NASA/CR—2019-220217

Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems

Patrick R. Darmstadt, Ralph Catanese, Allan Beiderman, Fernando Dones, Ephraim Chen, Mihir P. Mistry, Brian Babie, Mary Beckman, and Robin Preator
The Boeing Company, Philadelphia, Pennsylvania

June 2019

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NASA Technical Report Server—Registered (NTRS Reg) and NASA Technical Report Server—Public (NTRS) thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers, but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., "quick-release" reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Fax your question to the NASA STI Information Desk at 757-864-6500

- Telephone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Program
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/CR—2019-220217

Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems

Patrick R. Darmstadt, Ralph Catanese, Allan Beiderman, Fernando Dones, Ephraim Chen, Mihir P. Mistry, Brian Babie, Mary Beckman, and Robin Preator
The Boeing Company, Philadelphia, Pennsylvania

Prepared under Contract NNA15AB12B, Task Order 80ARC018F0121

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

June 2019

Acknowledgments

The authors express their gratitude to the NASA Revolutionary Vertical Lift Technology (RVLT) Team, the Federal Aviation Administration (FAA), and Dan Newman, Mark Robuck, and Adam Lubchansky, Boeing, for their helpful comments and suggestions. The authors would like to acknowledge the NASA RVLT Team for sponsoring this work and for their insight and forward-thinking nature and the FAA for their support in the execution of this project. Their continued insight and support throughout the duration of the project was invaluable.

This work was sponsored by the Advanced Air Vehicle Program
at the NASA Glenn Research Center

Level of Review: This material has been technically reviewed by NASA technical management.

Available from

NASA STI Program
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703-605-6000

This report is available in electronic form at http://www.sti.nasa.gov/ and http://ntrs.nasa.gov/

ABSTRACT

The primary objective of this research effort is to identify failure modes and hazards associated with the concept vehicles and to perform functional hazard analyses (FHA) and failure modes and effects criticality analyses (FMECA) for each. Boeing also created a Fault Tree Analysis (FTA) for each of the concept vehicles, as the FTA contains the connectivity between systems and is an accepted, top-down method to analyze the safety of an air-vehicle. Conceptual design of notional powertrain configuration for each of four (4) NASA RVLT Concept Vehicles were developed in as much detail as was necessary to support the reliability and safety analysis for this project. Functional block diagrams from each of the conceptual powertrain configurations were created and used to order the FHA, FMECA, and FTA. Hazards were identified and the severity of each were categorized in the FHA for use in a follow-up FMECA. The FTA took inputs from the FMECA and the functional block diagrams to develop the connectivity and develop a quantitative architecture that could be used to perform sensitivity studies, as related to vehicle safety.

Guidelines for reliability targets for both the air vehicle and the operation in the UAM mission are discussed. An industry literature search was performed in order to assess gaps in existing government regulations and industry specifications. The industry literature search led to air-vehicle and operational reliability discussions, as related to Distributed Electric/Hybrid-Electric Propulsion (DE/HEP) system operating in the UAM role. A discussion of results and recommendations for future work is also provided.

TABLE OF CONTENTS

Abstract i
Table of Contents iii
List of Figures v
List of Tables vi
List of Acronyms vii
1 Introduction 1
1.1 Research Objectives 1
1.2 Air-Vehicle Concept Configurations 2
1.3 Tilt-Wing Air Vehicle 2
1.4 Quad-Rotor Air Vehicle 2
1.5 Side-by-Side (Lateral-Twin) Description 3
1.6 Lift+Cruise Description 4
1.7 Mission Profile 4
2 Work Scope 5
2.1 Conceptual Powertrain Configurations Scope 5
2.2 Functional Hazard Assessment Scope 6
2.3 FMECA Scope 6
2.4 FTA Scope 7
3 Background 9
3.1 Literature Review 9
3.2 Nomenclature & Taxonomy 10
3.3 Functional Overlap of Distributed Propulsion and Distributed Flight Controls 11
3.4 Vehicle Level Reliability Metrics 12
4 Methodology and Common Assumptions 14
4.1 Configuration Assumptions 15
4.2 Functional Hazard Assessment Assumptions 20
4.3 FMECA Methodology & Assumptions 22
4.4 FTA Methodology & Assumptions 25
5 Conceptual Powertrain Configurations 29
5.1 Tilt-Wing Powertrain Configuration 29
5.2 Quad-Rotor Powertrain Configurations 30
5.3 Alternate Configuration – Quad-Rotor without Interconnecting Shafting 33
5.4 Lateral-Twin Powertrain Configuration 33
5.5 Lift+Cruise Powertrain Configuration 35
5.6 Thermal Management Systems 37
6 Functional Block Diagrams 40

6.1 Tilt-Wing Functional Block Diagram 40
6.2 Quad-Rotor Functional Block Diagram: 42
6.3 Alternate Configuration –Quad-Rotor without Interconnecting Shafting Functional Block Diagram 44
6.4 Lateral-Twin Functional Block Diagram 46
6.5 Lift+Cruise Functional Block Diagram 48
7 Functional Hazard Analysis 50
8 Failure Modes and Effects Criticality Analysis (FMECA) 52
8.1 Definitions of FMECA Worksheet Data Elements: 52
9 Fault Tree Analysis (FTA) 59
10 Discussion 62
10.1 Configuration 62
10.2 Reliability/Safety Analysis 65
10.3 Reliability Metrics for the UAM Mission 68
11 Conclusions 70
12 Lessons Learned & Recommendations 72
12.1 Lessons Learned 72
12.2 Recommendations – Operational Requirements 72
12.3 Recommendations for Future Work 76
13 References 79

Appendix A Functional Hazard Analysis (FHA) Tables A-1
Appendix B Failure Modes and Effects Criticality (FMECA) Worksheets B-1
Appendix C Tilt-Wing Fault Tree dIAGRAM C-1
Appendix D Quad-Rotor Fault Tree Diagram D-1
Appendix E Alternate Configuration – Quad-Rotor without Interconnecting Shafts E-1
Appendix F Lateral-Twin Fault Tree Diagram F-1
Appendix G Lift+Cruise Fault Tree Diagram G-1

LIST OF FIGURES

Figure 1: Tilt-Wing Air Vehicle 2
Figure 2: Quad-Rotor Air Vehicle 3
Figure 3: Side-by-Side (Lateral-Twin) Air Vehicle....3
Figure 4: Lift+Cruise Air Vehicle Concept 4
Figure 5: Proposed Vehicle Configuration Taxonomy. 11
Figure 6: Flight Control and Propulsion Systems' Functional Overlap for (a) Typical Variable Pitch DE/HEP Systems and (b) Typical Variable Speed DE/HEP Systems. 12
Figure 7: Example Stick Diagram with Rotating, Flight Control, and Thermal Management Systems overlaid. 14
Figure 8: Process Flow Used to Assess Reliability and Safety of NASA HA/FMECA 16
Figure 9: Weight Trend for one (1) Prop-Rotor Propulsion System of NASA RVLT Tilt-Wing Concept Vehicle. 18
Figure 10: FMECA Development and Design Flow. 22
Figure 11: FMECA Development Flow Chart. 24
Figure 12: Tilt-Wing Rotating System Schematic. 29
Figure 13: Tilt-Wing Powertrain Flight Control System Schematic 30
Figure 14: Quad-Rotor Rotating System Schematic. 32
Figure 15: Quad-Rotor Powertrain Flight Control System Schematic. 32
Figure 16: Lateral-Twin Rotating System Schematic. 34
Figure 17: Lateral-Twin Powertrain Flight Control Schematic. 34
Figure 18: Lift+Cruise Powertrain Rotating System Schematic. 36
Figure 19: Lift+Cruise Powertrain Flight Control System 36
Figure 20: Thermal Management System (TMS) Schematic 37
Figure 21: Notional Mission Power Usage Profile 38
Figure 22: Tilt-Wing Functional Block Diagram. 41
Figure 23: Quad-Rotor Functional Block Diagram. 43
Figure 24: Alternate Configuration –Quad-Rotor without Interconnecting Shafting Functional Block Diagram. 45
Figure 25: Lateral-Twin Functional Block Diagram. 47
Figure 26: Lift+Cruise Functional Block Diagram. 49
Figure 27: "AND" and "OR" Gate Symbols 59
Figure 28: Relationship of Power to Volume for Inverters and Rectifiers. 64
Figure 29: Example Height Velocity Chart Illustrating Takeoff Profile that Does Not Enter Avoid Regions. 67
Figure 30: Sensitivity Study of Failure Rate vs Time in OEI/OMI Avoid Region for Lateral-Twin. 68
Figure 31: Depiction of Loss-of-Function Reliability vs GVW vs Fleet Type. 74
Figure 32: Recommendation for Potential Certification Document Suite 75

LIST OF TABLES

Table 1: Mission Profile Summary of NASA RVLT Concept Vehicles 4
Table 2: Severity Classification Used in FMECA Worksheets. 23
Table 3: Applied Failure Rate (FR) used for FMECA and FTA. 25
Table 4: Tilt-Wing FMECA Severity Code I Summary 54
Table 5: Quad-Rotor FMECA Severity Code I Summary 55
Table 6: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FMECA Severity Code I Summary 56
Table 7: Lateral-Twin FMECA Severity Code I Summary 57
Table 8: Lift+Cruise FMECA Severity Code I Summary 58
Table 9: Tilt-Wing FTA Summary 60
Table 10: Quad-Rotor FTA Summary 60
Table 11: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FTA Summary 61
Table 12: Lateral-Twin FTA Summary 61
Table 13: Lift+Cruise FTA Summary 61
Table 14: Weight and Volume Estimates for Motors, Generators, Inverters, and Rectifiers. 65
Table 15: FMECA and FTA Summary. 66
Table 16: Sensitivity Study Summary – Failures per Flight Hour Against Time in OEI/OMI Avoid Region for Lateral-Twin Air-Vehicle. 68

Table A- 1: Tilt-Wing FHA A-1
Table A- 2: Quad-Rotor FHA A-4
Table A- 3: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FHA A-7
Table A- 4: Lateral-Twin FHA A-10
Table A- 5: Lift+Cruise FHA A-13

Table B- 1: Tilt-Wing FMECA Worksheet B-1
Table B- 2: Quad-Rotor FMECA Worksheet B-12
Table B- 3: Alternate Configuration –Quad-Rotor without Interconnecting Shafting FMECA Worksheet B-21
Table B- 4: Side-by-Side (Lateral-Twin) FMECA Worksheet B-29
Table B- 5: Lift+Cruise FMECA Worksheet B-34

LIST OF ACRONYMS

Acronym	Description
˚C	Degrees Celsius
˚F	Degrees Fahrenheit
AATE	Advanced Affordable Turbine Engine
AC	Alternating Current
AFDD	US Army Aeroflightdynamics Directorate
AGB	Accessory Gearbox
AGL	Above Ground Level
APU	Auxiliary Power Unit
ARP	Aerospace Recommended Practice
AS	Aerospace Standard
CGB	Collector Gearbox
CP	Compensating Provision
COTS	Commercial-Off-The-Shelf
DC	Direct Current
DE/HEP	Distributed Electric/Hybrid Electric Propulsion
DFC	Distributed Flight Controls
DGW	Design Gross Weight
DOD	Department of Defense
DP	Distributed Propulsion
DPFC	Distributed Propulsion and Flight Controls
DSR	Derive Safety Requirement
EASA	European Aviation Safety Agency
EIS	Entry into Service
ESC	Electronic Speed Controller
ETL	Effective Translation Lift
EU	European Union
FADEC	Full Authority Digital Electronic Control
FAR	Federal Aviation Regulation
FCC	Flight Control Computer
FCS	Flight Control System
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
FMI	Failure Mode Index
FR	Failure Rate

Acronym	Description
ft	Foot
ft-lbs	Foot-Pounds
ft^3	Cubic Foot
FTA	Fault Tree Analysis
GE	General Electric Company
GL-10	NASA VTOL DE/HEP Tilt-Wing Air Vehicle, “Greased Lightning”
GPS	Global Positioning System
HP	Horsepower
HV	High Voltage
ICAO	International Civil Aviation Organization
IGE	In Ground Effect
IMU	Inertial Measurement Unit
ITEP	Improved Turbine Engine Program
kPa	Kilopascals
kW	Kilowatts
lbs	Pounds (Force)
LCTR	Large Civil Tilt Rotor
LH	Left Hand
LIDAR	Light Detection and Ranging
LV	Low Voltage
m^3	Cubic Meter
MCP	Maximum Continuous Power
MGU	Motor/Generator Unit
MIL-STD	Military Standard
MIL-HDBK	Military Handbook
MRP	Maximum Rated Power
NASA	National Aeronautics and Space Administration
NDARC	NASA Design and Analysis of Rotorcraft
NPRD	Nonelectronic Parts Reliability Data
NTSB	National Transportation Safety Board
OEI	One Engine Inoperable
OGE	Out of Ground Effect
OMI	One Motor Inoperable
PMSM	Permanent Magnet Synchronous Motor
psi	Pounds per Square Inch
RADAR	Radio Detection and Ranging

Acronym	Description
RGB	Rotor Gearbox
RH	Right Hand
RPM	Rotations per Minute
RVLT	Revolutionary Vertical Lift Technology
RWB	Reliability Work Bench 12.1
SAE	Society of Automotive Engineers
SC	Special Condition
TAR	Time at Risk
TMS	Thermal Management System
UAM	Urban Air Mobility
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
VMS	Vehicle Management System
VTOL	Vertical Take-Off and Landing
X-57	NASA DE/HEP Prototype Air Vehicle, “Maxwell”
D_r	Outside Diameter of Rotor
D_s	Outside Diameter of Stator
k	Application Factor
L	Stack Length
p	Number of Pole Pairs
P	Power into Power Electronics (Inverters and Rectifiers)
Q	Peak Torque
V	Volume of Power Electronics (Inverters and Rectifiers)
V_r	Volume of Rotor
W	Weight
α	Failure Mode Ratio
β	Failure Mode Effect Probability
λ	Failure Rate
σ	Estimated Shear Strength Capability of Electric Motor

1 INTRODUCTION

The National Aeronautics and Space Administration (NASA) has advanced technology within the Vertical Take-Off and Landing (VTOL) 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) and Urban Air Mobility (UAM). Through programs such as GL-10, Greased Lightning, and X-57, Maxwell, NASA has helped pioneer DE/HEP air vehicle concepts and is continuing research in these topic areas through the Revolutionary Vertical Lift Technology (RVLT) Program. More recently, the RVLT Program developed a series of conceptual rotary wing airplanes 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-rotors, tandem-compound, and advancing blade concept vehicles. Through the noted trade studies, NASA found that the Large Civil Tilt Rotor (LCTR) concept showed the most promise for the specified mission of carrying 120 passengers for 1,200 nautical miles (ref. 1). 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 that were used in the current effort are intended to follow a similar research model, in which vehicle requirements and technology assumptions required to meet the stated mission objectives are used to drive system and sub-system research topics and open forum discussions. Four concept vehicles were defined and assessed in this research; all are intended to mature technologies required for similar aircraft that meet UAM mission objectives. Each concept vehicle was designed to be piloted, though future trade studies may include the impacts of incorporating various levels of autonomy. The focus of the research presented in this document addresses hazards and failure modes associated with the powertrain system of each of the RVLT concept vehicles.

1.1 Research Objectives

The primary objective of this research effort is to identify failure modes and hazards associated with the concept vehicles and to perform functional hazard analyses (FHA) and failure modes and effects criticality analyses (FMECA) for each. More specifically, this research aimed to and was successful in accomplishing the following objectives:

- To perform a conceptual design of the powertrain configuration for each configuration, in as much detail as is necessary to conduct subsequent elements of this research.
- To create functional block diagrams from each of the conceptual powertrain configurations in order to facilitate the FHA and FMECA.
- To identify potential hazards and perform a FHA for each configuration.
- For each configuration, identify and quantify the effects of the identified hazards, the severity and probability of their effects, their root cause and the likelihood of each cause.
- To discuss guidelines for development of reliability targets to compare the results contained herein against a benchmark and to enable the certification of similar UAM air-vehicle concepts.

1.2 Air-Vehicle Concept Configurations

Four RVLT air-vehicle concept configurations were used in this research effort, namely: a 15 passenger Tilt-Wing, a single-occupant Quad-Rotor, a six (6) occupant side-by-side, also referred to as a Lateral-Twin and a six (6) passenger Lift+Cruise concept vehicle that was included in the optional effort. A description of each of the RVLT concept vehicles is provided below.

1.3 Tilt-Wing Air Vehicle

The 15 passenger Tilt-Wing is shown in Figure 1 (ref. 2). It was designed to have a turboelectric powertrain, a 3,000 lbs payload, and a 400 nm range. The configuration includes four (4) rotors, two (2) rotors arranged on each tilting wing such that the wings are immersed in prop-wash. The Tilt-Wing under consideration was designed to have collective and single axis cyclic control at each rotor and interconnecting shafting between each rotor for emergency conditions. The installed power is provided by conventional aviation fuel powering a turboshaft engine, which supplies shaft-power to a generator. The generator provides electrical power to a battery network and four (4) 731 horsepower (HP) motors. The batteries are intended to be charged prior to flight and then recharged during the spec mission. The tip speed was set to 550 ft/sec in hover and 275 ft/sec in cruise for sizing runs; sizing runs resulted in 12.20 ft diameter rotors, or rotor shaft speeds of 861 RPM in hover and 431 RPM in cruise.

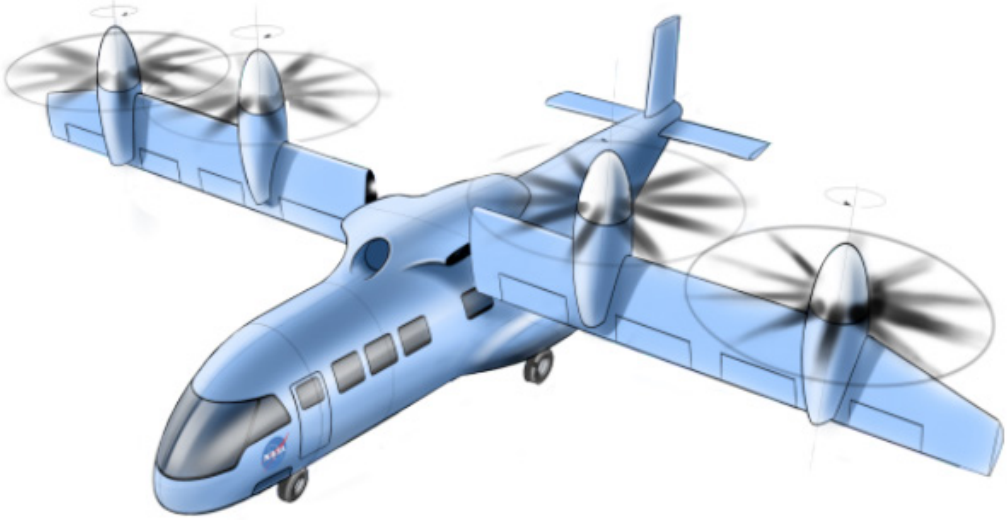


Figure 1: Tilt-Wing Air Vehicle

1.4 Quad-Rotor Air Vehicle

The single passenger Quad-Rotor is shown in Figure 2 (ref. 2). It was designed to have a fully electric powertrain, a 250 lbs 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 Quad-Rotor under consideration was designed to have, collective control at each rotor, articulated rotors, and interconnecting shafting for emergency conditions. A second powertrain configuration was also evaluated for the Quad-Rotor vehicle concept, one that removed the interconnecting shafting in favor of a direct-drive arrangement, still through a speed reducing gearbox for weight savings. The installed power is provided by a battery network that is charged prior to flight and which sends power to four (4) 21.6 HP motors. The tip speed was set to 450 ft/sec for sizing runs, resulting in rotor diameters of 12.62 ft or 681 RPM Rotor Shaft Speed.

Figure 2: Quad-Rotor Air Vehicle

1.5 Side-by-Side (Lateral-Twin) Description

The six (6) passenger side-by-side, or Lateral-Twin, configuration is presented in Figure 3 (ref. 2). This configuration was sized to accommodate a 1,200 lbs payload over a 200 nm range with a parallel hybrid propulsion system. The configuration features a single rotor attached to a pylon, outboard of the fuselage on each side of the aircraft. The 11.8 ft radius, four bladed rotors are indexed in order to enable intermeshing of the side-by-side rotors above the fuselage. The installed power is provided by a parallel hybrid-electric system that is primarily driven by two (2) 187 HP turboshaft engines, with power being augmented by a single 100 HP electric motor. The tip speed of each rotor is 550 ft/sec and the rotor diameter is 23.6 feet, resulting in a rotor speed of 444 RPM.

Figure 3: Side-by-Side (Lateral-Twin) Air Vehicle

1.6 Lift+Cruise Description

A six (6) passenger Lift+Cruise concept vehicle is presented in Figure 4 and features a fuselage configuration similar to that of the Lateral-Twin. The Lift+Cruise configuration is intended to represent a class of aircraft that feature distributed electric propulsion. In this effort, the Lift+Cruise configuration features eight (8), two-bladed rotors distributed across the wingspan, plus a single pusher propeller. Data are presented for this configuration performing an UAM mission with a 1,200 lbs payload over a 37.5 nm radius (ref. 3). The design gross weight (DGW) of the resulting Lift+Cruise air vehicle is 6,013 lbs. The powertrain features a single 3,376 HP turboshaft engine that drives an Alternating Current (AC) electric generator to provide power to the distributed electric motors at each rotor/propeller. The distinctive feature of this configuration is that the lifting rotors are stopped during cruise and aligned with the oncoming flow, effectively separating the sources of lift and propulsive force. The tip speed of each rotor is 546 ft/sec and the rotor diameter is 10.0 feet, resulting in a rotor speed of 1,043 RPM.

Figure 4: Lift+Cruise Air Vehicle Concept

1.7 Mission Profile

The RVLT Concept Vehicle payloads, range, type, propulsion system, and gross weight are summarized and listed in Table 1, for reference (ref. 2, 3). Note that the Lift+Cruise vehicle was sized for a shorter 37.5 nm mission radius.

Table 1: Mission Profile Summary of NASA RVLT Concept Vehicles

Passengers	Range	Type	Propulsion Architecture	Design Gross Weight	Reference
15	400 nm (8 x 50 nm)	Tilt-Wing	Turbo-electric	14,039 lbs	Ref. 2
1	50 nm	Quad-Rotor	All Electric	1,252 lbs	Ref. 2
6	200 nm (4 x 50 nm)	Lateral-Twin	Parallel Hybrid	3,950 lbs	Ref. 2
6	75 nm (2 x 37.5 nm)	Lift+Cruise	Turbo-Electric	6,013 lbs	Ref. 3

2 WORK SCOPE

In order to accomplish the noted research objectives conceptual powertrain configurations were developed with enough detail to support the FHA and FMECA. Functional Block Diagrams were created in order to support FHA and FMECA development and a Fault Tree Analysis (FTA) was performed for each vehicle configuration to examine the dependencies one system may have on another.

2.1 Conceptual Powertrain Configurations Scope

A conceptual powertrain configuration was developed for each of the four (4) RVLT air-vehicle concept configurations used in this research effort. The complexity and functional requirements of DE/HEP systems required that each RVLT air-vehicle conceptual powertrain configuration included a rotating system, a flight control system, and a thermal management system.

The rotating system was defined as the components or sub-assemblies within the powertrain that provided rotary motion to the rotor system. This included generators, motors, gearboxes, and interconnecting shafts. An initial trade study was performed to optimize the weight of the system within current state-of-the-art technology. Additional weight savings may be observed by further increasing reduction ratios, but additional technology development is recommended in order to increase the reduction ratio between the motor and rotors further. Rotating system schematics consisted of stick diagrams identifying gear ratios, mechanical interconnections, and rotational speeds at each junction. Each schematic was intended to provide enough detail to define the interconnections between major components; the input powers and speeds, output powers and speeds, intermediate or emergency interconnecting shafts, and accessories required for thermal management and primary airplane functions were conceptualized.

The flight control system was defined as the components or sub-assemblies within the powertrain that send/receive control signals to the primary propulsion system. Typically, the flight control system will send/receive signals from primary flight controls, pilot inputs, and the environment, among others. However, the research objectives for this study focused on the powertrain configurations and the reliability/safety, thereof. The typical flight control system functions were assumed to be unrelated to the current work because the reliability/safety of the typical functions of the flight control system were assumed to be unchanged when adding in the functions closely coupled to the powertrain, itself. The amount of coupling between a flight control computer and the propulsion system varies depending on architectural decisions related to flight control architectures or the location of feedback and control loops that command speed or power inputs to a propulsion system. In variable pitch, constant speed flight control systems, the propulsion system and flight control system are loosely coupled, but as functions are added to the propulsion system, as in the case of variable speed, constant pitch flight control systems, the coupling between the two (2) systems becomes tighter as they share tasks to complete a specified subset of functions. For this study, however, the flight control computing system reliability was considered to be a pass-through value in the reliability and safety assessment because government regulations and industry standards are available to guide the design of safe flight control computing systems. In practice, dual, triplex, or quad-computing architectures may be adopted in order to make the flight control computing system acceptably safe for the specified mission.

The thermal management system was defined as the components or sub-assemblies within the powertrain that are (1) required to regulate the temperature of powertrain components and (2) not associated with another systems integral lubrication or cooling system framework. The engine,

engine bay, generator, and rectifier (as applicable), the battery network, Electronic Speed Controllers (ESC), motors, and gearboxes were assumed to require thermal management system provisions. However, the engine and gearbox cooling have historically been performed by their own, independent cooling and lubrication systems and engine bay cooling is generally different from engine to engine, even within the same power class. For this activity the components that were cooled by the thermal management system included rectifiers, battery networks, and ESC's. Generators and motors were assumed to be cooled by a shared lubrication system with the gearbox due to their proximity to an already existing cooling/lubrication system.

2.2 Functional Hazard Assessment Scope

The FHA was executed per Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761. The scope of the FHA was to encompass the propulsion system for each air vehicle concept under study. A separate FHA was provided for each concept vehicle. The Quad-Rotor was analyzed for two (2) configurations. The baseline Quad-Rotor was assessed with the noted interconnecting shafts and an alternate configuration was assessed with the interconnecting shafts removed, similar to a direct-drive Quad-Rotor.

The format was a combination of aircraft level and system level FHA, as applicable. Systems aligned with, but not directly tied into providing propulsion for the air vehicle (flight controls, computer functions located in propulsion LRUs, but not directly related to propulsion) were addressed to the extent that they affect the availability of propulsion.

Typical items feeding into the loss of propulsion were individual and dual motor failures, electrical (battery, low and high power supply) failures, gearbox failures, cooling failures (both liquid cooling and forced air as applicable), electrical control LRU failures and generator failures.

Flight conditions were assessed from the perspective of the One Engine Inoperable (OEI) or One Motor Inoperable (OMI) avoid region. This defines the time at risk (TAR) where a single propulsion unit failure will result in loss of lift necessary to continue the flight. The air vehicles are uniformly assumed to spend 20% of their flight time within the OEI/OMI avoid region, in which a single loss of a propulsion unit's ability to provide torque to a rotor will result in power required exceeding power available and a hard landing sufficient to cause Critical or Severe damage to the aircraft or occupants.

For the hybrid-electric propulsion vehicle concepts, the FHA considered the loss of the turboshaft engine driving the main power AC Generator as a complete loss of propulsion. The battery only flight capabilities of the vehicles were addressed as part of the FTA.

Loss of control will be captured in the FHA with relevant effects being related to failures of the propulsion system. Since the topic of the trade study is uniquely looking at the architecture of hybrid propulsion systems, air vehicle control systems (cyclic actuators, flaperons, elevators, etc.) will not be evaluated for inducing loss of control in the FHA. Loss of control due to loss of propulsion or inability to provide thrust/lift will be evaluated and further explored in the FTA.

2.3 FMECA Scope

Functional block diagrams were created for each of the concept vehicles based on the conceptual powertrain configurations. Functions were defined at the equipment level to facilitate the development of meaningful functional failures. Each function was reviewed and potential failure modes were postulated for each function and assigned failure mode identification codes (FMECA ID

Code). The failure effects were based on assessment of each air-vehicle, as derived from the NASA technical papers (ref. 2, 3)

Failure rates can vary significantly based on detailed design, application, and use. Reliability is designed into equipment based on requirements, which would be developed based on the consequence, severity, or criticality of the failure effect, among others. Similar equipment to that of the conceptual equipment defined for this study were used to define failure rates.

Current, state-of-the-art components designed for specific DE/HEP airplane applications may be higher than the historical values used herein. However, these components likely take years to develop and the reliability of new components must be validated initially through analysis before entering a certification test program in order to validate component reliability in test. Once the component is fielded, then a tracking a records keeping process must be adopted to determine if reliability through the components life is meeting expectations or if earlier retirement lives or inspections intervals must be adopted.

2.4 FTA Scope

FTA is a top-down analysis meant to capture the propulsion components and to examine their interrelationships and allow the definition of cut-sets to show areas where system improvements would improve the top-level number. The roll-up of the propulsion FTAs are done so that loss of propulsion may also include loss of control, depending on air vehicle configuration. The FTA is meant to document a Catastrophic or Severe outcome top level, though lesser severity hazards may become evident due to FTA structure and execution.

Overall, the propulsion specific systems and their failures to provide propulsion function are what roll-up to the top-level hazard. The unique all-electric or hybrid-electric aspects of the propulsion system, the electronics that control the motor, the motor itself, batteries, thermal management system, and charging system were captured in the FTA. Systems that may be shared between propulsion and flight controls (e.g., rotor RPM and collective pitch) are examined only in their contribution to the top level loss of propulsion hazard. Loss of multiple propulsors may cause control problems that are considered a part of the loss of propulsion top level hazard.

The top level hazards defined from the propulsion system FHA were used to inform the top level of the fault tree. The FTA was done to a level of detail sufficient to show architectural impacts to the top-level hazard. The FTA may capture system effects that roll up to higher losses of functions captured in the FHA.

FTA was accomplished on the following configurations:

1. Tilt-Wing with hybrid electric propulsion in which a turboshaft engine charges batteries and provides electric motors with electrical power.
2. Quad-Rotor with electric propulsion with cross-shafting so that individual propulsion fails, with the exceptions of the local gearbox, can be compensated for by the remaining propulsors. Individual propulsor fails can conditionally roll up to the top level hazard if occurring in the OEI avoid region of low-speed, low-altitude flight.
3. Quad-Rotor with electric propulsion without cross-shafting so that if an individual propulsor fails, thrust must be reduced so that a measure of control can be maintained. It is assumed that a loss of motor/propulsor in this configuration would likely result in a Catastrophic or Severe outcome.

4. Lateral-Twin with turboshaft power and with electric motor to supplement for takeoff and landing. It is assumed that the electric propulsion is necessary to ensure adequate power during the hover. Additionally, due to the rotor overlap, the collector gearbox and interconnecting shafts are considered flight critical to avoid rotor to rotor contact and subsequent catastrophic outcome.
5. Lift+Cruise with hybrid electric propulsion in which a turboshaft engine charges batteries and provides electric motors with electrical power. It is assumed that one propulsion unit failure is not flight critical; however, the pusher propeller is used to aid in pitch control of the aircraft.

3 BACKGROUND

3.1 Literature Review

There exists a significant number of specification documents that provide guidelines for the design of various systems and sub-components on the aircraft. This sections presents a summarized description of a selection of documents which are pertinent to vertical lift vehicles with potential distributed propulsion/flight control designs.

The European Union's (EU) civil aviation safety organization is the European Aviation Safety Agency (EASA). Concurrent with the execution of this work scope, EASA published a draft of a proposed Special Condition (SC) for small category VTOL aircraft (SC-VTOL-01) with input from industry and academia. This document is largely aimed at providing regulatory guidelines for the design of distributed lift/thrust unit vehicles with the assumption that autorotation and/or gliding is not possible. The document proposes characterizing vehicle reliability requirements to be a function of operating area (congested/non-congested) and number of on-board passengers (less than 5). These guidelines as presented are meant for vehicles with a gross weight of less than 4,400 lbs regardless of the autonomous capabilities of the vehicle.

SAE has published numerous documents pertaining to providing guidelines for recommended practice of the design of aircraft. ARP94910, as such, provides reliability metric guidelines for flight control systems (FCS) of military Unmanned Aerial Vehicles (UAV). The document presents a scheme to characterize the FCS reliability based on two notional axes; Unmanned Aerial System (UAS) group and Operating Area. The UAS grouping is further discretized by vehicle weight, operational altitudes and speed. The operating area coverage ranges from restricted all the way to uncontrolled airspace (using International Civil Aviation Organization (ICAO) definitions of airspace). The guidelines provided are intended for rotorcraft and fixed wing UAV's alike.

SAE also have published aircraft design standard documents, including AS94900. This document provides reliability requirement design thresholds for flight control systems for military manned vehicles. Discretization of these thresholds is based on aircraft weight and maneuverability for fixed wing aircraft, whereas, for rotorcraft only a single threshold is provided.

The United States Department of Defense publishes and maintains a handbook (MIL-HDBK-516C) that provides guidance to achieve airworthiness certification for military aircraft. The contents of this documents applied to manned and unmanned fixed and rotary wing aircraft. The document is a resource for guidelines for sub-system reliability targets which are characterized differently based on the sub-system level details.

Aside from the above mentioned SAE documents, ARP4761 and ARP4754 cover the recommended practices with regards to processes and methods to conduct aircraft safety assessments and the overall aircraft development process respectively. These documents are intended to apply to both manned and unmanned fixed and rotary wing aircraft.

The Nonelectronic Parts Reliability Data (NPRD) document provides a very useful historical database of fielded parts reliability data. This document is a great resource to be used for safety and reliability assessment of a new aircraft design.

In the United States the civil aircraft airworthiness requirements are provided by Federal Aviation Regulations (FAR) parts 23, 25, 27 and 29. Parts 23 and 27 apply to normal category (general aviation) fixed wing and rotorcraft respectively. Parts 25 and 29 apply to transport category fixed wing and rotorcraft respectively. While the parts themselves do not provide reliability metric design requirements they are provided in associated advisory circulars for part 23, 25 and 29 aircraft

(AC23.1309, AC25.1309 and AC29.1309). The advisory circular associated with part 27 aircraft (normal category rotorcraft, AC27.1309) does not explicitly provide quantitative reliability guidelines for the aircraft level but instead references other documents as sources for guidelines (MIL-HDBK-217, manufacture reports and laboratory part life tests).

3.2 Nomenclature & Taxonomy

In order to facilitate the discussion of the coverage and gaps with regards to the design metrics for reliability it is important to provide a foundation for the organization of the various types of aircraft. It is proposed to organize the various types of aircraft as presented in Figure 5. The organization is based on two independent axes: Number of powerplants and Number of propulsors. The term powerplants refers to an onboard device which converts stored energy (fossil fuels, electrical energy etc.) to mechanical power output (torque and rotational speed), e.g. turbine engines, turboshaft engines, electric brushless motors etc. Propulsors on the other hand refer to aerodynamic force and moment generating devices on board the vehicles (e.g. rotors and propellers). Each of these axes is discretized into two levels; 1-3 and 3+ powerplants or propulsors. Note the intentionally introduced overlap in the levels; this has been done to recognize the non-discrete nature of aircraft design decomposition.

As noted in the table, aircraft with 1-3 powerplants and propulsors are categorized as conventional. These type of aircraft generally have good coverage from existing published design documents in terms of reliability metrics. These aircraft generally include a drive system to transmit and provide load sharing of the mechanical power (torque and rotational speed) between the on-board powerplants and propulsors. Typically, variable pitch (collective and cyclic) control schemes are implemented for these type of aircraft. Examples of these type of aircraft include but are not limited to, H-47, V-22, AH-64, H-6, H-60, R22, R44, S-76, and MH-139. Note that this category of vehicles can include electric powerplants.

Aircraft with a combination of either 3+ powerplants/1-3 propulsors or 1-3 powerplants/3+ propulsors are referenced as Distributed Propulsion (DP) or Distributed Flight Control (DFC) vehicles respectively. These types of aircraft typically have load sharing drive systems to transmit torque between the powerplants and propulsors. The configurations can have electric motors and/or turbines as their powerplants whereas the propulsors are typically controlled via a variable pitch scheme. Note that the variable pitch scheme can be collective only for the case of distributed flight control configurations. It may be possible to extend reliability metric guidelines presented for the conventional aircraft to this aircraft configuration type. Examples include the lateral twin configuration presented in this report (2 turbine, 1 electric motor powerplant with 2 rotors with variable pitch control).

Aircraft designs with 3+ powerplants and propulsors are categorized as distributed propulsion and flight control configurations (DPFC). These type of aircrafts typically involve the capability of direct torque transmission between the powerplants and the propulsors. Furthermore, variable speed control schemes are as likely to be used on these platforms as variable pitch control schemes. These type of configurations would be likely be designed to integrate either an all-electric or a hybrid electric propulsion system; deemed Distributed Electric/Hybrid Electric Propulsion (DE/HEP). There is little to no coverage of these type of vehicles with regards to reliability metric guidelines in existing publicly available literature. Examples this type of configuration include the Tilt-wing, Lift+Cruise and the Quad-rotor configurations discussed in this report.

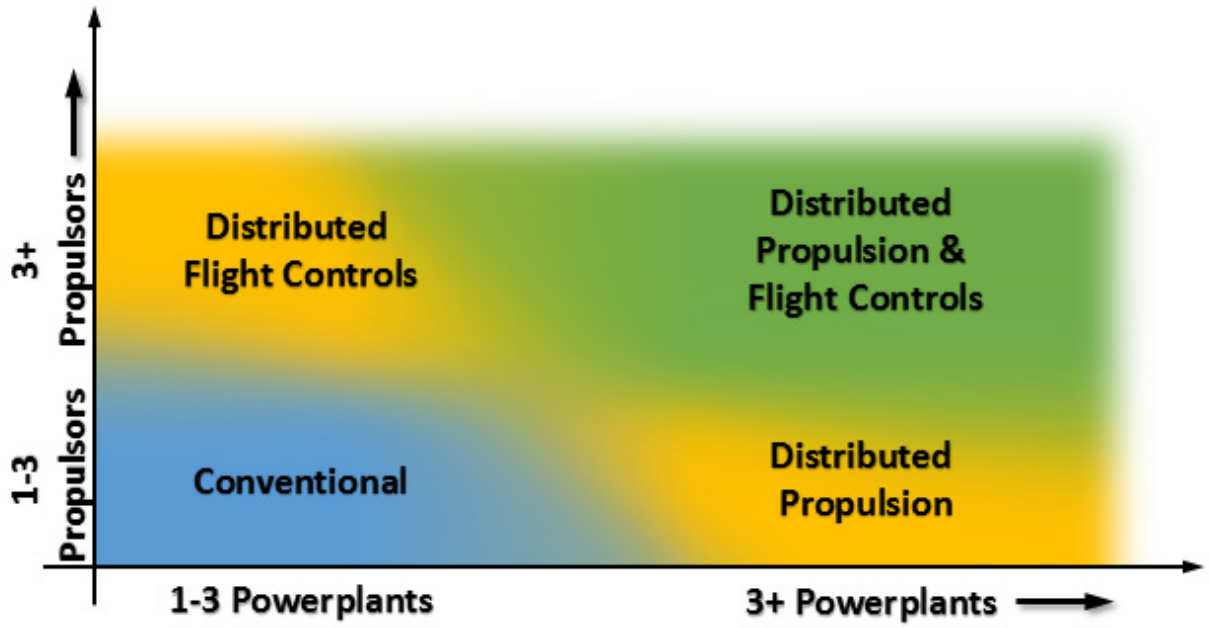


Figure 5: Proposed Vehicle Configuration Taxonomy.

