Hazard Analysis Failure Modes, Effects, and Criticality Analysis for NASA Revolutionary Vertical Lift Technology Concept Vehicles

Allan Beiderman
The Boeing Co.
Philadelphia, PA

Patrick R. Darmstadt
The Boeing Co.
Philadelphia, PA

Caitlin Dillard
The Boeing Co.
Philadelphia, PA

Chris Silva
NASA Ames Research Center
Moffett Field, CA

ABSTRACT

The scope of this paper is an analysis of the safety and reliability of novel urban air mobility (UAM) propulsion systems. Their potential effect on and coupling of adjacent and related systems such as flight controls and thermal management has been examined at a functional level. Propulsion systems were developed for National Aeronautics and Space Administration (NASA) concept aircraft to support the reliability and safety analysis.

The results of the safety and reliability analysis (on a representative UAM configuration, a quad-rotor (QR), is presented to guide industry on the effects of architecture and systems design on overall air vehicle safety. This will also inform the industry on various propulsion configurations and how they can be made to comply with certification requirements.

INTRODUCTION

The aerospace industry is developing novel propulsion systems to be able to meet mission parameters of reduced cost and noise and increased reliability and safety for the emerging UAM market. These novel propulsion systems (primarily distributed pure electric and hybrid electric combined with distributed flight controls) provide challenges to certification authorities in being able to ascertain the safety and reliability of these systems, especially in light of still developing certification specifications and rapid advancement of technology.

A total of five powertrain configurations and hazard assessments were developed and analyzed (Ref. 1). One powertrain configuration was developed for each of the NASA Revolutionary Vertical Lift Technology (RVLT) Side-by-Side, Tilt-Wing (TW), and Lift+Cruise (LC) vehicles. Two configurations were developed for the single occupant QR; one configuration included interconnecting shafts connecting each rotor for phasing and emergency conditions and the other configuration did not include interconnecting shafts.

An overview of the content of this paper is as follows:

- Description of the NASA RVLT QR concept vehicle;
- Overview of the safety and reliability assessment process;
- Design and analysis assumptions;
- Description of the QR powertrain configurations including functions functional failures, and failure modes;
- Functional block diagrams;
- Functional hazard assessment (FHA);
- Failure Modes, Effects, and Criticality Analysis (FMECA);
- Fault Tree Analysis (FTA);
- Discussion of EASA SC-VTOL-01 impacts to RVLT concept vehicles;
- Concluding remarks and recommended best practices for future safety analysis.

NASA RVLT CONCEPT VEHICLE

NASA has advanced technology within the Vertical Take-Off and Landing (VTOL)

Presented at the Vertical Flight Society's 77th Annual Forum And Technology Display, Virtual, May 10–14, 2021.

community for decades. Recently, NASA identified a need to extend the state-of-the-art in the more disruptive airspace of Distributed Electric/Hybrid Electric Propulsion (DE/HEP), Distributed Flight Controls (DFC), and Urban Air Mobility (UAM). Programs like NASA's GL-10 Greased Lightning (Ref. 2, Ref. 3), and X-57 Maxwell (Ref. 4), have helped pioneer DE/HEP and DFC air vehicle concepts and is continuing its research in these topic areas through the RVLT Program. More recently the RVLT Program developed a series of conceptual rotary wing airplanes (Ref. 5, Ref. 6) for the UAM mission. NASA has historically used concept vehicles to guide research and aim industry partners toward common goals and objectives.

In recent history, NASA used the Civil Heavy Lift Rotorcraft concept vehicles to guide research topics. NASA traded designs and configurations for tilt-rotor, tandem-compound, and advancing blade concept vehicles. Through the noted trade studies, NASA found that their Large Civil Tilt Rotor (LCTR) concept showed the most promise for their specified mission of carrying 120 passengers for 1,200 nautical miles (Ref. 7). Research efforts focused around the LCTR advanced powertrain, noise, and slowed rotor technologies, among others, which are applicable to today's thrust towards UAM.

The RVLT Concept Vehicles are expected to follow a similar research model, in which vehicle requirements and technology assumptions required to meet theoretical mission objectives are used to drive research topics and open forum discussions. Initially, three different concept vehicles were developed with departures into a fourth vehicle; all are intended to mature technologies required for similar airplanes that meet UAM mission objectives. Each concept vehicle was designed to be piloted, but future trade studies may include the impacts of incorporating various levels of autonomy.

The three vehicles conceptualized were: A single occupant QR designed for a 50 nautical mile (nm) mission range, a six occupant side-by-side, also known as Lateral-Twin (LT), designed for a 200 nm range and a 15 passenger TW designed for a 400 nm range (Ref. 6). Further development included the release of an additional six passenger LC concept vehicle designed for a 37.5 nm range, the single passenger QR was resized for six (6) passengers and a shorter, 37.5 nm range, and the six (6) passenger LT was resized for a shorter 37.5 nm range.

For each of the 3 vehicle types, numerous excursions have been performed, primarily examining propulsion system and rotor system approaches. These excursions provide an opportunity to quantify trades of performance, cost, and reliability for UAM missions. The present work expands on the prior design work by providing the quantitative evidence for reliability of these vehicles. Future vehicle design and technology development work will incorporate these calculated measures of reliability and apply the assessment approach established here. The present results and approach will also be of value to other vehicle design practitioners designing UAM vehicles and systems.

In this work, the single passenger QR is discussed. The 15 passenger TW, six (6) passenger LT and LC vehicles are discussed in the NASA contractor safety and reliability analysis that is available on NASA's Scientific and Technical Information Webpage.

The single passenger QR is shown in Figure 1 (Ref. 5). It was designed to have a fully electric powertrain, a 250 lb payload, and a 50 nm range. The rotors and supporting pylon structure are arranged in an "X" configuration with the rear rotors being higher than the forward rotors. The QR under consideration was designed to have, collective control at each rotor, fully articulated rotors, and interconnecting shafts for emergency conditions. The installed power is provided by a battery network that is charged prior to flight and which sends power to four 21.6 HP motors.

The tip speed was set to 450 ft/sec for sizing runs, resulting in rotor diameters of 12.62 ft and 681 revolutions per minute (RPM).

A second powertrain configuration was also evaluated for the QR vehicle concept. The interconnecting shafts were removed in favor of a direct-drive arrangement. Speed reducing gearboxes, similar to that in the baseline configuration, were included for weight savings. Collective, variable pitch control, similar to that in the baseline configuration, was included for pitch, roll, and yaw control.

Figure 1: Quad-Rotor Air Vehicle

RELIABILITY AND SAFETY ASSESSMENT PROCESS

A robust reliability and safety assessment process begins during the conceptual design phase and ends when the airplane is retired. The Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761 (Ref. 8) outlines the safety assessment process up through certification; however, most of an airplane's lifecycle is spent in commercial or military service. SAE ARP5150A (Ref. 9) and ARP5151 (Ref. 10) outline the safety assessment process for airplanes that are flying commercial service. While SAE ARP5150A and ARP5151 provide valuable information to anyone maintaining a fleet. Our focus is in the conceptual design phase, so SAE ARP 5150A and ARP5151 are not discussed further.

The reliability assessment process is not independently covered by a system of guiding documents for civil applications; however, SAE ARP4754A (Ref. 11) covers an outline of the design process and the integration of the safety assessment process covered in SAE ARP4761. The safety and reliability assessment process are so closely coupled, one can use both SAE ARP4754A and ARP4761 guidance to understand the reliability assessment process.

SAE ARP4761 outlines a means to certification, focused on Federal Aviation Regulation (FAR) Part 25.1309, Equipment, Systems, and Installations. The outlined assessment process has applicability when considering safety assessments of the powertrain. The assessment must be performed for all phases of flight, such as hover in ground effect, hover out of ground effect, cruise, flight maneuvers, etc. The assessments are qualitative and iterative in nature; both reliability and design information need to be passed to and from the safety assessment to comprehensively model the airplane. Figure 2 shows the graphic representation of the iterative nature of the safety analysis process.

