., Litt, J. S., (2017) "Control Design for an Advanced Geared Turbofan Engine," AIAA-2017-4820, AIAA Propulsion and Energy Forum, Atlanta, GA, June 10-12.
[28] Jaw, L.C., Mattingly, J.D., (2009), *Aircraft Engine Controls: Design, System Analysis and Health Monitoring*, American Institute of Aeronautics and Astronautics, 1801 Alexander Bell Drive, Suite 500, Reston, VA 20191-4344, USA.