Traditional aircraft platform system have a specific distinction between flight control and propulsion systems which is reflected in publicized guidance and specification documents. DPFC systems, on the other hand, have a much tighter coupling of flight control and propulsion functions. Current specification and guideline documents don't reconcile flight control/propulsion functional allocation for this aircraft propulsion/platform type. For example for variable speed flight control scheme systems reliability metric specifications tend to be applied to both flight controls and propulsion systems leading to potential conflict, overdesign and/or infeasible configurations. A discussion of this tighter coupling is detailed in section 5 of this report.

3.3 Functional Overlap of Distributed Propulsion and Distributed Flight Controls

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 (1) failure provides an opportunity for the pilot to land the airplane safely. DE/HEP concepts may be segregated into to 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 6 uses some example airplane functions to depict the overlap of typical variable pitch and variable speed DE/HEP 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 safety in failure mode conditions.

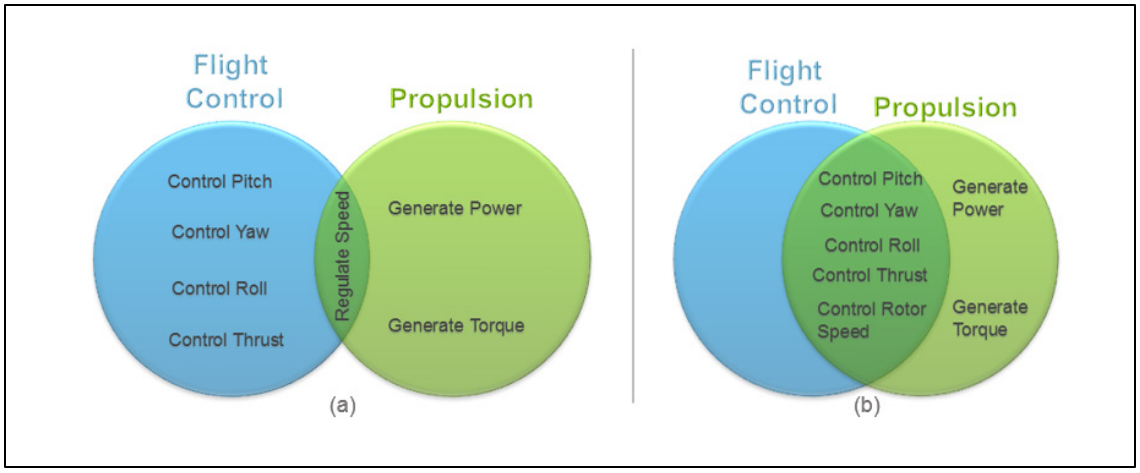


Figure 6: Flight Control and Propulsion Systems' Functional Overlap for (a) Typical Variable Pitch DE/HEP Systems and (b) Typical Variable Speed DE/HEP Systems.

Airplane functions, and thereby functional hazards, associated with DE/HEP 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.

3.4 Vehicle Level Reliability Metrics

Current FAR parts 23, 27, 25 and 29 provide guidance for reliability metrics for airworthiness of manned fixed and rotary wing (normal and transport category) aircraft. These aircraft are labeled "conventional" using the nomenclature described earlier (Figure 5). Depending on the specific aircraft configuration these regulations can be extended for manned DP or DFC scheme aircraft. For example, the EASA proposed special condition (SC-VTOL-01) is an attempt to cover distributed flight control scheme vehicles and is an adaptation of the FAR part 23 as is applicable.

Note that these documents do not provide coverage of guidelines of unmanned vehicles. Manned aircraft in this context are defined as vehicles with onboard crew stations and as a corollary unmanned aircraft are defined as ones that have no onboard crew station. Unmanned aircraft can be remotely piloted or operated. Manned aircraft for existing FAR guidance implies on-board crew is providing piloting functions and is not only limited to operator functions. While coverage of unmanned systems is important and requires the attentions of the various pertinent stakeholders, however, given the current surge in DE/HEP system designs there is a more pressing need for reliability metric guidelines for DE/HEP manned systems.

The existing regulations also do not provide coverage of any DPFC systems and by extension DE/HEP aircraft configurations. The FAA, currently, has not published any official guidelines that cover DPFC aircraft configurations explicitly. The Quad-rotor and the Lateral-Twin configurations discussed in this report are the only two configurations that would be covered under the EASA special condition guidelines. The other configurations would have no direct civil aviation reliability guideline specification available to apply. Note that the MIL-HDBK-516 document does provide metrics for military aircraft of similar size but with no distinction provided for DE/HEP configurations.

A gap exists in current publicly available documentation on design guidelines/specification for reliability metrics of distributed electric/hybrid-electric propulsion (DE/HEP) aircraft. This document pertains primarily to VTOL concepts and as such the following discussion is with regards to rotary wing vehicles only.

ARP94910 is a military UAS flight control system design document published and maintained by SAE. This document provides a suitable example to draw upon for developing DE/HEP system reliability metrics. To facilitate discussion consider the following configuration: Light UAS, 50 lbs. with a DE/HEP configuration operating around Class B/C airspace with an operating altitude limit 3500 above ground level (AGL) and an operating cruise speed of no greater than 30 knots. This aircraft under ARP94910 would be required to ensure that VMS failures that causes aircraft loss of control to occur no more often 10^{-6} per flight hour. As a rule of thumb this would result in an aircraft level equivalent catastrophic failure rate of 10^{-5} per flight hour. If this same aircraft were to be evaluated using EASA rules, assuming that the quantitative requirements are applicable, the required reliability metric for aircraft catastrophic failure rate is 10^{-9} per flight hour. The apparent difference in the reliability metric specified by both of these documents for the same aircraft can also be seen even if an order of magnitude correction was added to the ARP94910 value to account for civil aircraft considerations. The EASA special condition document, too broadly applies the most stringent recommendation across a wide variety of DPFC aircraft types operating in congested environments. If adopted as a regulation, this proposed special condition may potentially limit the economic growth of the relatively new sector of DE/HEP configurations. In conjunction with aircraft airworthiness definitions it is important to consider the regulations as they apply to operational use as well. FAA part 121 and 135 are the prime applicable regulation in the context of the aircraft configurations discussed in this report. Part 121 covers air carrier configurations which would typically use FAR 25 and 29 aircraft types. This regulation is developed in consideration with a scheduled service operational model. Part 135 covers on-demand commuter aircraft which can utilize FAR 23, 25, 27 or 29 aircraft types. This regulation is developed in consideration of on-demand, lower frequency and relatively short range service model (as compared to Part 121). Generally, the UAM concept has identified Part 135 regulation as the closest fit regulation to their proposed operational model (ref. 4). The paper further specifies that UAM vehicles will be designed to exceed the Part 135 operational catastrophic failure rate by four times. A gap in coverage of the Part 135 document exists, as its development is not consistent with the high frequency short flight operational model that coincides with overarching, UAM objectives. Furthermore, part 135 does not cover non-traditional airport traffic which is the primary model for UAM, i.e. high frequency operation in congested areas. In particular, the white paper argues that this model is required for economic viability.

It is recommended that additional guidance be developed to cover manned DE/HEP aircraft configuration types with regards to airworthiness, reliability and safety. Furthermore, additional consideration should also be given to operational requirements for the emerging high frequency, short haul, on-demand air-taxis service models aimed at densely populated metropolitan areas. This consideration, is recommended, to not be limited to simple extension of existing FAR's to DE/HEP configurations due to the tighter coupling of propulsion and flight control functions.

4 METHODOLOGY AND COMMON ASSUMPTIONS

In order to evaluate the reliability and safety of the NASA RVLT Concept Vehicles, improved powertrain configuration schematics needed to be developed in order to illustrate the connectivity between sub-systems and the major components of each sub-system. A process was developed in which "stick" diagrams could be utilized to develop enough detail to facilitate development of functional block diagrams, which could then, in turn, be used to populate the FHA, FMECA, and FTA. An example of a "stick" diagram is shown in Figure 7.

Rotors, low voltage batteries, flight control computers, wires, and other components that are typically found in helicopters that do not facilitate the operation of the powertrain were left out of the functional block diagrams and FMECA's because they were considered to be pass-through reliability values in the fault tree and the criticality number of these would be high enough in the FMECA that they would affect the Severity I criticality value. These components have been being designed for decades in an acceptably safe manner and it is expected that they will continue to be designed in such a manner, even though electrical energy storage is being utilized. For example, the low voltage batteries can be wired in a fail-safe and switched architecture with minimal weight penalty using decade's old techniques. For the finalized air-vehicle entering preliminary or critical design reviews, the rotor system and low

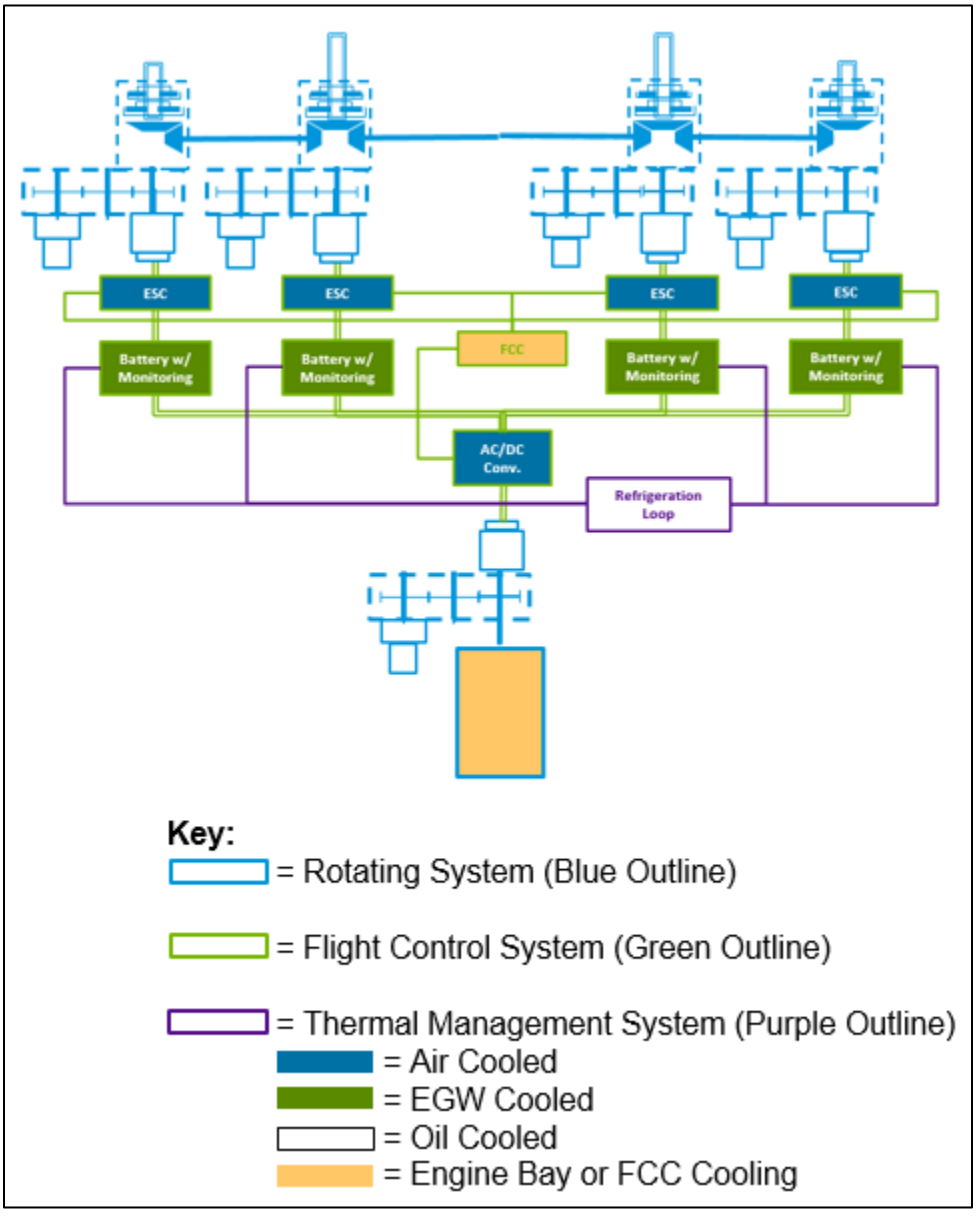


Figure 7: Example Stick Diagram with Rotating, Flight Control, and Thermal Management Systems overlaid.

voltage batteries would be included, but this study focused on the novel distributed electric propulsion architectures.

Items that were included in the functional block diagrams, FMECA's, and fault trees were critical in performing the safety assessment of each vehicle. For example, the gearboxes depicted in the "stick" diagrams have accepted reliability and are generally developed in safe manners, but the function of providing mechanical interconnection between rotors was deemed critical to completing the reliability and safety analysis of the NASA RVLT Concept Vehicles.

The process developed to analyze the safety of the NASA RVLT Concept Vehicles used the "stick" diagrams to develop functional block diagrams, in which ID codes and primary functions were developed. Sub-tier functions and hazards were then postulated in the FHA, in which end effects and severities were assigned to each functional failure. The data generated in the FHA was then passed into the FMECA, where additional sub-tier functions, reliability values, end effects, next higher effects, and other critical information sets were populated. The FTA then compiled information from the functional block diagrams, FHA, and FMECA to build the fault tree architecture and populate the failure rates for a given failure mode and next higher effect. The process flow is depicted in Figure 8.

As can be seen in Figure 8, the amount of data used to facilitate each analysis step steadily increases when moving through the reliability/safety assessment process. Historical data or analysis was used where appropriate; however, in some cases, assumptions had to be made that should be turned into derived requirements, if the airplanes continue along in their development. Assumptions needed to be developed because of the conceptual nature of the airplanes under scrutiny. Configuration, FHA, FMECA, and FTA assumptions were documented so that derived requirements and verification may take place as the airplanes mature.

4.1 Configuration Assumptions

As is common with the aircraft conceptual design process, design assumptions were defined and documented in order to enable the analysis described in this document. Some design assumptions were common across multiple vehicle configurations, while others were configuration specific. Design assumptions were used to address and document the state of technology used in each configuration and the scope covered in each of the configurations.

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 applicable and relevant information. 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.

Hazards for this study will focus on in-flight mission reliability, assume flight over populated, metropolitan areas, and assume that flight controls and neighboring systems unaffected by the change to an electrified propulsion system meet reliability requirements. Ground based hazards should be assessed as the systems mature. Examples of such hazards include overheating during charging, arcing, and fuel leaks. The UAM mission is intended to be flown over major cities to reduce roadway congestion and travel time (ref. 4); therefore, the UAM aircraft assessed here will be assessed against the metric that they operate over populated, metropolitan areas (ref. 4).

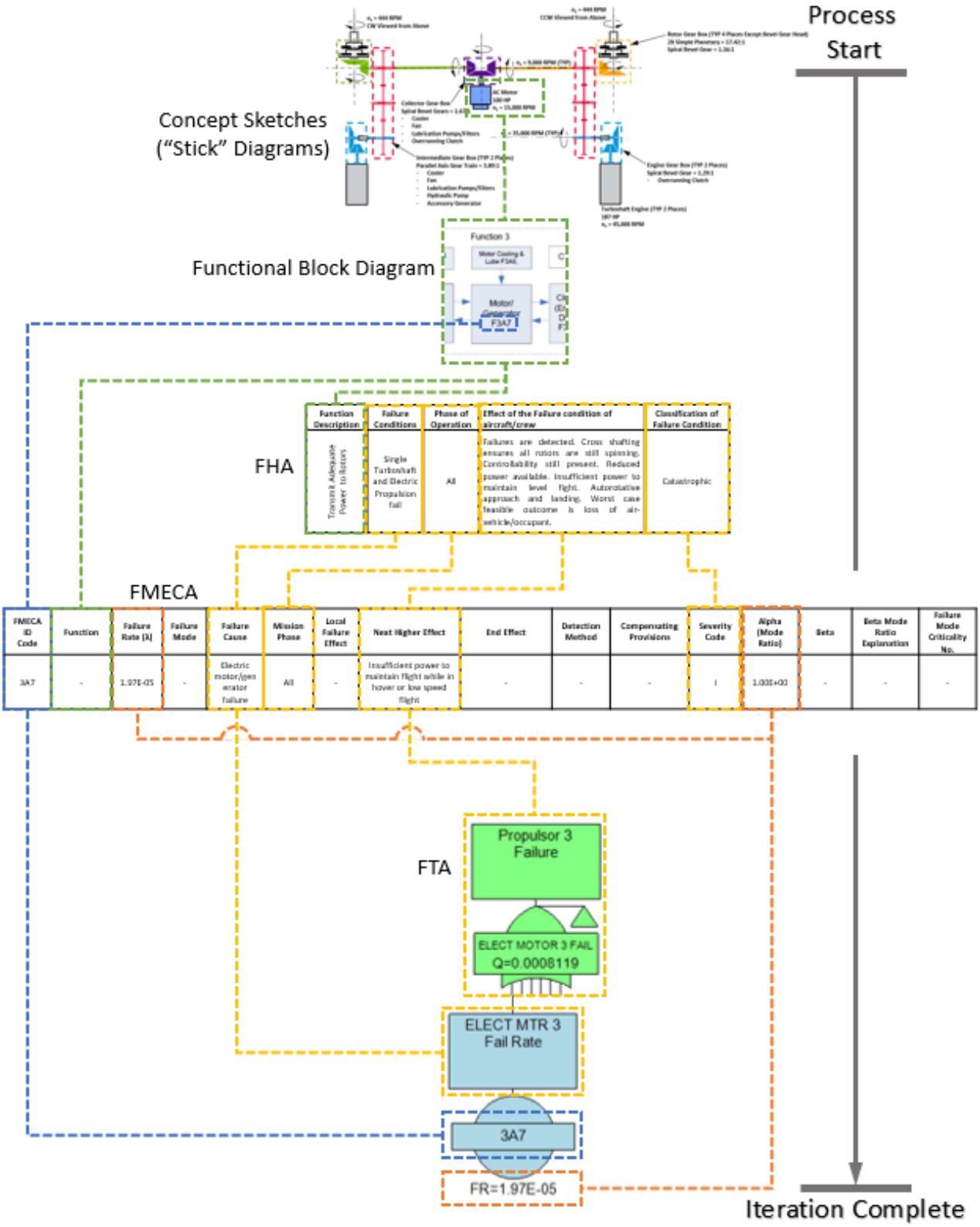


Figure 8: Process Flow Used to Assess Reliability and Safety of NASA HA/FMECA

Flight controls, environmental systems, or other sub-systems that are not directly impacted by the change from conventional propulsion to all-electric or hybrid-electric propulsion 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 and power-off, wing-borne flight are 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 Quad-Rotor without cross-shafting, for instance, may be theoretically able to autorotate, but in practice controlling the speed of all four (4) rotors independently may prove difficult.

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˚F to 113˚F (15 degrees Celsius (˚C) to 45˚C) degree for batteries, and a maximum box temperature for motors and gearboxes of 250˚F.

In order to manage risk and to develop inherently safe architectures, some components were intentionally physically or functionally isolated from others. The Flight Control Computer (FCC) was isolated from the motors by integrating motor control authority into each motor's individual 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 FCC signal is lost. Specifically, for this exercise, the ESC's will revert to their last recorded speed.

The rotors and cross shafting were isolated from each electric motor via emergency disconnect system in case of an ESC or motor failure. In some cases the emergency disconnect system takes the form of an overrunning clutch and in other cases takes the form of a friction disc clutch. Using the term "emergency disconnect system" was intended to provide design freedom while still maintaining the function of an overrunning clutch or friction disc clutch. 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 common reduction ratio rotor gearbox (RGB) was used for both the Quad-Rotor and Tilt-Wing RGB. The common reduction ratio was 17.42:1, which is a comfortable reduction ratio for a two (2) stage planetary system. Using the noted reduction ratio, the Quad-Rotor would utilize an 11,683 RPM Motor and the Tilt-Wing would utilize a 14,998 RPM motor, nominally. The torque capacity of the RGBs would be scaled from the 58 ft-lbs final stage design torque of the Quad-Rotor to the 1,920 ft-lbs final stage design torque of the Tilt-Wing. The baseline vehicles assumed 8,000 RPM motor output shaft speeds.

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 for weight buildups in NASA Design and Analysis of Rotorcraft (NDARC) (ref. 5). A weight trend was developed for the Tilt-Wing, assuming a Rotor Speed of 861 RPM and Motor of 731 HP Maximum Continuous Power (MCP) and 1,462 HP Maximum Rated Power (MRP). The weight trend was developed for a single Prop-Rotor, so a Main Rotor value of "1" was used for this weight trend. Figure 9 shows a 46 lbs weight savings per rotor by utilizing a 14,998 RPM Motor, resulting in nearly 200 lbs total weight savings

in the Propulsion System. A similar weight trend can be developed for the Quad-Rotor which will showing a notable weight savings over the baseline, 8,000 RPM Motor.

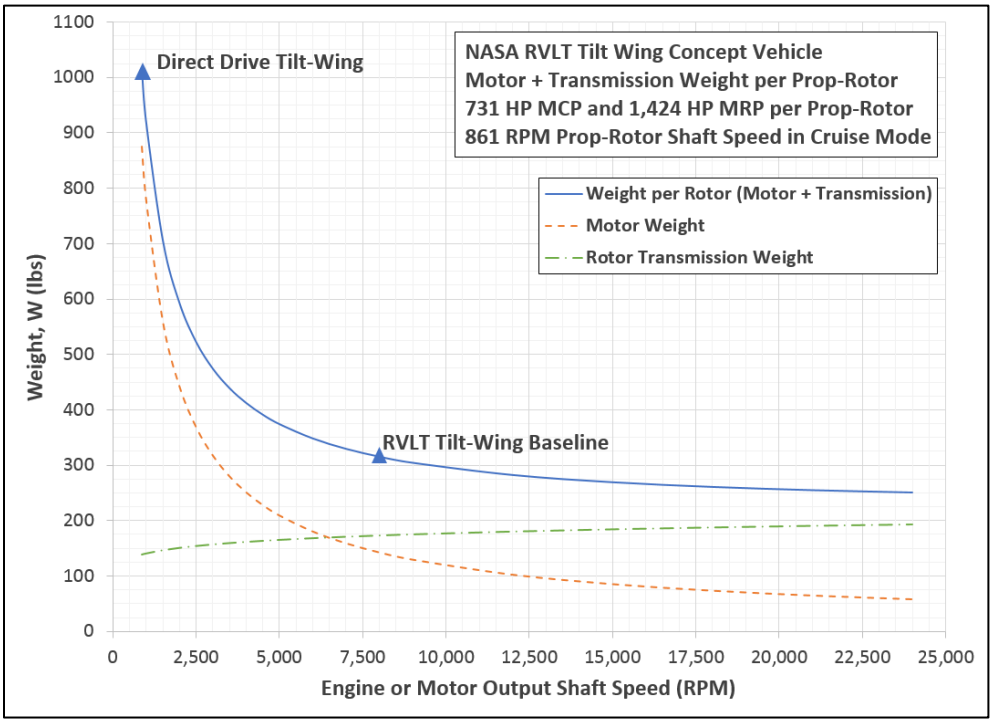


Figure 9: Weight Trend for one (1) Prop-Rotor Propulsion System of NASA RVLT Tilt-Wing Concept Vehicle.

The additional reduction ratio applied to the RGB was intended to reduce empty weight. Weight savings using the NDARC weights buildup estimates ~200 lbs saved in the drive system for the Tilt-Wing, which would result in ~500 lbs empty weight savings due to the iteration loop of typical VTOL airplane sizing (ref. 6). It is expected that fail-safe ESC's are required to meet projected reliability targets, which will add weight to the propulsion system; the added weight of the fail-safe ESC's could be offset by the weight savings of the gearboxes and motors for a weight neutral impact. Aircraft center of gravity was not considered, but Boeing recommends that future work includes a mass balance record of all airplane sub-systems to assess cg location.

4.1.1 Tilt-Wing Design Assumptions

It was assumed that the aircraft starter system, whether electric or conventional auxiliary power unit (APU) starting, is isolated from the primary propulsion system. Isolating the starting system significantly reduces the probability of failures of the lower-reliability starting system to generate failures in the primary propulsion system. The aircraft starter system was isolated from the primary propulsion system so that faults related to the starter system did not propagate into the propulsion system. The term "isolation" means, in this context, that a failure in the starter system will not cause a category I or II failure in the propulsion system, but the starter system and the propulsion system will still be coupled together as required for the starter system to perform its function.

Battery arrays were assumed to be physically isolated from one-another within the battery network of the Tilt-Wing configuration. The battery arrays were conceptualized to be placed near each electric motor and ESC; this assumption complicates battery thermal management and may require independent cooling loops for each battery array.

Hazards and FTA will focus on hover (rotary-wing-borne flight) and level-flight cruise (fixed-wing-borne flight) mission segments, considering percent time spent in each segment. Conversion/transition and climb/descent segments were not included in this analysis.

Hazards and FTA will assume the fuel system meets reliability requirements regardless of propulsion system for the Tilt-Wing. Both conventional (turboshaft engine burning fossil fuels turning rotors) and series-hybrid electric (turboshaft engine burning fossil fuels turning generator) will require effectively the same fuel system.

4.1.2 Quad-Rotor Design Assumptions

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.

4.1.3 Lateral-Twin Design Assumptions

It was assumed that the aircraft starter system, whether electric or conventional APU starting, is isolated from the primary propulsion system. Isolating the starting system significantly reduces the probability of failures of the lower-reliability starting system to generate failures in the primary propulsion system. The aircraft starter system was isolated from the primary propulsion system so that faults related to the starter system did not propagate into the propulsion system. The term "isolation" means, in this context, that a failure in the starter system will not cause a category I or II failure in the propulsion system, but the starter system and the propulsion system will still be coupled together as required for the starter system to perform its function.

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

Hazards and FTA will assume the fuel system meets reliability requirements irrespective of propulsion system for the Lateral-Twin. Both conventional (turboshaft engine burning fossil fuels turning rotors) and series-hybrid electric (turboshaft engine burning fossil fuels turning generator) will require effectively the same fuel system.

4.1.4 Lift+Cruise Design Assumptions

It was assumed that the aircraft starter system, whether electric or conventional APU starting, is isolated from the primary propulsion system. Isolating the starting system significantly reduces the probability of failures of the lower-reliability starting system to generate failures in the primary propulsion system.

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

Hazards and FTA will assume the fuel system meets reliability requirements irrespective of propulsion system for Lateral-Twin. Both conventional (turboshaft engine burning fossil fuels turning rotors) and series-hybrid electric (turboshaft engine burning fossil fuels turning generator) will require effectively the same fuel system.

4.2 Functional Hazard Assessment Assumptions

Hazards for this study will focus on in-flight mission reliability, assume flight over populated, metropolitan areas, and also assume that flight controls and adjacent systems unaffected by the change to an electrified propulsion system meet reliability requirements. Ground based hazards are not considered as part of the initial FHA. Examples of such hazards includes overheating during charging, arcing, and fuel leaks. The UAM mission is intended to be flown over major cities to reduce congestion and travel time (ref. 4); therefore, the UAM aircraft assessed here will be assessed against the metric that they are operate over populated, metropolitan areas.

Flight controls, environmental systems, or other sub-systems that are unaffected by the change from conventional propulsion to all-electric or hybrid-electric propulsion are not generally assessed in the FHA because it is assumed that both design authorities and regulating agencies are able to adequately assess the safety and reliability of these systems. Those systems will only be assessed to the extent that they uniquely interface into the propulsion system, especially in light of the FTA assessment feeding back potential common-cause failures as contributing to loss of function in the FHA

Hazards for this study are limited to power-on mission segments. Autorotation and power-off, wing-borne flight are not examined in this FHA. Autorotation and power-off flight will be considered as states the air vehicle reaches after the onset of the loss of examined function. The aircraft may be able to enter autorotation or power-off flight in the phase of flight under consideration, but additional stability and control and TAR analysis must be completed. 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 Quad-Rotor without cross-shafting, for instance, may be theoretically able to autorotate, but in practice control the speed of all four (4) rotor independently may prove difficult. These states and difficulties are noted as required in the FHA.

4.2.1 Tilt-Wing FHA Assumptions

It was assumed that the aircraft starter system, whether electric or conventional APU starting, is isolated from the primary propulsion system. Isolating the starting system significantly reduces the probability of failures of the lower-reliability starting system to generate failures in the primary propulsion system.

The vehicle configuration of the Tilt-Wing allowed to physically isolate battery arrays from one-another within the battery network. The battery arrays were conceptualized to be placed near each electric motor and ESC; the FHA assumes a common battery cooling system with two (2) pumps acting in parallel, either one capable of supplying adequate flow and pressure.

Hazards and FTA will focus on hover (rotary-wing-borne flight) and level-flight cruise (fixed-wing-borne flight) mission segments, considering percent time spent in each segment. Conversion/transition and climb/descent flight are not considered in the current analysis.

Hazards and FTA will assume the fuel system meets reliability requirements regardless of propulsion system for Tilt-Wing. Both conventional (turboshaft engine burning fossil fuels turning rotors) and series hybrid propulsion (turboshaft engine burning fossil fuels turning generator) will require effectively the same fuel system.

Loss of the turboshaft engine or other components necessary to keep the batteries charged will result in the air vehicle relying on batteries alone for propulsive power. The batteries are assumed to last two (2) minutes, and the air vehicle is assumed to be within two (2) minutes of a suitable landing zone 60% of the time.

Prop-rotors are assumed to connect by cross-shafting. This is done to mitigate potential propulsion imbalance, uneven lift, and attendant controllability issues. Single loss of gearboxes that will result in one of the prop-rotors is assumed to be non-catastrophic due to adequately sized controls to deal with any adverse yaw. Any dual gearbox loss is assumed to be catastrophic due to lack of thrust and potentially due to controllability issues.

4.2.2 Quad-Rotor FHA Assumptions

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

Two cross-shafting configurations were evaluated. In the cross-shafted configuration, all four (4) rotors are interconnected via common collector gearbox and associated drive-shafts. In the configuration without drive-shafting, all rotors are driven independently by their propulsors (motor and gearboxes).

For the Quad-Rotor without cross-shafting, any single loss of a propulsor is considered loss of air vehicle due to the rotors not being cross-shafted together. 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 Quad-Rotor is cross-shafted, a loss of a single propulsor is Minor at altitude, and only potentially Catastrophic when the air vehicle is being operated in the OEI avoid region.

Additionally, the effects of the position of any dual rotor failures is separately examined in the FHA for the Quad-Rotor air vehicle that is not cross-shafted. Controllability impacts are different for 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 two FHAs are color coded to assist the analyst in identifying changes between the two configurations. The “Effect of the Failure” Column is color coded yellow where differences exist between the cross-shafted Quad-Rotor and the example without cross-shafting. Additionally, the “Classification of Failure” column is colored red in the FHA for the Quad-Rotor without cross-shafting if the failure effect is more severe than the equivalent fail in the cross-shafted Quad-Rotor.

4.2.3 Lateral-Twin FHA Assumptions

The lateral twin has two conventional turboshaft engines driving rotors and an electric motor driven by a battery used for takeoff and landing. The lateral twin has cross-shafting so that the loss of any propulsor will not affect the ability to provide lift through both rotors. The loss of any of the given propulsor, either of the turboshafts or the electric motor, is examined in the FHA.

4.2.4 Lift+Cruise FHA Assumptions

The loss of any single propulsor, even in OEI, will not result in loss of lift sufficient to result in a hard-landing outcome. The air vehicle is, per the NASA Urban VTOL paper (ref. 3), capable of hovering with the loss of one propulsion unit, with the differential thrust being balanced out with a power reduction on another unit to control potential roll or yaw excursion.

Single propulsor fails are assumed to include the components that allow that propulsor to function: the gearbox, Motor, ESC, ESC Power, and the high voltage (HV) battery power. Any single propulsor failure is considered a Minor failure; dual propulsor failures are considered Major failures.

Gearbox failures are assumed to be the same outcome as loss of propulsor in the hover region due to the RPM based thrust control, and the lack of interconnection between the engines. The FHA separately examines loss of the ability to align the propellers edge-wise to the relative wing to reduce drag. Drag increase due to one propeller is minor, as are two on opposite wings, but yaw control authority with two failed gearboxes on one wing where the propellers are not able to be turned edgewise to minimize drag may result in a Major outcome due to degraded yaw control.

The turboshaft engine and associated gearbox, AC Generator, and AC/Direct Current (DC) convertor are grouped together so that the loss of any of those components will result in the air vehicle relying on battery power alone for continued flight. If within 2 minutes of an acceptable landing spot, the failure of the charging components is considered Severe. If more than 2 minutes from an acceptable landing spot, than the outcome is assumed Catastrophic.

4.3 FMECA Methodology & Assumptions

A FMECA is a tabular document containing postulated failure modes of the propulsion system. A FMECA was performed on the four (4) NASA RVLT Concept Vehicles to determine system failure modes and their associated criticality characteristics from a bottoms-up, function analysis. This examination of the system aids in identifying potential safety concerns.

The FMECA process is a methodology for comprehensively identifying the failure modes for a system or component. It progresses and matures in line with the design process and increases in detail along with the design. The FMECA process begins in the conceptual design phase with initial planning and requirements review. This lays the groundwork for the actual FMECA itself. System models and block diagrams are typically developed in this stage to aid in the identification of functions and functional decomposition. Figure 10 shows the approximate alignment of FMECA development with the design process similar to what is described in SAE ARP5580 (ref. 7).

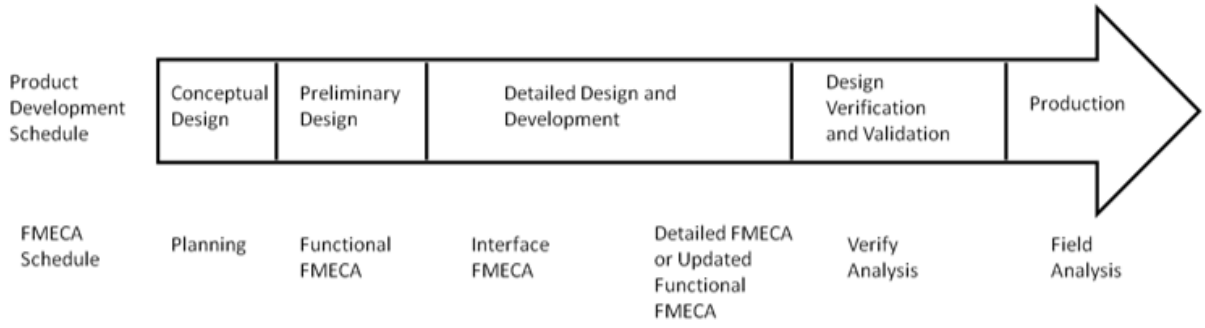


Figure 10: FMECA Development and Design Flow.

The first level of analysis occurs in the preliminary design phase with the functional analysis. This approach postulates the functions and functional failure modes associated with overall system performance. It creates the basis by which the system level FMECA is constructed in detail to support the design elements as they are defined (at Critical Design Review), and indicates component level candidates which may become the subject of separate FMECA efforts. This functional

FMECA purposely focuses on the overall functions of the system elements. In this sense, many of the components are analyzed as "black boxes," with detailed internal functions and functional failure modes reserved for analysis at the individual component level.

As the details of the design become more refined, so does the FMECA. The second level of FMECA refinement is captured in the interface analysis, which incorporates the known features responsible for interfacing with other systems (e.g. where a gearbox is mounted to airframe structure or where an oil temperature sensor interfaces with the electrical system). This assessment is typically developed early in the detailed design phase after preliminary design has been completed. In some cases, enough detail is available that some of the interface information can be incorporated prior to preliminary design completion.

The FMECA is completed as the detailed design phase comes to a close in support of detailed or critical design reviews. This analysis may explore sub-systems of the functional analysis' subsystems or even deeper. The FMECA captures failure modes to the level necessary to support follow-on safety, R&M, and logistics analyses.

The FMECA also serves the purpose of providing a basis for validation throughout the lifecycle of the system. System testing and production phases are used to validate the existence of the postulated failure modes, their frequency of occurrence, and the effectiveness of cited compensating provisions. This lifecycle validation helps to identify opportunities for future designs.

Each phase of FMECA development follows a similar process after the FMECA is initially planned and functional requirements are analyzed (during the conceptual design phase). The planning and block diagrams are used to identify functions and function (one at a time). These are used to postulate failure modes for each functional failure (one at a time). These failure modes are analyzed for their consequences from which severity codes may be assigned. Severity is divided into four categories as defined in MIL-STD-1629A (ref. 8). Severity category is assigned to provide a qualitative measure of the worst potential consequences resulting from design error or item failure. The severity classifications are described in Table 2.

Table 2: Severity Classification Used in FMECA Worksheets.

Category	Severity of Effect
I	Catastrophic: A failure which can cause death of system loss (i.e. aircraft, tank, missile, ship).
II	Critical: A failure which can cause severe injury, major property damage, or major system damage which will result in mission loss.
III	Marginal: A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.
IV	Minor: A failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.

Finally, failure mode frequency is determined for each failure mode. A flow chart of the FMECA development process which was adapted from SAE ARP5580 (ref. 7) is shown in Figure 11. 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. Table 3

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. 9).

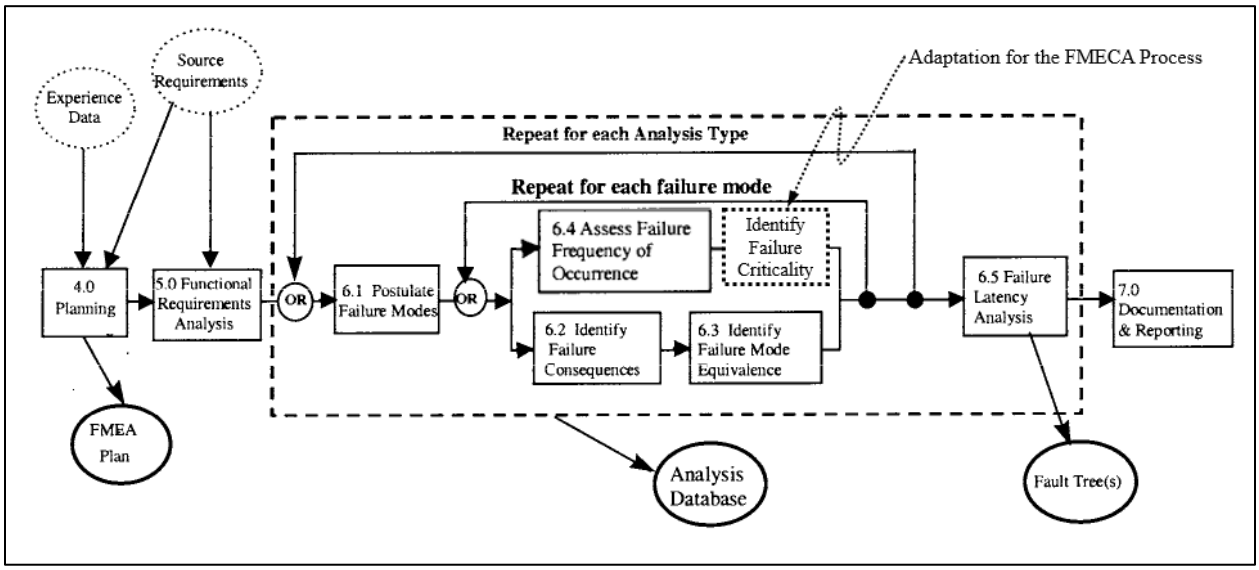


Figure 11: FMECA Development Flow Chart

Table 3: Applied Failure Rate (FR) used for FMECA and FTA.