Figure 2: Iterative Nature of Safety and Reliability Assessments.

The relevant portion of the process outlined in ARP4761 begins with a FHA during the airplane conceptual development. However, one can argue that the reliability assessment can begin the reliability/safety assessment iteration loop. In either case, design information is required to facilitate the reliability and safety assessment process.

Stick diagrams were developed in order to show the connectivity between components and sub-systems in order to support the reliability and

safety assessment process. The QR powertrain was split into three sub-systems for this exercise; a rotating system, flight control system, and thermal management system. The rotating system consisted of the motors and gearboxes. The flight control system consisted of batteries, inverters, flight control computers, actuators, and associated wiring. The thermal management system consisted of battery and ESC cooling.

Once the powertrain configuration was conceptualized, a functional block diagram was created. The functional block diagram is a graphic representation of the functions to be analyzed and is developed by the Reliability and Maintainability organization. The functional block diagram is used to inform functional failures evaluated in the FHA, the components evaluated in the FMECA, and FTA, derived from the FHA.

The FHA is used to evaluate the functions and corresponding failure conditions and severity classifications. The FHA is a tabular document in which qualitative, investigative analysis is applied in order to populate hazards associated with the aircraft. The FHA documents any ground rules and assumptions and is used to generate requirements that will be taken up to the aircraft level and cascade down into the system design.

The functional block diagram and outputs of the FHA were then used in the next leg of the reliability assessment. For this exercise, a FMECA was generated, but in practice a Failure Modes and Effects Analysis (FMEA) may be used to generate the associated failure rates used in the FTA. The primary difference between a FMECA and FMEA being the application of the failure effect probability, β, to determine the criticality of each FMECA line item. β is the analyst's judgment as to the conditional probability that a failure effect results in the identified severity code, ie the worst possible outcome, given that the specified failure mode occurs. The analyst may use pilot actions, preventative maintenance, real-time monitoring, or other to develop and substantiate β. Utilizing a FMEA rather than a FMECA for FTA generation would cause more work as the most critical failure effect assumptions would need to be documented in the fault tree and time-at-risk (TAR) would also need to be considered at the event level.

In general, as part of the FMEA or FMECA process, operational requirements are used to apply qualitative values to each severity classification in the FHA. However, operational requirements for UAM were not available for this study. The European Aviation Safety Agency (EASA) has released SC-VTOL-01 which contains failure condition severity classifications and their applicable aircraft level failure rates (Ref. 12). Once agreed upon operational requirements are available, the reliability assessment would use operational requirements for severity classification, compensating provisions, β, or other.

A FTA was generated in conjunction with the FHA and FMECA in order to define the vehicle-level failure rate that would be compared against the operational requirement, like that specified in SC-VTOL-01. The FTA, which is built off the catastrophic and critical FHA hazards, can then be used to show the sensitivity of the system to the connectivity and inter-relationships of each sub-system. Once a fault tree has been configured for a given architecture, cut-sets may be used to perform said sensitivity studies by changing the relative relationship one component has on the subject hazard. As previously mentioned, the reliability and safety assessment process is iterative and should be closely coupled with design decisions. Figure 2 shows the graphic representation of this safety/reliability iteration loop and Figure 3 shows the process utilized to study the NASA RVLT QR Concept Vehicle.

DESIGN AND ANALYSIS ASSUMPTIONS

As is common with the aircraft conceptual design process, design assumptions were defined

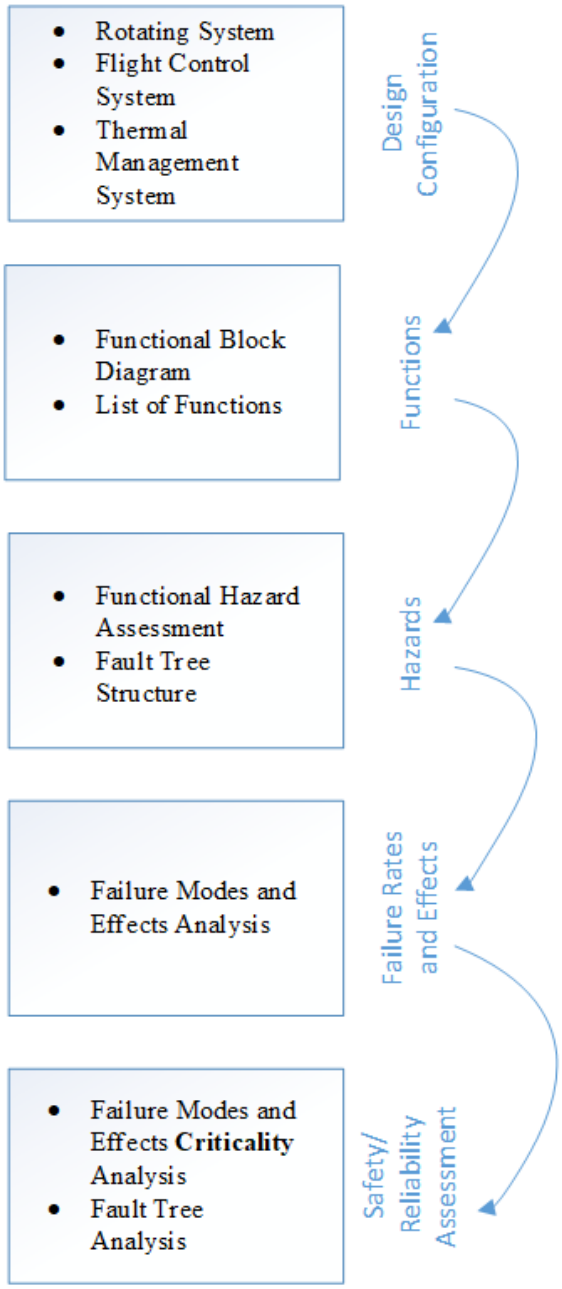

Figure 3: Reliability and Safety Assessment Process used to assess the NASA RVLT Quad Rotor Concept Vehicle.

and documented in order to enable the reliability and safety analysis described herein. In many cases design decisions had to be made that could not be comprehensively assessed with the amount of design detail available; it is in these cases where assumptions were made based on experience, anticipated regulations, cursory analytical results, or other details gleaned from past UAV or electric aircraft design experience.

In practice, design assumptions made early in the program are intended to keep the design space open and design assumptions that limit the design space may become system requirements as the program matures.

The UAM mission is intended to be flown over major cities to reduce roadway congestion and travel time (Ref. 13); therefore, the UAM aircraft assessed here will be assessed against the metric that they operate over populated, metropolitan areas for a majority of their life.

For comparison purposes, aspects of the flight controls, environmental systems, or other sub-systems that are not directly impacted by the change from conventional propulsion to DE/HEP are not assessed because it is assumed that the safety and reliability of these systems are expected to be invariant when introducing various propulsion system configurations, except as noted herein.

Hazards for this study are limited to power-on mission segments. Autorotation is excluded from the current study. The ability to autorotate or maintain an intended flight path with primary power turned off requires complex analysis and/or test, depending on configuration. The QR without interconnecting shafts, for instance, may be theoretically able to autorotate, but in practice managing the energy of all four rotors independently may prove difficult. As a result, all cases in the FHA that have loss of power and possible autorotative descent are listed as Catastrophic outcomes. Additionally, further guidance from SC-VTOL-01 had shown that autorotative descents are not allowed to be considered mitigation for any Category Enhanced aircraft.

Temperature limits considered in this study include a maximum ambient temperature of 125 degrees Fahrenheit (˚F), a maximum box temperature of 131˚F for speed controllers and inverters/rectifiers, an operating temperature range of 59-113˚F for batteries, and a maximum

box temperature for motors and gearboxes of 260˚F.

In order to manage risk and to develop inherently safe architectures, some components were intentionally physically or functionally isolated from others in the safety model. The Flight Control Computer (FCC) was isolated from the motors by integrating motor control authority into each motor's individual Electronic Speed Controller (ESC); thereby isolating the function of speed regulation in the event signal is lost between the FCC and ESC. The ESC has the ability to regulate rotor speed through a local control loop and can revert to a set speed if the FCC signal is lost. Specifically, for this exercise, the ESC's were assumed to revert to their last recorded speed.