Item	Base FR (failures per 10^6 hours)	Data Source Reference	Applied Environmental Factor	Applied FR (failures per 10^6 hours)
Turbine Engine	2.67	Ref. 10	1	2.67
Generator, AC	13	Ref. 11	10	130
Gearbox assembly	0.5	Ref. 12	10	5
Gearbox assembly, manual	4.8	Ref. 12	10	48
Gearbox assembly, motor driven	2.6	Ref. 12	10	26
Battery, lithium	9.31	Ref. 12	10	93.1
Controller, motor	4.75	Aircraft Maintenance Data	10	47.5
Motor-Generator	19.72	Ref. 13	10	197.2
Electric Motor, General	9.24	Ref. 13	10	92.4
Pump, general	43.65	Ref. 13	1	43.65
Electronic Motor Drive	54	Ref. 14	5	270
Air conditioner [Battery cooling system]	508	Ref. 13	1	508
Heat exchanger	8.08	Ref. 13	1	8.08
Motor cooling system	51.73	(pump + Heat ex-changer)	1	51.73
Airborne power supply	200	Ref. 15	1	200
Clutch, General	5.01	Ref. 13	1	5.01
Clutch, Overrunning	0.42	Ref. 12	1	0.42
Shaft, General	0.93	Ref. 13	1	0.93
Drive Link Assembly (drive shaft)	1.495	Ref. 13	1	1.495

4.4 FTA Methodology & Assumptions

The FTA are developed in parallel with, and are informed by, the Functional Block Diagram. The FMECA provides the numbers utilized in the fault trees. The FTA component assignments are titled after the FMECA ID code where applicable. In some cases multiple FMECA codes are covered by one FTA event. In this case the FTA title block will reflect the associated FMECA codes.

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 Alpha (Mode Ratios).

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.

4.4.1 Tilt-Wing FTA Assumptions

The Tilt-Wing FTA was executed with the following assumptions:

- The air vehicle is capable of wing-borne flight on any three remaining motors as long as air vehicle is in the region of Effective Translational Lift (ETL) or faster. ETL onset is assumed around 25 kts based on typical helicopter and tilt-rotor behavior. Any loss of a motor or propulsion unit above 25 kts is assumed to be recoverable. Any loss of a motor or propulsion unit below 25 kts will require adequate altitude to increase the speed of the air vehicle above 25 kts to continue flight. Any failure below 25 kts at low altitudes is analogous to a multi-engine helicopter losing an engine in the OEI avoid region. For such failures, a hard landing and potential catastrophic outcome is conservatively assumed.
- While the presence of cross-shafting will mitigate potential directional/roll control deficits at critical speeds (not addressed in propulsion FTA), the cross-shaft is assumed to provide no mitigation for power deficit below 25 kts.
- It is assumed that the aircraft will be primarily operated over densely populated urban and suburban areas affording potentially few emergency landing possibilities. The mission length is assumed (ref. 2) as 2 minutes hover (takeoff), 15 minutes cruise (50 nm at 200 kts), and 2 minutes hover (landing). It is assumed that the air vehicle will spend approximately 78% of time in the short-haul cruise phase. 11% spent in takeoff and climb, and 11% during descent and landing.
- Typical cruising altitudes are assumed to be 5,000 feet or below for the short haul leg. If longer cruise legs are specified, 10,000 feet will be assumed. An aggressive high-rate of descent profile would be necessary for the aircraft to reach the ground and execute a landing prior to loss of battery and all air vehicle propulsion. This will result in approximately a 3.33 mile radius (assuming 200 kts during descent) of potential emergency landing locations. Potential landing spots include golf courses, high school football stadiums, etc. These may not be present in dense urban areas.
- It is assumed that the landing would be executed with the wing tilted vertically to minimize landing roll-out. This may need to be balanced against increased power (electricity) requirements once the aircraft has transitioned away from wing-borne flight.
- Based on the power-limited ability to land vertically; but balanced against the short duration of remaining pure electrical battery power and primary suburban/urban use, it is qualitatively assessed that the hybrid tilt-wing vehicle would be able to execute a successful (minimal damage/injuries) emergency landing 40% of the time.
- Cooling systems used failure criticality numbers from the FMECA that assumed pilot interaction at time of leak detection. A failure of the ESC is assumed to lead to a failure of the propulsor to provide thrust.

4.4.2 Quad-Rotor FTA Assumptions

The Quad-Rotor FTA was executed with the following assumptions:

- Due to shorter mission legs and slower speeds than the tilt-wing, the Quad-Rotor is assumed to be in the OEI avoid region for 25% of its time as opposed to the tilt-wings 20%.

- The low voltage battery powers the ESC and the FCC is necessary for speed control of the propulsor RPM. Loss of either of those components is assumed to result in the loss of all propulsors.
- Loss of a single rotor gearbox (RGB) 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 cross shaft failure OR a collector gearbox failure AND a loss of any propulsor results in a catastrophic outcome.
- The fault tree for the Quad-Rotor without interconnection lacks the logical input of the cross shafting 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.

4.4.3 Lateral-Twin FTA Assumptions

The Lateral-Twin FTA was executed with the following assumptions:

- Any contact between the overlapped left and right rotor blades is assumed to be Catastrophic. For this reason a failure of any of the following interconnecting shaft components will set the top gate true: Right INTX, Left INTX, collector gearbox, Intermediate Gearbox, Intermediate Gearbox 2.
- A failure of the low voltage (LV) battery or the FCC is assumed to set the Propulsor 2 failure (electric propulsor) to true. It is assumed that the two (2) turboshaft engines have their own full authority digital electronic control (FADEC) powered by their own sources that are dissimilar to the electric propulsor.
- It is assumed that the aircraft will be operating at weights that necessitate the burst power of the electric propulsor during takeoff, hover, and landing. A loss of any of the propulsors in the OEI avoid region will result in a potential Catastrophic outcome. A loss of any of the propulsors, turboshaft or electric, is assumed to allow adequate power for an adequate amount of time to execute a no-hover or roll-on landing.
- The HV Battery fail in the fault tree is derived from the FMECA representing complete loss of HV battery power. The fault tree does not attempt to address reduced battery power or partial battery fails effects on the air vehicle.
- An engine gearbox fail will serve to disconnect the local turboshaft engine from the drivetrain. A failure of the CGB is assumed to disconnect the electric motor from the drivetrain. A failure of either of the cross-shafts is assumed to disconnect the power output from the electric motor from the rotor on the side of the failed driveshaft. Potential unequal power to each rotor was not addressed in the FHA or air vehicle FHA.

4.4.4 Lift+Cruise FTA Assumptions

The Tilt-Wing FTA was executed with the following assumptions:

- The air-vehicle is capable of hover flight following the loss of a single motor as long as a complementary motor on the opposing wing reduces its torque output to maintain static equilibrium.

- The air-vehicle is dependent upon the aft mounted propulsor for pitch control (ref. 3).
- Cooling systems used failure criticality numbers from the FMECA that assumed pilot interaction at time of leak detection. A failure of the ESC is assumed to lead to a failure of the propulsor to provide thrust.

5 CONCEPTUAL POWERTRAIN CONFIGURATIONS

5.1 Tilt-Wing Powertrain Configuration

5.1.1 Tilt-Wing Rotating System

The rotating system of the Tilt-Wing is depicted in Figure 12. The Tilt-Wing rotating system contains electric motors remotely located, near each rotor to reduce the power demands on the interconnecting shafting. Each motor spins at 14,999 RPM and provides power into an overrunning, sprag clutch mounted inside an accessory gearbox (AGB). The AGB 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, AGB, and RGB. 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 RGB (also known as Prop-Rotor Gearbox for Tilt-Wing and Tilt-Rotor aircraft) through the noted sprag clutch and associated shafting. The parallel axis gear train in the AGB does not carry primary power. Power enters the RGB and is transferred through a dual stage, simple planetary system with an overall reduction ratio of 17.42:1 to achieve a rotor speed of 861 RPM.

In addition to the primary power path, a secondary power path is included in the rotor gear box for OMI conditions and synchronization of the rotors. A spiral bevel gear mesh with a 1.67:1 ratio is mounted between the AGB and the dual stage, simple planetary system. The spiral bevel gear mesh sends power through interconnecting shafts to a RGB. Limited, if any, sweep of the wing and limited, if any, dihedral means that an additional collector gearbox centered in the fuselage is not required.

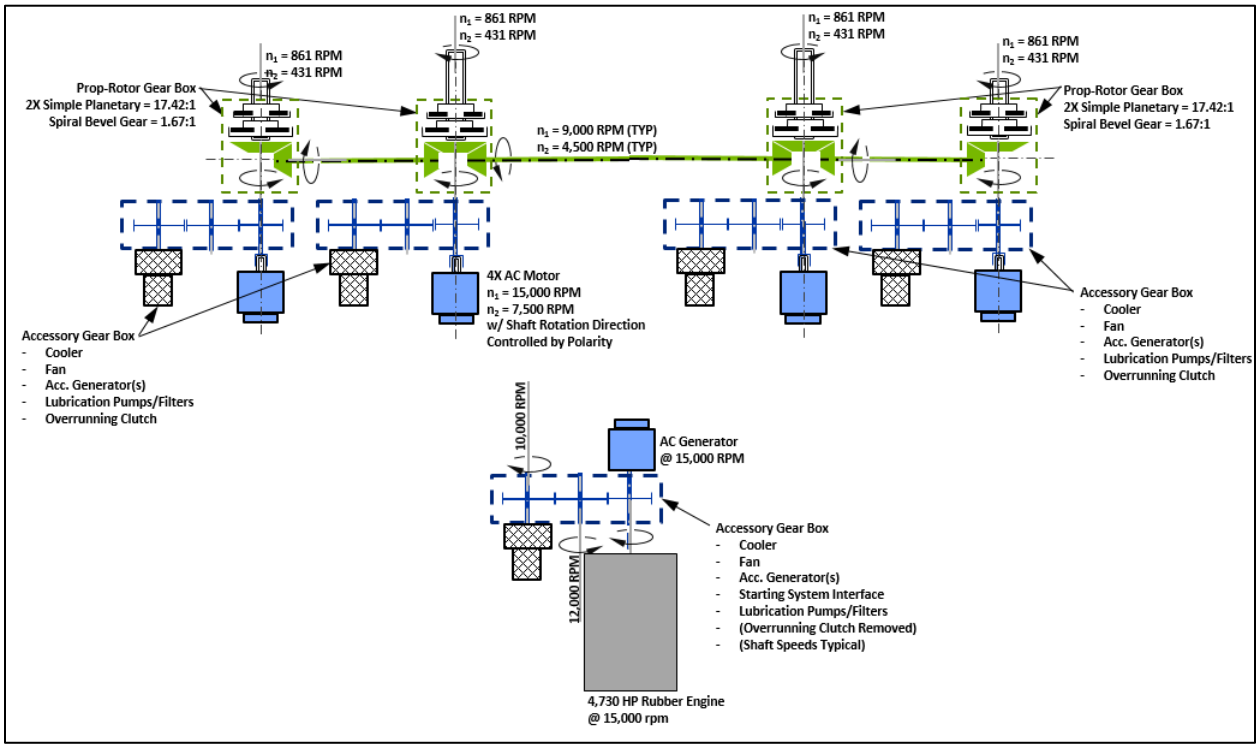


Figure 12: Tilt-Wing Rotating System Schematic.

5.1.2 Tilt-Wing Flight Control System

The Tilt-Wing FCS arrangement is shown in Figure 13. Each rotor is connected to a rotor gearbox. Each of these gearboxes is also connected to an electric motor as well as to a cross-shaft. Each motor is controlled by an individual ESC which takes commands from a FCC. The ESC's accept HV power to drive the motors and uses an in-built DC-DC convertor to power itself. The source of the HV power is either a battery network or directly from an AC generator through an AC/DC convertor. The AC/DC convertor also provides low voltage to power the FCC's. The AC generator is driven via direct connection with a turbo shaft engine.

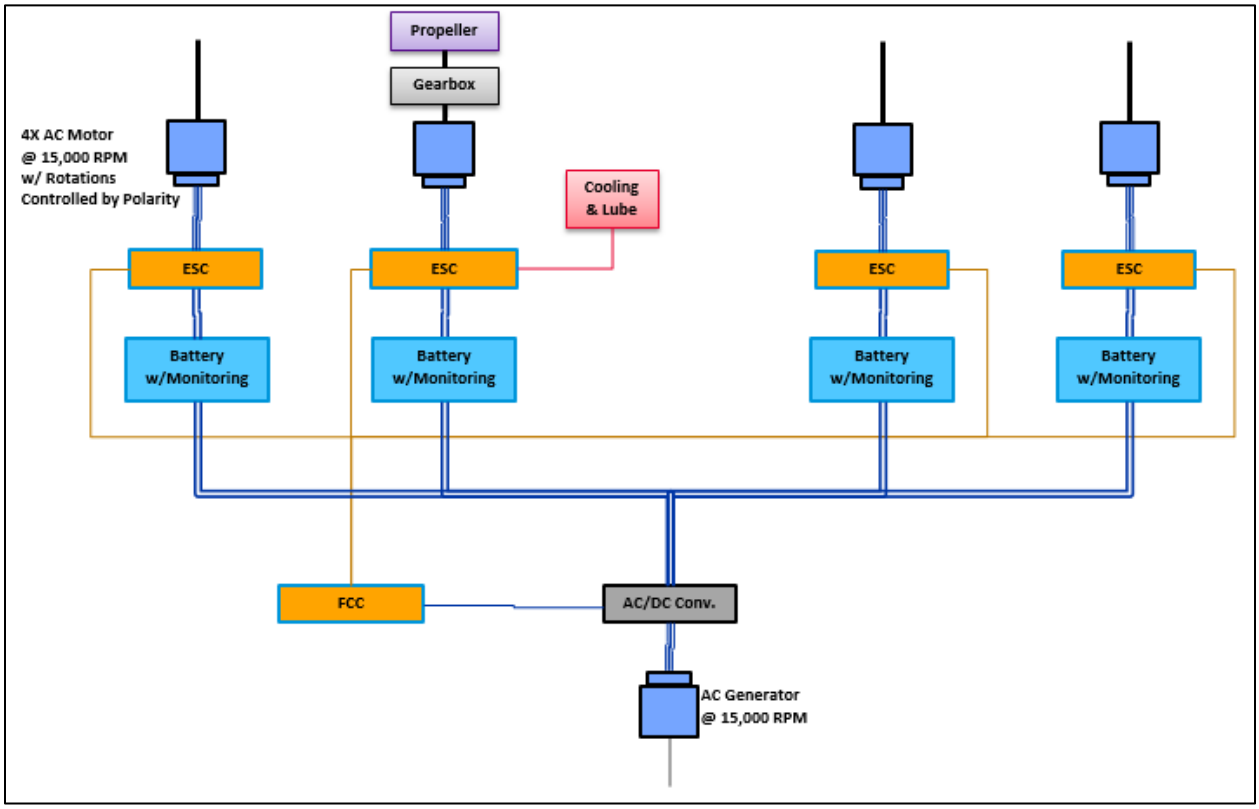


Figure 13: Tilt-Wing Powertrain Flight Control System Schematic

5.2 Quad-Rotor Powertrain Configurations

The Quad-Rotor design developed by the NASA RVLT team included four (4) remotely located rotors, each with collective pitch control for pitch, yaw, and roll stability. The collective control allows for mechanical interconnection of each rotor via cross 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 single motor failure or OMI condition.

The powertrain configuration for the Quad-Rotor is broken into three (3) primary sub-sections. As defined here, the rotating system includes the motors, gearboxes, and cross-shafting. The FCS includes the ESC, 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 motors, gearboxes, and ESC's.

5.2.1 Quad-Rotor Rotating System

The rotating system of the Quad-Rotor is shown in Figure 14. The Quad-Rotor rotating system contains electric motors remotely located, near each rotor, similar to the Tilt-Wing rotating system. 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 mechanical drive a cooling fan and lubrication pumps. The cooling fan draws air across a heat exchanger which cools the motor, accessory gearbox, and RGB. 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 RGB through the noted sprag clutch and associated shafting. The parallel axis gear train in the AGB does not carry primary power. Power enters the RGB and is transferred through a dual stage, simple planetary system with an overall reduction ratio of 17.42:1 to achieve a rotor speed of 681 RPM.

In addition to the primary power path, a secondary power path is included in the rotor gear box for OMI conditions and synchronization of the rotors. A spiral bevel gear mesh with a 1.16:1 ratio is mounted between the AGB and the dual stage, simple planetary system. The spiral bevel gear mesh sends power through cross shafting to a collector gearbox (CGB). Power from the front, left rotor passes through the front, left cross shafting and is transferred into a forward spiral bevel gear mesh in the CGB. Power is split at the forward spiral bevel gear mesh; power is sent to the front, right rotor through the complimentary side of the forward spiral bevel gear mesh. 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. 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 (2) spiral bevel gears and one (1) spiral bevel pinion, for a total of six (6) spiral bevel gears.

An alternate CGB arrangement may be obtained through four (4) spiral bevel or face gears meshing with a common ring gear, either spiral bevel or face. However, this still results in a similar number of gears and restricts the configuration of the aircraft, limiting the sweep angles and dihedral of each strut.

5.2.2 Quad-Rotor Flight Control System

Quad-Rotor FCS assumption schematic is shown in Figure 15. Each rotor shaft is connected to a RGB. Collective blade pitch is controlled using a swashplate actuated by a singular electric actuator. The gearbox connected to each rotor is connected to an electric motor through an overrunning clutch as well as to a central CGB (for the case with interconnecting shafts). 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. The low voltage power source provides power to the FCC which is sending control signals to the ESC and the electric actuators driving the rotor swashplates as well.

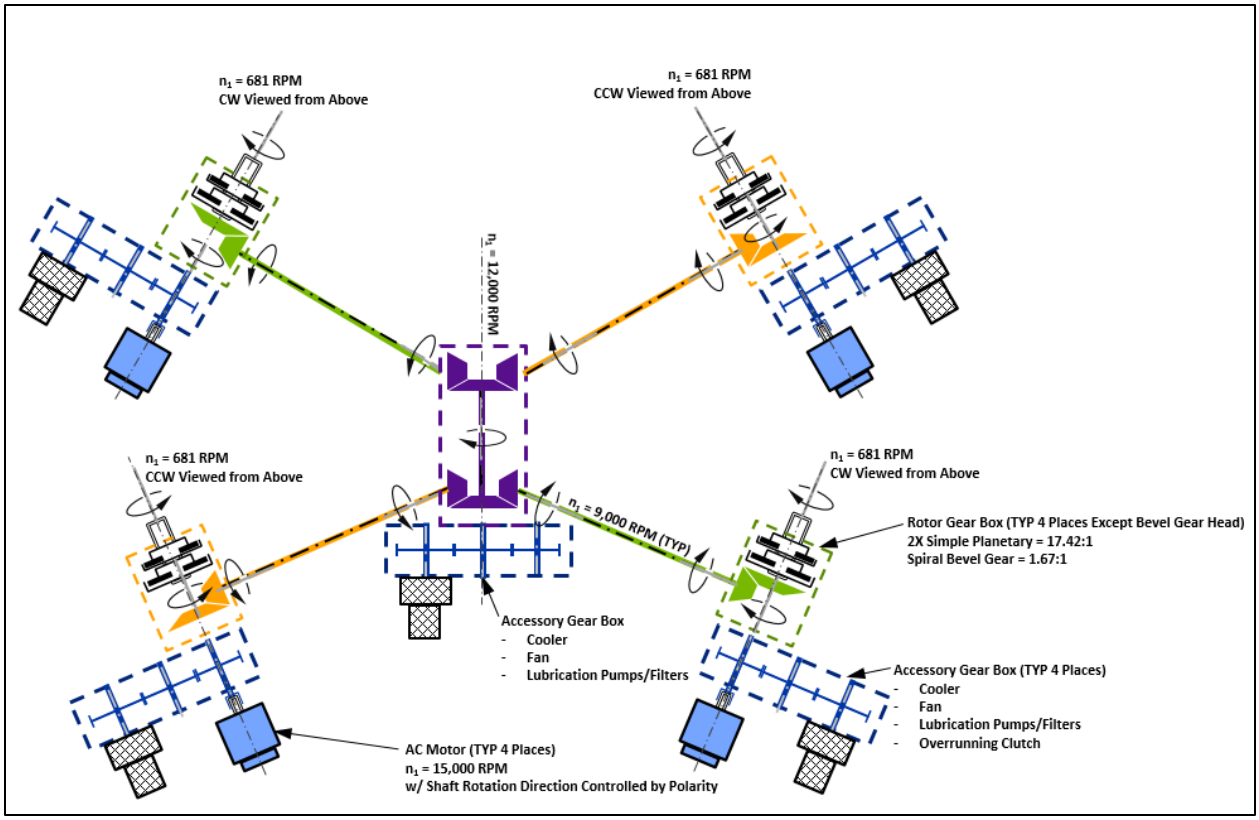


Figure 14: Quad-Rotor Rotating System Schematic.

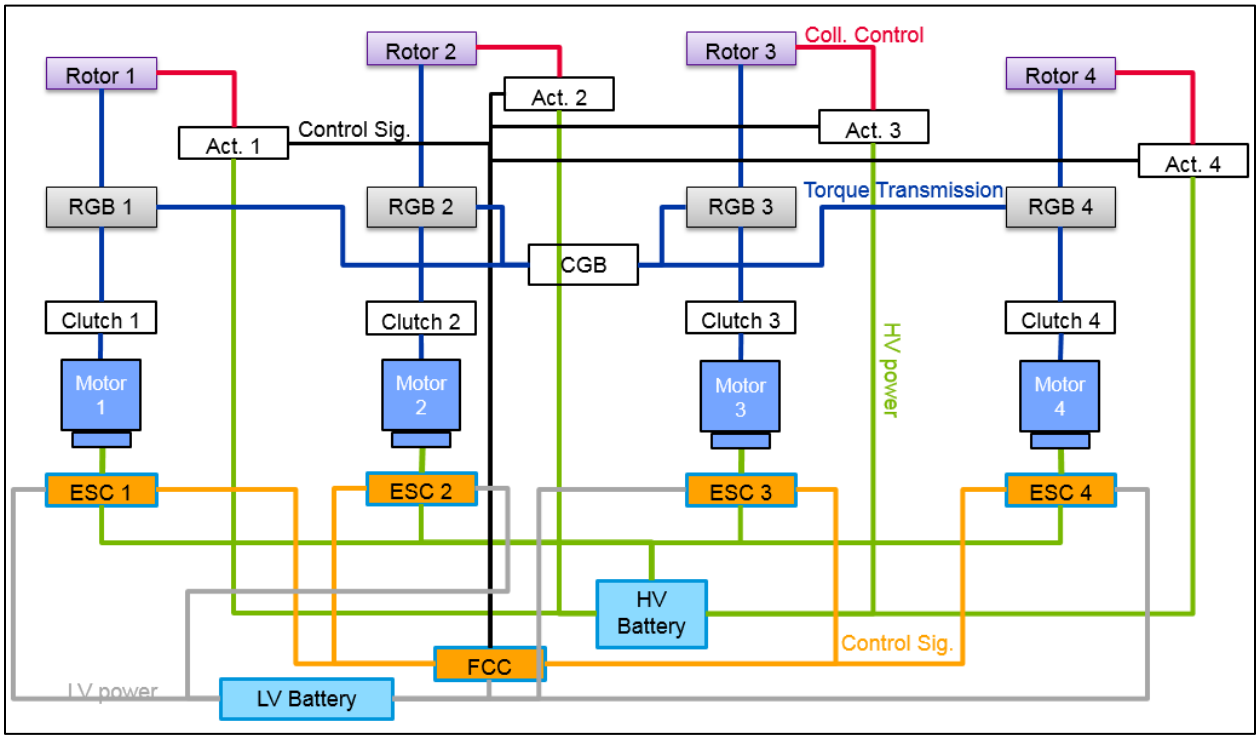


Figure 15: Quad-Rotor Powertrain Flight Control System Schematic.

5.3 Alternate Configuration – Quad-Rotor without Interconnecting Shafting

The Quad-Rotor was also conceptualized without the use of interconnecting shafting as part of the reliability and safety assessment. The overall powertrain configuration remains similar to the baseline Quad-Rotor powertrain configuration. The rotating system architecture is modified from the baseline. The difference being the absence of the interconnecting cross shafting, the CGB, and the AGB required to lubricate and cool the CGB. The FCS and TMS are similar to the baseline, as well.

5.4 Lateral-Twin Powertrain Configuration

5.4.1 Lateral-Twin Rotating System

The rotating system of the Lateral-Twin is shown in Figure 16. The Lateral-Twin rotating system contains two (2) turboshaft engines remotely located underneath each rotor and an electric motor/generator unit (MGU) located above the fuselage. Each engine spins at 45,000 RPM and sends power into an overrunning, sprag clutch mounted inside a left hand (LH) and right hand (RH) engine gearbox. Each LH and RH engine gearbox is similar and contains a spiral bevel gear set in order to turn the direction of power into the LH and RH intermediate gearbox. Each LH and RH intermediate gearbox sends power to mechanically driven cooling fans, lubrication pumps, hydraulic pumps, and accessory generators. Each intermediate gearbox sends power into a LH and RH RGB where power is sent to each LH and RH rotor system. Each RGB contains a spiral bevel gear mesh that redirects power to the rotor system centerline and a dual-stage, simple planetary system.

In addition to the primary power path, a secondary power path is included in order to mechanically synchronize the rotors and to provide a path for power to flow into and out of the electric MGU. A spiral bevel gear mesh is mounted above the fuselage and sends power along a synchronization shaft set to each LH and RH rotor gearbox, through a pass-through shaft in the intermediate gearbox. A friction disc clutch is located between the output of the MGU and the spiral bevel gear mesh. The friction disc clutch is used to couple or decouple the MGU from the primary driveline. Detailed mission planning a usage spectrum information is required to determine the schedule for clutch engagement and disengagement, but it is likely that the clutch would be disengaged (decoupling the MGU from the driveline) during start up and in emergency conditions and engaged (coupling the MGU and driveline) during flight while the MGU powers the rotors or while the MGU is being charged by the turboshaft engines.

5.4.2 Lateral-Twin Flight Control System

The Lateral-Twin FCS assumption is shown in Figure 17 schematic. The system consists of two articulated rotors whose blade pitch is controlled via swashplate through three hydraulic actuators each. Each of the rotor shafts are connected to an equivalent RGB which in turn is connected to a turboshaft engine via an overrunning clutch. Each of the equivalent RGB is also connected to a mid-wing gearbox which in turn is connected to a motor/generator via a controllable clutch. The motor/generator is connected to an ESC/AC-DC convertor. This pathway can operate as a motor/ESC or a generator/AC-DC convertor. The ESC/AC-DC convertor is connected to a HV battery from which power is drawn when in the motor/ESC configuration (hover) and vice-versa when in the generator/AC-DC convertor configuration (cruise). Each of the RGB drives a hydraulic pump and accessory generator. The hydraulic pump in turn drives the swashplate hydraulic actuators of the rotors, while the accessory generator power output goes onto the vehicle LV power bus. The

LV bus powers the FCC and the hydraulic actuators servos. A LV battery is also on the bus which serves as the backup source of LV power. The LV battery can charge itself via the LV bus as well as provide power to the bus as required (e.g. when accessory generators are unavailable). Control signals from the FCC are routed to the ESC/AC-DC convertor and the hydraulic actuators.

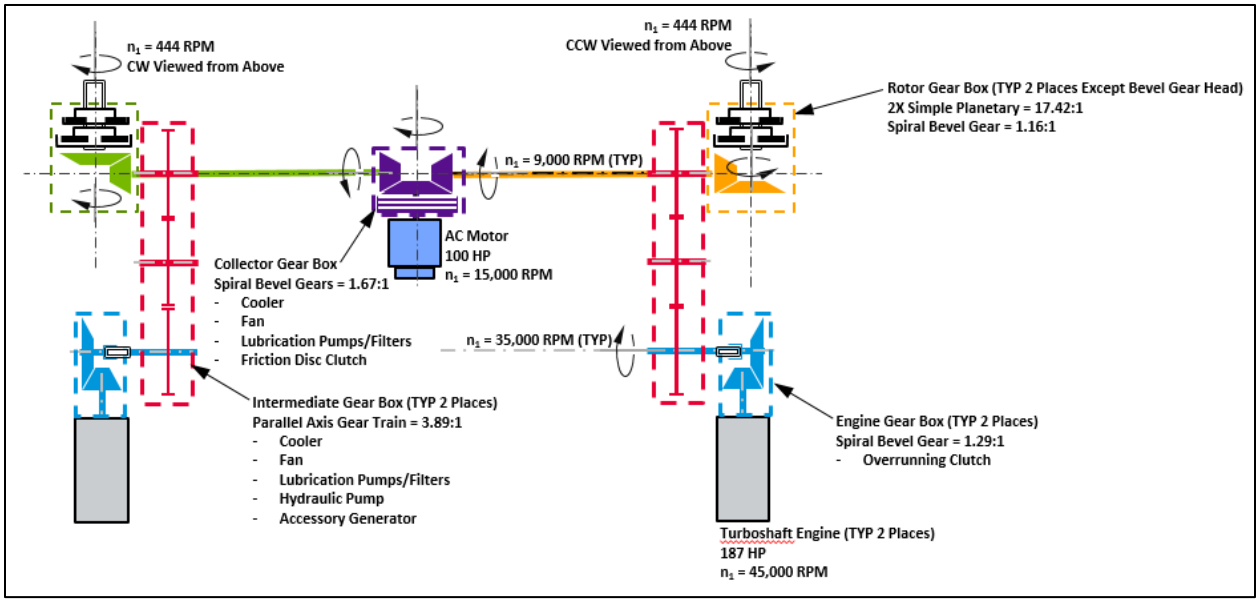


Figure 16: Lateral-Twin Rotating System Schematic.

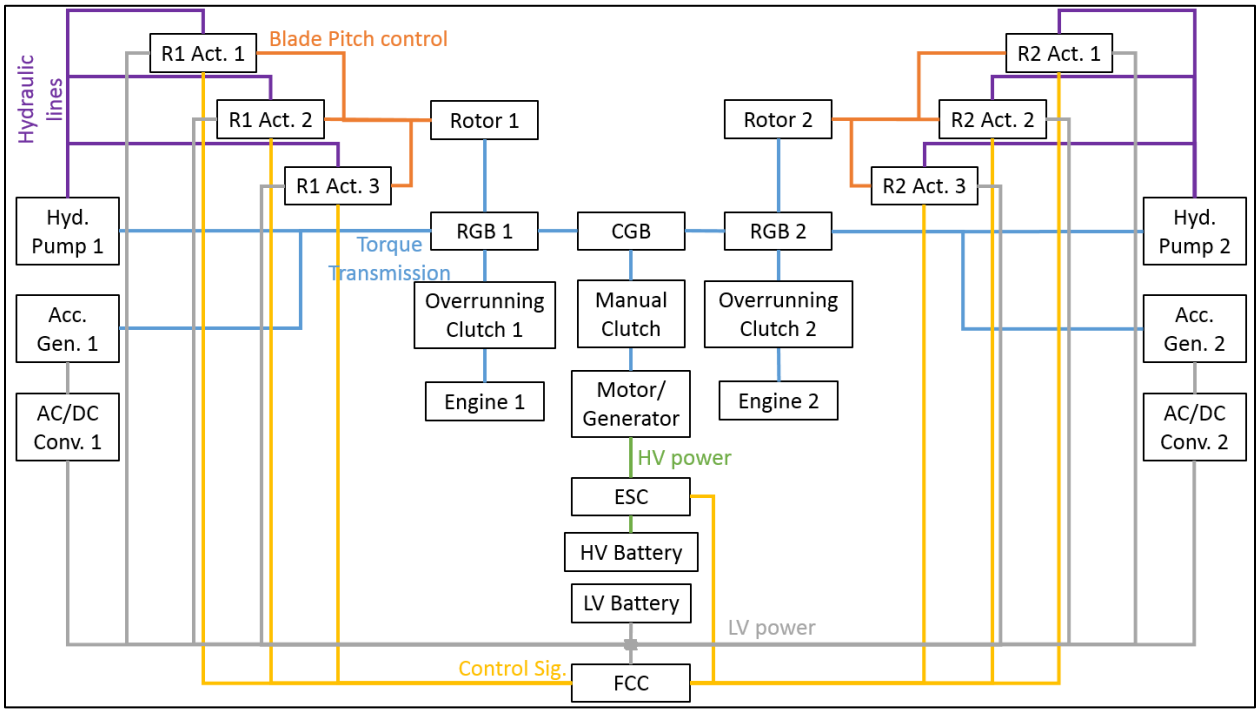


Figure 17: Lateral-Twin Powertrain Flight Control Schematic.

5.5 Lift+Cruise Powertrain Configuration

5.5.1 Lift+Cruise Rotating System

The rotating system of the Lift+Cruise is shown in Figure 18. The Lift+Cruise rotating system contains one (1) turboshaft engine centrally located, inside the fuselage, eight (8) electric motors located near each rotor, and an electric motor located near the propulsor. Each of the drive motors spin at 18,169 rpm (rotor motor) or 22,176 rpm (propulsor motor), sending power into an overrunning sprag clutch located inside the respective AGB. Each AGB is similar and sends power to mechanically driven cooling fans, lubrication pumps, hydraulic pumps, and accessory generators through a parallel axis gear train. Each AGB sends power into a RGB where power is sent to each rotor or propulsor system. Each RGB contains a two (2) stage planetary system with a 17.42:1 total reduction ratio. The motor spins at 18,169 RPM based on the 17.42:1 planetary system reduction ratio. The planetary systems used to drive the rotors are rated for 88 HP (ref. 3).

The local propulsor powertrain is assumed to be similar to that of the rotor powertrain in that a motor is connected to the propulsor through an AGB and a two (2) stage planetary system. The propulsor spins at 1,273 RPM design speed, requiring a motor output speed of 22,176 RPM (dependent upon the final selected planetary reduction ratio). The AGB includes a cooler, mechanically driven fan, and lubrication pump necessary to cool the motor, AGB, and RGB.

The turboshaft engine has an assumed output speed of 20,000 rpm similar to that of the General Electric Company's (GE) CT7 turboshaft engine series (ref. 16). The output of the turboshaft engine enters an AGB, similar to the AGB mounted underneath each rotor. The AGB includes a cooler to cool the AGB and the AC Generator, a mechanically driven fan, starting system interfaces, such as a power turbine air starter interface, and lubrication pumps and filters. The AGB mounted to the front of the turboshaft engine does not include an overrunning clutch.

5.5.2 Lift+Cruise Flight Control System

The Lift+Cruise FCS schematic is shown in Figure 19. Nine RPM-controlled rotors (eight lifting, one pusher) are each driven by an electric motor controlled by an ESC. The ESCs route HV power to the motors from the HVDC power bus. They are assumed to be powered by an internal DC-DC converter fed by the same HVDC bus. The HVDC bus is fed by an HVDC battery system, which is charged by an AC generator via AC-DC converter. The ESCs are controlled by the FCC, which is powered by a LV accessory generator via another AC-DC converter. The HV and LV generators are driven by the turboshaft engine.