The rotors and interconnecting shafts were isolated from each electric motor via an overrunning clutch system in case of an ESC or motor failure. ESC failure could result in a transient torque spike or similar physical event that could overload components and cause downstream components to fracture. Motor failures could include rotor/stator contact or locked rotors, in which case fire or large braking loads could cause fracture to downstream components.

A 17.42:1 reduction ratio was conceptualized for the rotor gearboxes. The 17.42:1 reduction ratio is a comfortable reduction ratio for a two stage, simple planetary system. Using the noted reduction ratio, the QR would utilize an 11,863 RPM motor, nominally. The torque capacity of the rotor gearboxes is 58 ft-lbs at the final stage design torque. The baseline vehicles assumed 8,000 RPM motors, which is slower than the conceptualized 11,863 RPM motor.

A weight trend to show the impact of the noted higher speed motors can be easily developed using the US Army Aeroflightdynamics Directorate (AFDD) Drive System Weight Model AFDD00 and the NASA Motor Weight Model, NASA15, both of which are used for weight buildups in NASA Design and Analysis of Rotorcraft (NDARC) (Ref. 14). A weight trend was developed for the QR, assuming a Rotor Speed of 681 RPM and Motor of 22 HP Maximum Continuous Power (MCP). The weight trend was developed for a single rotor, so a Main Rotor value of "1" was used for this weight trend. Figure 4 shows a notable weight savings per rotor by utilizing an 11,863 RPM Motor.

Battery packs were assumed to be distributed and isolated from one-another inside the fuselage. Although represented as a single block of High Voltage Batteries in the configuration diagrams, they were conceptualized to include fail-safe switching and are assumed to be physically isolated from one-another such that a failure in one module does not propagate to all modules.

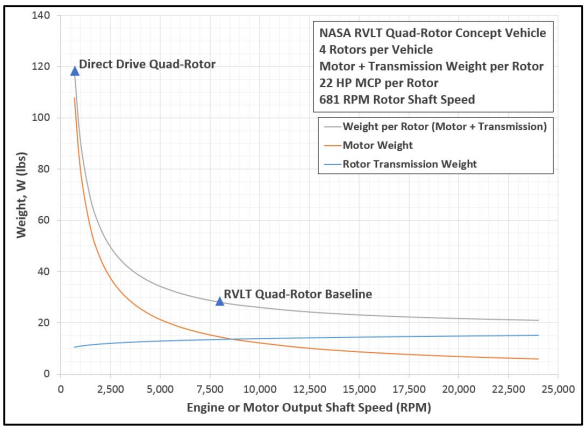

Figure 4: Weight Trend for Single Prop-Rotor Propulsion System of NASA RVLT Tilt-Wing Concept Vehicle.

POWERTRAIN CONFIGURATIONS

BASELINE CONFIGURATION

The QR design developed by the NASA RVLT team included a distributed propulsion and DFC architecture, herein referred to as a DPFC architecture. The propulsion system is considered "distributed" because it integrates propulsion units remotely located near each rotor. The flight control system is considered "distributed" because pitch, yaw, and roll control are established by mixing inputs from

remotely located rotors with single-axis collective blade pitch control. Specifically, the QR uses four main rotors with single-axis, collective control and four, associated motors to achieve lift and control. The collective, variable pitch control (as opposed to variable speed control) allows for mechanical interconnection of each rotor via interconnecting shafts and gearboxes. The mechanical interconnection is a secondary load path intended to dampen rotor-to-rotor modes and provide power to all rotors in the event of a one motor inoperative (OMI) condition.

The powertrain configuration for the QR is broken into three primary sub-categories. As defined here, the rotating system includes the motors, gearboxes, and interconnecting shafts. The FCS includes the ESC's, low voltage battery arrays for low power computing and actuation, high voltage batteries for high power energy storage necessary to drive the rotors, and associated wiring. The Thermal Management System (TMS) includes systems for managing the temperature of the ESC's and batteries.

Rotating System

The rotating system of the QR is shown in Figure 5. The QR rotating system contains four electric motors remotely located, near each rotor. Each motor spins at 11,863 RPM and sends power into an overrunning, sprag clutch mounted inside an accessory gearbox. The accessory gearbox contains a parallel axis gear train in order to mechanically drive a cooling fan and lubrication pumps. The cooling fan draws air across a heat exchanger which cools the motor, accessory gearbox, and rotor gearbox. The lubrication pump pressurizes the cooling and lubrication loop for the heat exchanger.

The motor's primary power passes through the accessory gearbox and into the rotor gearbox through the noted sprag clutch and associated shafts. The parallel axis gear train in the accessory gearbox does not carry primary power. Power enters the rotor gearbox and is transferred through a dual stage, simple planetary system with an overall reduction ratio

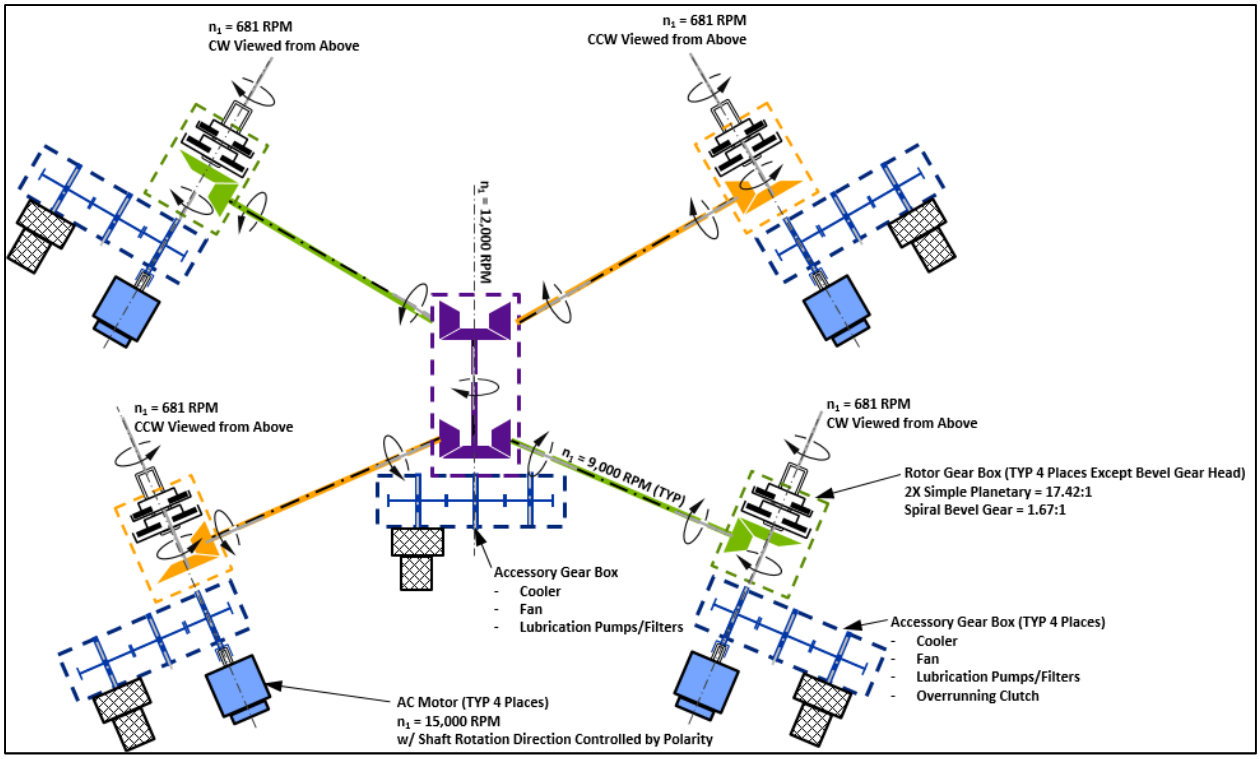

Figure 5: Quad Rotor Rotating System Schematic.

of 17.42:1 to achieve a rotor speed of 681 RPM.