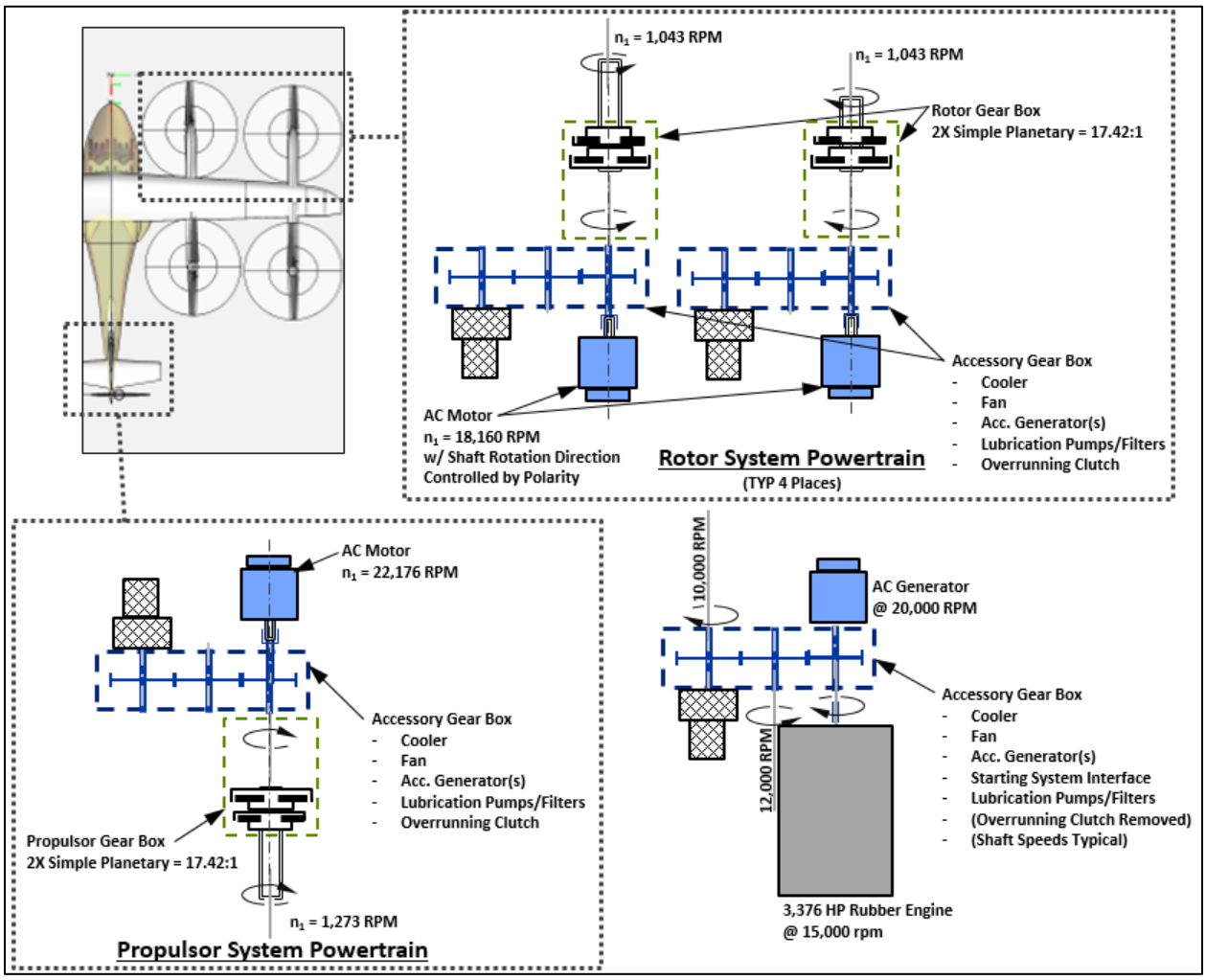


Figure 18: Lift+Cruise Powertrain Rotating System Schematic

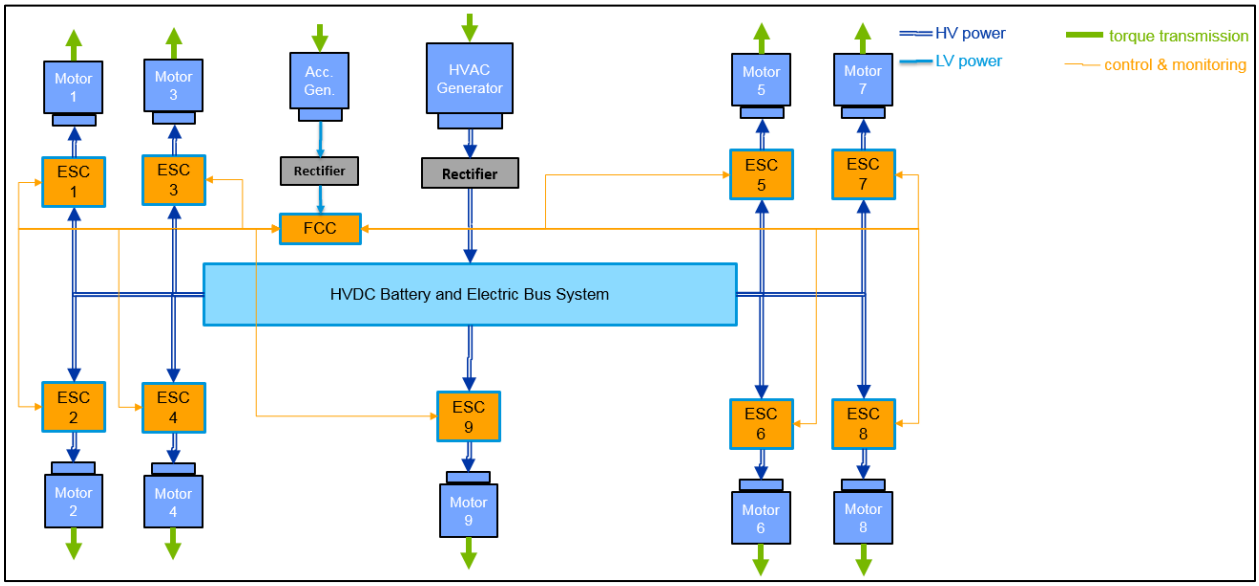


Figure 19: Lift+Cruise Powertrain Flight Control System

5.6 Thermal Management Systems

Electric propulsion 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 considered in this study is shown in Figure 20. 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 21. 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.

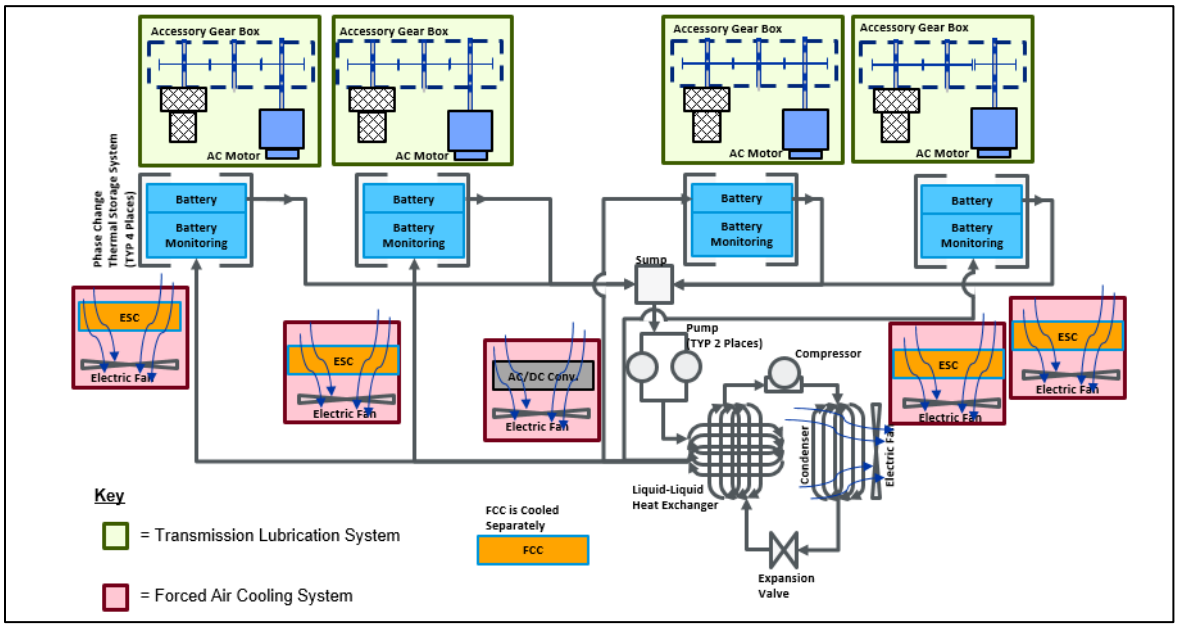


Figure 20: Thermal Management System (TMS) Schematic

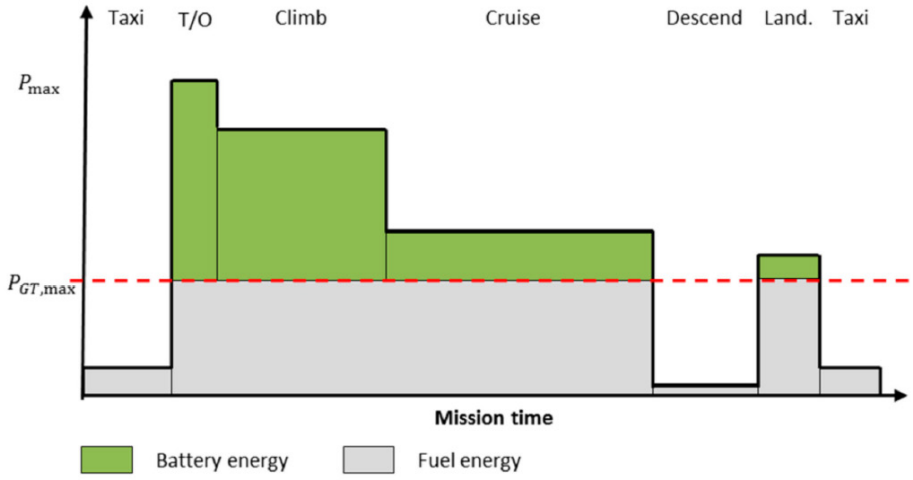


Figure 21: Notional Mission Power Usage Profile

Engine bay cooling requirements and designs can vary from engine to engine, even within the same power class, so an engine bay cooling system was not configured. Generator and 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, consistent with current technology devices. High density or future technology components may dictate the need for more specialized cooling, which would be determined during system design. The TMS shown in Figure 20 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.

The Li-ion batteries are the most temperature critical components in each of the concept vehicles powertrain system. Current technology batteries operate most efficiently and reliably between 15˚C and 45˚C (59˚F and 113˚F), with battery temperatures above 80˚C (176˚F) 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 pressure 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 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.

A number of TMS configuration trade studies should be conducted during system design. These include the following:

- Eliminate the liquid cooling system and use conditioned air for battery cooling. While the liquid cooling system can provide increased heat transfer rates and more uniform battery temperatures than air cooling, a detailed design study may show that air cooling is acceptable. In this case, the vapor cycle system would provide cooling to the air via an air to refrigerant evaporator.
- If the ambient temperature profile is compatible with the battery operating temperature range, it may be possible to eliminate the vapor cycle cooling system. Retaining liquid cooling for the batteries may be advantageous as the liquid system provides improved heat transfer rates and better temperature distribution within the batteries. Heat removed from the batteries via the liquid would be shed to ambient air in a liquid to air heat exchanger.
- And finally, it may be possible to provide battery cooling with ambient air only. The ambient temperature profile and battery operating temperature limitations would need to be evaluated. The air flow rate required to maintain battery temperatures is an important consideration in this trade.

6 FUNCTIONAL BLOCK DIAGRAMS

The Functional Block Diagrams are a graphic representation of the functions analyzed. The shaded blocks were analyzed in this study. The FMECA uses the FBD as a basis to postulate failure modes and analyze effects. The corresponding FMECA 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. The FMECA uses the functional block diagram as a basis to postulate failure modes and analyze effects. Equipment such as low voltage electrical power, flight control system, actuators, and rotors are illustrated with dashed lines on the FBD, but not assigned functions as they are not considered in the analysis.

6.1 Tilt-Wing Functional Block Diagram

The Tilt-Wing propulsion system was assigned 5 functions, which are considered essential functions of the propulsion system.

- Function 1: Provide High Voltage DC to propulsion system and batteries. This consists of the turbo-shaft engine, gearbox, AC Generator, and AC/DC converter. Loss of any one of these components would result in loss of the same function.
- Function 2: Provide battery storage of electrical energy. Each electric motor is considered to have its own battery, such that a battery failure would only affect power provided to a single motor. Internal battery failure could result in thermal runaway and aircraft fire, or could have reduced output or no output to the associated electric motor. This is delineated by the individual failure modes in the FMECA worksheet.
- Function 3: Convert High Voltage DC electrical energy to shaft torque: This function consists of the ESC, electric motor, and associated cooling components. The functions for motor cooling and motor lube were assumed as a single function.
- Function 4: Provide shaft torque to prop-rotors. The clutches and gearboxes transfer the motor torque to the prop-rotors.
- Function 5: Provide system cooling for batteries: As the electrical power is normally provided by the turbo-shaft engine, the battery cooling function would only affect the propulsion system in cases where loss of function 1 has already occurred.

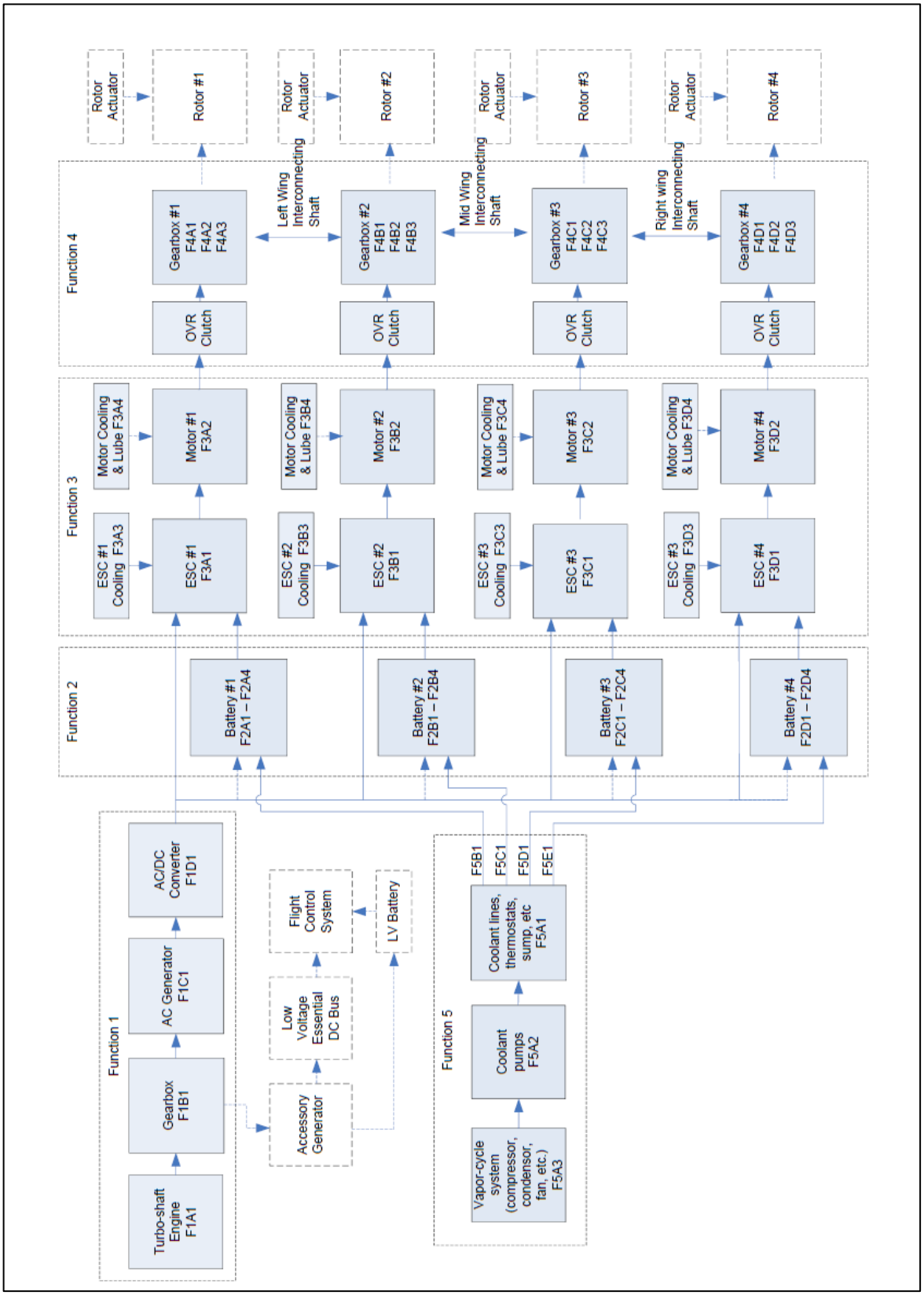


Figure 22: Tilt-Wing Functional Block Diagram.

6.2 Quad-Rotor Functional Block Diagram:

The Quad-Rotor with cross shaft propulsion system 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 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 collector gearbox re-distributes the remaining available torque to keep all 4 rotors operating.

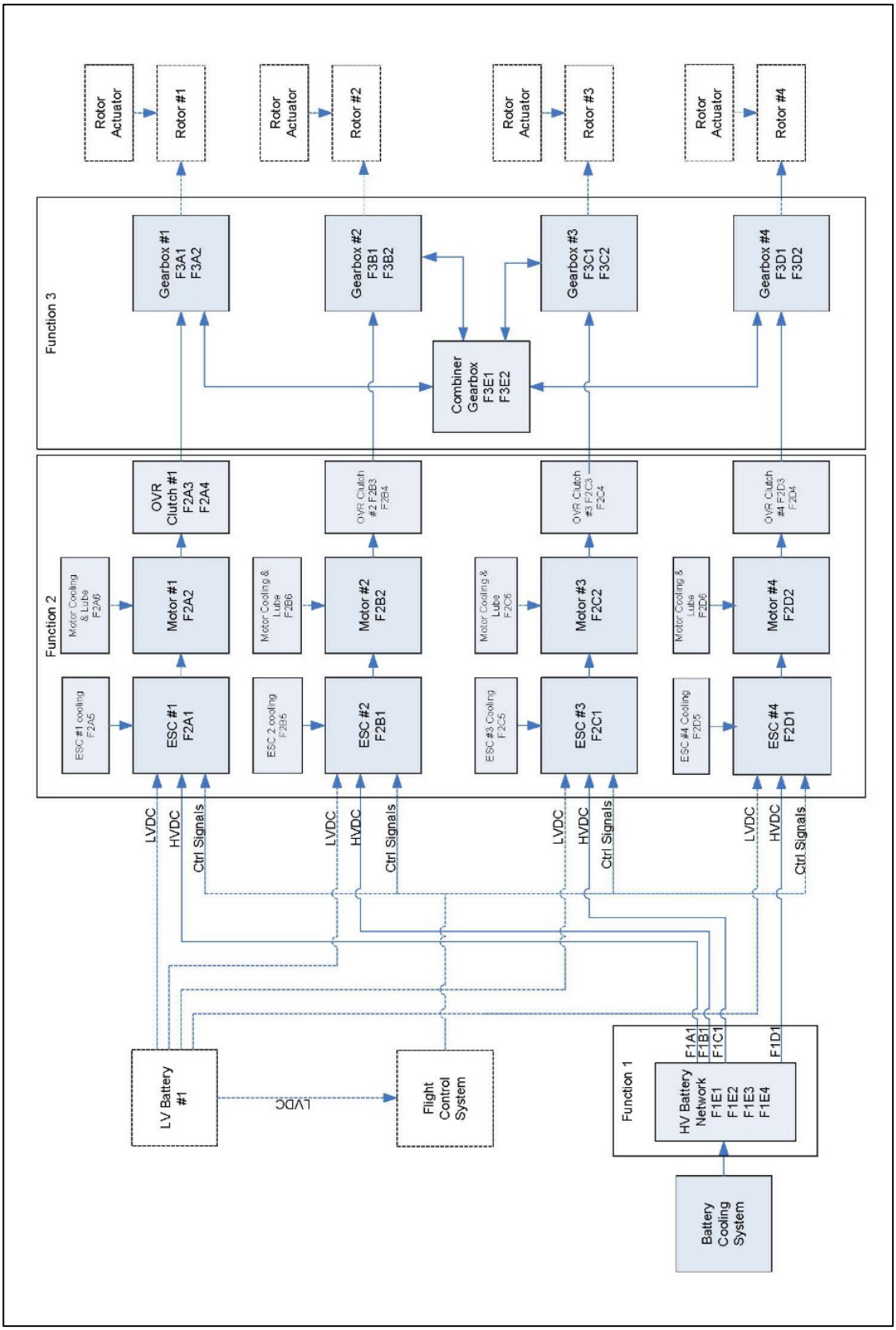


Figure 23: Quad-Rotor Functional Block Diagram.

6.3 Alternate Configuration –Quad-Rotor without Interconnecting Shafting Functional Block Diagram

The Quad-Rotor without cross shaft propulsion system differs only in function 3, where there is no function to transfer power in the event of a motor failure:

- 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 1E5
- Function 2: Convert electrical energy to shaft torque. This function consists of the 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 prop-rotors.

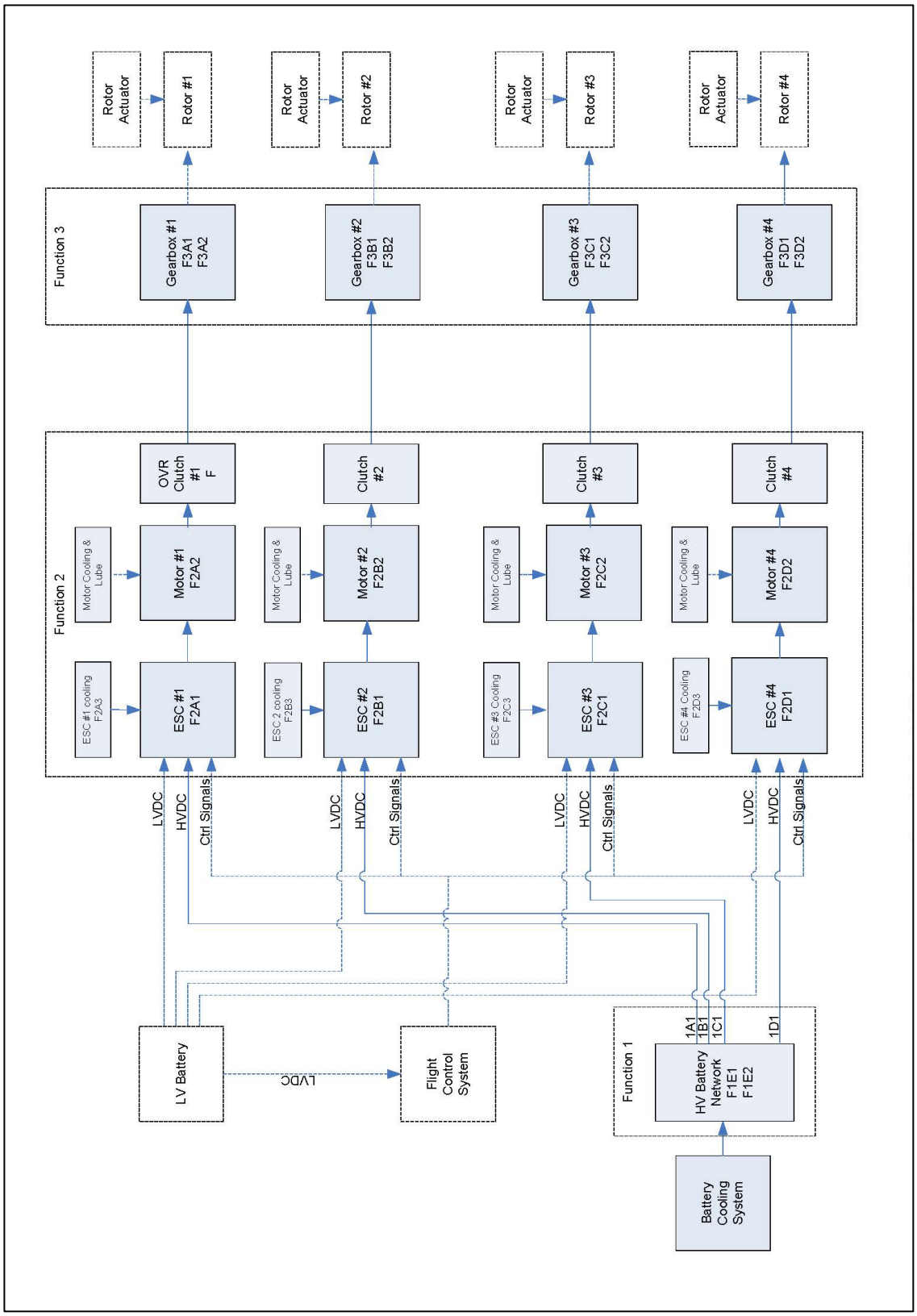


Figure 24: Alternate Configuration –Quad-Rotor without Interconnecting Shafting Functional Block Diagram.

6.4 Lateral-Twin Functional Block Diagram

The lateral twin propulsion system was divided into 3 main functions:

- Function 1: Provide main engine torque to intermediate gearboxes. This consists of main engines, engine gearboxes, and overrunning clutch.
- Function 2: Transfer shaft torque from engines to rotors and provide rotor synchronization. This consists of the gearboxes and interconnecting shafts.
- Function 3: Provide electric motor boost power for hover and low speed flight. This includes the battery system, ESC, motor-generator, and emergency disconnect. The electric motor is providing boost torque in Functions 3A, and is charging the battery network in function 3B. For the motor-generator and the battery circuits, it is assumed that any failure would cause loss of both the boost function and the battery charge function, so loss of ability to charge the battery becomes irrelevant if you also lost the ability to use the battery power. For this reason, failure modes for boost mode only were considered. The ESC was considered different, and assumed to have failure modes that would be unique to charge only mode, or to boost mode only. The emergency disconnect system may manifest itself as an overrunning clutch, shaft with a shear section, friction disc clutch, or other practical means to separate the MGU from the driveline.

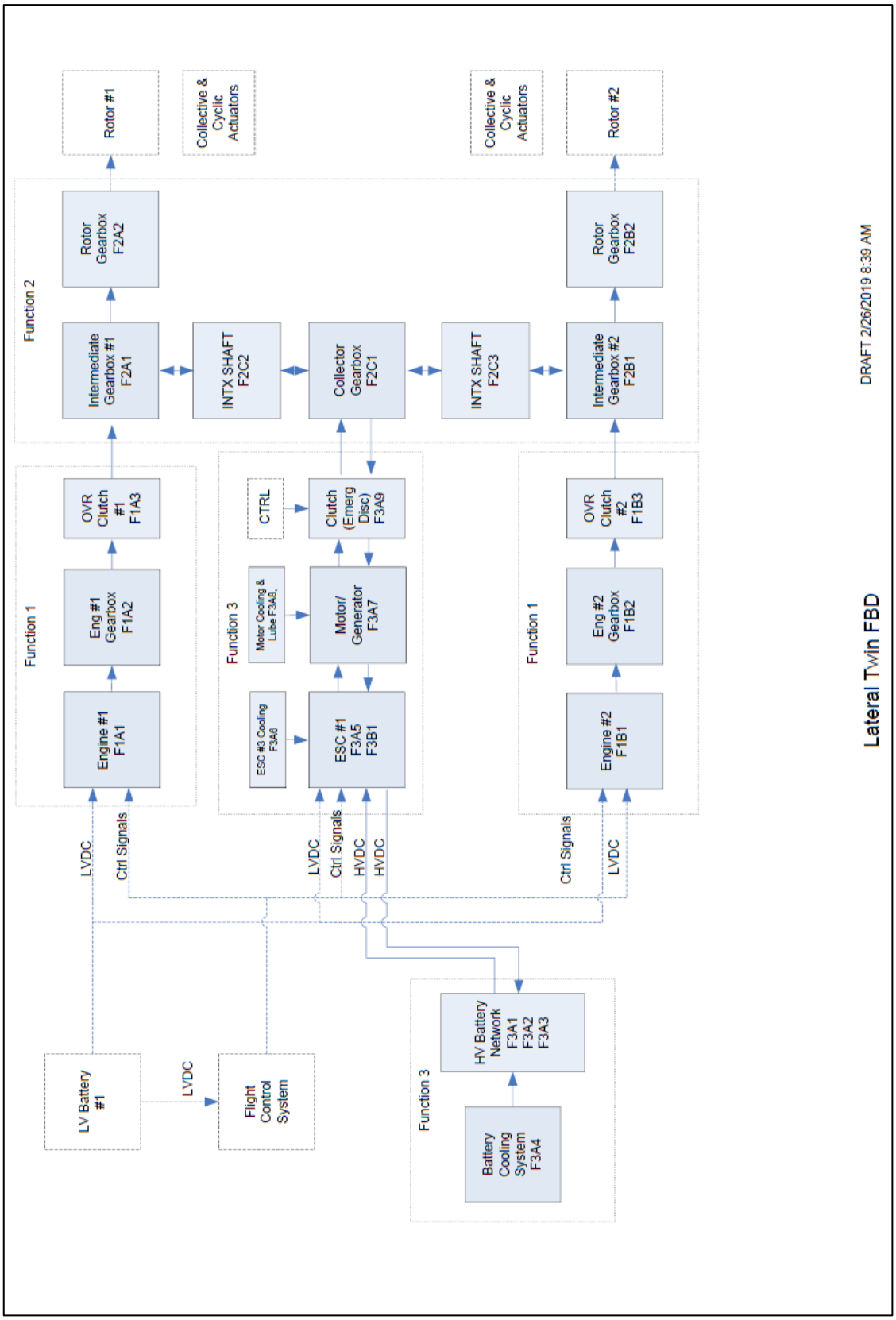


Figure 25: Lateral-Twin Functional Block Diagram.

6.5 Lift+Cruise Functional Block Diagram

The Lift+Cruise propulsion system was divided into 4 main functions.

- Function 1: Provide High voltage DC power for propulsion and to charge batteries: This includes the turbo-shaft engine, gearbox, AC Generator, and AC/DC converter.
- Function 2: Provide High Voltage DC electrical power to motors. This function consists of battery system and associated wiring
- Function 3: Provide torque to lifting rotors: Each of the 8 individual lifting rotors is powered independently by a dedicated ESC, electric motor, and gearbox.
- Function 4: Provide torque to thrust propeller: The thrust function is completely independent of the lifting function. Although the detailed design would be significantly different, the functional layout is similar to the lifting rotors.

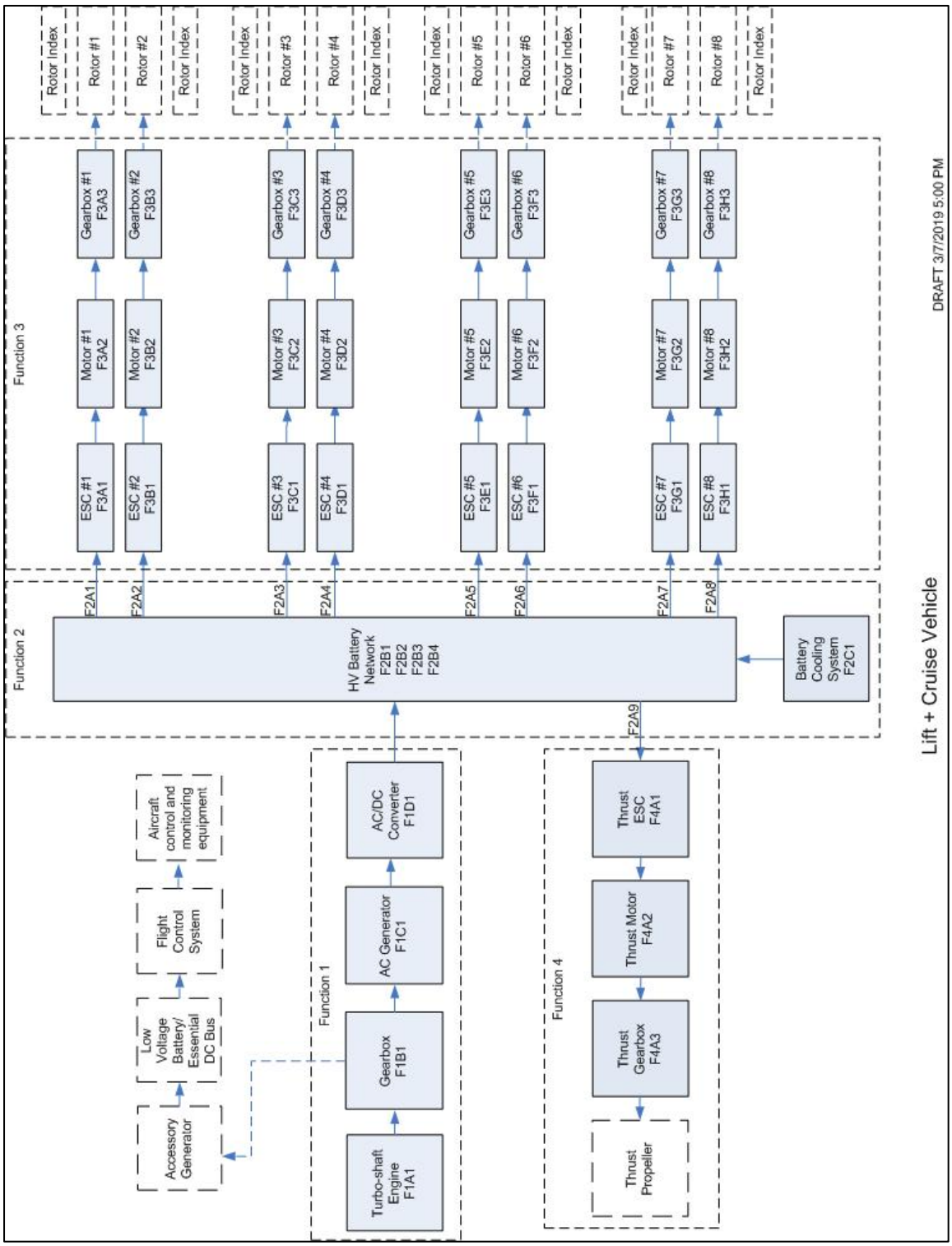


Figure 26: Lift+Cruise Functional Block Diagram.

7 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. The FHA's for each of the NASA RVLT Concept Vehicles may be found in Appendix A.

The safety analysis process for this study began with a FHA. The FHA is a structured analysis technique which systematically analyzes hazards arising from functional failures of a system. A FHA considers the functions of the system under analysis, and identifies the failure conditions by considering the effects of loss of the function, incorrect operation of the function, or inadvertent occurrence of the function when not desired. The FHA typically considers all flight phases of the aircraft, as well as different operating environmental conditions, and how they affect functional failure severity. However, do to the conceptual nature of this exercise, only a few phases of flight were considered, namely hover, flight within the OEI/OMI avoid region, and flight outside the OEI/OMI avoid region.

The result of the FHA is a list of functional failures with an assigned severity, which depends on the possible outcome of the failure. A severity of catastrophic, severe, major, or minor is assigned to each functional failure, in accordance with SAE ARP4761 (ref. 17). Another result of the FHA is a list of Derived Safety Requirements (DSR) needed to help mitigate and control the resulting hazard of the functional failure. The DSRs are provided to the Systems Engineering requirements management organization, and flowed down into appropriate design specifications in accordance with the requirements management process.

Following the FHA, the resulting functional failures are consolidated into a more concise list of hazards. Each hazard is assigned a severity, in accordance with the severity of the functional failure(s) encompassed by the hazard, and is also assigned a hazard probability. Different techniques have been employed at the discretion of safety analysts, to determine the hazard probabilities for each hazard.

The Tilt-Wing was designed to be controlled via collective pitch at each of its rotors for roll and yaw control. Single-axis cyclic control was envisioned for pitch control and interconnecting shafting is envisioned between each rotor for emergency conditions. The FHA associated with the Tilt-Wing is shown in Table A- 1.

The Quad-Rotor was designed to be controlled via collective pitch at each of its rotors. However, the rotors do not intermesh so it is conceivable that pitch, roll, and yaw control can be obtained via constant pitch, varying speed propellers. The baseline system varies collective pitch at each rotor for control in all axes. The hazards associated with Quad-Rotor with cross shafting are listed in Table A- 2.

If future excursions change the configuration of the Quad-Rotor to constant pitch, varying speed propellers, then additional hazards are now attributable to the powertrain. The hazards associated with Quad-Rotor without cross shafting are listed in Table A- 3. In the case of the Quad-Rotor without cross shafting, loss of a single propulsor must be considered a functional hazard in all flight modes. Control and trim of the aircraft should be considered in sub-system or aerodynamic stability and control simulations to mitigate this hazard.

The Lateral-Twin was designed to have lateral and longitudinal cyclic control and collective control at each rotor. The rotors overlapped, which requires that the rotors be mechanically synchronized via interconnecting shafts. The Lateral-Twin FHA is provided in Table A- 4.

The Lift+Cruise vehicle was designed to be controlled by a variable speed, fixed pitch rotor system. Based on NASA's guiding principles behind the Lift+Cruise Concept Vehicle (ref. 3), it was assumed that one (1) propulsion unit may be lost without a catastrophic outcome. The Lift+Cruise FHA is provided in Table A- 5.

8 FAILURE MODES AND EFFECTS CRITICALITY ANALYSIS (FMECA)

The FMECA is a tabular document containing postulated failure modes of the propulsion system. The FMECA worksheets contain the following data elements. Having identified the functions for each component, the FMECA worksheets were populated and functional failures were derived. From the functional failures and based on reliability data, Table 3, the postulations for failure modes and failure effects were developed and added to the worksheet. Failure effects were extrapolated through the system and to the end item to help identify the severity associated with each failure mode. Failure causes for each mode were then postulated utilizing information from several data repositories. Additional information was added to identify system design related compensating provisions and failure detection methods.

The FR prediction for each FMECA component was derived from an industry search for historical component failure rates. Within those numbers, distributions were derived and associated with each of the postulated functional failures. A rate was determined for each functional failure mode specific to each sub-system and tabulated in the worksheet, along with the conditional probability that the failure effect results in the identified severity code, given that the failure mode occurs (Beta) and the mode criticality number. All Beta values are based on engineering judgment.

8.1 Definitions of FMECA Worksheet Data Elements:

- **FMECA ID Code:** The FMECA identification is an indentured code which assigns a unique identifier for each failure mode. This is a combination of the Failure Mode Index (FMI) Function, FMI Mode, and FMI Cause, as defined here:
  - 1st character (1 to 9) identifies the function;
  - 2nd character (A to Z) identifies the failure mode.
  - 3rd character (1 to 9) identifies the cause.
- **Function:** A description of the function under analysis.
- **Failure Rate (λ):** The frequency (or rate) with which an item will be unable to perform its intended function in the operational environment for which it was designed. This is expressed as failures per flight hour.
- **Failure Mode:** A description of the functional or equipment failure. Failure modes are determined by examination of the functional outputs identified on the applicable Functional Block Diagram or based on the system description.
- **Failure Cause:** A description of the unique component or equipment or functional loss.
- **Mission Phase:** Describes the flight regime or maneuver that the aircraft is executing when the functional failure occurs. The default condition is “ALL”, indicating that the failure mode is applicable to all phases of flight and ground maneuvering.
- **Local Failure Effect:** The consequence the failure has on the operation, function, or status of the specific item being analyzed.
- **Next Higher Effect:** The consequence the failure has on the operation, functions, failed equipment or other system components, including automatic enabling of backup and/or redundant systems.

- **End Effect:** This category defines the worst case end effect the defined failure has on the operation, function, or status of the aircraft. The effect shall be written in such a way that the severity determination is substantiated.
- **Detection Method:** The means or mechanism by which the defined failure can be discovered.
- **Compensating Provision (CP):** Design provisions or operator actions which circumvent or mitigate the effects of a failure. Compensating design provisions are features at any indenture level that will nullify the effects of a malfunction or failure, but do not prevent its occurrence.
- **Severity Code:** Severity is divided into four categories as defined in MIL-STD-1629A. Severity category is assigned to provide a qualitative measure of the worst potential consequences resulting from design error or item failure. The severity classifications are described in Table 2.
- **Failure Mode Ratio (α):** The fraction of item failures related to the failure mode under consideration. The sum of all failure modes related to a specific equipment or item will equal one (1). When a particular equipment or item has more than one possible failure effect, the mode ratio was is distributed evenly.
- **Failure Effect Probability (β):** The conditional probability that the failure end effect will result in the identified severity classification given that the failure mode occurs. A 1.0 value indicates that the failure mode results in an actual loss in all instances. A value of less than 1.0 indicates a lower probability of actual loss.
- **Beta Mode Ratio Explanation:** The description of why/how a particular Failure Effect Probability was selected.
- **Failure Mode Criticality Number:** The probability that a failure for a component resulting from a particular failure mode with result in the severity classification identified. The mission time is, by default, one hour in duration.
- **Incipient Fail Symptoms:** Description of symptoms that can provide early warning before the failure event actually occurs, either through health monitoring, observation of abnormal condition, or scheduled maintenance inspections. Incipient failure symptoms help avoid worst case end effect, and are considered when determining Beta.

Appendix B contains the FMECA worksheets for the NASA RVLT Concept Vehicles analyzed. Table 4 contains the FMECA summary for Tilt-Wing severity code I failure modes. Table 5 contains the FMECA summary for Quad-Rotor severity code I failure modes. Table 6 contains the FMECA summary for Alternate Configuration Quad-Rotor severity code I failure modes, in which interconnecting shafting is not utilized to mechanically link each rotor system. Table 7 contains the FMECA summary for Lateral-Twin severity code I failure modes. Table 8 contains the FMECA summary for Lift+Cruise severity code I failure modes.

Table 4: Tilt-Wing FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide HVDC power to propulsion system and batteries	Engine, gearbox, AC Generator, AC/DC Converter	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	I	3.33×10^{-4}	1.98×10^{-4}
2	Provide battery storage of electrical energy	Battery Failure	Aircraft fire damages critical systems, causing loss of aircraft	I	1.00×10^{-6}	1.00×10^{-9}
3	Convert HVDC Electrical energy to shaft torque	Electronic Speed Controllers, Electric Motors,	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	I	1.45×10^{-3}	2.90×10^{-4}
4	Provide torque to prop-rotors	Prop--rotor gearboxes, clutches, and shafts	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	I	2.00×10^{-5}	4.00×10^{-6}
5	Provide system cooling for batteries	Battery cooling system	Aircraft fire, loss of controlled flight	I	5.22×10^{-4}	1.72×10^{-7}
				Severity Code I Summary:		**4.92×10^{-4}**

Table 5: Quad-Rotor FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide HVDC power to electric motors	HV Batteries	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	I	1.00×10^{-6}	2.00×10^{-7}
			Aircraft descends to ground. Autorotation employed to provide soft landing	II	5.00×10^{-7}	5.00×10^{-9}
2	Convert HV electrical energy to shaft torque	ESC's, Motors, Clutches, ESC cooling, motor cooling	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	I	2.03×10^{-3}	3.02×10^{-4}
3	Transfer motor torque to rotors	Rotor gearboxes, collector gearbox	Aircraft descends to ground with limited control.	I	2.50×10^{-5}	1.00×10^{-5}
				Severity Code I Summary:		**2.47×10^{-4}**

Table 6: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide HVDC power to electric motors	HV Batteries	Aircraft descends to ground with limited control.	I	1.00×10^{-6}	5.00×10^{-7}
			Aircraft descends to ground. Autorotation employed to provide soft landing.	II	5.00×10^{-7}	5.00×10^{-9}
2	Convert HV electrical energy to shaft torque	ESC's, Motors, Clutches, ESC cooling, motor cooling	Aircraft descends to ground with limited control.	I	2.03×10^{-3}	1.01×10^{-3}
3	Transfer motor torque to rotors	Rotor gearboxes, collector gearbox	Aircraft descends to ground with limited control.	I	2.00×10^{-5}	1.00×10^{-5}
				Severity Code I Summary:		**1.01×10^{-3}**

Table 7: Lateral-Twin FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide main engine torque to intermediate gearboxes	Engine, Gearbox, clutch failure	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	I	1.62×10^{-5}	3.24×10^{-6}
2	Transfer shaft torque from engines to rotors and provide rotor synchronization	Intermediate gearbox, rotor gearbox, collector gearbox	Loss of controlled flight. Loss of aircraft.	I	3.52×10^{-5}	3.52×10^{-5}
3	Provide electric motor boost power for hover and low speed flight	Battery, ESC, electric motor, motor cooling	Loss of ability to hover or fly at low speed. Loss of aircraft if failure occurs while in OMI avoid region.	I	2.90×10^{-4}	5.80×10^{-5}
				Severity Code I Summary		**9.65×10^{-5}**

Table 8: Lift+Cruise FMECA Severity Code I Summary

Function No.	Function	Failure Cause	End Effect	Severity Code	Mode Failure Rate	Failure Mode Criticality No.
1	Provide HVDC for propulsion and to charge batteries	Turbo-shaft engine, gearbox, AC generator, AD/DC converter	Loss of propulsion if pilot cannot land safely before batteries are discharged. Loss of aircraft.	I	3.00×10^{-4}	1.80×10^{-4}
2	Provide HVDC electrical power to motors	Battery Failure	Aircraft descends to ground. Glide may be possible depending upon conditions at time of failure. Loss of control of aircraft	I	5.10×10^{-4}	1.04×10^{-4}
3	Provide torque to lifting rotors	ESC, lift motor, or gearbox failure	No Cat I or Cat II single point failure in lift function	NA	NA	NA
4	Provide torque to thrust propeller	Thrust ESC, thrust motor, or thrust gearbox failure	Aircraft speed and range significantly reduced. Ability to hover is unaffected. Loss of aircraft if pilot cannot find safe landing area within range	I	3.67×10^{-4}	1.84×10^{-4}
				Severity Code I Summary		**4.67×10^{-4}**

9 FAULT TREE ANALYSIS (FTA)

Following the FHA, the resulting functional failures are consolidated into a more concise list of hazards. Each hazard is assigned a severity, in accordance with the severity of the functional failure(s) encompassed by the hazard, and is also assigned a hazard probability. Different techniques have been employed at the discretion of safety analysts, to determine the hazard probabilities for each hazard. For this study, a FTA was performed in order to model the connectivity between components, systems, and functions.

FTA is a top-down analysis meant to capture the propulsion components and to examine their interrelationships and allow the definition of cut-sets to show areas where system improvements would improve the top-level number. The roll-up of the propulsion FTAs are done so that loss of propulsion may also include loss of control, depending on air vehicle configuration. The FTA is meant to document a Catastrophic or Severe outcome top level, though lesser severity hazards may become evident due to FTA structure and execution.

Overall, the propulsion specific systems and their failures to provide propulsion function are what roll-up to the top-level hazard. The unique DE/HEP aspects of the propulsion system, the electronics that control the motor, the motor itself, batteries, thermal management system, and charging system were captured in the FTA. Systems that may be shared between propulsion and flight controls (e.g., rotor speed and collective pitch) are examined only in their contribution to the top level loss of propulsion hazard. Loss of multiple propulsors may cause control problems that are considered a part of the loss of propulsion top level hazard.

The top level hazards defined from the propulsion system FHA were used to inform the top level of the fault tree. The FTA was done to a level of detail sufficient to show architectural impacts to the top-level hazard. The FTA may capture system effects that roll up to higher losses of functions captured in the FHA.

The FTA's performed for this study used a series of "AND" and "OR" gates to build the fault tree architecture in Reliability Workbench (RWB) (ref. 18). The symbols used in the associated fault tree diagrams are shown in Figure 27. RWB calculates the output of the "AND" and "OR" gates as shown in Equations (1) and (2), respectively. Equations (1) and (2) use the three (3) input examples shown in Figure 27, but more inputs may be applied by adding terms.

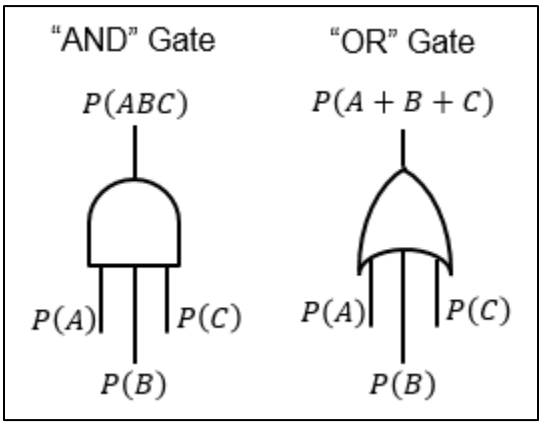


Figure 27: "AND" and "OR" Gate Symbols

$$P(ABC) = P(A) * P(B) * P(C) \quad (1)$$

$$P(A+B+C) = P(A) + P(B) + P(C) - P(A) * P(B) - P(A) * P(C) - \\ -P(B) * P(C) + P(A) * P(B) * P(C) \quad (2)$$

The Tilt-Wing Fault Tree Diagram may be found in Appendix C with a summary provided in Table 9 of the top level hazard, Branch ID #1, and the 2nd tier hazards, Branch ID #2-6. The FTA predicts 5.95 X 10^{-4} failures per flight hour for the Tilt-Wing.

Table 9: Tilt-Wing FTA Summary

Branch ID	Description	Failure Rate per Flight Hour
1 (Top Level)	**Loss of Power Transmission**	**5.95 X 10^{-4}**
2	Dual Electric Motor Fail	1.03 X 10^{-5}
3	Dual Gearbox Fail	1.50 X 10^{-10}
4	OEI Propulsion Loss	5.53 X 10^{-4}
5	Complete Propulsion Loss	1.32 X 10^{-4}
6	Dual ESC Fail	1.20 X 10^{-5}

The Quad-Rotor Fault Tree Diagram may be found in Appendix D with a summary provided Table 10 of the top level hazard, Branch ID #1, and the 2nd tier hazards, Branch ID #2-4. The FTA predicts 2.10 X 10^{-4} failure per flight hour for the Quad-Rotor.

Table 10: Quad-Rotor FTA Summary

Branch ID	Description	Failure Rate per Flight Hour
1 (Top Level)	**Loss of Power Transmission**	**2.10 X 10^{-4}**
2	Dual Electric Motor Fail	1.06 X 10^{-5}
3	OEI Propulsion Loss	2.00 X 10^{-4}
4	Loss of Ability to Drive a Rotor	4.01 X 10^{-16}

The Alternate Configuration Quad-Rotor, in which the interconnecting shafts are removed from the vehicle, Fault Tree Diagram may be found in Appendix E with a summary provided Table 11 of the top level hazard, Branch ID #1, and the 2nd tier hazards, Branch ID #2-4. The FTA predicts 7.97 X 10^{-4} failure per flight hour for the Alternate Configuration Quad-Rotor, which is roughly four (4) times less safe than the baseline Quad-Rotor.

Table 11: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FTA Summary

Branch ID	Description	Failure Rate per Flight Hour
1 (Top Level)	**Loss of Power Transmission**	**7.97×10^{-4}**
2	Dual Electric Motor Fail	1.06×10^{-5}
3	OEI Propulsion Loss	2.00×10^{-4}
4	Loss of Ability to Drive a Rotor	7.97×10^{-4}

The Lateral-Twin Fault Tree Diagram may be found in Appendix F with a summary provided Table 12 of the top level hazard, Branch ID #1, and the 2nd tier hazards, Branch ID #2-5. The FTA predicts 1.92×10^{-4} failure per flight hour for the Lateral-Twin.

Table 12: Lateral-Twin FTA Summary

Branch ID	Description	Failure Rate per Flight Hour
1 (Top Level)	**Loss of Power Transmission**	**1.92×10^{-4}**
2	Dual Engine or Motor Fail	1.32×10^{-8}
3	OEI Propulsion Loss	1.66×10^{-4}
4	Loss of Ability to Drive a Rotor	1.00×10^{-5}
5	Either Interconnecting Shaft Fails	6.86×10^{-6}

The Lift+Cruise Fault Tree Diagram may be found in Appendix G with a summary provided Table 13 of the top level hazard, Branch ID #1, and the 2nd tier hazards, Branch ID #2-4. The FTA predicts 2.88×10^{-4} failure per flight hour for the Lift+Cruise.

Table 13: Lift+Cruise FTA Summary

Branch ID	Description	Failure Rate per Flight Hour
1 (Top Level)	**Loss of Power Transmission**	**2.88×10^{-4}**
2	Dual Rotor Loss	6.25×10^{-6}
3	Reduced Pitch Force	4.91×10^{-8}
4	Out of Battery Charge	1.80×10^{-4}

10 DISCUSSION

10.1 Configuration

Many assumptions were made during the initial sizing and development of the NASA RVLT Concept Vehicles, which is common practice in airplane sizing iteration loops. As they apply to this study, technology factors were applied to all major sub-systems.

As an example, the installed specific energy of batteries was assumed to be 400 Wh/kg, which, with usage and installation effects, means that the battery cell's specific energy is roughly 650 Wh/kg (ref. 2). The NASA RVLT Team has noted that current cell specific energy is 240 Wh/kg leading to installed specific energy or 93.3 Wh/kg.

As can be seen in the battery example, there is a large technology gap between currently available commercial-off-the-shelf (COTS) products and some of the assumptions in the sizing of the NASA RVLT Concept Vehicles. COTS equipment and weight/volume information was compiled for the powertrain configurations described in Section 5. The following includes a discussion on COTS engines and weight and volume estimates for motors, generators, inverters, and rectifiers used in the RVLT Concept Vehicle powertrain configurations. The impacts that motor, generator, inverter, and rectifier designs have on the Thermal Management System are also discussed.

A variety of COTS engines are capable of providing the design power requirements used in the NASA RVLT Concept Vehicle sizing iterations. NASA used COTS turboshaft engine decks from the CTS800, Allison 250-C40B, RR300, and Allison 250/T63-A-5 to scale engine parameters during airplane sizing loops. Additionally, an Advanced Affordable Turbine Engine (AATE) model was used. The GE T901 was named the winner of the competitive Improved Turbine Engine Program (ITEP), which succeeded the AATE Program. The GE T901 has an expected Entry into Service (EIS) of 2025.

The Tilt-Wing included one (1) turboshaft engine to power the generator. Based on an efficiency of 80.6% (assuming 95% efficiency of each generator, rectifier, inverter, and motor and 99% electrical power transmission efficiency), the turboshaft engine needed 4,730 HP for takeoff. The T55-GA-714A is rated for 4,777 HP takeoff power at an output shaft speed of 15,066 RPM (ref. 19).

The Lateral-Twin included two (2) 187 HP turboshaft engines. The RR300 engine makes 240-300 HP but, the forward facing output gearboxes included may make lightweight integration into the Lateral-Twin nacelles difficult due to concerns related to spatial integration, aircraft center of gravity, and induced loads on the struts supporting each rotor. It was assumed that a modified RR300 could be utilized in which the power turbine output speed was roughly ~40,000 RPM. The RR300 is based on the Allison 250 which has a variety of configurations with different gearboxes and power turbine speeds. The Allison 250-C30G/2 was found to have a takeoff rating of 557 HP, gearbox output speed of 9,545 RPM and power turbine output speed of 30,737 RPM (ref. 20). The rotating system schematic may be updated with the appropriate power turbine (or gearbox output speed) in the future once an engine selection has been completed.

The Lift+Cruise included one (1) turboshaft engine to power the generator. Based on the same 80.6% efficiency as the 15 passenger Tilt-Wing, the turboshaft engine of the six (6) passenger Lift+Cruise required takeoff power of 3,376 HP. The T55-GA-714A would meet the power requirement, but may be too large for the application. The GE T901 may be a good candidate engine for this application; however, this engine is still under development and is likely not going to be available for commercial applications. The Safran Aneto-1K may also be a good candidate, as it

is a commercial engine that began flight testing in 2017 (ref. 21); publically available takeoff power could not be found at this time, but takeoff power is expected to be near the 3,000 HP mark.

A variety of COTS motors, generators, inverters and rectifiers are available, but reliability data is not generally available for these COTS components, particularly for rotorcraft applications. Motor and generator weight may be estimated using the NDARC parametric motor weight model with an application factor of 1.1 applied to generator weight.

$$W = .5382kQ^{.8129} \tag{3}$$

Where: W = weight (lbs);

k = application factor (1.0 for motors, 1.1 for generators);

Q = peak torque (ft-lbs).

The weight of the inverter and rectifier can be assumed to be directly related to power output. COTS inverters and rectifiers may be found for 10 kW/kg, but more advanced inverters and rectifiers may be obtained with 15 kW/kg.

The volume of permanent magnet synchronous motors (PMSM) is proportional to their torque output (ref. 22), so a convenient method to estimate the volume of the PMSM is analytically derived. Output torque, Q (ft-lbs), of a PMSM can be estimated from the following relationship:

$$Q = 288V_r\sigma \tag{4}$$

Where: σ = estimated shear stress capability of electric machine (psi);

V_r = volume of the PMSM rotor (ft^3);

$$V_r = \frac{\pi}{4}{D_r}^2 L \tag{5}$$

D_r = outside diameter of rotor (ft);

L = stack length (ft).

However, the diameter of the rotor, D_r, is not the outer diameter of the electric machine. The outer diameter of the electric machine is essentially the outer diameter of the stator, D_s. The outer diameter of the stator, D_s, and the diameter of the rotor, D_r, may be related through the number of pole pairs, p, as follows in Equation (6) (ref. 22):

$$D_s = D_r\left(\frac{\pi}{5p} + \frac{1}{.7}\right) \tag{6}$$

Plugging Equations (5) and (6) into Equation (4), rearranging to solve for D_s, and assuming that $L = 1.28*D_s$, we obtain:

$$D_s = \left[\frac{4kQ}{\pi 368.64\sigma}\left(\frac{\pi}{5p} + \frac{1}{.7}\right)^2\right]^{1/3} \tag{7}$$

Reasonable estimates for estimated shear stress capability of the electric machine, σ, range from 3 psi (20.7 kPa) to 5 psi (34.5 kPa) (ref. 22). The number of pole pairs will vary between designs, but at least three (3) pole pairs are recommended for reliability, so that if one (1) pole pair shorts, it may be disconnected and operation of the electric motor may continue at reduced power levels. Designers may find that higher pole pairs are necessary if designing a motor to lose one (1) pole pair and continue to operate; as an example, torque ripple may be high for a motor with only two (2) of its originally designed three (3) pole pairs functioning.

The volume of inverters and rectifiers are not as easy to estimate through analytical means, so an industry survey was performed. 27 inverters and rectifiers were used to develop a relationship

between design rated power (kW) and volume (m^3). Figure 28 shows this relationship and Equation (8) shows the associated equation for Volume, V, as related to electrical power, P. Note, power, P, is in kilowatts, volume, V, is in cubic meters, and the application factor, k, is 1.0 for inverters, and 1.1 for rectifiers.

$$V = k * 3 \times 10^{-5}(P)^{1.3275} \tag{8}$$

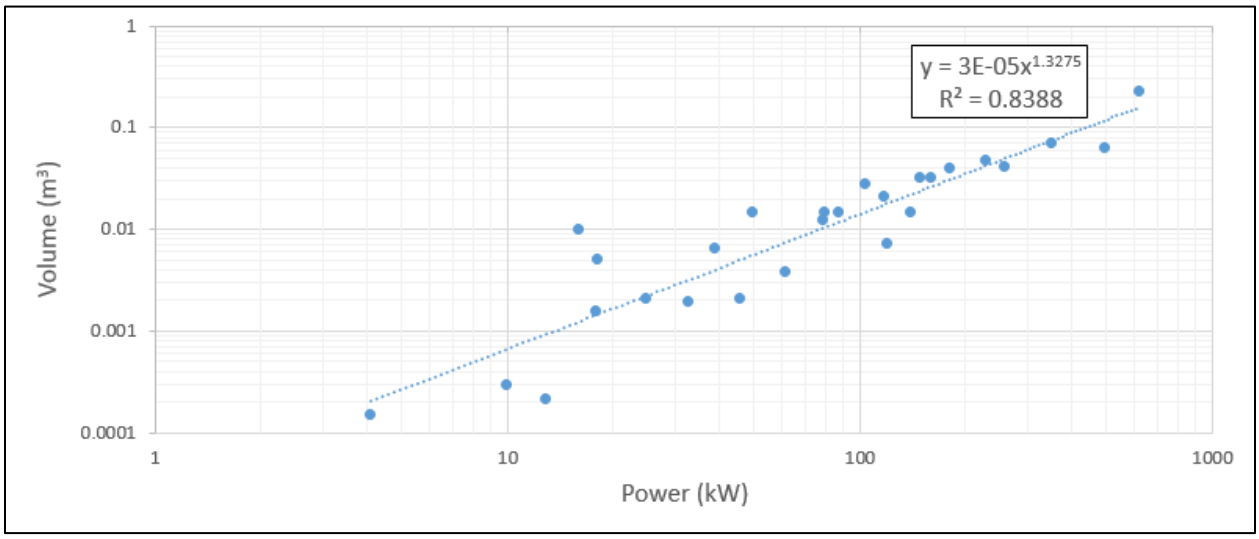


Figure 28: Relationship of Power to Volume for Inverters and Rectifiers.

Table 14 shows the estimated weights and volumes for the motors, generators, inverters, and rectifiers for each RVLT Concept Vehicle. Each motors assumed a 2.5 psi design shear stress, σ, and eight (8) pole pairs and the length, L, to be 1.28 times the stator diameter, D_s.

Wire weight may be estimated easily via calculating ampacity requirements for a given power and voltage and selecting the appropriate wire gage. SAE AS50881 (ref. 23) provides ampacities for a given wire material and gage and derating factors for bundling and altitude. Wire weight depends heavily on the length of the wire run.

The weight of the Thermal Management Systems can depend heavily on the efficiency of the motors, generators, inverters, and rectifiers selected. In the case of the powertrain configurations described in Section 5 the motors and generators are cooled by a mechanically driven cooling system to reduce vehicle weight. However, the size of the pumps, heat exchangers, and cooling fans will be driven by the efficiency of the motor/generator. Likewise, the fans used to air-cool the inverters and rectifiers will be sized by the efficiency of the inverters/rectifiers. The weight of the Thermal Management System is sensitive to the efficiencies of these components. An efficiency of 92% as opposed to 96% would result in doubling the size, and therefore weight, of thermal management system components.

Table 14: Weight and Volume Estimates for Motors, Generators, Inverters, and Rectifiers.

	Description	Tilt-Wing	Quad-Rotor	Lateral-Twin	Lift+Cruise "Lifters"	Lift+Cruise "Propulsor"
Design Parameters	Generator Power (HP)	3,445	-	100	1,355	
	Generator Shaft Speed (RPM)	14,999	-	15,002	20,000	
	Generator Torque, Q (ft-lbs)	1,206	-	35	356	
	Rectifier Power, P (HP [kW])	3,273 [2,440]	-	112 [83]	1,287 [960]	
	Inverter Power, P (HP [kW])	777 [580]	94 [70]	106 [79]	749 [558]	474 [354]
	Total Motor Power (HP)	2,924	88	100	704	446
	Motor Power (HP)	731	22	100	88	446
	Motor Speed (RPM)	14,999	11,863	15,000	18,160	9,080
	Motor Torque, Q (ft-lbs)	256	10	35	25	258
Weight Estimate	Electric Generator Weight (lbs)	189.3	-	10.7	70.2	
	Rectifier Weight (lbs)	358.7	-	12.3	141.1	
	Inverter Weight (lbs)	85.2	10.3	11.7	82.0	52.0
	Electric Motor Weight (lbs)	48.8	3.4	9.7	7.5	49.1
Volume Estimate	Design Shear Stress, σ (psi)			5.0		
	Number of Pole Pairs, p			12		
	Electric Generator Volume (ft^3)	2.021	-	0.059	0.596	
	Rectifier Volume (ft^3)	36.587	-	0.414	10.600	
	Inverter Volume (ft^3)	4.933	0.297	0.352	4.693	2.560
	Electric Motor Volume (ft^3)	0.390	0.015	0.053	0.039	0.393

10.2 Reliability/Safety Analysis

Results from the reliability and safety analysis are summarized in Table 15. Review of the FMECA, predominantly used in reliability analysis, and the FTA, predominantly used in safety analysis, shows good correlation between the two methods. The FMECA could be used in conjunction with the expertise of an experienced analyst to estimate the safety of a given vehicle architecture. The FTA, however, uses data from supporting reliability analysis and draws the connectivity between systems and functions to perform a top-down safety analysis.

Table 15: FMECA and FTA Summary.

NASA RVLT Concept Vehicle	Propulsion System Description	Flight Control Description	Variable Pitch, Fixed Speed	Fixed Pitch, Variable Speed	Severity Code I Failures per Flight Hour		Percent Time in OEI/OMI Avoid Region
					FMECA Criticality	FTA Reliability	
Tilt-Wing	Series Hybrid	Collective and 1-Axis Cyclic	X		4.92×10^{-4}	6.95×10^{-4}	20%
Quad-Rotor	All Electric	Collective Only	X		2.47×10^{-4}	2.10×10^{-4}	25%
Quad-Rotor (No Shafts)	All Electric	Collective Only	X		1.01×10^{-3}	7.97×10^{-4}	20%
Lateral-Twin	Parallel Hybrid	Full Cyclic and Collective	X		9.65×10^{-5}	1.91×10^{-4}	20%
Lift+Cruise	Series Hybrid	RPM Controlled		X	4.67×10^{-4}	2.88×10^{-4}	**0%**
EASA Draft SC-VTOL-01	Proposed Air-Vehicle Requirement				10^{-9} (1)	10^{-9} (1)	–

Note:

1) Air-vehicle level requirement. Propulsion system will likely need to be 10^{-10} or higher to meet proposed SC-VTOL-01 requirements.

Due to the good correlation of the FMECA and FTA, the concept vehicles analyzed displayed similar trends from one analysis method to the other. The Lateral-Twin resulted in the best (lowest failure rate) reliability, due to the architectural decision to have two (2) turboshaft engines mechanically connected to the rotor system. The Quad-Rotor had the next best reliability, followed by the Lift+Cruise, then the Tilt-Wing, then, finally, the Quad-Rotor without cross shafting.

A common theme between all configurations is that sub-system reliability within the propulsion system (and thereby vehicle safety) must be improved in order to meet anticipated regulations, such as the EASA draft SC-VTOL-01. Corresponding safety objectives for subsystems and components that make up the aircraft would be developed from the application of the processes outlined in ARP4761 and ARP4754 (ref. 17, 24), as exemplified by the analysis in this report. FTAs and Failure Modes and Effects Analysis (FMEAs) are developed from aircraft design information such as functional block diagrams and system schematics. FTA results are compared with aircraft safety objectives – any discrepancies are addressed with design updates, and so on as the whole process iterates until convergence. In the end, a set of subsystem and component reliability requirements designed to meet aircraft-level specifications is generated. As alluded to in this report, it is a general rule of thumb that the subsystems needs relatively higher reliability than the aircraft level objective in order to meet the aircraft-level objective; it is likely that the propulsion system would need to have 10^{-10} failure rates per flight hour, or less, in order to meet the EASA Draft SC-VTOL-01 air vehicle requirement of 10^{-9} catastrophic failures per flight hour.

The reliability of the Tilt-Wing, Quad-Rotor, and Lateral-Twin was closely coupled to the assumption that each vehicle spends 1/5 to 1/4 of its mission duration within the OEI or OMI avoid region. The Lift+Cruise was assumed to not have an OEI or OMI avoid region in accordance with NASA's guiding principles behind the Lift+Cruise configuration, "Multicopter-style redundancy can be employed to deal with failures in the lifting system. Any number of rotors greater than 6 allows a fairly simple and manageable continuation of controlled 6 degree-of-freedom flight," (ref. 3).

Avoid regions are developed for all FAA certified airplanes. Avoid regions may include spatial restrictions, such as altitude, airport, or airspace restrictions, time-based restrictions, such as night operations, weather restrictions, gross weight restrictions, or power restrictions, among others. OEI and OMI avoid regions are restrictions based on power-available, altitude, forward airspeed, and vehicle gross weight. Complex, multivariable analysis is required to define the OEI/OMI avoid region for a given air vehicle. Mission spectrum plays a role in developing the OEI/OMI avoid region and it is foreseeable that OMI/OEI power available may be derived from a desired OEI/OMI avoid region profile. Figure 29 shows an example height-velocity chart to illustrate how an avoid region may be avoided through airplane design and mission planning.

Mission planning, in/out of ground effect hover (IGE/OGE), and airport, heliport, or vertiport instrument take-off ratings may be incorporated into the airplane design mission so that a conventional airplane (non-DPFC/DP) does not spend time within an OEI/OMI avoid region. In example, losing power IGE provides a manageable situation for a trained, certified pilot to land the aircraft in a controlled manner in-which risk to occupant safety is low. However, for this study a conservative estimate of time spent in the OEI/OMI region was assumed since the airplane performance in all flight regimes was not yet defined.

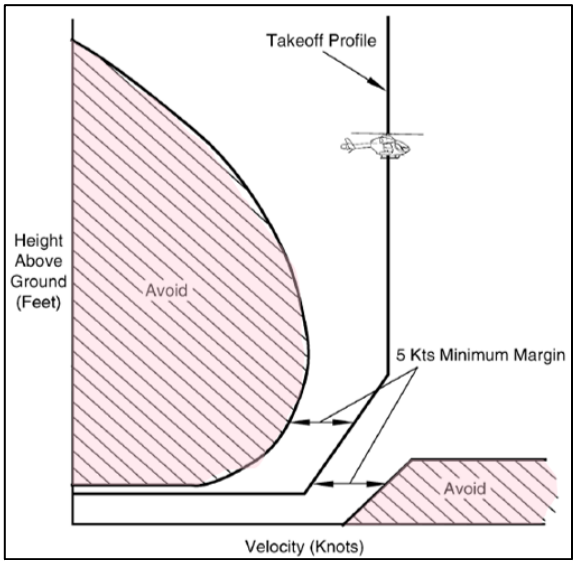


Figure 29: Example Height Velocity Chart Illustrating Takeoff Profile that Does Not Enter Avoid Regions.

A sensitivity analysis was performed to assess the impacts of time spent in OEI/OMI avoid region on the safety of the vehicle within its intended mission. The Lateral-Twin was used to perform the sensitivity study. The "In OEI Avoid Region" event probability was adjusted from 0.2 to 0.0. Appendix F includes the baseline FTA for the Lateral-Twin and Table 16 presents the results. Note that an event probability of .20 correlates to 20% time spent in the OEI/OMI avoid region, .10 to 10%, etc. The mission duration was calculated to be 60.6 minutes, which includes two (2) legs of two (2) minutes hover on takeoff, 26 minutes of cruise, and two (2) minutes of hover on landing (ref. 2).

It was found that nearly an order of magnitude safety improvement was obtained by adjusting the time spent in the OEI/OMI avoid region. A graph of the results, Figure 30, shows a roughly linear relationship between failure rate and 0% to 20% time spent in the OEI/OMI Avoid Region.

It is believed that as the design of these vehicles mature, that the OEI/OMI Avoid Region would be reduced from the values shown for the Tilt-Wing, Quad-Rotor, and Lateral-Twin. Additionally, it is believed that the Lift+Cruise air vehicle will have an OMI/OEI avoid region, reducing the inherent safety of the vehicle. Avoid regions for all of the NASA RVLT Concept Vehicles under consideration for future work should be developed in order to more accurately assess the safety of the configuration against its intended mission.

Table 16: Sensitivity Study Summary – Failures per Flight Hour Against Time in OEI/OMI Avoid Region for Lateral-Twin Air-Vehicle.

Percent Time in OEI/OMI Avoid Region	Time in OEI/OMI Avoid Region	Failures per Flight Hour FTA Reliability
20%	12.1 minutes	1.91×10^{-4}
10%	6.1 minutes	1.09×10^{-4}
5%	3.0 minutes	6.80×10^{-5}
3.25%	2.0 minutes	5.16×10^{-5}
2%	1.2 minutes	4.33×10^{-5}
1%	0.6 minutes	3.51×10^{-5}
0%	0.0 minutes	2.69×10^{-5}

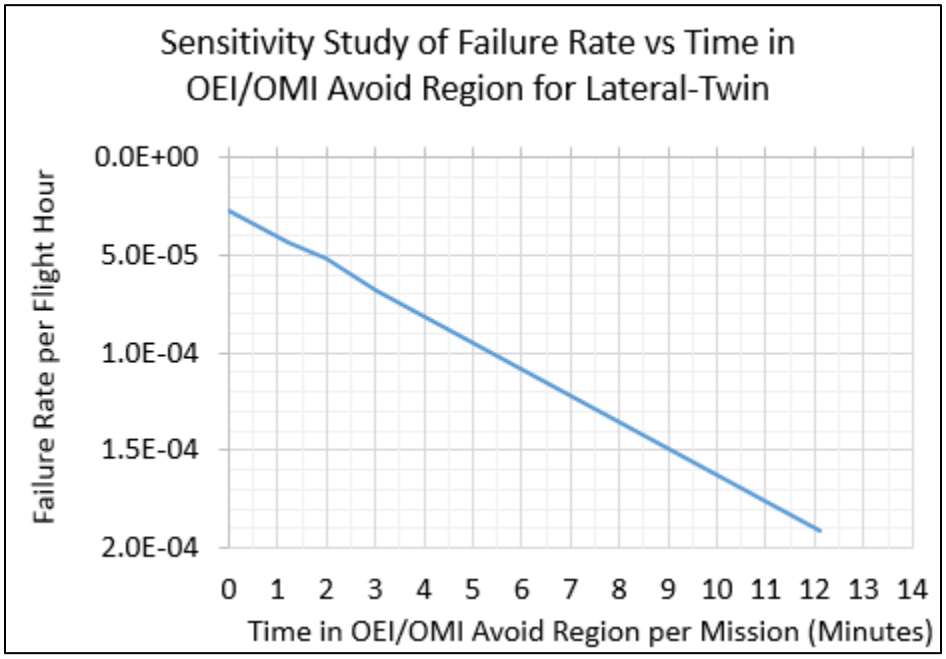


Figure 30: Sensitivity Study of Failure Rate vs Time in OEI/OMI Avoid Region for Lateral-Twin.

10.3 Reliability Metrics for the UAM Mission

The UAM operator concepts are looking to operate high frequency, high density routes over and around major metropolitan areas and presents routes in the vicinity of 15 minutes in duration covering distances up to 50 miles as nominal cases for operation (ref. 4). UAM operational concepts are also looking to provide this service in high frequency in order to make it economically viable (ref. 4). As mentioned in section 3.1, the UAM community points to the consideration of Part 135 as the closest FAR specification that applies to the UAM operational model. Furthermore, the authors of the document specify a target of no more than 0.3 fatalities per 100 million passenger

miles as the design requirement (this equates to a rate of 10^{-8} catastrophic failures per operational hour). This target, the report claims, is four times better than Part 135 fatality rates. For a representative UAM aircraft the EASA proposed special condition specifies a rate of 10^{-9} catastrophic failures per operational hour. Furthermore, ARP94910, specifies a Vehicle Management System (VMS) reliability metric for a representative sized aircraft to be designed with a catastrophic failure rate of 10^{-8} (per operational hour). This equates to approximately a rate of 10^{-7} catastrophic failures per operational hour at the aircraft level. As observed there is a significant variability in the guidelines presented in various pertinent documents with respect to reliability metrics. See Section 3.1 for more supporting evidence related to variability in available specifications and potential gaps in coverage.

Recently there has been a flood of activity in industry (ref. 25), academia and government labs alike around similar operational concepts as the UAM model. As with the introduction of any commercial aircraft there needs to be design guidance available which are reviewed and maintained by civil organizations that cover vehicle and sub-system level reliability specifications. The UAM community specifically identifies DE/HEP VTOL aircraft types as the choice of configuration to support their operational model. Therefore, it is recommended that there be a significant focus on development of regulations and associated design guidelines to cover operations of UAM vehicles with DE/HEP configurations operating in/around congested and/or rural areas with no more than six on-board passengers or crew. While there is a possibility to use vehicles with capacity for more than 6 passengers to be viable for the UAM type concept, given the current state of DE/HEP concepts there is plausibly less urgency to fully address this category. Furthermore, guidance for scheduled transport-category DE/HEP VTOL aircraft carrying more than six passengers could more suitably leverage existing regulations and regulations developed UAM vehicles of 6 people of less.

11 CONCLUSIONS

The primary objective of this research effort was to identify failure modes and hazards associated with the concept vehicles and to perform FHA and FMECA for each. More specifically, this research was successful in accomplishing the following objectives:

- To perform a conceptual design of the powertrain configuration for each configuration, in as much detail as is necessary to conduct subsequent elements of this research.
- To create functional block diagrams from each of the conceptual powertrain configurations in order to facilitate the FHA and FMECA.
- To identify potential hazards and perform a FHA for each configuration.
- For each configuration, identify and quantify the effects of the identified hazards, the severity and probability of their effects, their root cause and the likelihood of each cause.
- To discuss guidelines for development of reliability targets to compare the results contained herein against a benchmark and to enable the certification of similar UAM air-vehicle concepts.

As part of a cursory industry search it was determined that available vehicle reliability/safety requirements are not well suited for the UAM mission. It was also found that currently small Unmanned Aerial Vehicles (UAV's) are grouped with large, passenger carrying vehicles. However, this could unnecessarily prohibit the use of small UAV's and, therefore, should not be grouped with people-carrying, large vehicles. Momentum based requirements would help distinguish the difference between a 50 lbs vehicle a few hundred feet overhead, as compared to a 4,000 lbs vehicle thousands of feet overhead. Subtle differences, like the variability in size of vehicle, may make it difficult to extend an existing FAR for the UAM Mission. Vehicles for the UAM mission will likely require their own FAR.

Powertrain configurations were developed to support the FHA/FMECA process. A total of four (4) distinct configurations were developed with an alternate configurations for the Quad-Rotor Concept Vehicle in which interconnecting shafting was not utilized. Connectivity between each system of components was developed in order to support development of functional block diagrams. Approximate weights and sizes were provided in Table 14.

Historical data and industry accepted environmental factors were used to generate reliability numbers for components in this study. The electrical components utilized in the various architectures were the drivers for the reliability/safety analysis using the noted historical reliability numbers and the applied environmental factors. Reliability improvements may be made by placing inverters and rectifiers in parallel, but adjustments to the weight trends must be made in order to account for the fail-safe inverter and/or rectifiers. Reliability improvements are likely able to be made to electric motors and generators, but it is unlikely that a motor or generator will meet reliability requirements for the UAM mission. Similar to inverters and rectifiers, motors and generators will likely need to be placed in fail-safe architectures to increase vehicle safety to acceptable standards.

The FMECA's performed on the subject vehicles found that the Tilt-Wing, Quad-Rotor, and Lateral-Twin criticality numbers were all driven by the applied failure rates of the motors and inverters. In the case of the Tilt-Wing, the turbogeneration function had similar criticality to the electrical energy conversion to shaft torque function. The criticality of the turbogeneration function was driven by the reliability of the generator and rectifier. The sensitivity study performed on the

Quad-Rotor with and without interconnecting shafts yielded an order of magnitude lower reliability when interconnecting shafting was not included in the vehicle architecture. The Lift+Cruise Category I Functions all had similar 10^{-4} criticality numbers to that of the Tilt-Wing, Quad-Rotor, and Lateral-Twin concept vehicles.

The reliability of the Tilt-Wing, Quad-Rotor, and Lateral-Twin was driven by the assumption that each concept vehicle spent 20% time in the OEI/OMI avoid region. In the case of the Alternate Configuration Quad-Rotor, the reliability was driven by the motor/inverter reliability. An additional finding is that adding more rotors to the Quad-Rotor would not improve the reliability. Lift+Cruise reliability was driven by the Category I loss of the turbogeneration unit.

Overall, the FMECA and FTA agreed with one-another, showing similar criticality and reliability, respectively. The assumption that the Tilt-Wing, Quad-Rotor, and Lateral-Twin spent 20% of their time in the OEI/OMI avoid region may be conservative and, conversely, the assumption that the Lift+Cruise does not have an OMI avoid region is likely optimistic.

12 LESSONS LEARNED & RECOMMENDATIONS

12.1 Lessons Learned

This study has shed light on many different challenges ahead of the UAM community. Following the current UAM industry trend, the reliability and safety assessment process was underestimated. Reliability and safety assessment were performed with results that can be used to guide architecture changes, but the time and resources allotted to perform the work proved challenging. This is a new challenge, though, and processes and tools are being developed to improve the reliability and safety assessment process, particularly early in the conceptual design phase.

Challenges that most in the UAM community are familiar with relate to range, speed, and payload. Design decisions and technology development associated with 400Wh/kg batteries or power-dense electronics plague the UAM configurator as business cases must be closed and novel architectures must be developed to create competitive advantages in an over-crowded marketplace.