In addition to the primary power path going from the motor to the rotor, a secondary power path is included in the rotor gearbox for OMI conditions and synchronization of the rotors. A spiral bevel gear mesh with a 1.16:1 ratio is mounted between the accessory gearbox and the dual stage, simple planetary system. The spiral bevel gear mesh sends power through interconnecting shafts to a combiner gearbox. Power from the front, left rotor passes through the front, left interconnecting shafts and is transferred into a forward spiral bevel gear mesh in the combiner gearbox. Power is split at the forward spiral bevel gear mesh; power is transferred from the front, right rotor through the complimentary side of the forward spiral bevel gear mesh and interconnecting shafts. Power is sent aft through a short quill shaft and enters an aft spiral bevel gear mesh which splits the power to the left and right aft rotors through a series of interconnecting shafts. The forward and aft sweep of the forward and aft struts, respectively, and the dihedral of each require that each, forward and aft, spiral bevel mesh contains two spiral bevel gears and one spiral bevel pinion, for a total of six spiral bevel gears.

Flight Control System

The QR FCS schematic is shown in Figure 6. Although not depicted, the FCS is assumed to be triple redundant to meet the safety needs of UAM. Each rotor shaft is integral with a rotor gearbox. Collective blade pitch is controlled using a single degree of freedom swashplate actuated by a singular electromechanical actuator (EMA). The gearbox connected to each rotor is connected to an electric motor through an overrunning clutch as well as to a central, combiner gearbox. Each electric motor is controlled by an individual electronic speed controller which accepts both high voltage (to power motor) and low voltage (to power the controller, itself) sources. The high voltage power source also powers the electric actuators used for collective blade pitch control. The low voltage power source provides power to the FCC which is sending control signals to the ESC and the EMAs driving the rotor swashplates as well.

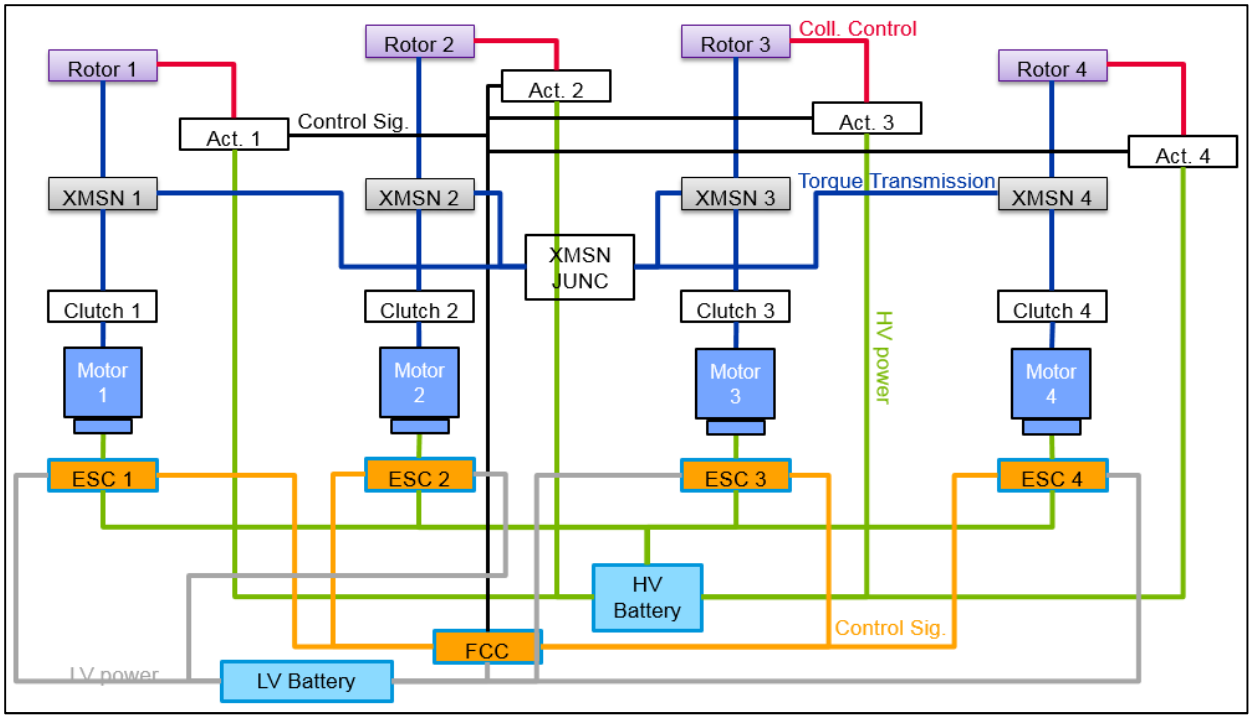

Figure 6: Quad Rotor Powertrain Flight Control System Schematic.

Thermal Management System

DE/HEP systems introduce components which present thermal management challenges. These components include high power density electric motors, electric generators, power electronics/speed controllers for driving and controlling motor operation, power converters, and Lithium-ion (Li-ion) batteries for energy storage. Thermal losses from power distribution cables must also be considered as they impact the environment within which they are located.

A generalized TMS for the vehicles was configured for this study. The system was configured to address the unique thermal requirements of each of the major propulsion system components. System trade studies and detailed system sizing are recommended for future work. During detailed design, the heat dissipation for each component is typically determined for each phase of the mission profile, similar to the notional power usage profile shown in Figure 7. The ambient temperature profile and component operating temperature limitations would also be established. This information would be used to define cooling system requirements, including opportunity for the use of thermal storage materials for peak heat loads.

Motor cooling requirements were combined with gearbox lubrication and cooling requirements in order to reduce the weight and complexity of the TMS.

Speed controllers and power converters are cooled with ambient air. High density or future technology components may dictate the need for more specialized cooling, which would be determined during system design. The TMS includes individual electric fans located in proximity to each component to draw air over the device to manage temperature. During cruise flight, it may be possible to turn off the fans and rely on external aerodynamics to provide cooling air flow, depending on ambient temperature and vehicle flight speed.

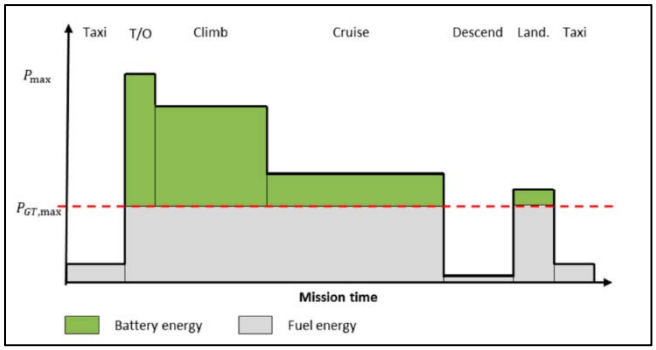

Figure 7: Notional Power Usage Spectrum.

The Li-ion batteries are the most temperature critical components in each of the concept vehicle powertrain systems. Current technology batteries operate most efficiently and reliably between 59°F (15°C) and 113°F (45°C), with battery temperatures above 176°F (80°C) increasing the risk of thermal runaway. It is also desirable to minimize temperature variation across the battery pack for optimal performance. The battery cooling system defined for the concept vehicles addresses each of these concerns.

The battery cooling system consists of a vapor cycle refrigeration system that provides cooling to a liquid loop (water/glycol) used to cool each of the battery packs. A phase change material (PCM) is included in the battery pack design, providing thermal storage to help minimize temperature spikes during transient conditions (highest load) or in the event of a cooling system failure. Material selection and sizing would be part of a system detailed design. It is anticipated that proper PCM selection could reduce the size of the vapor refrigeration system. Selection of a PCM should consider the melting point temperature of the material, the peak heat dissipation of the batteries, and the time over which the peak occurs.

The vapor cycle system operates as a typical vapor compression refrigeration system. Low pressure, low temperature refrigerant gas (R134a) is routed to the compressor, where it first absorbs the heat dissipated by the compressor motor. After compression, the high

pressure gas is routed to the air cooled condenser, where the gas is cooled and condensed into liquid. Under most conditions, the refrigerant is cooled below the saturation temperature, and this sub-cooling provides additional system capacity. The high pressurized liquid refrigerant is then routed to the thermal expansion valves at each evaporator, which provide the pressure drop necessary to produce the cooling effect. As the pressure of the refrigerant is reduced in each valve, the temperature is also reduced as a fraction of the liquid that flashes into vapor. The low temperature, two phase mixture is then routed into the evaporator, where the system heat load is absorbed and the remaining liquid within the mixture is evaporated. The refrigerant exits the evaporator as a low temperature, low pressure gas, and is routed back to the compressor and the cycle repeats.

The liquid cooling loop consists of a pump package which is used to circulate the cooling fluid. The pump package contains two redundant, independent pumps with each pump having its own motor controller and associated level sensor. The two level sensors are installed in a common reservoir on the pump package. The two pumps also share a common filter and bypass loop in case the filter gets clogged. The liquid cooling system is a closed loop system that interfaces with the vapor cycle refrigeration system via the evaporator. The cooled liquid is pumped through the battery packs where it picks up the heat generated by the batteries. The liquid also helps to maintain the batteries at uniform temperature, improving battery performance. The warm liquid flows from the battery packs to the evaporator where the heat is transferred to the vapor cycle refrigerant.

ALTERNATE CONFIGURATION – QUAD ROTOR WITHOUT INTERCONNECTING SHAFTS

The QR was also conceptualized without the use of a combiner gearbox or interconnecting shafts as part of the reliability and safety assessment. The overall powertrain configuration remains similar to the baseline QR powertrain configuration. The rotating system architecture is similar to the baseline, except the interconnecting shafts, the combiner gearbox, and the accessory gearbox required to lubricate and cool the combiner gearbox are removed. The FCS and TMS are similar to the baseline.

FUNCTIONAL BLOCK DIAGRAMS

The Functional Block Diagram is a graphic representation of the functions analyzed. The shaded blocks were analyzed in this study. The corresponding FMECA Identification (ID) codes are identified in the functional blocks to which they reference. Components not analyzed, such as rotors and flight control components, were not considered as part of this FMECA, and are represented with unshaded blocks and dashed lines. Loss of those components may still have been utilized in the FTA as undeveloped events to illustrate how those components would feed up to the top level hazard. Figure 8 shows the functional block diagram for the baseline QR, in which the rotors are interconnected, and Figure 9 shows the functional block diagram for the alternate configuration QR, in which the rotors are not interconnected.

The QR with interconnecting shafts was divided into three main functions:

- Function 1: Provide High Voltage DC power to electric motors. The battery system was postulated as a single component with multiple outputs. Battery failure modes could result in loss of a single output to a single motor, [Failure Modes 1A1 through 1D1] or an internal failure that could result in reduced output, or possible thermal runaway and aircraft fire [Modes 1E1 through 1E4].
- Function 2: Convert electrical energy to shaft torque. This function consists of the Electronic Speed Controller (ESC), electric motor, and associated cooling components. The functions for motor

cooling and motor lube were assumed as a single function.

- Function 3: Transfer motor torque to rotors. The clutches and gearboxes transfer the motor torque to the rotors. In the event of loss of output from a single motor, the combiner gearbox re-distributes the remaining available torque to keep all four rotors operating.

The QR without interconnecting shafts differs only in Function 3, where there is no function to transfer power in the event of a motor failure.