However, this study has uncovered an entirely new set of challenges, which the already burdened UAM configurator must attend to. Safety of UAM vehicles must be improved in order to both enter and maintain a UAM industry. The good news is that the UAM configurator should not be traveling this path alone; regulators, government agencies, and even sub-system suppliers should be sharing the burden of safety from the regulatory requirements to the sub-system reliability. However, no amount of component reliability will overcome architecture decisions made by the configurator if vehicle configuration that is inherently unsafe.

This is where the challenge in safety exists today; incorporating robust reliability and safety assessments early in a programs infancy, which follows ARP4751 and ARP5754 guidance (ref. 17, 24), in order to develop inherently safe architectures. Reliability and safety assessment needs to be performed early, at an air-vehicle functional level in order to drive clear requirements into the sub-system architecture and into the component.

Elements of the mission that affect safety should be defined early, so that power demands and handling qualities can be designed to meet mission objectives safely. One large contributor to safety as related to the mission profile is the time spent in the OEI/OMI avoid region. Focusing on the macro aircraft functions, as opposed to component configurations early in the program would help derive requirements that could be used by the appropriate component design teams.

Developing safety requirements early will be key in future development of the NASA RVLT Concept Vehicles and is likely plaguing the UAM community. By developing the functional requirements the component designers can then use that information to develop reliable components that reside in inherently safe architectures. As can be seen from the results shown, commercially available components required for DE/HEP systems are not readily available with adequate reliabilities. Bespoke, application specific component design efforts are likely required for each application considering DE/HEP configurations, and the reliability of those application specific designs should be demonstrated through a rigorous design, analysis, and test approach in which reliability and safety are intertwined.

12.2 Recommendations – Operational Requirements

It is clear that new FAA advisories, as well as standard industry guidance and specifications are needed to provide a path for certification of the wide spectrum of DE/HEP aircraft classes and reliability guidance dependent on usage (e.g., airspace, passengers on board, weight and/or speed) and levels of autonomy (e.g., from automated systems assisting pilots to supervised autonomy).

Therefore, careful consideration needs to be established to allow affordable development of future avionics and propulsion systems and to guide industry in the design of safe and reliable aircraft platforms to operate in National Airspace under FAA and ICAO regulations.

The operational vehicle momentum is intended to capture the variation of aircraft size and operational speed as it can be interpreted from the National Transportation Safety Board (NTSB) data depicted in Figure 31. Boeing recommends a robust characterization approach when developing design guidelines for these type of aircraft. In particular, the guidelines framework should be developed to provide discretization based on operational vehicle momentum, operational altitude, payload type (passenger/freight), operational airspace and operational states. This variation is important as it can provide a metric to ascertain the impact to bystanders due to catastrophic failures at the aircraft level. For example consider a relatively heavy freight carrying vehicle operating at a cruise speed of 40 knots, compared to a mid-gross weight passenger carrying vehicle operating at 100 knots. These two aircraft look and operate differently but may have similar energy and momentum impacts to people and property on the ground in the event of a mishap. Similarly, operational altitude should be used to set safety requirements because aircraft operating at higher altitudes have more potential energy that could translate to destructive potential on the ground if catastrophic aircraft propulsion failure occurs. Whether an aircraft carries paying-passengers or cargo only should have a bearing on safety requirements because, other factors being the same, vehicles carrying passengers should be held to higher safety standards than vehicles that only carry freight. Operating airspace should influence DE/HEP aircraft safety requirements by accounting for reduced impacts from catastrophic failures in sparsely populated areas, and vice versa. In contrast with general aviation flight patterns with aircraft regulated by FAR Part 23 and hub-and-spoke route patterns, UAM flight patterns are expected to operate much higher frequency air taxi traffic in point-to-point routes. For congested areas, there will likely be the assumption that ground-air transitions occur at prepared zones, i.e. no operation to/from street and road traffic. Possible ways to parameterize this dimension include normalizing airspace to the number of expected passengers flying overhead, or simply using ICAO airspace classes. Finally, the use of operational states discretizes the reliability requirements for a given aircraft class (momentum, altitude, payload, operating airspace) as a function of failure consequence or criticality. For example, ARP94910 defines a range of FCS operating states from ‘Normal Operation’ to ‘Loss of Control’ and assigns more stringent requirements on failures resulting in more degraded end states.

The defense industry, government and industry, has already published recommended guidance for safety and reliability of flight controls system presented in ARP94910 that include a diverse set of usage and operational environments. However, Boeing suggests that there are gaps in the guidance and specifications of sensory and algorithms for unmanned operations. These gaps can be addressed by the development of an Aerospace Recommended Practice and/or a Guidance Document to address development of Critical Sensory Systems, as well as Guidance for the Sensory Development Life-Cycle similar to, but not replacement of DO-297 and DO-178.

This can be considered by the FAA for such systems and tailored by means of Advisory Circulars and complementary industry guidance or requirements documents. Boeing suggests that the FAA could use ARP94910 as a starting point for development of Flight Controls for new civil unmanned/autonomous aircraft. Figure 32 depicts a recommended framework of documents that can be used as a plan for definition of certification. In Figure 32, dashed lines represent ties of certification requirements and guidance, as well as requirements down flow from ARP94910/ARP4754 for development of safety aspects of software and firmware (DO-297, DO-

254 and DO-178). In addition, Boeing has been in contact with NAVAIR in Patuxent River, Maryland with the idea to add a document(s) to address a void in safety requirements for sensors that will be used to make autonomous decisions, where resolution of time-critical Byzantine Faults cannot be achieved with redundancy. Sensors such as IMUs, LIDARs, RADARs, Electro Optical Cameras, and Infrared Cameras are designed with the assumption that a Pilot will detect a sensor failure. However, for UAVs, software will be required to detect time critical failures that cannot be identified/detected by a human, or where timing is not sufficient to request resolution from operator control stations. Boeing has also engaged the US Army and Helicopter industry to collectively participate in an endeavor to develop design and certification guidance for such sensors and flight-critical algorithms through the SAE-International organization, under the A6 group responsible for Flight Controls. Boeing plans to submit a proposal to SAE-International to work on such effort to address this underlying guidance, navigation and controls problem.

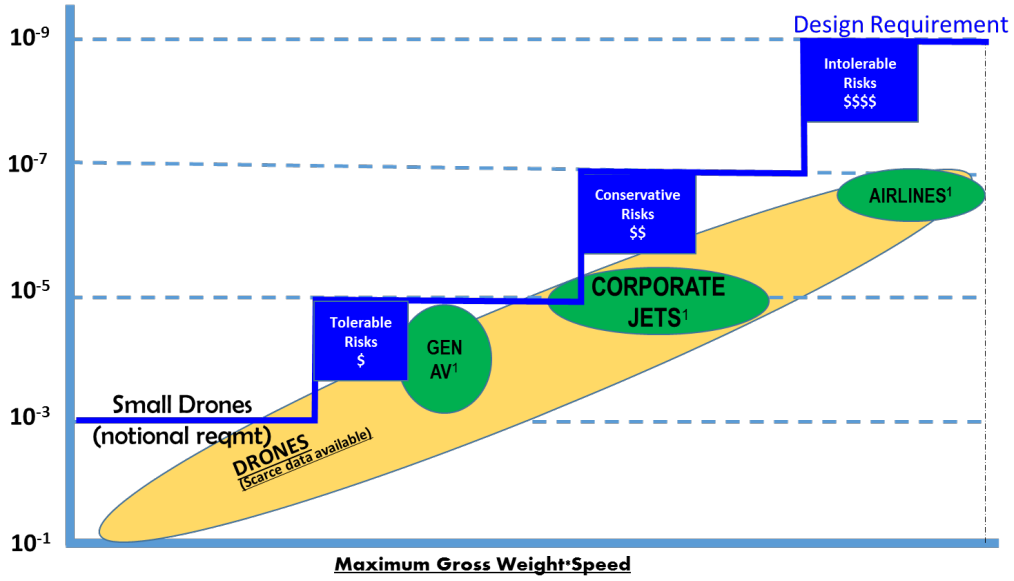


Figure 31: Depiction of Loss-of-Function Reliability vs GVW vs Fleet Type.

In addition, as the propulsion system for some aircraft configurations is all-electric and/or RPM controlled, a designer will need to consider the safety effect of a propulsion thruster failure within the guidance of the FHA in accordance with ARP4754. Such consideration should include the assignment of the motor as part of flight controls or as part of the propulsion system. Such a matter needs to be considered when it is determined that the safety-reliability assessment indicates that a single (or a set of) thruster require the level of scrutiny that a flight controls design architecture or component undertakes. This detail is brought up as an outcome of several debated conversations on this topic during the analysis of the configurations within this program: that is, which technology branch should own the motor when one (or a specific combination of) thruster configuration failure can cause a catastrophic event. Boeing encourages the FAA to have participation or monitoring in this activity, since such development/dialog benefits industry and airworthiness agencies (Department of Defense (DOD), FAA, EASA, etc.) in the process to align usage within Military specifications and Civil Airspace certifications, and therefore safety within airspace usage. This approach is attainable, but will require a rigorous dialog between airworthiness and safety organizations, in order to force comprehensive industry analyses of the different development aspects of the vehicle-systems and mission-systems architectures, functions, and sensors, as it relates to safety.

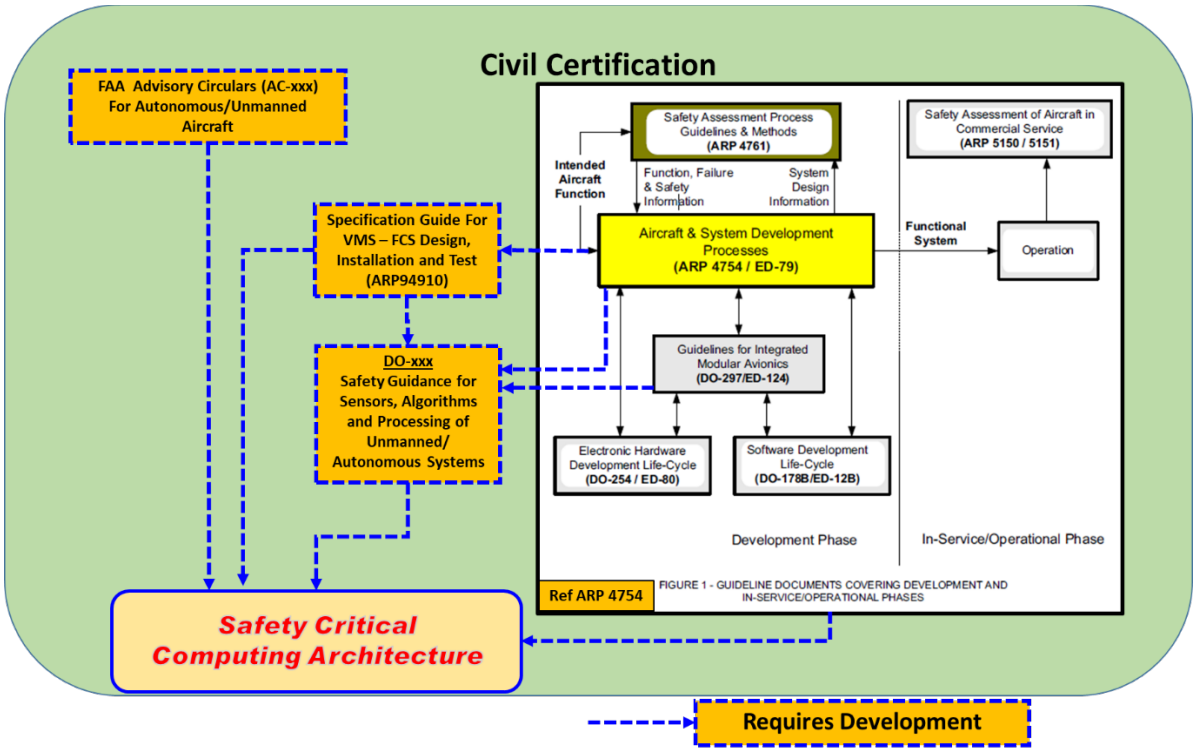


Figure 32: Recommendation for Potential Certification Document Suite

The context of Figure 32 assumes the need for contingency of critical faults resolution (similar to the ones pilot or an operator currently have responsibilities for), and therefore advocates that sensory systems/components require certification guidance and self-health monitoring to enable resolution of establish Byzantine faults. Examples of such systems are listed below:

- External sensory systems to assist out-the-window SA (situational awareness)
  - Sensors to assist operations in Degraded Visual Environments
  - Sensors that support un-cooperative surveillance (obstacle avoidance)
  - Landing zone identification, near and on-ground operations, and landing
  - Sensors to enable Terrain Following – Terrain Avoidance operations
  - Altitude above terrain
  - Geo Location (GPS, air or ground based systems)
- Internal Sensors for diagnosis of identification of critical components and/or systems failures
  - Flight Controls and navigation functions
  - Critical Actuation sensors
  - Electrical Systems (as applicable)
  - Hydraulics System (as applicable)
  - Propulsion sensors
  - Fuel System sensors
  - Transmissions and dynamic sensors
  - Sensors for rotor systems and other aerodynamic surfaces
  - Environmental Control Systems (when critical)
  - Sensors for Landing Gear
  - Sensors for fire detection and Fire Extinguishing system

- Algorithms
    - Sensor analysis
    - Determinism and Numerical Stability of Decision making Algorithm
    - Measurable Rating of Correctness relative to: Human reaction or Verified Mathematical or Physics models
    - Flight Safety Assessment from failure of algorithm

12.3 Recommendations for Future Work

Part of the National Aeronautics and Space Administration (NASA) Revolutionary Vertical Lift (RVLT) Project focus is to work collaboratively with the Federal Aviation Administration (FAA) Aircraft Certification Service on research that supports development of certification standards for Urban Air Mobility (UAM) vehicle propulsion systems. This includes characterizing failure modes and mitigation/recovery for common UAM propulsion systems and identifying physical and functional reliability and redundancy requirements to meet certification standards. To enable this research, NASA designed four (4) concept vehicles to identify crucial technologies, define research requirements, and explore a range of propulsion systems.

The research performed herein was in support of NASA's RVLT Project and can be used as a measuring stick to guide component technology development, define research requirements for future work, and explore the design space for inherently safe propulsion systems for the UAM mission. The primary objective of the research performed herein was to identify failure modes and hazards associated with NASA's RVLT Concept Vehicles and to perform a reliability and safety assessment. Conceptual designs of the powertrain configuration for each concept vehicle were developed using the provided architectures. Hazards related to the powertrain were identified and the effects of those hazards were quantified using industry standard reliability and safety analysis methods. Gaps between the UAM air vehicles/mission and existing regulations/specifications were identified that need to be resolved if Distributed Electric/Hybrid-Electric Propulsion (DE/HEP) air vehicles move people and things in the anticipated volumes over metropolitan areas (ref. 4). Future work should further explore leveraging or modifying existing FAR guidance for onboard operator case in both conventional or DE/HEP propulsion.

Boeing recommends extending this research to develop DE/HEP components with improved reliability, down-selecting from the four (4) concept vehicles analyzed herein, and exploring powertrain architectures and connectivity to provide inherent air-vehicle safety, in order to take advantage of higher reliability components. Selecting one (1) concept vehicle to continue to research will allow greater depths of research activities in specialized technologies, as opposed to broader stroke research projects in which many concept vehicles are researched at a higher, systems level. Research would follow a similar approach to that of the NASA Civil Heavy Lift Rotorcraft Project in which initial vehicle level trade studies were used to down-select to component level research using the NASA Large Civil Tilt-Rotor (LCTR) vehicle.

Boeing recommends selecting a vehicle that is expected to fall within the size and weight restrictions of the EASA Draft SC-VTOL-01. Due to the 4,400 lbs weight limit in the EASA Draft SC-VTOL-01, the only two (2) vehicles that fall within this criteria are the Quad-Rotor and the Lateral-Twin (ref. 2). Furthermore, the Quad-Rotor was resized to carry six (6) people on board (ref. 3), and it still fell within the 4,400 lbs weight limit, which adds to its applicability to the UAM mission and future research areas. Down-selecting between the Quad-Rotor and the Lateral-Twin is more difficult. The two (2) platforms, similar to the two (2) heavier RVLT Concept Vehicles, are both interesting research platforms, as well as good candidate aircraft platforms. The Tilt-

Wing or the Lift+Cruise vehicles could be used to conduct trade studies on FCC's powered by HV systems, e.g. from HVDC bus to FCC, using DC-DC converter, examining reliability impacts (high power switches, digital components, microcontrollers, heat, etc.) and swap, efficiency.

The Lateral-Twin is a more efficient aircraft than the Quad-Rotor when considering similar payloads (ref. 3) and can be modified to accept conventional powertrains, series-hybrid (turboelectric) powertrains, or all-electric powertrains. Future work could explore adding a DC-DC converter in addition to the LV battery and accessory generator to improve reliability of the FCS and reduce the weight of the LV batteries or accessory generators. More exploration into engine selection could be performed. The engines are anticipated to have higher power demands then originally estimated because they require power to charge HV and LV batteries in cruise, in addition to flight power required and accessory loads. Examining a pilot's energy management (Fuel vs. Battery) displays and strategy may shed light on future cockpit requirements, as well as, optimal electrical vs. chemical energy use in future designs.

However, the Quad-Rotor has similar flexibility in regards to powertrain configurating. Similar exploration into energy management and interplay between HV and LV systems may be explored, but the Quad-Rotor has the added benefit of being able to flexibly research both variable pitch, fixed speed propulsion system architectures as well as fixed pitch, variable speed system architectures and further investigate the value of interconnecting shafting, although safety of the Quad-Rotor was notably reduced by removing the interconnecting shafts. Control laws (CLAWS) could be developed to assist in autorotation in the alternate configuration in which interconnecting shafting is not utilized. Additionally, multi-rotor research can be performed in interesting manners; adding stacked rotors to make an octo-rotor or removing one (1) rotor to make a tri-rotor are both interesting possibilities, as well as adding one (1) rotor to make a penta-rotor.

Research into adding rotors (i.e. penta or octo-rotor) would help determine if fail safe rotor systems will inherently make the vehicle safer. The study performed herein did not show the Lift+Cruise, which is a variable speed octo-rotor with a pusher propeller, to be safer than the Quad-Rotor; however, additional research considering all aspects of the flight regime that an optimal rotor configuration exists for safety. Three (3) or more rotors could be traded using NASA's proposed collective only control scheme to determine the optimal rotor configuration for safety.

Once a vehicle architecture for future study has been down-selected, Boeing recommends trade studies related to powertrain architectures necessary to meet the EASA Draft SC-VTOL-01 air-vehicle requirement of 10^{-9} failures per flight hour. As a rule of thumb this would require a propulsion system architecture that has approximately 10^{-10} failures per flight hour or less. The reliability and safety analysis method provided here may be extended to review the critical functions that are required within the propulsion system and levy requirements down to the sub-system and component level. Exploration into novel methods to improve safety, such as energy transfer from the LV battery to the HV system in emergency conditions could be considered for smaller vehicles, like the single-person Quad-Rotor.

Future work should improve sub-system reliability through component improvements. Electric motors, generators, inverters, and rectifiers require more reliable designs in order to be used for primary propulsion in commercial applications. Detailed design and analysis efforts should be undertaken to develop reliability models that can be used to assess the reliability of a design prior to extensive test programs. SAE ARP4761 and ARP4754 include guidance necessary to perform detailed reliability analysis and should be used to improve motor and generator reliability through a data-driven approach. Although testing and fielding will inevitably determine the reliability of

a component, being able to analytically predict the reliability will aid in regulatory and industry specification development.

Boeing recommends down-selecting a single vehicle configuration and then performing a more pointed functional reliability and safety assessment to develop an architecture and architectural requirements necessary to attain a propulsion system with no more than 10^{-10} failures per flight hour. Once the detailed reliability and safety assessment is performed, derived requirements may be driven into component level research with motor or inverter suppliers to improve the state-of-the-art technology for the aerospace industry. NASA will need to work closely with the sub-contractor to explore the complex flight dynamics in ground effect, out of ground effect, maneuvers, and environmental factors that may impact the reliability requirements necessary to meet the 10^{-10} failures per flight hour threshold. Deliverables of the study could include the functional reliability and safety assessment in all phases of flight, a model of the propulsion system integrated into the down-selected air-vehicle including sensor and software packages that may be required, a mass balance record of all airplane sub-systems to assess cg location, and initial component level reliability assessments to develop more focused areas for technology improvement.

13 REFERENCES

1 Johnson, W., Yamauchi, G., and Watts, M.: Designs and Technology Requirements for Civil Heavy Lift Rotorcraft. AVS Vertical Lift Aircraft Design Conference, San Francisco, CA, January, 2006.

2 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.

3 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.

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

5 Johnson, W. "NDARC. NASA Design and Analysis of Rotorcraft." NASA TP 2015-218751, April 2015.

6 Darmstadt, P. and Robuck, M.: Composites for Advanced Drive Systems, a Systems Analysis – Revolutionary Vertical Lift Technology (RVLT). AHS International 74th Annual Forum & Technology Display, Phoenix, AZ, May, 2018.

7 SAE ARP5580 – Aerospace Recommended Practice: Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications, 2012-05.

8 MIL-STD-1629A – Military Standard: Procedures for Performing a Failure Mode, Effects, and Criticality Analysis, 24 November 1980.

9 MIL-HDBK-217F – Military Handbook: Reliability Prediction of Electronic Equipment, 2 December, 1991.

10 Piancastelli, L.: Powerplant Reliability Issues and Wear Monitoring in Aircraft Piston Engines. Part II: Engine Diagnostic. Drones. 2. 10. 10.3390/drones2010010, 2018.

11 Rossi, M.J.: Nonelectronic Parts Reliability Data. NPRD-3, Griffiss A.F.B, NY, 1985.

12 Nonelectronic Parts Reliability Data. NPRD-16, Quanterion Solutions Incorporated, Utica, NY, 2016.

13 Rome Laboratory Reliability Engineer's Toolkit. Systems Reliability Division, Rome Laboratory, Air Force Material Command (AFMC), Griffiss AFB, NY, April, 1993.

14 Song, Y. and Wang, B.: Quantitative Evaluation for Reliability of Hybrid Electric Vehicle Powertrain. 4th International Conference on Power Engineering, Energy, and Electrical Drives, Istanbul, Turkey, May, 2013.

15 System Reliability Toolkit. Quanterion Solutions Incorporated, Utica, NY, 2000.

16 EASA Type-Certificate Data Sheet – General Electric Company CT7-series engines, 07.02.2018.

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

18 Reliability Workbench. (2015). Isograph Ltd.

19 Aerospace.honeywell.com. (2019). T55 Turboshaft Engine. [online] Available

at: https://aerospace.honeywell.com/en/products/engines/t55-turboshaft-engine.

20 Forecastinternational.com. (2019). The Market for Aviation Turboshaft Engines, Product Code #F642. [online] Available at: https://www.forecastinternational.com/samples/F642_CompleteSample.pdf.

21 Safran Helicopter Engines. (2019). Aneto. [online] Available at: https://www.safran-helicopter-engines.com/helicopter-engines/over-2000-shp/aneto.

22 Soong, W. (2008). Power Engineering Briefing Note Series, Sizing of Electrical Machines, PEBN #9. [online] Eleceng.adelaide.edu.au. Available at: http://www.eleceng.adelaide.edu.au/research/power/pebn/pebn009%20sizing%20of%20electrical%20machines.pdf.

23 SAE AS50881 - Aerospace Standard: (R) Wiring Aerospace Vehicle, 2015-05.

24 SAE ARP4754 – Aerospace Recommended Practice: (R) Guidelines for Development of Civil Aircraft and Systems, 2010-12.

25 *Electric VTOL News*™. [online] Electric VTOL News™. Available at: http://evtol.news/ [April, 2019].

APPENDIX A FUNCTIONAL HAZARD ANALYSIS (FHA) TABLES

Table A- 1: Tilt-Wing FHA

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of air-craft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Any loss of single pro-pulsor fail	Away from OEI region	Aircrew detects failure and compensates with remaining thrust to continue flight	Minor
		In OEI re-gion	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
	Any com-bination of Dual pro-pulsor Fail	All	Failures are detected. Cross shafting en-sures all rotors are still spinning. Control-lability still present. Reduced power avail-able. Insufficient power to maintain level fight. Gliding approach to airplane mode or Run-On Landing (ROL). If adequate room exists for flare and roll-out, no damage or loss of occupants. Worst case feasible out-come is loss of air-vehicle/occupant	Catastrophic
	Complete Propulsion loss	Within 2 minutes of suitable landing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are adequate to provide power for a normal hover or (ROL).	Severe
		More than 2 minutes from a suit-able land-ing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are NOT adequate to pro-vide power for a normal hover or (ROL). Gliding approach without suitable landing area. Loss of air vehicle and occupants	Catastrophic
Transmit Adequate Power to Rotors	Dual esc fail	Dual ESC failed high: all phases	Failures are detected. Cross shafting en-sures all rotors are still spinning. Control-lability still present. Pilots will need to re-duce engine power to land. If hover power can be managed than land normally. If ad-equate room exists for flare and roll-out as required, no damage or loss of occupants. Worst case feasible outcome is air-vehicle damage and occupant injury	Severe

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
		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. Gliding approach to airplane mode or Run-On Landing (ROL). If adequate room exists for flare and roll-out, no damage or loss of occupants. Worst case feasible outcome is loss of air-vehicle/occupant. Hazard classification is the same whether OEI or out of OEI avoid region.	Catastrophic
	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 Gliding approach to airplane mode or Run-On Landing (ROL).If adequate room exists for flare and roll-out as required, no damage or loss of occupants. Hover landings should still be possible with careful modulation of thrust via aircrew action	Major
		ESC Failed Low: Not OEI Avoid region	Effective loss of torque output from one motor. Pilot detects failure and compensates. ROL required.	Minor
		ESC Failed Low: OEI Avoid region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
Transmit Adequate Power to Rotors	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. Pilot compensation possible via directional control. Safe flight to ROL possible. Air-crew workload impact. Must be within range of suitable landing area.	Major

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
	Dual gearbox fail	Opposite wings	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications. Loss of ability to spin rotor associated with any two gearbox will result in loss of sufficient power for airplane mode level flight. Pilot compensation possible via directional control. Safe flight to ROL possible, but will require adequate Aircrew workload impact. Possible loss of air vehicle and occupants.	Catastrophic
		Same Wings	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications. Loss of ability to spin rotor associated with two gearbox on the same wing will result in loss of sufficient power for airplane mode level flight. If is also assumed to result in loss of flight path control due to excessive yaw. Pilot compensation not possible via directional control. Loss of air vehicle and occupants.	Catastrophic

Table A- 2: 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
		Other than OEI Avoid Region	Aircrew detects failure and compensates with remaining thrust to continue flight	Minor

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	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

Table A- 3: Alternate Configuration – Quad-Rotor without Interconnecting Shafts FHA

Note: *Red text denotes changes to "Classification of Failure Condition" from the baseline Quad-Rotor, with interconnecting shafts, and orange text denotes added or removed "Failure Conditions" to be when comparing the baseline and alternate Quad-Rotor configurations.*

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. Lack of cross-shafting will require immediate cut of power to diagonal side rotor to continue controlled flight. Lack of power will require autorotative or dual engine fail descent profile. ROL required due to lack of ability to flare during autorotative landing. Potential catastrophic outcome with loss of air vehicle /occupants.	Catastrophic
		In OEI region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Potential for diminished controllability due to one rotor no longer producing thrust/lift. Hard landing with potential loss of aircraft/occupants.	Catastrophic
	Any combination of Dual propulsor Fail	Both on one side (fore/aft, or Left/Right)	Failures are detected. Either fore/aft or left/right propulsors fail. All remaining thrust causes uncontrolled pitch/yaw moments. Loss of control w/o immediate thrush reduction from remaining rotors. Insufficient power to maintain level fight. Autorotative approach requires suitable landing area. Limited ability for a collective flare. Likely outcome is loss of air vehicle/occupant.	Catastrophic
		Diagonal from each other	Failures are detected. Diagonal thrust may be able to be modulated to drive a degree of pitch, roll, and yaw control. Insufficient lift for continued flight. Will require an autorotative descent. Possibility of limited use of power to flare the air vehicle for landing. Worse case realistic outcome is catastrophic loss of air vehicle and occupants.	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

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Dual ESC Fail	Dual ESC Failed High: All phases	Failures are detected. Rotors will continue to spin. Controllability heavily degraded in combination of pitch/roll/yaw axis. Ability to descend to landing under control in doubt. Worse case realistic outcome is catastrophic loss of air vehicle and occupants.	Catastrophic
		Dual ESC Failed Low: All phases	Failures are detected. Insufficient thrust remain for level flight. Remaining thrust causes uncontrolled pitch/yaw moments. Loss of control w/o immediate thrush reduction from remaining rotors to balance out forces. Autorotative approach requires suitable landing area. Limited ability for a collective flare. Likely outcome is loss of air-vehicle/occupant.	Catastrophic
	Single ESC Fail	ESC Failed Hi: All phases	Failures are detected. All rotors are still spinning. System will need to modulate engine power on other rotors to allow degraded controllability to a hover landing or a no hover landing with some forward speed to maximize Effective Translational Lift (ETL). Pilot workload issue.	Severe
		ESC Failed Low: Not OEI Avoid region	Failures are detected. Rotor associated with failed ECS will not produce adequate thrust to allow for controllability unless other rotors allow for degraded control modes. Pilots will need to execute a no hover landing with some forward speed to maximize Effective Translational Lift (ETL) and potential controllability. If degraded control modes are present, then Severe outcome for pilot workload. Otherwise, Catastrophic outcome due to loss of flight path control.	Catastrophic
		ESC Failed Low: OEI Avoid region	Failure is detected. Degraded/loss of control due to degraded thrust. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	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 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. Degradation in thrust from that rotor could result in degraded controllability. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/occupants	Catastrophic
		Other than OEI Avoid Region	Aircrew detects failure. Degraded thrust from associated rotor. Depending on nature of battery fail, controllability could be severely degraded or lost. Severe outcome if a partial battery failure. Catastrophic outcome for complete loss of that portion of the batteries function.	Catastrophic
	LV Battery Fail	All	Loss of power to all 4 ESC and FCC. Collective control of rotor lost. Loss of flight Path Control results in Catastrophic outcome.	Catastrophic
Note: NOT PRESENT due to lack of interconnecting shafts	~~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~~

Table A- 4: Lateral-Twin 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. Controllability not degraded due to cross shafting.	Minor
		In OEI region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	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 and landing. Worst case feasible outcome is loss of air-vehicle/occupant	Catastrophic
	Dual Turboshaft Failure	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 and landing. Worst case feasible outcome is loss of air-vehicle/occupant	Catastrophic
	Single Turboshaft and Electric Propulsion 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 and landing. Worst case feasible outcome is loss of air-vehicle/occupant	Catastrophic
	ESC Fail	ESC Failed Hi: All phases	Failures are detected. Cross shafting ensures all rotors are still spinning. Controllability still present. Pilots' control of turboshaft output will allow for sufficient power decrement to allow a normal descent to landing. Hover landing is possible with careful modulation of thrust via aircrew action	Major
		ESC Failed Low: Not OEI Avoid region	Effective loss of torque output from electric motor. Pilot detects failure and compensates. ROL required due to lack of hover power.	Minor

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors		ESC Failed Low: OEI Avoid region	Failure is detected. Power Required is greater than Power available (Pr>Pa). Hard landing with potential loss of aircraft/crew.	Catastrophic
	Single Rotor Gearbox Fail	All	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications). Loss of ability to spin rotor associated with that gearbox. Assuming rotor tops spinning due to GB fail, control will be lost with a Catastrophic loss of air vehicle and occupants.	Catastrophic
	Cross shafting fail (includes junction gear box)	While in OEI	Failures detected and annunciated to aircrew (chip light, temp/ pressure indications. Loss of ability to apply torque to the rotor associated with the failed engine. System will need to immediately drop collective on the rotor still producing thrust. Must enter autorotative descent to a landing. If pilot reaction or system reaction is delayed, loss of flight path control and catastrophic outcome may occur. Possibility or rotor to rotor contact (see entry below).	Catastrophic
	Combiner Gearbox Fail or cross shaft failure	All	Failures detected and annunciated to aircrew (chip light, temp/ pressure) indications. All motors continue to operate. Electric motor is unable to provide power to one or more main rotors. Reduced power will necessitate ROL. Failure mode considered catastrophic due to rotor overlap. Gearboxes utilized in cross-shafting will serve to balance out delta-Qm between rotors and keep the rotor phased. Any failure of any gearbox utilized in cross-shafting will also result in loss of Qm equalization. Once the cross-shafting is gone, differences in Qm will result in changes to rotor phasing. Rotor contact is considered Catastrophic and will result in loss of flight path control and possible loss of vehicle structural integrity. Loss of air vehicle and 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	LV Battery Fail	All	Loss of power to ESC and FCC. Loss of ECS result in loss of electric propulsor. See single propulsor fail above for failure effects given flight modes and conditions.	Catastrophic
	FCC Fail	All	Potential loss of electric motor. Severity tied to flight condition and failure mode. If power command fails to low in OEI avoid region, potentially catastrophic. If the fails command to current value or to high power, then Major outcome due to pilot workload.	Catastrophic; Major (see effect of failure)
	Complete HV Battery Fail	Other than OEI avoid region	Complete loss of all High Voltage Power to electric propulsor. Complete loss of electric propulsion. Turboshaft engine proves sufficient power for level flight away from OEI avoid region. Run on/ no hover landing is required.	Major
		OEI avoid region	Failure is detected. Power Required is greater than Power available (Pr>Pa) due to loss of electrical motor resulting in hover power deficit. Potential hard landing with potential loss of aircraft/crew.	Catastrophic

Table A- 5: Lift+Cruise 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	All	Aircrew and air vehicle detects failure. Air vehicle throttles back one additional engine and adds power to others to compensate with additional thrust to continue flight	Minor
	Any combination of Dual propulsor Fail	All	Failure detected and annunciated to Flight Crew. Four propulsors now at reduced power (two failed and corresponding two at reduced power) Air vehicle unable to hover. Airplane mode landing required.	Major
	Complete turboshaft Propulsion loss or associated battery charging hardware.	Within 2 minutes of suitable landing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are adequate to provide power for a normal hover or (ROL).	Severe
		More than 2 minutes from a suitable landing area	Loss of ability to maintain battery charge. Electric motors running off battery power alone. Batteries are NOT adequate to provide power for a normal hover or (ROL). Gliding approach without suitable landing area. Loss of air vehicle and occupants	Catastrophic
	Single Gearbox Fail	All	Fail to spin rotor captured under single propulsor fail. This is for a failure to align rotor with relative wind when transitioning to wingborne flight. For fail during hover flight, see loss of single propulsor fail. Annunciation to pilots would require sensor to measure alignment. Extra drag on one wing due to propeller not being aligned with the relative wind.	Minor

Function Description	Failure Conditions	Phase of Operation	Effect of the Failure condition of aircraft/crew	Classification of Failure Condition
Transmit Adequate Power to Rotors	Dual Gearbox Fail	Same wing	Fail to spin 2 rotors captured under dual propulsor fail. This is for a failure to align rotor with relative wind when transitioning to wingborne flight. For fail during hover flight, see loss of dual propulsor fail. Annunciation to pilots would require sensor to measure alignment. Extra drag on one wing due to two propellers not being aligned with the relative wind. Adequate roll control, yaw control will be degraded.	Major
		Opposite Wings	Fail to spin 2 rotors captured under dual propulsor fail. This is for a failure to align rotor with relative wind when transitioning to wingborne flight. For fail during hover flight, see loss of dual propulsor fail. Annunciation to pilots would require sensor to measure alignment. Extra drag on both wings due to two propellers not being aligned with the relative wind. Adequate roll control. Adequate degraded yaw control should be assured via design.	Major
	Rear propulsor fail	All	Air vehicle will lose forward thrust. Air vehicle will have to slow and land as soon as practicable. Per "VTOL Urban" a reduction in pitch authority will take place. Any additional single loss of any of the 8 propulsors on the wing will result in a Severe outcome with heavily degraded pitch authority.	Major/Severe

Table B- 1: Tilt-Wing FMECA Worksheet

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1A1	Provide HVDC power to propulsion system and batteries	2.67E-06	Turboshaft engine fails to provide output shaft power to gearbox	Turboshaft engine failure (no output)	All	Loss of Engine power output to gearbox, AC generator and accessory loads	Loss of electrical power to drive motors and accessory loads. Batteries provide electric power for 2 minutes.	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	Visual and audible warning provided to pilot. Pilot detects abnormal engine noise	Emergency procedures defined in flight manual	I	1.00	1.200E-01	80% chance that engine performance degradation is detected with ample time to land safely before complete engine failure.	3.20E-07
1B1	Provide HVDC power to propulsion system and batteries	5.00E-07	Engine gearbox assembly failure	Internal gearbox assembly failure	All	Failure prevents input torque from being transferred to AC generator	Loss of electrical power to drive motors. Batteries provide electric power for 2 minutes.	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	Visual & audible warning provided to pilot	Emergency procedures defined in flight manual	I	1.00	1.200E-01	Estimated that 80% of failures can be detected before loss of function and 40% chance that the pilot will be able to land safely within 2 minutes of the failure.	6.00E-08
1C1	Provide HVDC power to propulsion system and batteries	1.30E-04	AC Generator failure	Complete failure of AC generator output (generator unit or GCU)	All	Loss of electrical power input to AC-DC converter.	Loss of HVDC output from AC-DC converter. Batteries provide electric power for 2 minutes.	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	Visual & audible warning provided to pilot	Emergency procedures defined in flight manual	I	1.00	6.000E-01	Estimated 40% chance that the pilot will be able to land safely within 2 minutes of the failure.	7.80E-05
1D1	Provide HVDC power to propulsion system and batteries	2.00E-04	No HVDC output from AC-DC converter	AC-DC converter failure	All	Loss of power output to drive motors and charge batteries.	Batteries provide electric power for 2 minutes.	Loss of all propulsion after battery power is depleted. Loss of aircraft if pilot cannot find safe landing area and land within 2 minutes.	Visual & audible warning provided to pilot	Emergency procedures defined in flight manual	I	1.00	6.000E-01	Estimated 40% chance that the pilot will be able to land safely within 2 minutes after the failure.	1.20E-04