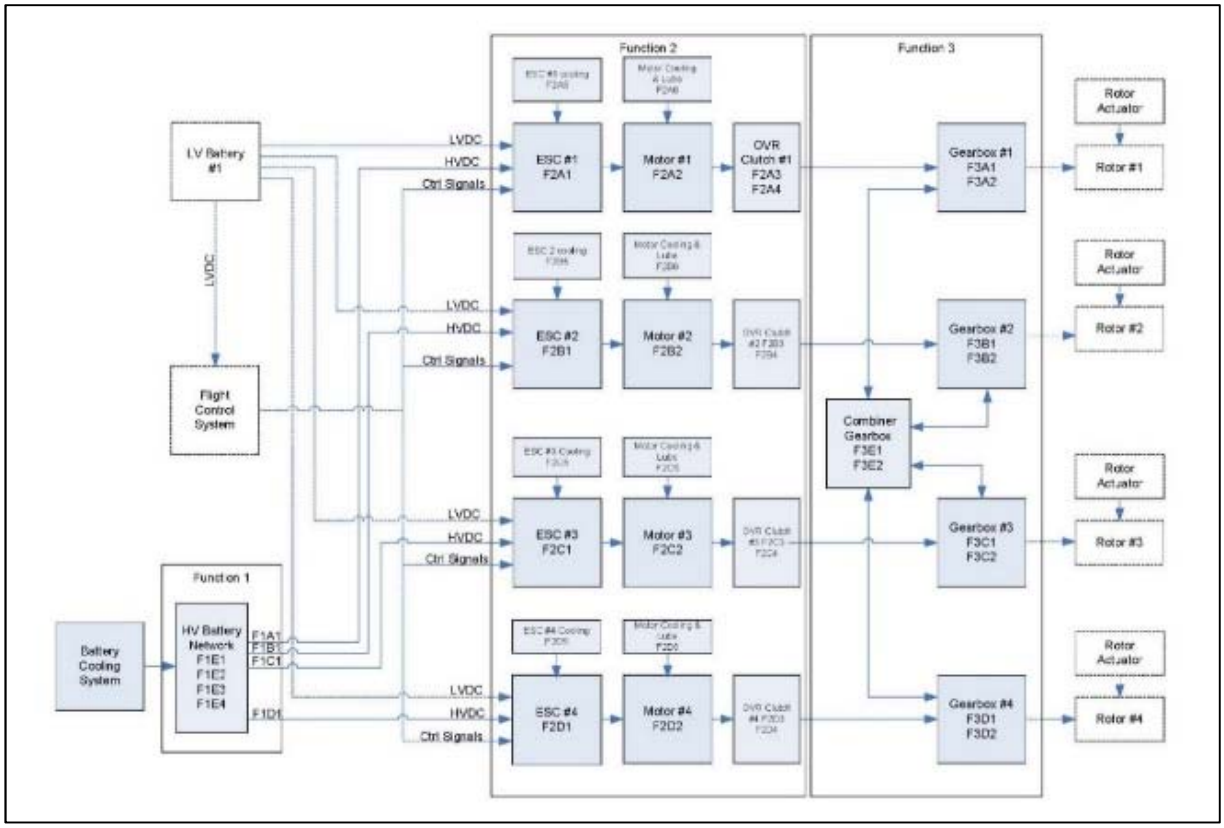

Figure 9: Functional Block Diagram of Baseline Quad Rotor

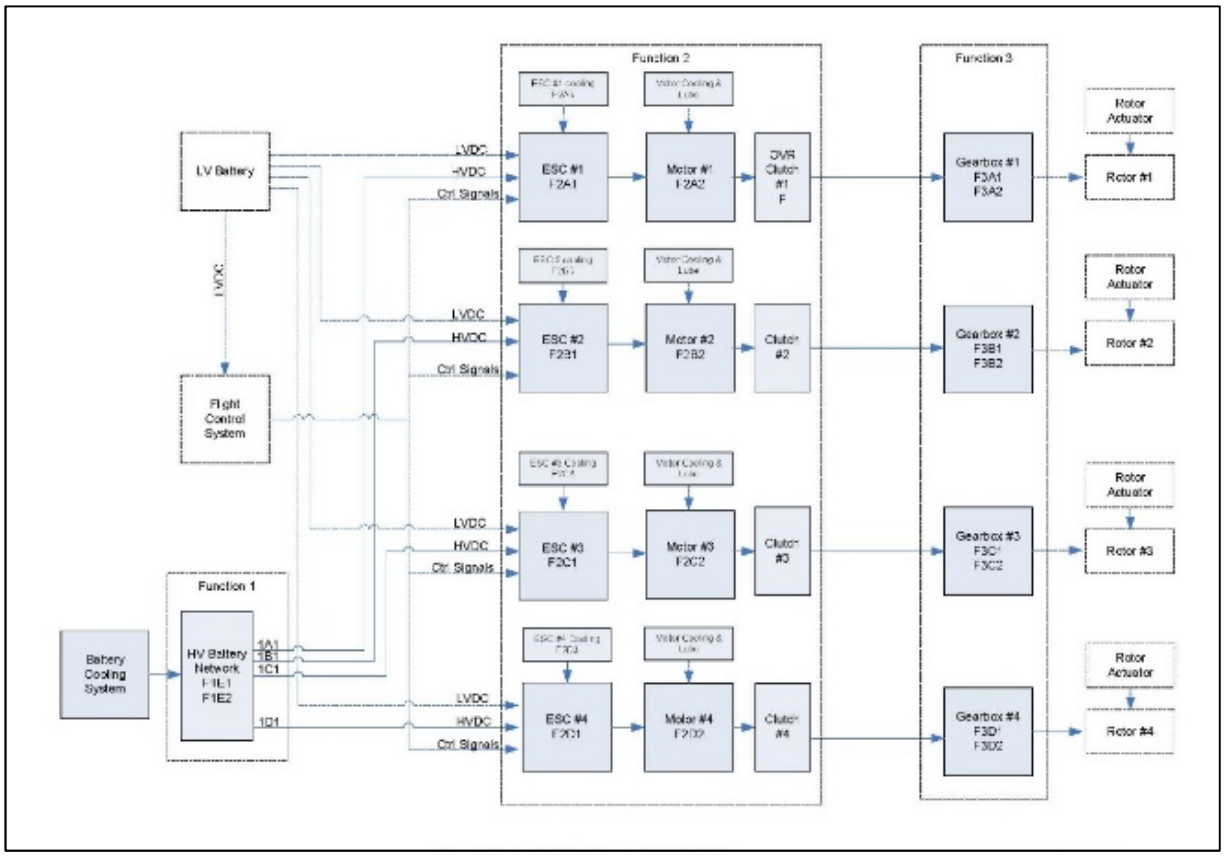

Figure 9: Functional Block Diagram of Alternate Configuration Quad Rotor (No Interconnecting Shafts)

Functional Hazard Analysis

The FHA is used to evaluate the functions and corresponding failure conditions and severity classifications. An associated FTA will be used in conjunction with the FHA in order to begin defining and allocating safety requirements to sub-systems. The FHA and the safety assessment will typically expand and evolve alongside the airplane development.

Functions at an air vehicle level may be shared by sub-systems; however, critical functions, such as pitch control and thrust, are generally segregated so that one failure provides an opportunity for the pilot to land the airplane safely. DE/HEP concepts may be segregated into two smaller categories, wherein control is provided by a variable pitch rotor system which has a light functional coupling to the propulsion system, or wherein control is provided by varying the speed of the rotor system, which tends to create a tight functional coupling between airplane control and propulsion. Figure 10 uses some example airplane functions to depict the overlap of typical variable pitch and variable speed DPFC systems. As more functions, and therefore more functional failures, are attributable to the propulsion system, then either the reliability requirements for the propulsion system increase or the vehicle architecture must be designed with appropriate levels of fail-safety.

Airplane functions, and thereby functional hazards, associated with DPFC systems can be extensive depending on whether the propulsion system includes control of the vehicle. Either the FHA may include more functions in the air-vehicle level FHA or, as is in the case of this FHA, apply loss of control or other hazards up through the primary, loss of propulsion hazard.

The FHA for the baseline QR may be found in Appendix A as taken from the NASA contractor safety and reliability analysis. The contractor report also contains the FHA for the quad rotor without interconnecting shafts.

For the quad rotor without interconnecting shafts, any single loss of a propulsor is considered loss of air vehicle due to the rotors not being interconnected. The system may be configured to automatically reduce lift on the diagonal side rotor. This will result in reduced controllability and control coupling. The reduction in lift from two propulsors (one lost, the other pulled back automatically) will result in an autorotative approach, and the feasible outcome for this scenario is a loss of air vehicle/occupants. By contrast, in the example where the rotors are interconnected, a loss of a single propulsor is Minor at altitude, and only potentially Catastrophic when the air vehicle is being operated in the OMI avoid region.

Additionally, the effects of the position of any

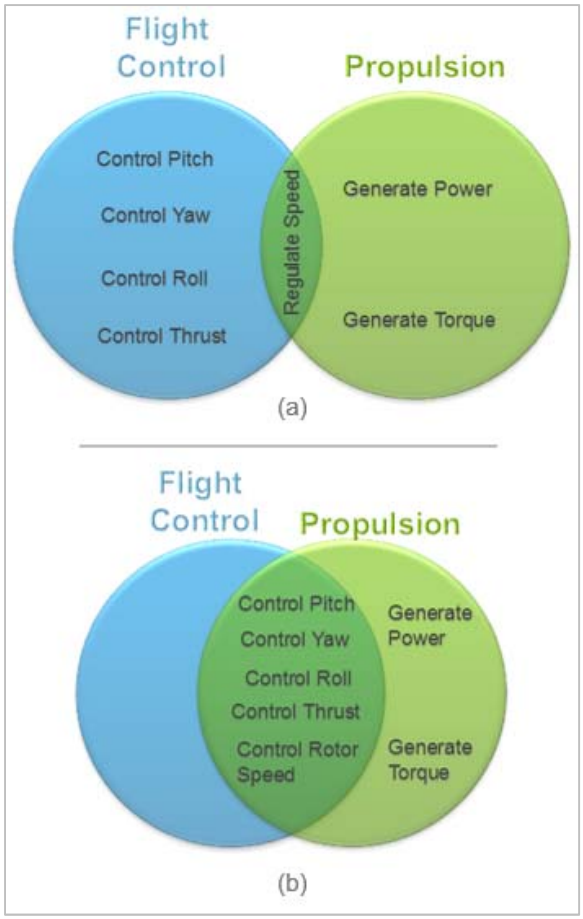

Figure 10: Flight Control and Propulsion Systems' Functional Overlap for (a) Common Variable Pitch DE/HEP Systems and (b) Common Variable Speed DE/HEP Systems.

dual propulsor failures is separately examined in the FHA for the quad rotor without interconnecting shafts. Controllability impacts are different whether the propulsors are diagonal to each other or not, though in all cases the likely outcome for a dual propulsor failure is Catastrophic in all flight conditions.

The QR was designed to be controlled via single-axis collective blade pitch at each of its rotors. However, the rotors do not intermesh and the number and configuration of the rotors make it conceivable that pitch, roll, and yaw control can be obtained via constant pitch, variable speed rotors. In light of the extra demands made on the propulsion system using variable RPM for air vehicle control as typified in Figure 10, it is recommended that future work assess the impacts to the safety of the vehicle when using variable speed rotors as the vehicles primary attitude control.

FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS

For this study, failure rates of similar equipment were taken from various sources, then, depending on the source information and engineering judgment, environmental factors were applied to generate a failure rate that is realistically achievable with state-of-the-art technology (Ref. 15). Appendix B contains a summary of each item, base failure rate, data source (reference material), applied environmental factor, and the applied failure rate. The base failure rate was taken from the noted data source and multiplied by the applied environmental factor, in which engineering judgment was used to apply environmental factors in accordance with MIL-HDBK-217 (Ref. 16).

Table 1 provides a summary of the Category I Failure Mode Criticality Numbers. The complete FMECA worksheets may be found in the NASA contractor safety and reliability analysis (Ref. 1).

Table 1: Summary of Category 1 Failure Mode Criticality Numbers.

Function No.	**Failure Mode Criticality No.**	
	Baseline Config.	Alternate Config.
1	2.00×10^{-7}	5.00×10^{-7}
2	3.02×10^{-4}	1.01×10^{-3}
3	1.00×10^{-5}	1.00×10^{-5}

FAULT TREE ANALYSIS

The tree structure and the connectivity of the FTA are developed in parallel with, and are informed by, the functional block diagram. The failure rates of the FTA are informed by the FMECA. In some cases multiple FMECA codes are covered by one FTA event, in which case engineering judgment is used to select the appropriate failure rate.

The failure rate or failure criticality number will be used as appropriate in the fault tree. In some cases the individual failure to function in the FMECA will not roll up to the top level hazard. In this case the failures associated with the appropriate functions will be utilized, weighted by their corresponding mode ratios, α.

Common points of failure are modeled on the fault tree. Mitigations and system redundancy are modeled through appropriate gating. Cut-sets help show independence in system architecture.

The QR FTA was executed with the following assumptions:

- The QR is conservatively assumed to be in the OMI avoid region for 25% of its mission time.

- Loss of a single rotor gearbox is assumed to result in the top level hazard due to an inability to drive the rotor and create thrust. The fault tree models the interconnection between gearboxes such that a interconnecting shaft failure AND a loss of any propulsor OR a combiner gearbox failure AND a loss of any propulsor results in a catastrophic outcome.
- The fault tree for the QR without interconnection lacks the logical input of the interconnecting shafts AND a propulsor fail to prevent the top level occurrence. While the OEI avoid region is modeled, the cut set for the fault tree is that any loss of a single propulsor will set the top gate event true.

An example of the FHA flow to the QR FTA is seen in Figure 11. In this case, any combination of dual propulsor failure is a Catastrophic failure. This is modeled in the fault tree with six

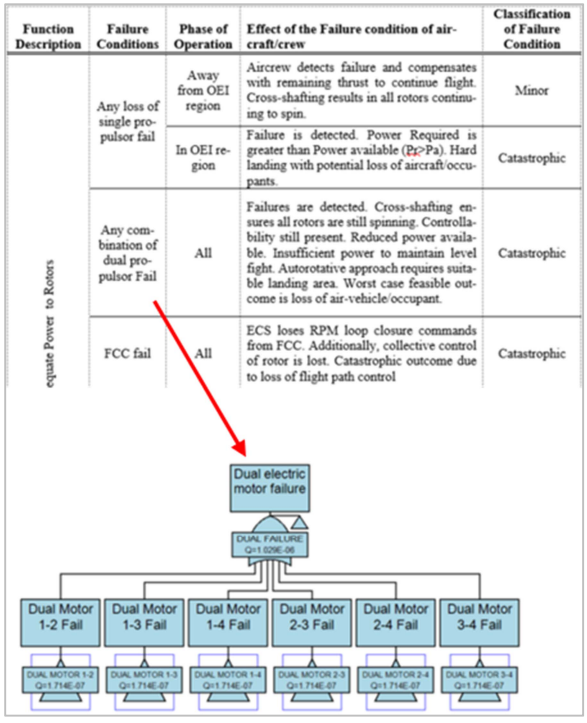

Figure 11: FHA to FTA flow down of a catastrophic hazard hazard to a mid-FTA single fail summary gate in the Quad-Rotor FTA.

unique AND gates associated with each dual propulsor combination. Note: each Dual Motor Failure is a cutset (symbolized by a triangle), showing that each of the Single Motor Failure events contribute to other failures in the fault tree in addition to the dual electric motor failure.

Table 2 includes the failure rate of the top level hazard, Branch 1, as well as the three second level branches for the baseline and alternate configurations; loss of Function 1: Provide High voltage DC power to electric motors, loss of Function 2: Convert electrical energy to shaft torque, and loss of Function 3: Transfer motor torque to rotors.

Table 2: Summary of Fault Tree Analysis.

Branch ID	**Description**	**Failure Rate per Flight Hour** Baseline	Alternate
1 (Top)	**Loss Of Power**	**2.0×10^{-4}**	**8.0×10^{-4}**
2	Dual Electric Motor Fail	1.1×10^{-5}	1.1×10^{-5}
3	OMI Propulsion Loss	2.0×10^{-4}	2.0×10^{-4}
4	Loss Of Ability To Drive A Rotor	4.0×10^{-6}	8.0×10^{-4}

DISCUSSION OF EASA SC-VTOL-01 IMPACTS TO RVLT CONCEPT VEHICLES

Since the publication of the NASA contractor safety and reliability analysis for the four concept air vehicles, further guidance on SC-VTOL-01 has become available with the draft release of acceptable means of compliance (MOC) in MOC SC-VTOL (Ref. 17). The work presented herein focused on top-level safety results, in order to meet requirements like VTOL.2510, or similar. However, the MOC

released additional guidance on single failure criteria that may be just as difficult to attain.

MOC VTOL.2250(c) states that for Category Enhanced, no single point failures, noted in the MOC as structural elements to include the rotor head and drive train, but not specifically limited to those areas, is allowed to result in a catastrophic consequence."

This differs greatly from past acceptable rotorcraft practices. FAR 29 rotorcraft have been able to utilize critical part designations for such components as gearboxes, pitchlinks, and rotors. Critical part designations allow parts that could otherwise contribute to single point failures to go through a rigorous design, certification, manufacturing process, and maintenance/life monitoring philosophy that allows their use even though they are a single point for catastrophic failure.

The concept air vehicle architectures will need to be further evaluated against the SC-VTOL-01 Single Fail Criteria and the MOC guidelines. Future work should understand the impact of the more stringent guidance to ascertain impacts this will have on all aircraft covered by SC-VTOL-01. VTOL.2250(c) has far reaching implications, even within simplified architectures, such as direct drive rotors connected to fixed-pitch rotors. Additionally, future work is required to meet VTOL.2510, which also has similar, far reaching implications.

CONCLUSIONS

1. Electrical Component reliability (ESC Motor, and HVDC power supply) resulting in loss of propulsion was the most significant numerical driver into the loss of propulsion FTA top event.
2. Existing electrical motor and power inverter assumptions will not meet the top level EASA SC-VTOL-01 requirements. Motor controller redundancy, changes to motor architecture to allow redundancy (multiple windings as one possibility), or redundant motors will be required to meet or exceed 1E-9 per flight hour catastrophic outcome requirement, per VTOL.2510.
3. The depth of fault tree analysis was such that cut-sets tended to reveal many of the common mode failures that were present in the architecture of the vehicles. As the air vehicle depth of examination in the FTA increases, complexity of system interactions increases such that cut-sets alone cannot always be relied upon to reveal common modes of failure. This can be due to proximity, systems packaging, or environmental effects not able to be modeled in the FTA.

RECOMMENDATIONS

1. Further development of the propulsion and related controls FHAs down to the system level, and the beginnings of allocating system level safety requirements using a Preliminary System Safety Assessment (PSSA).
2. Recommend the execution of Common Cause Analysis (CCA) as part of the continued system level definitions. The novel layout of some of the concept air vehicles may result in system or components packaging difficulties that could result in the need to further develop best design practices to avoid the situations typically sought out in those types of analysis.
3. Evaluate alternatives to the modeled Thermal Management System to optimize the weight and safety/reliability trades necessary for the RVLT vehicles.
4. Quantify electrical component reliability and develop electrical components and architectures with sufficient reliability to meet or exceed the vehicle-level safety criteria. The NASA RVLT project is presently following this recommendation and performing electrical propulsion component research as part of a Technical Challenge.

5. Examine the coupled flight control and propulsion safety implications for aircraft with multiple electrically-powered rotors, and especially where rotor speed is used for flight control. The NASA RVLT project has awarded study contracts to Boeing and Georgia Tech/The Ohio State University to perform analysis of coupled control/propulsion multirotor systems, and these contractors will be publishing reports in 2021.

Email contact information:

Allan Beiderman

- allan.r.beiderman@boeing.com

Patrick R. Darmstadt

- patrick.r.darmstadt@boeing.com

Caitlin Dillard

- caitlin.dillard@boeing.com

Christopher Silva

- christopher.silva@nasa.gov

RECOMMENDED BEST PRACTICES

Severity outcomes of hazards should not be lowered based on assumed operator intervention. Pilot actions should be noted and human factors interactions can be derived as safety requirements. These actions can been seen as lowering the probability of the worst case safety outcome, but not the severity. Engineering controls are necessary to lower the severity of an outcome. Lowered severity IF operator outcome is successful can be noted, but worst case safety outcome will still exist at a lower probability.