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2A1	Provide battery storage of electrical energy	1.00E-06	Battery 1 failure	Failure of single branch of battery array (1 of N) (open circuit or high impedance)	All	Reduced battery capacity,	2 minute reserve power slightly compromised	None	Visual & audible warning provided to pilot	None	IV	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2A2	Provide battery storage of electrical energy	1.00E-06	Battery 1 failure	Failure of single battery cell in array (1 of N) (internal short circuit)	All	Rapid release of heat and gas at shorted battery cell; heat transfers to adjacent cells	Adjacent cells overheat and also short, causing thermal runaway. Intense heat causes fire	Aircraft fire damages critical systems, causing loss of aircraft	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire	I	0.25	1.000E-03	Assume that Battery cooling and fire protection systems will be 99.9% effective to control battery fire	2.50E-10
2A3	Provide battery storage of electrical energy	1.00E-06	Battery 1 failure	Failure of single branch of battery array (1 of N) (internal short circuit)	All	Internal temperature increases rapidly	Battery protection device contains failed battery cell	Reduced battery capacity, reserve power slightly reduced	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2A4	Provide battery storage of electrical energy	1.00E-06	Battery 1 failure	Main battery terminal loose or broken.	All	No battery output. System health monitoring detects battery #1 fault.	Loss of ability to operate Motor #1in case of engine, generator, or AC/DC converter failure	Loss of redundancy. Loss of ability to operate motor #1 in event of loss of main AC power source	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2B1	Provide battery storage of electrical energy	1.00E-06	Battery 2 failure	Failure of single branch of battery array (1 of N) (open circuit or high impedance)	All	Reduced battery capacity,	2 minute reserve power slightly compromised	None	Visual & audible warning provided to pilot	None	IV	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2B2	Provide battery storage of electrical energy	1.00E-06	Battery 2 failure	Failure of single battery cell in array (1 of N) (internal short circuit)	All	Rapid release of heat and gas at shorted battery cell; heat transfers to adjacent cells	Adjacent cells overheat and also short, causing thermal runaway. Intense heat causes fire	Aircraft fire damages critical systems, causing loss of aircraft	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire	I	0.25	1.000E-03	Assume that Battery cooling and fire protection systems will be 99.9% effective to control battery fire	2.50E-10
2B3	Provide battery storage of electrical energy	1.00E-06	Battery 2 failure	Failure of single branch of battery array (1 of N) (internal short circuit)	All	Internal temperature increases rapidly	Battery protection device contains failed battery cell	Reduced battery capacity, reserve power slightly reduced	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2B4	Provide battery storage of electrical energy	1.00E-06	Battery 2 failure	Main battery terminal loose or broken.	All	No battery output. System health monitoring detects battery #2 fault.	Loss of ability to operate Motor #2in case of engine, generator, or AC/DC converter failure	Loss of redundancy. Loss of ability to operate motor #2 in event of loss of main AC power source	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2C1	Provide battery storage of electrical energy	1.00E-06	Battery 3 failure	Failure of single branch of battery array (1 of N) (open circuit or high impedance)	All	Reduced battery capacity,	2 minute reserve power slightly compromised	None	Visual & audible warning provided to pilot	None	IV	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2C2	Provide battery storage of electrical energy	1.00E-06	Battery 3 failure	Failure of single battery cell in array (1 of N) (internal short circuit)	All	Rapid release of heat and gas at shorted battery cell; heat transfers to adjacent cells	Adjacent cells overheat and also short, causing thermal runaway. Intense heat causes fire	Aircraft fire damages critical systems, causing loss of aircraft	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire	I	0.25	1.000E-03	Assume that Battery cooling and fire protection systems will be 99.9% effective to control battery fire	2.50E-10
2C3	Provide battery storage of electrical energy	1.00E-06	Battery 3 failure	Failure of single branch of battery array (1 of N) (internal short circuit)	All	Internal temperature increases rapidly	Battery protection device contains failed battery cell	Reduced battery capacity, reserve power slightly reduced	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2C4	Provide battery storage of electrical energy	1.00E-06	Battery 3 failure	Main battery terminal loose or broken.	All	No battery output. System health monitoring detects battery #3 fault.	Loss of ability to operate Motor #3 in case of engine, generator, or AC/DC converter failure	Loss of redundancy. Loss of ability to operate motor #3 in event of loss of main AC power source	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2D1	Provide battery storage of electrical energy	1.00E-06	Battery 4 failure	Failure of single branch of battery array (1 of N) (open circuit or high impedance)	All	Reduced battery capacity,	2 minute reserve power slightly compromised	None	Visual & audible warning provided to pilot	None	IV	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2D2	Provide battery storage of electrical energy	1.00E-06	Battery 4 failure	Failure of single battery cell in array (1 of N) (internal short circuit)	All	Rapid release of heat and gas at shorted battery cell; heat transfers to adjacent cells	Adjacent cells overheat and also short, causing thermal runaway. Intense heat causes fire	Aircraft fire damages critical systems, causing loss of aircraft	Visual & audible warning provided to pilot	battery cooling system and fire protection system contain the heat/fire	I	0.25	1.000E-03	Assume that Battery cooling and fire protection systems will be 99.9% effective to control battery fire	2.50E-10

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2D3	Provide battery storage of electrical energy	1.00E-06	Battery 4 failure	Failure of single branch of battery array (1 of N) (internal short circuit)	All	Internal temperature increases rapidly	Battery protection device contains failed battery cell	Reduced battery capacity, reserve power slightly reduced	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
2D4	Provide battery storage of electrical energy	1.00E-06	Battery 4 failure	Main battery terminal loose or broken.	All	No battery output. System health monitoring detects battery #4 fault.	Loss of ability to operate Motor #4 in case of engine, generator, or AC/DC converter failure	Loss of redundancy. Loss of ability to operate motor #4 in event of loss of main AC power source	Visual & audible warning provided to pilot	None	III	0.25	1.000E+00	Beta = 1 for severity III and IV	2.50E-07
3A1	Convert HVDC Electrical energy to shaft torque	2.70E-04	Motor #1 fails to provide output torque	Electronic Speed Controller #1 Failure	All	No ESC output to motor #1	Motor #1 cannot provide output torque, interconnecting shaft transfers torque from other motors to prop-rotor #1	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.40E-05
3A2	Convert HVDC Electrical energy to shaft torque	9.24E-05	Motor #1 fails to provide output torque	Motor #1 Failure	All	Motor #1 fails to provide output torque.	Interconnecting shaft transfers torque from other motors to prop-rotor #1.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	1.85E-05
3A3	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #1 fails to provide output torque	ESC #1 cooling fan failure	All	Loss of cooling for ESC #1. Limited performance envelope for Motor #1.	Interconnecting shaft transfers torque from other motors to prop-rotor #1.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Ram air will be sufficient to cool ESC while in forward flight. Pilot can minimize time in hover to avoid overheating ESC. Pilot can avoid operating conditions that will cause ESC to overheat.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3A4	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #1 fails to provide output torque	Motor #1 Cooling & Lube Failure	All	Loss of Lube and cooling for Motor #1. Damage to Motor #1 possible.	Health management system automatically shuts down Motor #1 if not in OMI avoid region. Interconnecting shaft transfers torque from other motors to prop-rotor #1.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Motor #1 may be operated for short time to land safely if. Pilot can avoid operating conditions that require Motor #1.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05
3B1	Convert HVDC Electrical energy to shaft torque	2.70E-04	Motor #2 fails to provide output torque	Electronic Speed Controller #2 Failure	All	No ESC output to motor #2	Motor #2 cannot provide output torque, interconnecting shaft transfers torque from other motors to prop-rotor #2	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.40E-05
3B2	Convert HVDC Electrical energy to shaft torque	9.24E-05	Motor #2 fails to provide output torque	Motor #2 Failure	All	Motor #2 fails to provide output torque.	Interconnecting shaft transfers torque from other motors to prop-rotor #2.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	1.85E-05
3B3	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #2 fails to provide output torque	ESC #2 cooling fan failure	All	Loss of cooling for ESC #2. Limited performance envelope for Motor #2.	Interconnecting shaft transfers torque from other motors to prop-rotor #2.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Ram air will be sufficient to cool ESC while in forward flight. Pilot can minimize time in hover to avoid overheating ESC. Pilot can avoid operating conditions that will cause ESC to overheat.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3B4	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #2 fails to provide output torque	Motor #2 Cooling & Lube Failure	All	Loss of Lube and cooling for Motor #2. Damage to Motor #2 possible.	Health management system automatically shuts down Motor #2 if not in OMI avoid region. Interconnecting shaft transfers torque from other motors to prop-rotor #2.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Motor #2 may be operated for short time to land safely if. Pilot can avoid operating conditions that require Motor #2.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05
3C1	Convert HVDC Electrical energy to shaft torque	2.70E-04	Motor #3 fails to provide output torque	Electronic Speed Controller #3 Failure	All	No ESC output to motor #3	Motor #3 cannot provide output torque, interconnecting shaft transfers torque from other motors to prop-rotor #3	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.40E-05
3C2	Convert HVDC Electrical energy to shaft torque	9.24E-05	Motor #3 fails to provide output torque	Motor #3 Failure	All	Motor #3 fails to provide output torque.	Interconnecting shaft transfers torque from other motors to prop-rotor #3.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	1.85E-05
3C3	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #3 fails to provide output torque	ESC #3 cooling fan failure	All	Loss of cooling for ESC #3. Limited performance envelope for Motor #3.	Interconnecting shaft transfers torque from other motors to prop-rotor #3.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Ram air will be sufficient to cool ESC while in forward flight. Pilot can minimize time in hover to avoid overheating ESC. Pilot can avoid operating conditions that will cause ESC to overheat.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3C4	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #3 fails to provide output torque	Motor #3 Cooling & Lube Failure	All	Loss of Lube and cooling for Motor #3. Damage to Motor #3 possible.	Health management system automatically shuts down Motor #3 if not in OMI avoid region. Interconnecting shaft transfers torque from other motors to prop-rotor #3.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Motor #3 may be operated for short time to land safely if. Pilot can avoid operating conditions that require Motor #3.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05
3D1	Convert HVDC Electrical energy to shaft torque	2.70E-04	Motor #4 fails to provide output torque	Electronic Speed Controller #4 Failure	All	No ESC output to motor #4	Motor #4 cannot provide output torque, interconnecting shaft transfers torque from other motors to prop-rotor #4	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.40E-05
3D2	Convert HVDC Electrical energy to shaft torque	9.24E-05	Motor #4 fails to provide output torque	Motor #4 Failure	All	Motor #4 fails to provide output torque.	Interconnecting shaft transfers torque from other motors to prop-rotor #4.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft in OMI avoid region. Loss of control of aircraft if failure occurs while aircraft is in OMI region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	1.00	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	1.85E-05
3D3	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #4 fails to provide output torque	ESC #4 cooling fan failure	All	Loss of cooling for ESC #4. Limited performance envelope for Motor #4.	Interconnecting shaft transfers torque from other motors to prop--rotor #4.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Ram air will be sufficient to cool ESC while in forward flight. Pilot can minimize time in hover to avoid overheating ESC. Pilot can avoid operating conditions that will cause ESC to overheat.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3D4	Convert HVDC Electrical energy to shaft torque	5.17E-05	Motor #4 fails to provide output torque	Motor #4 Cooling & Lube Failure	All	Loss of Lube and cooling for Motor #4. Damage to Motor #4 possible.	Health management system automatically shuts down Motor #4 if not in OMI avoid region. Interconnecting shaft transfers torque from other motors to prop-rotor #4.	Some loss of propulsion system power depending on conditions. Reduced ability to operate in hover for extended period of time.	Visual & audible warning provided to pilot	Motor #4 may be operated for short time to land safely if. Pilot can avoid operating conditions that require Motor #4.	III	1.00	1.000E+00	Beta = 1 for severity III and IV	5.17E-05
4A1	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #1 failure	Input shaft of gearbox fails (or clutch), causing loss of torque from motor #1.	All	loss of torque from motor #1	Torque from other 3 motors transferred to prop-rotor #1 via interconnecting shaft	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
4A2	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #1 failure	Complete gearbox failure	All	loss of torque from motor #1 and loss of torque output to prop-rotor #1	No output to prop-rotor #1; unable to transfer motor #1 torque to other prop-rotors. 25% loss of propulsion system power.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, possible loss of ability to hover depending on aircraft weight. Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
4B1	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #2 failure	Input shaft of gearbox fails (or clutch), causing loss of torque from motor #2.	All	loss of torque from motor #2	Torque from other 3 motors transferred to prop-rotor #2 via interconnecting shaft	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
4B2	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #2 failure	Complete gearbox failure	All	loss of torque from motor #2 and loss of torque output to prop-rotor #2	No output to prop-rotor #2; unable to transfer motor #2 torque to other prop-rotors. 25% loss of propulsion system power.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, possible loss of ability to hover depending on aircraft weight. Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
4C1	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #3 failure	Input shaft of gearbox fails (or clutch), causing loss of torque from motor #3.	All	loss of torque from motor #3	Torque from other 3 motors transferred to prop-rotor #3 via interconnecting shaft	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
4C2	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #3 failure	Complete gearbox failure	All	loss of torque from motor #3 and loss of torque output to prop-rotor #3	No output to prop-rotor #3; unable to transfer motor #3 torque to other prop-rotors. 25% loss of propulsion system power.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, possible loss of ability to hover depending on aircraft weight. Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
4D1	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #4 failure	Input shaft of gearbox fails (or clutch), causing loss of torque from motor #4.	All	loss of torque from motor #4	Torque from other 3 motors transferred to prop-rotor #4 via interconnecting shaft	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
4D2	Provide torque to prop-rotors	5.00E-06	Prop-rotor Gearbox #4 failure	Complete gearbox failure	All	loss of torque from motor #4 and loss of torque output to prop-rotor #4	No output to prop-rotor #4; unable to transfer motor #4 torque to other prop-rotors. 25% loss of propulsion system power.	25% loss of propulsion system power. Aircraft handling qualities affected. Insufficient power available to control aircraft at airspeeds below 25 knots. Loss of control of aircraft if failure occurs while aircraft is in OMI avoid region.	Visual & audible warning provided to pilot	Limited flight envelope, possible loss of ability to hover depending on aircraft weight. Pilot diverts to alternate landing location and executes roll-on landing above 25 kts.	I	0.50	2.000E-01	Assumed to be in hover/OMI avoid region 20% of the time	5.00E-07
5A1	Provide system cooling for batteries	1.00E-05	Failure to provide chilled water to batteries	coolant leak	All	Coolant leaks until reservoir is empty and pump runs dry. No coolant provided to batteries; batteries quickly overheat	Battery cell failure, battery goes into thermal runaway. Battery catches fire, Reduced power available to 1 or more electric motors.	Aircraft fire, loss of controlled flight	System Health monitoring provides alert to pilot	(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	3.30E-09
5A2	Provide system cooling for batteries	1.90E-09	Failure to provide chilled water to batteries	Dual electrically driven pump failure. (both pumps failed)	All	No coolant flow from failed pumps.	Battery cell failure, battery goes into thermal runaway. Battery catches fire, Reduced power available to 1 or more electric motors.	Aircraft fire, loss of controlled flight	System Health monitoring provides alert to pilot	((1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00E+00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	6.27E-13
5A3	Provide system cooling for batteries	0.000508	Failure to provide chilled water to batteries	Vapor-cycle system failure, compressor, condenser, electric fan, etc.	All	Coolant temperature rises while circulating through all batteries. All batteries become equally hot.	Batteries overheat, causing battery cell failure, battery goes into thermal runaway. Battery catches fire. Reduced power available to 1 or more electric motors.	Aircraft fire, loss of controlled flight	System Health monitoring provides alert to pilot	(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	1.68E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
5B1	Provide system cooling for batteries	1.00E-06	Battery 1 cooling failure	clogged or kinked coolant line, clogged battery heat exchanger, defective bypass valve, or thermostat	All	Restricted coolant flow through battery. Battery temperature rises to critical temperature Causing battery failure.	Loss of ability to operate motor #1 from battery power in case of loss of main HVDC power source. Possible battery fire	Loss of motor #1 output. Battery fire causes loss of aircraft		(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	3.30E-10
5C1	Provide system cooling for batteries	1.00E-06	Battery 2 cooling failure	clogged or kinked coolant line, clogged battery heat exchanger, defective bypass valve, or thermostat	All	Restricted coolant flow through battery. Battery temperature rises to critical temperature Causing battery failure.	Loss of ability to operate motor #1 from battery power in case of loss of main HVDC power source. Possible battery fire	Loss of motor #2 output. Battery fire causes loss of aircraft		(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	3.30E-10
5D1	Provide system cooling for batteries	1.00E-06	Battery 3 cooling failure	clogged or kinked coolant line, clogged battery heat exchanger, defective bypass valve, or thermostat	All	Restricted coolant flow through battery. Battery temperature rises to critical temperature Causing battery failure.	Loss of ability to operate motor #1 from battery power in case of loss of main HVDC power source. Possible battery fire	Loss of motor #3 output. Battery fire causes loss of aircraft		(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	3.30E-10
5E+1	Provide system cooling for batteries	1.00E-06	Battery 4 cooling failure	clogged or kinked coolant line, clogged battery heat exchanger, defective bypass valve, or thermostat	All	Restricted coolant flow through battery. Battery temperature rises to critical temperature Causing battery failure.	Loss of ability to operate motor #1 from battery power in case of loss of main HVDC power source. Possible battery fire	Loss of motor #4 output. Battery fire causes loss of aircraft		(1) Automatic disconnect of batteries when they become hot. (2) Battery fire protection system contains battery failure to mitigate fire.	I	1.00	3.300E-04	Batteries only used in case of Primary HVDC source failure.	3.30E-10
										Criticality Summary	I				4.92E-04
											II				0.00E+00
											III				4.16E-04
											IV				1.00E-06

Table B- 2: Quad-Rotor FMECA Worksheet

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1A1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #1	HV Battery output failure or associated wiring. Loss of output to ESC #1 only.	All	No power to ESC #1; Motor #1 fails to provide output torque	Torque from other 3 motors is transferred to gearbox #1 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	2.50E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.00E-08
1B1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #2	HV Battery output failure or associated wiring. Loss of output to ESC #2 only.	All	No power to ESC #2; Motor #2 fails to provide output torque	Torque from other 3 motors is transferred to gearbox #2 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	2.50E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.00E-08
1C1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #3	HV Battery output failure or associated wiring. Loss of output to ESC #3 only.	All	No power to ESC #3; Motor #3 fails to provide output torque	Torque from other 3 motors is transferred to gearbox #3 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	2.50E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.00E-08
1D1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #4	HV Battery output failure or associated wiring. Loss of output to ESC #4 only.	All	No power to ESC #4; Motor #4 fails to provide output torque	Torque from other 3 motors is transferred to gearbox #4 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	2.50E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.00E-08
1E1	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure - No runaway.	All	Loss of output from single branch within battery network. Battery output voltage slightly reduced. Increased current draw from remaining battery cells	Output voltage slightly reduced to one or more motors.	Reduced range and/or slight degradation of motor performance.	Visual and audible warning provided to pilot.	Battery monitoring system must detect and isolate the fault. Continued operation with failed cell may put additional stress on other battery cells which must be managed to prevent catastrophic failure	IV	2.50E-01	1.00E+00	Beta = 1 for Cat III & Cat 4 FM's	2.50E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1E2	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure - Thermal runaway. - contained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery monitoring system detects failure, disconnects and isolates the defective battery cell.	Reduced battery system capacity, slight degradation of battery output voltage provided to one or more electric motors. Battery may catch fire. Excess heat generated may affect adjacent battery cells.	Reduced range and/or degradation electric motor performance.	Visual and audible warning provided to pilot.	Battery cooling and fire protection system must contain battery temperature to prevent loss of aircraft	III	2.50E-01	1.00E+00	Beta = 1 for Cat III & Cat 4 FM's	2.50E-07
1E3	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure internal short - thermal runaway - uncontained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery catches fire. Loss of all HVDC output.	No power provided to electric motors. Loss of torque output to rotors	Aircraft descends to ground. Autorotation employed to provide soft landing	Visual and audible warning provided to pilot. Pilot detects loss of power	Flight control system and rotor pitch control actuators are powered by a low voltage battery which is still operational. Controlled landing possible through autorotation	II	2.50E-01	1.00E-02	It is assumed that in most cases, battery failure will occur gradually giving the pilot time to land safely.	2.50E-09
1E4	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Complete HV battery failure; low voltage or no voltage output. (Battery discharged)	All	Loss of all HVDC output	No power provided to electric motors. Loss of torque output to rotors	Aircraft descends to ground. Autorotation employed to provide soft landing	Visual and audible warning provided to pilot. Pilot detects loss of power	Flight control system and rotor pitch control actuators are powered by a low voltage battery which is still operational. Controlled landing possible through autorotation	II	2.50E-01	1.00E-02	It is assumed that in most cases, battery voltage would decrease gradually, giving the pilot time to land safely.	2.50E-09
2A1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #1 to Gearbox #1	ESC #1 failure	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #1 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.40E-05
2A2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #1 to Gearbox #1	Motor #1 failure	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #1 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.85E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2A3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #1 to Gearbox #1	Clutch #1 failure - failure to engage	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #1 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	5.00E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.20E-08
2A4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #1 to Gearbox #1	Clutch #1 failure - failure to disengage	All	No effect on normal operation. In the event of motor failure, clutch failure will transfer torque from other motors.	Torque from other 3 motors forces motor #1 to continue to spin. In case of motor- stator contact, friction causes excessive heat to be generated, causing motor to catch fire.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	None	Fire detection and suppression system must contain fire.	I	5.00E-01	4.62E-05	Probability of motor bearing failure or motor-stator contact assumed to be half of motor failure rate.	9.70E-12
2A5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #1 to Gearbox #1	ESC #1 cooling fan failure	All	ESC temperature rises rapidly.	ESC #1 fails, loss of Motor #1 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	System health monitoring detects cooling failure, Motor #1 output can be reduced or turned off either manually or automatically to prevent overheating of ESC. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.85E-06
2A6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #1 to Gearbox #1	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #1 overheats.	Motor #1 fails, loss of Motor #1 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Motor oil temperature and/or pressure indication provided to pilot.	System health monitoring detects cooling failure, Motor #1 output can be reduced or turned off either manually or automatically to prevent overheating. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.03E-06
2B1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #2 to Gearbox #2	ESC #2 failure	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #2 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.40E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2B2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #2 to Gearbox #2	Motor #2 failure	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #2 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.85E-05
2B3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #2 to Gearbox #2	Clutch #2 failure - failure to engage	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #2 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	5.00E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.20E-08
2B4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #2 to Gearbox #2	Clutch #2 failure - failure to disengage	All	No effect on normal operation. In the event of motor failure, clutch failure will transfer torque from other motors.	Torque from other 3 motors forces motor #2 to continue to spin. In case of motor- stator contact, friction causes excessive heat to be generated, causing motor to catch fire.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	None	Fire detection and suppression system must contain fire.	I	5.00E-01	4.62E-05	Probability of motor bearing failure or motor-stator contact assumed to be half of motor failure rate.	9.70E-12
2B5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #2 to Gearbox #2	ESC #2 cooling fan failure	All	ESC temperature rises rapidly.	ESC #2 fails, loss of Motor #2 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating of ESC. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.85E-06
2B6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #2 to Gearbox #2	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #2 overheats.	Motor #2 fails, loss of Motor #2 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Motor oil temperature and/or pressure indication provided to pilot.	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.03E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2C1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #3 to Gearbox #3	ESC #3 failure	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #3 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.40E-05
2C2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #3 to Gearbox #3	Motor #3 failure	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #3 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.85E-05
2C3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #3 to Gearbox #3	Clutch #3 failure - failure to engage	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #3 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	5.00E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.20E-08
2C4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #3 to Gearbox #3	Clutch #3 failure - failure to disengage	All	No effect on normal operation. In the event of motor failure, clutch failure will transfer torque from other motors.	Torque from other 3 motors forces motor #3 to continue to spin. In case of motor- stator contact, friction causes excessive heat to be generated, causing motor to catch fire.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	None	Fire detection and suppression system must contain fire.	I	5.00E-01	4.62E-05	Probability of motor bearing failure or motor-stator contact assumed to be half of motor failure rate.	9.70E-12
2C5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #3 to Gearbox #3	ESC #3 cooling fan failure	All	ESC temperature rises rapidly.	ESC #3 fails, loss of Motor #3 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating of ESC. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.85E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2C6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #3 to Gearbox #3	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #3 overheats.	Motor #3 fails, loss of Motor #3 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Motor oil temperature and/or pressure indication provided to pilot.	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.03E-06
2D1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #4 to Gearbox #4	ESC #4 failure	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #4 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	5.40E-05
2D2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #4 to Gearbox #4	Motor #4 failure	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #4 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	1.00E+00	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.85E-05
2D3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #4 to Gearbox #4	Clutch #4 failure - failure to engage	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	Torque from other 3 motors is transferred to gearbox #4 through collector gearbox. Available power reduced	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Visual and audible warning provided to pilot.	Pilot can avoid flight conditions which require maximum torque. Pilot can use energy stored in rotors to provide soft landing (autorotate)	I	5.00E-01	2.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.20E-08
2D4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #4 to Gearbox #4	Clutch #4 failure - failure to disengage	All	No effect on normal operation. In the event of motor failure, clutch failure will transfer torque from other motors.	Torque from other 3 motors forces motor #4 to continue to spin. In case of motor- stator contact, friction causes excessive heat to be generated, causing motor to catch fire.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	None	Fire detection and suppression system must contain fire.	I	5.00E-01	4.62E-05	Probability of motor bearing failure or motor-stator contact assumed to be half of motor failure rate.	9.70E-12

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2D5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #4 to Gearbox #4	ESC #4 cooling fan failure	All	ESC temperature rises rapidly.	ESC #4 fails, loss of Motor #4 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating of ESC. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.85E-06
2D6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #4 to Gearbox #4	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #4 overheats.	Motor #4 fails, loss of Motor #4 output.	Limited flight envelope. Reduced maximum speed and insufficient power to take off or hover at max weight. Loss of air raft Possible hard landing if failure occurs while in OMI avoid region (< 20 kts)	Motor oil temperature and/or pressure indication provided to pilot.	System health monitoring detects cooling failure, Motor output can be reduced or turned off either manually or automatically to prevent overheating. Full power may still be available for short periods.	I	1.00E+00	2.00E-02	Assume pilot will be able to prevent overheat and avoid ESC failure 90% of the time.	1.03E-06
3A1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #1 to Rotor #1 and transfer torque to/from collector gearbox	Gearbox #1 Failure, failure to transfer torque from motor #1 or collector gearbox to Rotor #1	All	Unable to transfer torque to Rotor #1.	No lift available to Rotor #1. Torque From Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3A2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #1 to Rotor #1 and transfer torque to/from collector gearbox	Gearbox #1 seized;	Flight	Unable to transfer torque Rotor #1. Potential damage to interconnecting drive shaft and collector gearbox.	Excess drag on collector gearbox consumes power from remaining 3 motors.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3B1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #2 to Rotor #2 and transfer torque to/from collector gearbox	Gearbox #2 Failure, failure to transfer torque from motor #2 or collector gearbox to Rotor #2	All	Unable to transfer torque to Rotor #2.	No lift available to Rotor #2. Torque From Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3B2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #2 to Rotor #2 and transfer torque to/from collector gearbox	Gearbox #2 seized;	Flight	Unable to transfer torque Rotor #2. Potential damage to interconnecting drive shaft and collector gearbox.	Excess drag on collector gearbox consumes power from remaining 3 motors.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3C1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #3 to Rotor #3 and transfer torque to/from collector gearbox	Gearbox #3 Failure, failure to transfer torque from motor #3 or collector gearbox to Rotor #3	All	Unable to transfer torque to Rotor #3.	No lift available to Rotor #3. Torque From Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3C2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #3 to Rotor #3 and transfer torque to/from collector gearbox	Gearbox #3 seized;	Flight	Unable to transfer torque Rotor #3. Potential damage to interconnecting drive shaft and collector gearbox.	Excess drag on collector gearbox consumes power from remaining 3 motors.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3D1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #4 to Rotor #4 and transfer torque to/from collector gearbox	Gearbox #4 Failure, failure to transfer torque from motor #4 or collector gearbox to Rotor #4	All	Unable to transfer torque to Rotor #4.	No lift available to Rotor #4. Torque From Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3D2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #4 to Rotor #4 and transfer torque to/from collector gearbox	Gearbox #4 seized;	Flight	Unable to transfer torque Rotor #4. Potential damage to interconnecting drive shaft and collector gearbox.	Excess drag on collector gearbox consumes power from remaining 3 motors.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control and soft landing	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3E1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque between motors and rotors	Combiner Gearbox Failure, unable to transfer torque	All	Loss of ability to transfer torque between rotor gearboxes.	Loss of ability to cross-shaft power in the event of a motor failure	None	Visual and audible alert provided to pilot	None	I	5.00E-01	3.64E-04	probability of loss of single motor output	9.10E-10
3E2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque between motors and rotors	Combiner gearbox seized	All	collector gearbox stops turning and causes sudden stop of interconnecting Drive shafts.	Potential damage to interconnecting drive shafts and rotor gearboxes.	Loss of power to all 4 rotors. Loss of control of aircraft. Loss of aircraft and crew	Visual and audible alert provided to pilot	None	I	5.00E-01	3.64E-04	probability of loss of single motor output	9.10E-10

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
										Criticality Summary:	I				3.08E-04
											II				0.00E+00
											III				2.50E-07
											IV				2.50E-07

Table B- 3: Alternate Configuration –Quad-Rotor without Interconnecting Shafting FMECA Worksheet

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1A1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #1	HV Battery output failure or associated wiring. Loss of output to ESC #1 only.	All	Unable to transfer torque to Rotor #1.	No lift available to Rotor #1. Torque from Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts controls to other 3 rotors to maintain limited control as aircraft descends to ground	I	2.50E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-07
1B1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #2	HV Battery output failure or associated wiring. Loss of output to ESC #2 only.	All	No power to ESC #2; Motor #2 fails to provide output torque	No lift available to Rotor #2. Torque from Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts controls to other 3 rotors to maintain limited control as aircraft descends to ground	I	2.50E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-07
1C1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #3	HV Battery output failure or associated wiring. Loss of output to ESC #3 only.	All	No power to ESC #3; Motor #3 fails to provide output torque	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts controls to other 3 rotors to maintain limited control as aircraft descends to ground	I	2.50E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-07
1D1	Provide HVDC power to electric motors	1.00E-06	Failure to provide HVDC electrical energy to ESC #4	HV Battery output failure or associated wiring. Loss of output to ESC #4 only.	All	No power to ESC #4; Motor #4 fails to provide output torque	No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts controls to other 3 rotors to maintain limited control as aircraft descends to ground	I	2.50E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-07
1E+1	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure - no runaway.	All	Loss of output from single branch within battery network. Battery output voltage slightly reduced. Increased current draw from remaining battery cells	Output voltage slightly reduced to one or more motors.	Reduced range and/or slight degradation of motor performance.	Visual and audible warning provided to pilot.	Battery monitoring system must detect and isolate the fault. Continued operation with failed cell may put additional stress on other battery cells which must be managed to prevent catastrophic failure	IV	2.50E-01	1.00E+00	Beta = 1 for Cat III & Cat 4 FM's	2.50E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1E+2	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure - Thermal runaway. - contained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery monitoring system detects failure, disconnects and isolates the defective battery cell.	Reduced battery system capacity, slight degradation of battery output voltage provided to one or more electric motors. Battery may catch fire. Excess heat generated may affect adjacent battery cells.	Reduced range and/or degradation electric motor performance.	Visual and audible warning provided to pilot.	Battery cooling and fire protection system must contain battery temperature to prevent loss of aircraft	III	2.50E-01	1.00E+00	Beta = 1 for Cat III & Cat 4 FM's	2.50E-07
1E+3	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Battery cell failure internal short - thermal runaway - uncontained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery catches fire. Loss of all HVDC output.	No power provided to electric motors. Loss of torque output to rotors	Aircraft descends to ground. Autorotation employed to provide soft landing	Visual and audible warning provided to pilot. Pilot detects loss of power	Flight control system and rotor pitch control actuators are powered by a low voltage battery which is still operational. Controlled landing possible through autorotation	II	2.50E-01	1.00E-02	It is assumed that in most cases, battery failure will occur gradually giving the pilot time to land safely.	2.50E-09
1E+4	Provide HVDC power to electric motors	1.00E-06	Internal battery failure	Complete HV battery failure; low voltage or no voltage output. (Battery discharged)	All	Loss of all HVDC output	No power provided to electric motors. Loss of torque output to rotors	Aircraft descends to ground. Autorotation employed to provide soft landing	Visual and audible warning provided to pilot. Pilot detects loss of power	Flight control system and rotor pitch control actuators are powered by a low voltage battery which is still operational. Controlled landing possible through autorotation	II	2.50E-01	1.00E-02	It is assumed that in most cases, battery voltage would decrease gradually, giving the pilot time to land safely.	2.50E-09
2A1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #1 to Gearbox #1	ESC #1 failure	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	No lift available to Rotor #1. Torque from Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.35E-04
2A2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #1 to Gearbox #1	Motor #1 failure	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	No lift available to Rotor #1. Torque from Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.62E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2A3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #1 to Gearbox #1	Clutch #1 failure - failure to engage	All	No output from ESC #1 to Motor #1. Motor #1 fails to provide output torque.	No lift available to Rotor #1. Torque from Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Clutch must be engaged for normal operation	1.05E-07
2A4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #1 to Gearbox #1	Clutch #1 failure - failure to disengage	All	No effect on normal operation.	None	None	None		IV	5.00E-01	1.00E+00		2.10E-07
2A5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #1 to Gearbox #1	ESC #1 cooling fan failure	All	ESC temperature rises rapidly.	ESC #1 fails, loss of Motor #1 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid ESC failure 50% of the time.	4.62E-05
2A6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #1 to Gearbox #1	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #1 overheats.	Motor #1 fails, loss of Motor #1 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	Motor oil temperature and/or pressure indication provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid Motor failure 50% of the time.	2.59E-05
2B1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #2 to Gearbox #2	ESC #2 failure	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	No lift available to Rotor #2. Torque from Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.35E-04
2B2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #2 to Gearbox #2	Motor #2 failure	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	No lift available to Rotor #2. Torque from Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.62E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2B3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #2 to Gearbox #2	Clutch #2 failure - failure to engage	All	No output from ESC #2 to Motor #2. Motor #2 fails to provide output torque.	No lift available to Rotor #2. Torque from Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Clutch must be engaged for normal operation	1.05E-07
2B4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #2 to Gearbox #2	Clutch #2 failure - failure to disengage	All	No effect on normal operation.	None	None	None		IV	5.00E-01	1.00E+00		2.10E-07
2B5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #2 to Gearbox #2	ESC #2 cooling fan failure	All	ESC temperature rises rapidly.	ESC #2 fails, loss of Motor #2 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid ESC failure 50% of the time.	4.62E-05
2B6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #2 to Gearbox #2	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #2 overheats.	Motor #2 fails, loss of Motor #2 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	Motor oil temperature and/or pressure indication provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid Motor failure 50% of the time.	2.59E-05
2C1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #3 to Gearbox #3	ESC #3 failure	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.35E-04
2C2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #3 to Gearbox #3	Motor #3 failure	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.62E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2C3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #3 to Gearbox #3	Clutch #3 failure - failure to engage	All	No output from ESC #3 to Motor #3. Motor #3 fails to provide output torque.	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Clutch must be engaged for normal operation	1.05E-07
2C4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #3 to Gearbox #3	Clutch #3 failure - failure to disengage	All	No effect on normal operation.	None	None	None		IV	5.00E-01	1.00E+00		2.10E-07
2C5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #3 to Gearbox #3	ESC #3 cooling fan failure	All	ESC temperature rises rapidly.	ESC #3 fails, loss of Motor #3 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid ESC failure 50% of the time.	4.62E-05
2C6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #3 to Gearbox #3	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #3 overheats.	Motor #3 fails, loss of Motor #3 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	Motor oil temperature and/or pressure indication provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid Motor failure 50% of the time.	2.59E-05
2D1	Convert HV electrical energy to shaft torque	2.70E-04	Failure to provide output torque from Motor #4 to Gearbox #4	ESC #4 failure	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.35E-04
2D2	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #4 to Gearbox #4	Motor #4 failure	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	4.62E-05

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2D3	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #4 to Gearbox #4	Clutch #4 failure - failure to engage	All	No output from ESC #4 to Motor #4. Motor #4 fails to provide output torque.	No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible warning provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Clutch must be engaged for normal operation	1.05E-07
2D4	Convert HV electrical energy to shaft torque	4.20E-07	Failure to provide output torque from Motor #4 to Gearbox #4	Clutch #4 failure - failure to disengage	All	No effect on normal operation.	None	None	None		IV	5.00E-01	1.00E+00		2.10E-07
2D5	Convert HV electrical energy to shaft torque	9.24E-05	Failure to provide output torque from Motor #4 to Gearbox #4	ESC #4 cooling fan failure	All	ESC temperature rises rapidly.	ESC #4 fails, loss of Motor #4 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	ESC cooling fan failure indication provided to pilot. ESC Hot indication provided if ESC overheats	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid ESC failure 50% of the time.	4.62E-05
2D6	Convert HV electrical energy to shaft torque	5.17E-05	Failure to provide output torque from Motor #4 to Gearbox #4	Motor cooling oil pump failure or oil leak	All	Loss of cooling/lube oil pressure or oil flow, Motor #4 overheats.	Motor #4 fails, loss of Motor #4 output.	Aircraft fire. Substantial damage to aircraft, Possible loss of aircraft.	Motor oil temperature and/or pressure indication provided to pilot.	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	1.00E+00	5.00E-01	Assume pilot will be able to prevent overheat and avoid Motor failure 50% of the time.	2.59E-05
3A1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #1 to Rotor #1	Gearbox #1 Failure, failure to transfer torque from motor #1 to Rotor #1	All	Unable to transfer torque to Rotor #1.	No lift available to Rotor #1. Torque from Motor #1 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3A2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #1 to Rotor #1	Gearbox #1 seized; Motor and rotor stop rotation	Flight	Unable to transfer torque Rotor #1. Potential damage to motor #1 and rotor.		Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3B1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #2 to Rotor #2	Gearbox #2 Failure, failure to transfer torque from motor #2 or collector gearbox to Rotor #2	All	Unable to transfer torque to Rotor #2.	No lift available to Rotor #2. Torque from Motor #2 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3B2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #2 to Rotor #2	Gearbox #2 seized;	Flight	Unable to transfer torque Rotor #2. potential damage to motor and		Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3C1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #3 to Rotor #3	Gearbox #3 Failure, failure to transfer torque from motor #3 or collector gearbox to Rotor #3	All	Unable to transfer torque to Rotor #3.	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3C2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #3 to Rotor #3	Gearbox #3 seized;	Flight	Unable to transfer torque Rotor #3.	No lift available to Rotor #3. Torque from Motor #3 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06
3D1	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #4 to Rotor #4	Gearbox #4 Failure, failure to transfer torque from motor #4 or collector gearbox to Rotor #4	All	Unable to transfer torque to Rotor #4.	No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3D2	Transfer motor torque to rotors	5.00E-06	Failure to transfer torque from Motor #4 to Rotor #4	Gearbox #4 seized;	Flight	Unable to transfer torque Rotor #4.	Potential damage to motor and rotor assembly. No lift available to Rotor #4. Torque from Motor #4 unusable. Unable to maintain level flight.	Aircraft descends to ground with limited control.	Visual and audible alert provided to pilot	Flight control system adjusts speed and pitch to other 3 rotors to maintain limited control as aircraft descends to ground	I	5.00E-01	5.00E-01	Beta will be highly dependent upon detailed design and controllability of aircraft with limited power	1.25E-06