ACKNOWLEDGMENTS

The scope of this paper includes a portion of the work commissioned by NASA to evaluate the NASA RVLT Concept Vehicles under Contract #NNA15AB12B, Task Order 80ARC018F0121. The work provided herein includes the configuration of a propulsion system required to perform a reliability and safety analysis of one of NASA's RVLT Concept Vehicles.

REFERENCES

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

[2] Fredericks, J., McSwain, R., Beaton, B., Klassman, D., Theodore, C. *Greased Lightning (GL-10) Flight Testing Campaign*, NF1676L-25116, July 2017.

[3] McSwain, R., Glaab, L., Theodore, C. Rhew, R., North, D., *Greased Lightning (GL-10) Performance Flight Research: Flight Data Report,* NASA/TM-2017-219794, November 2017

[4] NASA Armstrong Fact Sheet – *NASA X-57 Maxwell*, September 2018.

[5] Johnson, W., Silva, C. and Solis, E.: "Concept Vehicles for Air Taxi Operations." AHS Aeromechanics Design for Transformative Vertical Flight, San Francisco, CA, January 2018.

[6] Silva, C., Johnson, W., Solis, E., Patterson, M., and Antcliff, K.: "VTOL Urban Air Mobility Concept Vehicles for Technology Development." 2018 Aviation Technology, Integration, and Operations Conference, AIAA Aviation Forum, 2018.

[7] Johnson, W., Yamauchi, G., and Watts, M.: "Designs and Technology Requirements for Civil Heavy Lift Rotorcraft," AHS Vertical Lift Aircraft Design Conference, San Francisco, CA, January, 2006.

[8] SAE ARP4761 - *Aerospace Recommended Practice: Guidelines and Methods for Conducting The Safety Assessment Process on Civil Airborne Systems and Equipment*, 1996-12.

[9] SAE ARP5150A – *Aerospace Recommended Practice: (R) Safety Assessment of Transport Airplanes in Commercial Service*, 2019-01.

[10] SAE ARP5151 – *Aerospace Recommended Practice: Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service*, 2013-05.

[11] SAE ARP4754A – *Aerospace Recommended Practice: (R) Guidelines for Development of Civil Aircraft and Systems*, 2010-12.

[12] EASA SC-VTOL-01 – *Special Condition: Vertical Take-Off and Landing (VTOL) Aircraft*, October 15, 2018.

[13] Goel, N. and Holden, J.: *Fast-Forwarding to a Future of On-Demand Urban Air Transportation*. Uber Elevate, October 27, 2016.

[14] Johnson, W. *NDARC. NASA Design and Analysis of Rotorcraft*. NASA TP 2015-218751, April 2015.

[15] NPRD-2016 – *Nonelectronic Parts Reliability Data Publication*, Quanterion Solutions Inc., 2015

[16] MIL-HDBK-217F – *Military Handbook: Reliability Prediction of Electronic Equipment*, 02-Dec-1991

[17] MOC SCVTOL 01 – *Proposed Means of Compliance with the Special Condition VTOL*; 25 May 2020

Appendix A: Quad-Rotor FHA

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Any loss of single propulsor fail	Away from OEI region	Aircrew detects failure and compensates with remaining thrust to continue flight. Cross-shafting results in all rotors continuing to spin.	Minor
		In OEI region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/occupants.	Catastrophic
	Any combination of dual propulsor Fail	All	Failures are detected. Cross-shafting ensures all rotors are still spinning. Controllability still present. Reduced power available. Insufficient power to maintain level fight. Autorotative approach requires suitable landing area. Worst case feasible outcome is loss of air-vehicle/occupant.	Catastrophic
	FCC fail	All	ECS loses RPM loop closure commands from FCC. Additionally, collective control of rotor is lost. Catastrophic outcome due to loss of flight path control	Catastrophic
	Dual ESC fail	Dual ESC failed high: all phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots will need to reduce engine power to land. If hover power can be properly managed than land normally. Worst case feasible outcome is air-vehicle damage and occupant injury	Severe
		Dual ESC Failed Low: All phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Reduced power available. Insufficient power to maintain level fight. Autorotative landing required. Worst case feasible outcome is loss of air-vehicle/occupant. Hazard classification is the same whether OEI or out of OEI avoid region.	Catastrophic

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Single ESC fail	Esc failed hi: all phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots will need to manually modulate engine power to a hover landing or a no hover landing with some forward speed to maximize Effective Translational Lift (ETL). Pilot workload issue.	Minor
		ESC Failed Low: Not OEI Avoid region	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots will need to execute a no hover landing with some forward speed to maximize Effective Translational Lift (ETL). Pilot workload issue.	Minor
		ESC Failed Low: OEI Avoid region	Failure is detected. Cross shafting ensures controllability. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
	Single gearbox fail	All	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications). Loss of ability to spin rotor associated with that gearbox. Loss of flight-path control and subsequent catastrophic loss of air vehicle/occupants	Catastrophic
	Dual gearbox fail	All	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications). Loss of ability to spin rotors associated with those gearbox. Loss of flight-path control and subsequent catastrophic loss of air vehicle/occupants	Catastrophic
	Complete HV Battery fail	All	Complete loss of all High Voltage Power to motors. Complete loss of propulsion. Autorotative landing required. Worst case feasible outcome is loss of air-vehicle/occupant.	Catastrophic
	Individual portions of HV Battery Fail	OEI Avoid Region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/occupants	Catastrophic

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors		Other than OEI Avoid Region	Aircrew detects failure and compensates with remaining thrust to continue flight	Minor
	LV battery fail	All	Loss of power to all 4 ESC and FCC. Collective control of rotor lost. Loss of flight Path Control and air vehicle	Catastrophic
	Combiner gearbox/cross shaft fail	All	Annunciated to pilot. Need proper anti-flail in place on driveshaft. Possible minor handling qualities impact, lack of redundancy available for follow-on propulsion single or dual failures. This fail is and of itself is not Catastrophic.	Minor

Appendix B: Quad-Rotor FHA: Applied Failure Rate (FR) used for FMECA

Item	Base FR (failures per 10^6 hours)	Data Source	Applied Environmental Factor	Applied FR (failures per 10^6 hours)
Turbine Engine	2.67	"Powerplant Reliability and Wear Monitoring in Aircraft Piston Engines. Part II Engine Diagnostic" by Luca Piancastelli published 6 March 2018	1	2.67
Generator, AC	13	NPRD-3, 1985	10	130
Gearbox assembly	0.5	NPRD-2016	10	5
Battery, lithium	9.31	NPRD-2016	10	93.1
Controller, motor	4.75	Attack aircraft maintenance data	10	47.5
Motor-Generator	19.72	RAC reliability toolkit	10	197.2
Electric Motor, General	9.24	RAC reliability toolkit	10	92.4
Pump, general	43.65	RAC reliability toolkit	1	43.65
Electronic Motor Drive	54	Quantitative Evaluation for Reliability of Hybrid Electric Vehicle Powertrain, Yantao Song and Bingsen Wang, Department of Electrical and Computer Engineering Michigan State University	5	270
Air conditioner [Battery cooling system]	508	RAC reliability toolkit	1	508
Heat exchanger	8.08	RAC reliability toolkit	1	8.08
Motor cooling system	51.73	(pump + Heat exchanger)	1	51.73
Airborne power supply	200	Quanterion System Reliability Toolkit (2000 - 20000 MTBF)	1	200
Clutch, General	5.01	RAC Reliability Toolkit	1	5.01
Clutch, Overrunning	0.42	NPRD-2016	1	0.42
Shaft, General	0.93	RAC Reliability Toolkit	1	0.93
Drive Link Assembly (drive shaft)	1.495	RAC Reliability Toolkit	1	1.495