Criticality Summary		
	I	1.02E-03
	II	0.00E+00
	III	2.50E-07
	IV	1.09E-06

Table B- 4: Side-by-Side (Lateral-Twin) FMECA Worksheet

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1A1	Provide main engine torque to intermediate gearboxes	2.67E-06	Failure to provide engine torque to the Intermediate gearbox #1	Engine #1 Failure	All	Loss of primary power output to Intermediate gearbox #1.	Intermediate gearbox #1 draws power from engine #2 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible alert provided to pilot	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	5.34E-07
1A2	Provide main engine torque to intermediate gearboxes	5.00E-06	Failure to provide engine torque to the Intermediate gearbox #1	Engine #1 gearbox failure,	All	Loss of primary power output to Intermediate gearbox #1.	Intermediate gearbox #1 draws power from engine #2 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible warning provided to pilot.	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	1.00E-06
1A3	Provide main engine torque to intermediate gearboxes	4.20E-07	Failure to provide engine torque to the Intermediate gearbox #1	Engine #1 overrunning clutch fails to engage	All	Loss of primary power output to Intermediate gearbox #1.	Intermediate gearbox #1 draws power from engine #2 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible warning provided to pilot.	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	8.40E-08
1B1	Provide main engine torque to intermediate gearboxes	2.67E-06	Failure to provide engine torque to the Intermediate gearbox #2	Engine #2 Failure	All	Loss of primary power output to Intermediate gearbox #2.	Intermediate gearbox #2 draws power from engine #1 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible alert provided to pilot	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	5.34E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1B2	Provide main engine torque to intermediate gearboxes	5.00E-06	Failure to provide engine torque to the Intermediate gearbox #2	Engine #2 gearbox failure,	All	Loss of primary power output to Intermediate gearbox #2.	Intermediate gearbox #2 draws power from engine #1 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible warning provided to pilot.	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	1.00E-06
1B3	Provide main engine torque to intermediate gearboxes	4.20E-07	Failure to provide engine torque to the Intermediate gearbox #2	Engine #2 overrunning clutch fails to engage	All	Loss of primary power output to Intermediate gearbox #2.	Intermediate gearbox #2 draws power from engine #1 and electric motor through collector gearbox. Insufficient power to maintain flight in hover OEI avoid region. Reduced or no power available to charge batteries	Loss of aircraft if failure occurs while in OEI avoid region of flight. Reduced maximum speed in forward flight. Loss of ability to hover below specified minimum forward speed.	Visual and audible warning provided to pilot.	Pilot diverts to alternate landing area where landing in forward flight is possible. Pilot must manage cruise speed to preserve battery power which will be needed for landing.	I	1.00E+00	2.00E-01	Assumed that the aircraft is in hover/ OEI avoid region 20% of flight time	8.40E-08
2A1	Transfer shaft torque from engines to rotors and provide rotor synchronization	5.00E-06	Failure to transfer torque to rotor #1	Intermediate gearbox #1 failure; failure to receive transfer torque input. To output.	All	Loss of output torque to rotor gearbox #1.	Loss of control of output to rotor #1. No control over rotor speed and position. Rotor-rotor contact possible	Loss of controlled flight. Loss of aircraft.	Visual and audible warning provided to pilot.	None.	I	1.00E+00	1.00E+00	Assume that gearbox failure in flight will always result in loss of aircraft	5.00E-06
2A2	Transfer shaft torque from engines to rotors and provide rotor synchronization	5.00E-06	Failure to transfer torque to rotor #1	Rotor gearbox #1 failure	All	Loss of output torque to rotor gearbox #1.	Loss of control of output to rotor #1. No control over rotor speed and position. Rotor-rotor contact possible	Loss of controlled flight. Loss of aircraft.	Visual and audible warning provided to pilot.	None.	I	1.00E+00	1.00E+00	Assume that gearbox failure in flight will always result in loss of aircraft	5.00E-06
2B1	Transfer shaft torque from engines to rotors and provide rotor synchronization	5.00E-06	Failure to transfer torque to rotor #2	Intermediate gearbox #2 failure; failure to receive transfer torque input. To output.	All	Loss of output torque to rotor gearbox #2.	Loss of control of output to rotor #2. No control over rotor speed and position. Rotor-rotor contact possible	Loss of controlled flight. Loss of aircraft.	Visual and audible warning provided to pilot.	None.	I	1.00E+00	1.00E+00	Assume that gearbox failure in flight will always result in loss of aircraft	5.00E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2B2	Transfer shaft torque from engines to rotors and provide rotor synchronization	5.00E-06	Failure to transfer torque to rotor #2	Rotor gearbox #2 failure	All	Loss of output torque to rotor gearbox #2.	Loss of control of output to rotor #2. No control over rotor speed and position. Rotor-rotor contact possible	Loss of controlled flight. Loss of aircraft.	Visual and audible warning provided to pilot.	None.	I	1.00E+00	1.00E+00	Assume that gearbox failure in flight will always result in loss of aircraft	5.00E-06
2C1	Transfer shaft torque from engines to rotors and provide rotor synchronization	5.00E-06	Failure to transfer power and provide synchronization between rotor #1 and rotor #2	Collector gearbox failure	All	Loss of ability to synchronize rotors. Power from electric motor is unusable	Rotor to rotor contact causes damage to rotors. Reduced net power available to hover/land.	Unable to hover. Loss of controlled flight if damage causes rotor failure. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot diverts to alternate landing site and lands as soon as possible in forward flight.	I	1.00E+00	1.00E+00	Assume that loss of synch will always result in loss of aircraft	5.00E-06
2C2	Transfer shaft torque from engines to rotors and provide rotor synchronization	9.30E-07	Failure to transfer power and provide synchronization between rotor #1 and rotor #2	Interconnect shaft #1 failure	All	Loss of ability to synchronize rotors. Power from electric motor cannot be transferred to rotor #1	Rotor to rotor contact causes damage to rotors. Net power available to hover/land slightly reduced.	Limited ability to hover. Loss of controlled flight if damage causes rotor failure. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot lands as soon as possible. (assume that vertical landing is still possible)	I	1.00E+00	1.00E+00	Assume that loss of synch will always result in loss of aircraft	9.30E-07
2C3	Transfer shaft torque from engines to rotors and provide rotor synchronization	9.30E-06	Failure to transfer power and provide synchronization between rotor #1 and rotor #2	Interconnect shaft #2 failure	All	Loss of ability to synchronize rotors. Power from electric motor cannot be transferred to rotor #2	Rotor to rotor contact causes damage to rotors. Net power available to hover/land slightly reduced.	Limited ability to hover. Loss of controlled flight if damage causes rotor failure. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot lands as soon as possible. (assume that vertical landing is still possible)	I	1.00E+00	1.00E+00	Assume that loss of synch will always result in loss of aircraft	9.30E-06
3A1	Provide electric motor boost power for hover and low speed flight	1.00E-06	Failure to provide shaft power from electric motor	Battery cell failure, no runaway	All	Loss of output from single branch within battery network. Battery output voltage slightly reduced. Increased current draw from remaining battery cells	slight reduction in battery power available to electric motor	Slight reduction in available power during hover, maximum time in hover slightly reduced.	Visual and audible alert provided to pilot	Pilot must compensate for slight reduction in hover capability	III	3.33E-01	1.00E+00	beta = 1 for Category III and IV	3.33E-07

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3A2	Provide electric motor boost power for hover and low speed flight	1.00E-06	Failure to provide shaft power from electric motor	Battery cell failure, thermal runaway contained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery monitoring system detects failure, disconnects and isolates the defective battery cell.	Reduced battery system capacity, slight degradation of battery output voltage provided to one or more electric motors. Battery may catch fire. Excess heat generated may affect adjacent battery cells.	Slight reduction in available power during hover, maximum time in hover slightly reduced.	Visual and audible alert provided to pilot	None	III	3.33E-01	1.00E+00	beta = 1 for Category III and IV	3.33E-07
3A3	Provide electric motor boost power for hover and low speed flight	1.00E-06	Failure to provide shaft power from electric motor	Battery cell failure, thermal runaway uncontained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery catches fire. Loss of all HVDC output.	No HVDC power available to power motor. No electric motor power available.	Loss of motor power necessary for hover and low speed flight. Loss of aircraft if failure occurs while in OMI avoid region of flight.	Visual and audible alert provided to pilot	Pilot must exit OMI avoid region ASAP. Pilot diverts to alternate landing site and lands in forward flight.	I	3.34E-01	2.00E-01		6.68E-08
3A4	Provide electric motor boost power for hover and low speed flight	5.08E-04	Failure to provide shaft power from electric motor	Battery cooling system failure	All	Battery temperature rises rapidly, battery failure occurs if not	Battery availability limited, availability of electric motor significantly reduced.	Unable to continue to hover or maintain low speed flight.	Visual and audible alert provided to pilot	Pilot must exit OMI avoid region ASAP. Pilot diverts to alternate landing site and lands in forward flight.	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	5.08E-04
3A5	Provide electric motor boost power for hover and low speed flight	2.70E-04	Failure to provide shaft power from electric motor	ESC failure	All	No electrical output to drive motor. Motor fails to provide output power	No boost power available from electric motor. Insufficient power to maintain flight while in hover or low speed flight	Loss of ability to hover or fly at low speed. Loss of aircraft if failure occurs while in OMI avoid region.	Visual and audible alert provided to pilot	Pilot must divert to alternate landing site and land in forward flight.	I	1.00E+00	2.00E-01	assume that aircraft is in hover or low speed flight 20% of the flight time	5.40E-05
3A6	Provide electric motor boost power for hover and low speed flight	9.24E-06	Failure to provide shaft power from electric motor	ESC cooling fan failure	All	ESC temperature increases	ESC shuts down or limits output due to over temperature. Reduced or no boost power available from electric motor. Insufficient power to maintain flight while in hover or low speed flight.	Unable to continue to hover or maintain low speed flight.	Visual and audible alert provided to pilot	Pilot must exit OMI avoid region ASAP. Hover for short periods might be possible depending on conditions. Pilot may divert to alternate landing site and lands in forward flight.	II	1.00E+00	1.00E+00		9.24E-06
3A7	Provide electric motor boost power for hover and low speed flight	1.97E-05	Failure to provide shaft power from electric motor	Electric motor/generator failure	All	No boost power available from electric motor.	Insufficient power to maintain flight while in hover or low speed flight	Loss of ability to hover or fly at low speed. Loss of aircraft if failure occurs while in OMI avoid region.	Visual and audible alert provided to pilot	Pilot must exit OMI avoid region ASAP. Pilot diverts to alternate landing site and lands in forward flight.	I	1.00E+00	2.00E-01	assume that aircraft is in hover or low speed flight 20% of the flight time	3.94E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3A8	Provide electric motor boost power for hover and low speed flight	5.17E-05	Failure to provide shaft power from electric motor	Electric motor cooling and lube failure	All	Increased friction and temperature in motor.	Motor temperature rises, eventually causing motor failure.	Loss of ability to hover or fly at low speed. If failure occurs while in OMI avoid region pilot must exit OMI avoid region immediately.	Visual and audible alert provided to pilot	Pilot must exit OMI avoid region ASAP. Pilot diverts to alternate landing site and lands in forward flight.	II	1.00E+00	1.00E+00		5.17E-05
3A9	Provide electric motor boost power for hover and low speed flight	5.01E-06	Failure to provide shaft power from electric motor	Clutch (emergency disconnect) failure	All	Loss of ability to disconnect motor/generator in case of motor/generator failure	None during normal operation; potential damage/ aircraft fire in case of motor generator failure.	Aircraft fire,	Visual and audible alert provided to pilot	Fire suppression system contains fire.	I	9.75E-06	2.00E-01	assume that loss of function does not impact flying qualities and pilot is already operating in emergency procedures because of electric motor failure	9.77E-12
3B1	Provide electric motor boost power for hover and low speed flight	2.70E-02	Failure to provide electrical power to charge battery	ESC failure. Loss of charge capability	All	Loss of HVDC output to charge batteries,	Unable to charge battery during cruise.	Hover capability is limited to remaining charge in battery.	Visual and audible alert provided to pilot	Pilot must manage available battery charge to complete flight and land safely	III	1.00E+00	1.00E+00		2.70E-02

Criticality Summary:		
	I	9.65E-05
	II	6.10E-05
	III	2.75E-02
	IV	0.00E+00

Table B- 5: Lift+Cruise FMECA Worksheet

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
1A1	Provide HVDC for propulsion and to charge batteries	2.67E-06	Failure to provide shaft power to gearbox	Turbo-shaft engine failure	All	Loss of HVDC electrical power to drive lift and thrust motors and to charge batteries	Electric motors operate from battery power only. Increased power demand from batteries. Batteries rapidly discharge.	Loss of propulsion if pilot cannot land safely before batteries are discharged. Loss of aircraft.	Visual and audible alert provided to pilot	Pilot follows emergency procedures to find safe landing area and land immediately	I	1.00E+00	6.00E-01	Assume that pilot will be able to find a safe landing area within before batteries discharge 40% of the time.	1.60E-06
1B1	Provide HVDC for propulsion and to charge batteries	5.00E-06	Failure to provide shaft power to AC generator	Gearbox failure	All	Loss of HVDC electrical power to drive lift and thrust motors and to charge batteries	Electric motors operate from battery power only. Increased power demand from batteries. Batteries rapidly discharge.	Loss of propulsion if pilot cannot land safely before batteries are discharged. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot follows emergency procedures to find safe landing area and land immediately	I	1.00E+00	6.00E-01	Assume that pilot will be able to find a safe landing area within before batteries discharge 40% of the time.	3.00E-06
1C1	Provide HVDC for propulsion and to charge batteries	9.24E-05	Failure to convert shaft power to AC electrical power	AC Generator failure	All	Loss of HVDC electrical power to drive lift and thrust motors and to charge batteries	Electric motors operate from battery power only. Increased power demand from batteries. Batteries rapidly discharge.	Loss of propulsion if pilot cannot land safely before batteries are discharged. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot follows emergency procedures to find safe landing area and land immediately	I	1.00E+00	6.00E-01	Assume that pilot will be able to find a safe landing area within before batteries discharge 40% of the time.	5.54E-05
1D1	Provide HVDC for propulsion and to charge batteries	2.00E-04	Failure to convert AC electrical power to HVDC electrical power	AC/DC converter failure	All	Loss of HVDC electrical power to drive lift and thrust motors and to charge batteries	Electric motors operate from battery power only. Increased power demand from batteries. Batteries rapidly discharge.	Loss of propulsion if pilot cannot land safely before batteries are discharged. Loss of aircraft.	Visual and audible alert provided to pilot	Pilot follows emergency procedures to find safe landing area and land immediately	I	1.00E+00	6.00E-01	Assume that pilot will be able to find a safe landing area within before batteries discharge 40% of the time.	1.20E-04
2A1	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #1 only.	All	No power to ESC #1 Motor #1 fails to provide output torque to rotor.	No lift available to Rotor #1. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A2	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #2 only.	All	No power to ESC #2 Motor #2 fails to provide output torque to rotor.	No lift available to Rotor #2. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
2A3	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #3 only.	All	No power to ESC #3 Motor #3 fails to provide output torque to rotor.	No lift available to Rotor #3. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A4	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #4 only.	All	No power to ESC #4 Motor #4 fails to provide output torque to rotor.	No lift available to Rotor #4. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A5	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #5 only.	All	No power to ESC #5 Motor #5 fails to provide output torque to rotor.	No lift available to Rotor #5. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A6	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #6 only.	All	No power to ESC #6 Motor #6 fails to provide output torque to rotor.	No lift available to Rotor #6. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A7	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #7 only.	All	No power to ESC #7 Motor #7 fails to provide output torque to rotor.	No lift available to Rotor #7. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A8	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC #8 only.	All	No power to ESC #8 Motor #8 fails to provide output torque to rotor.	No lift available to Rotor #8. Flight handling qualities affected.	Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2A9	Provide HVDC electrical power to motors	1.00E-06	Failure to provide HVDC electrical energy single ESC (all other ESC's still have power)	HV Battery output failure or associated wiring. Loss of output to ESC (thrust motor) only.	All	No power to thrust ESC. Thrust motor fails to provide output torque to propeller.	No forward thrust available for forward flight. Aircraft reverts to hover for remainder of flight.	Aircraft speed and range significantly reduced. Ability to hover is unaffected. Loss of aircraft if pilot cannot find safe landing area within range.	Visual and audible alert provided to pilot	Aircraft may have limited glide capability depending on altitude and forward speed at time of failure. Pilot must find safe landing area within range.	III	1.00E+00	5.00E-01	Assume 50% probability that the pilot will find safe landing area within reduced range	5.00E-07
2B1	Provide HVDC electrical power to motors	1.00E-06	Internal battery failure	Battery cell failure, no runaway	All	Loss of output from single branch within battery network. Battery output	Output voltage slightly reduced to one or more motors. Slight degradation of motor	None. Pilot still maintains control of aircraft.	Battery fault advisory provided to pilot	Battery monitoring system detects and isolates the fault. Continued operation with	IV	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
						voltage slightly reduced. Increased current draw from remaining battery cells	performance during hover.			failed cell may put additional stress on other battery cells which must be managed to prevent catastrophic					
2B2	Provide HVDC electrical power to motors	1.00E-06	Internal battery failure	Battery cell failure, thermal runaway contained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery monitoring system detects failure, disconnects and isolates the defective battery cell(s).	Reduced battery system capacity, degradation of battery output voltage provided to one or more electric motors. Battery may catch fire. Excess heat generated may affect adjacent battery cells.	Reduced system power available. Pilot still maintains control of aircraft.	battery fault advisory provided to pilot	Battery cooling and fire protection system must contain battery temperature to prevent loss of aircraft	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	1.00E-06
2B3	Provide HVDC electrical power to motors	1.00E-06	Internal battery failure	Battery cell failure, thermal runaway uncontained	All	Battery cell temperature rises rapidly, causing thermal runaway. Battery catches fire. Loss of all HVDC output.	Aircraft fire; possible damage to other flight critical systems. No battery power available for electric motors. Motors may still operate from HVDC provided by the engine and generator	Loss of propulsion and/or other critical systems required for flight. Loss of aircraft.	Visual and audible warning provided to pilot. Pilot detects loss of power	Flight control system and flight control surfaces are powered by a low voltage battery which is still operational.	I	1.00E+00	1.00E+00	Catastrophic outcome is assumed.	1.00E-06
2B4	Provide HVDC electrical power to motors	1.00E-06	Internal battery failure	Complete HV system failure; no voltage output to power electric motors.	All	Loss of all HVDC output to all motors	No HVDC power available for electric motors. Flight control system and control surfaces are powered by a low voltage battery which is still operational.	Aircraft descends to ground. Glide may be possible depending upon conditions at time of failure. Loss of control of aircraft	Visual and audible warning provided to pilot. Pilot detects loss of power	Glide may be possible depending on altitude and speed at time of failure	I	1.00E+00	1.00E+00	Catastrophic outcome is assumed.	1.00E-06
2C1	Provide HVDC electrical power to motors	5.08E-04	Provide cooling of battery system	Battery cooling system failure	All	Loss of cooling ability for batteries.	Limited ability to hover depending upon conditions at time of failure. Battery may overheat and go into uncontained thermal runaway.	Loss of propulsion and/or other critical systems required for flight. Loss of aircraft.	Visual and audible warning provided to pilot.	Pilot executes emergency procedures to minimize power demand on batteries and land as soon as possible	I	1.00E+00	2.00E-01	Assume 20% probability that uncontained thermal runaway will occur.	1.02E-04
3A1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #1	ESC #1 failure	All	No output power to Motor #1. No torque provided to rotor.	No lift available to Rotor #1. Flight control system adjusts power to other rotors to	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04

FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
							maintain control of aircraft.								
3A2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #1	Motor #1 failure	All	No motor output provided to gearbox. No torque provided to rotor #1.	No lift available to Rotor #1. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3A3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #1	Gearbox #1 failure	All	No torque provided to rotor #1.	No lift available to Rotor #1. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3B1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #2	ESC #2 failure	All	No output power to Motor #2. No torque provided to rotor.	No lift available to Rotor #2. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3B2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #2	Motor #2 failure	All	No motor output provided to gearbox. No torque provided to rotor #2.	No lift available to Rotor #2. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3B3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #2	Gearbox #2 failure	All	No torque provided to rotor #2.	No lift available to Rotor #2. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3C1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #3	ESC #3 failure	All	No output power to Motor #3. No torque provided to rotor.	No lift available to Rotor #3. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3C2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #3	Motor #3 failure	All	No motor output provided to gearbox. No torque provided to rotor #3.	No lift available to Rotor #3. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05

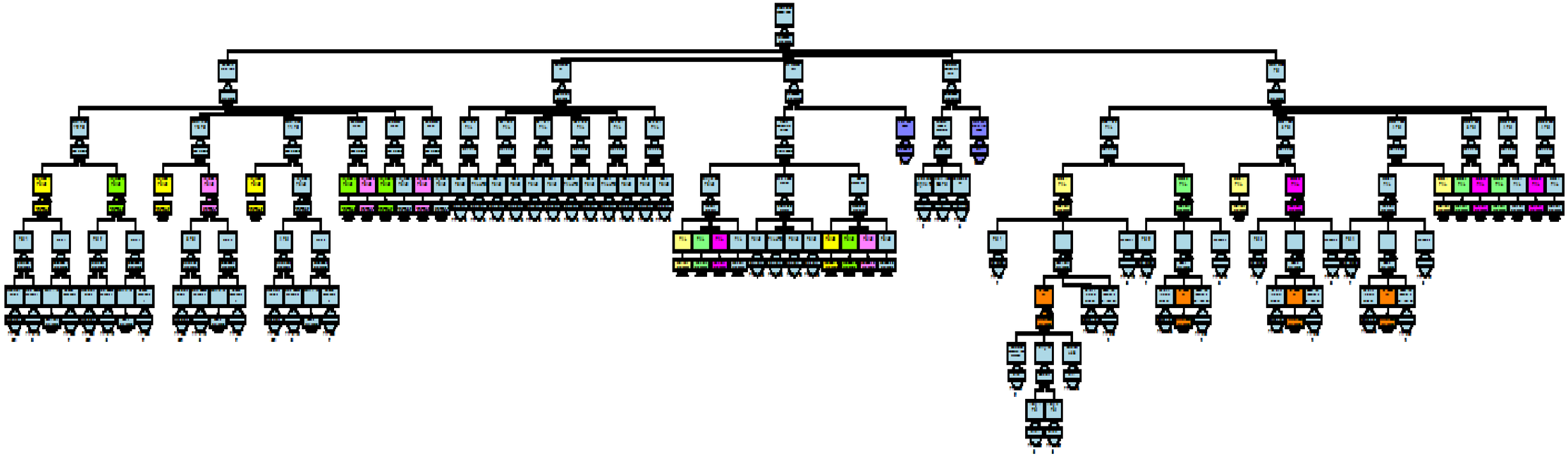
FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3C3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #3	Gearbox #3 failure	All	No torque provided to rotor #3.	No lift available to Rotor #3. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3D1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #4	ESC #4 failure	All	No output power to Motor #4. No torque provided to rotor.	No lift available to Rotor #4. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3D2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #4	Motor #4 failure	All	No motor output provided to gearbox. No torque provided to rotor #4.	No lift available to Rotor #4. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3D3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #4	Gearbox #4 failure	All	No torque provided to rotor #4.	No lift available to Rotor #4. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3E+1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #5	ESC #5 failure	All	No output power to Motor #5. No torque provided to rotor.	No lift available to Rotor #5. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3E+2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #5	Motor #5 failure	All	No motor output provided to gearbox. No torque provided to rotor #5.	No lift available to Rotor #5. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3E+3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #5	Gearbox #5 failure	All	No torque provided to rotor #5.	No lift available to Rotor #5. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3F1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #6	ESC #6 failure	All	No output power to Motor #6. No torque provided to rotor.	No lift available to Rotor #6. Flight control system adjusts power to other rotors to	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04

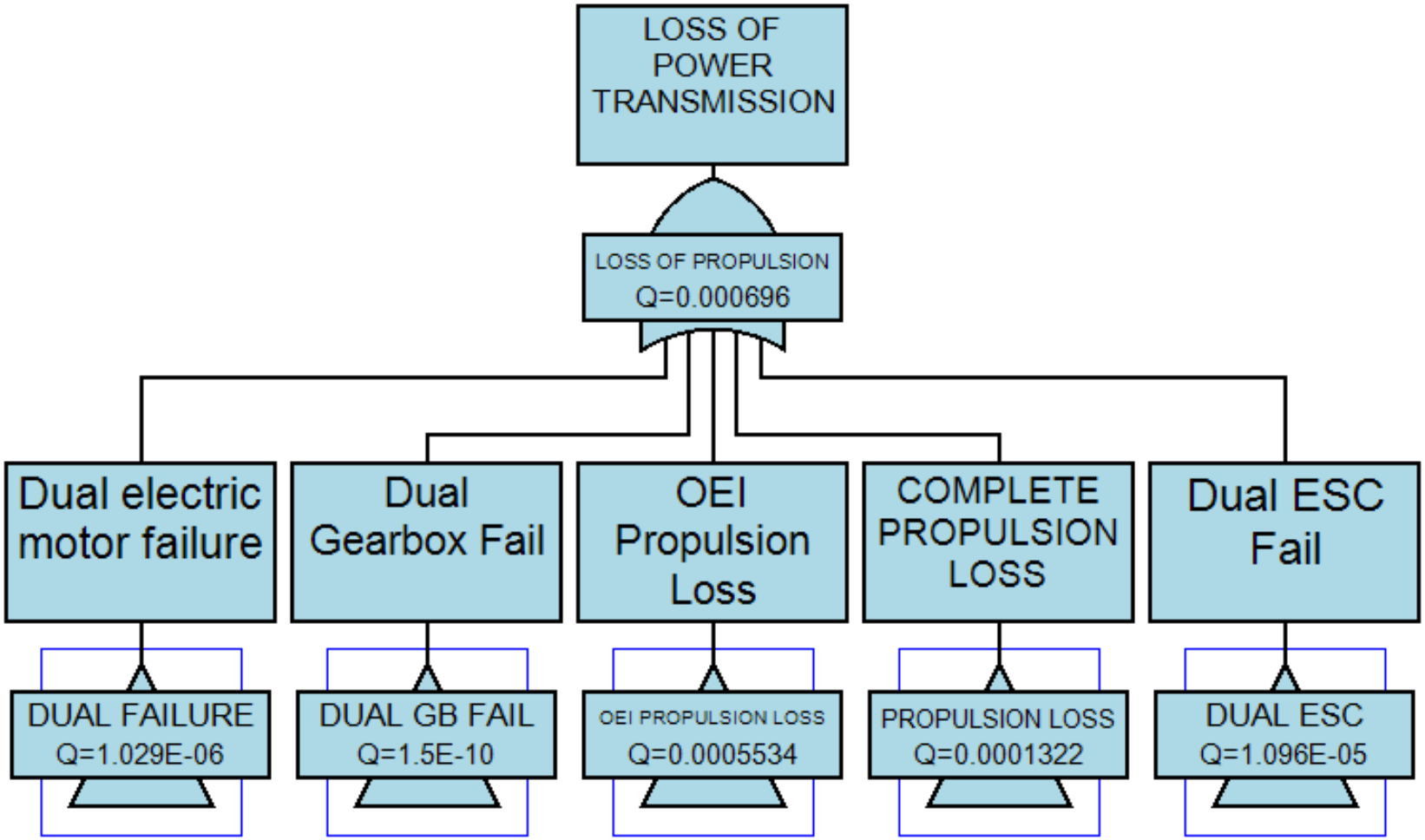
FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
							maintain control of aircraft.								
3F2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #6	Motor #6 failure	All	No motor output provided to gearbox. No torque provided to rotor #6.	No lift available to Rotor #6. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3F3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #6	Gearbox #6 failure	All	No torque provided to rotor #6.	No lift available to Rotor #6. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3G1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #7	ESC #7 failure	All	No output power to Motor #7. No torque provided to rotor.	No lift available to Rotor #7. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3G2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #7	Motor #7 failure	All	No motor output provided to gearbox. No torque provided to rotor #7.	No lift available to Rotor #7. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05
3G3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #7	Gearbox #7 failure	All	No torque provided to rotor #7.	No lift available to Rotor #7. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
3H1	Provide torque to lifting rotors	2.70E-04	Failure to provide shaft power to lift rotor #8	ESC #8 failure	All	No output power to Motor #8. No torque provided to rotor.	No lift available to Rotor #8. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	Beta = 1 for severity III & IV	2.70E-04
3H2	Provide torque to lifting rotors	9.24E-05	Failure to provide shaft power to lift rotor #8	Motor #8 failure	All	No motor output provided to gearbox. No torque provided to rotor #8.	No lift available to Rotor #8. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	1.00E+00	beta = 1 for Category III and IV	9.24E-05

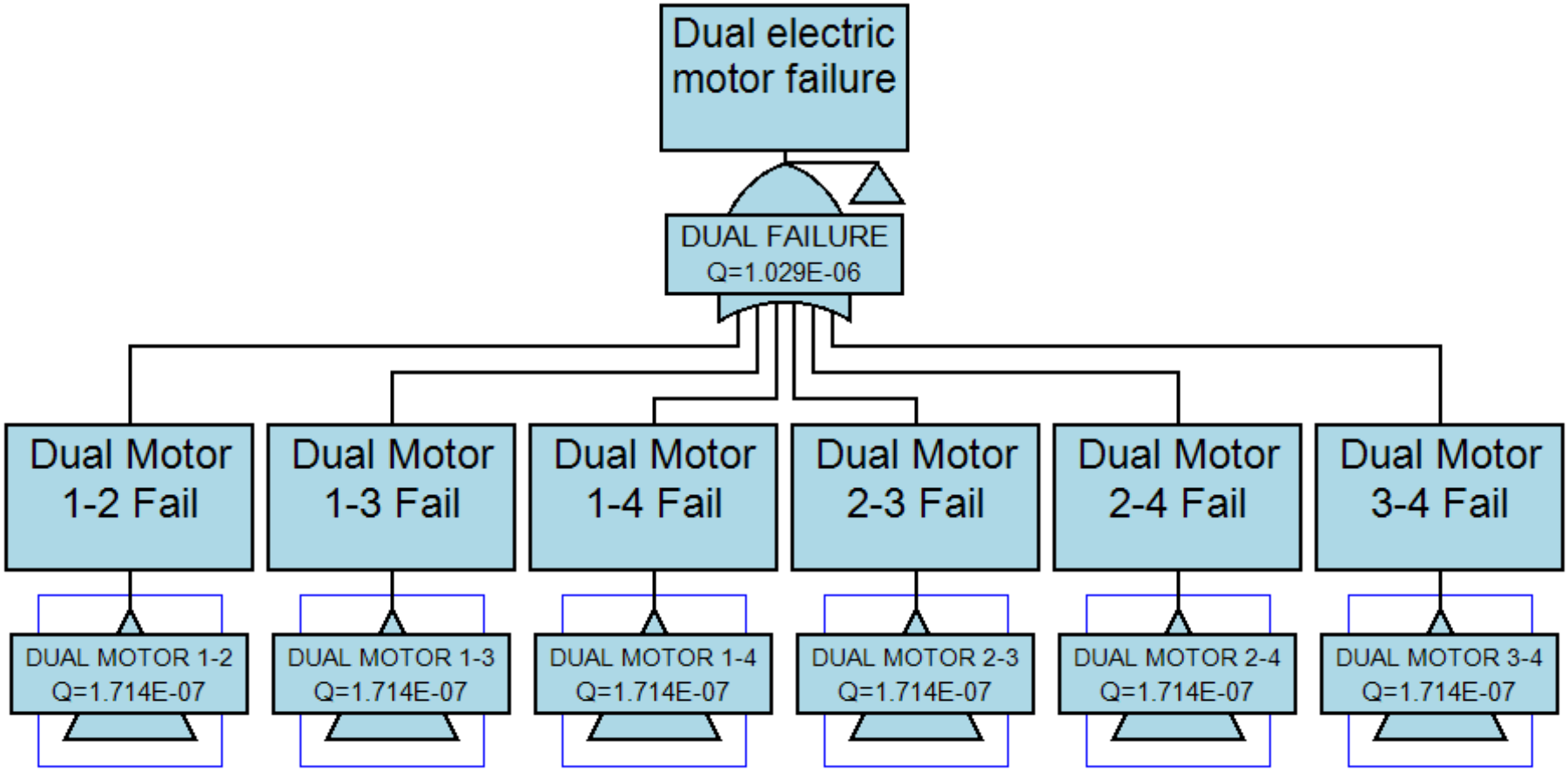
FMECA ID Code	Function	Failure Rate (λ)	Failure Mode	Failure Cause	Mission Phase	Local Failure Effect	Next Higher Effect	End Effect	Detection Method	Compensating Provisions	Severity Code	Alpha (Mode Ratio)	Beta	Beta Mode Ratio Explanation	Failure Mode Criticality No.
3H3	Provide torque to lifting rotors	5.00E-06	Failure to provide shaft power to lift rotor #8	Gearbox #8 failure	All	No torque provided to rotor #8.	No lift available to Rotor #8. Flight control system adjusts power to other rotors to maintain control of aircraft.	Flight handling qualities affected. Reduced maneuverability in hover.	Visual and audible warning provided to pilot.	Flight control system adjusts control to remaining rotors to maintain controlled flight	III	1.00E+00	2.00E-01	beta = 1 for Category III and IV	1.00E-06
4A1	Provide torque to thrust propeller	2.70E-04	Failure to provide torque to thrust propeller	Thrust ESC failure	All	No power to thrust ESC Thrust motor fails to provide output torque to propeller.	No forward thrust available for forward flight. Aircraft reverts to hover for remainder of flight.	Aircraft speed and range significantly reduced. Ability to hover is unaffected. Loss of aircraft if pilot cannot find safe landing area within range...	Visual and audible alert provided to pilot	Aircraft may have limited glide capability depending on altitude and forward speed at time of failure. Pilot must find safe landing area within range.	I	1.00E+00	5.00E-01	Assume 50% probability that pilot will find safe landing area within reduced range	1.35E-04
4A2	Provide torque to thrust propeller	9.24E-05	Failure to provide torque to thrust propeller	Thrust motor failure	All	No power to thrust ESC Thrust motor fails to provide output torque to propeller.	No forward thrust available for forward flight. Aircraft reverts to hover for remainder of flight.	Aircraft speed and range significantly reduced. Ability to hover is unaffected. Loss of aircraft if pilot cannot find safe landing area within range...	Visual and audible alert provided to pilot	Aircraft may have limited glide capability depending on altitude and forward speed at time of failure. Pilot must find safe landing area within range.	I	1.00E+00	5.00E-01	Assume 50% probability that pilot will find safe landing area within reduced range	4.62E-05
4A3	Provide torque to thrust propeller	5.00E-06	Failure to provide torque to thrust propeller	Thrust gearbox failure	All	No power to thrust ESC Thrust motor fails to provide output torque to propeller.	No forward thrust available for forward flight. Aircraft reverts to hover for remainder of flight.	Aircraft speed and range significantly reduced. Ability to hover is unaffected. Loss of aircraft if pilot cannot find safe landing area within range...	Visual and audible alert provided to pilot	Aircraft may have limited glide capability depending on altitude and forward speed at time of failure. Pilot must find safe landing area within range.	I	1.00E+00	5.00E-01	Assume 50% probability that pilot will find safe landing area within reduced range	2.50E-06

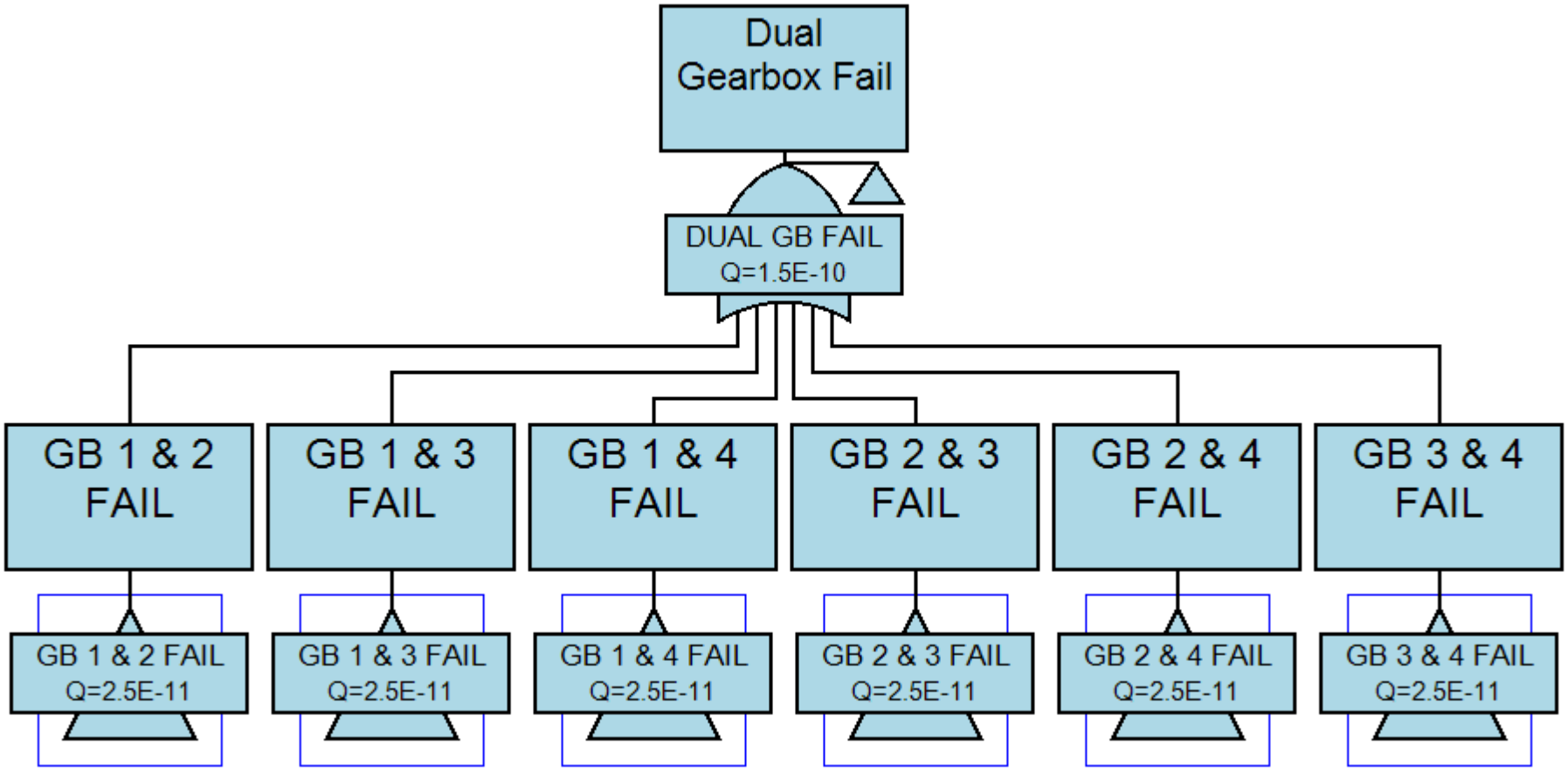
Criticality Summary		
	I	4.67E-04
	II	0.00E+00
	III	2.92E-03
	IV	1.00E-06

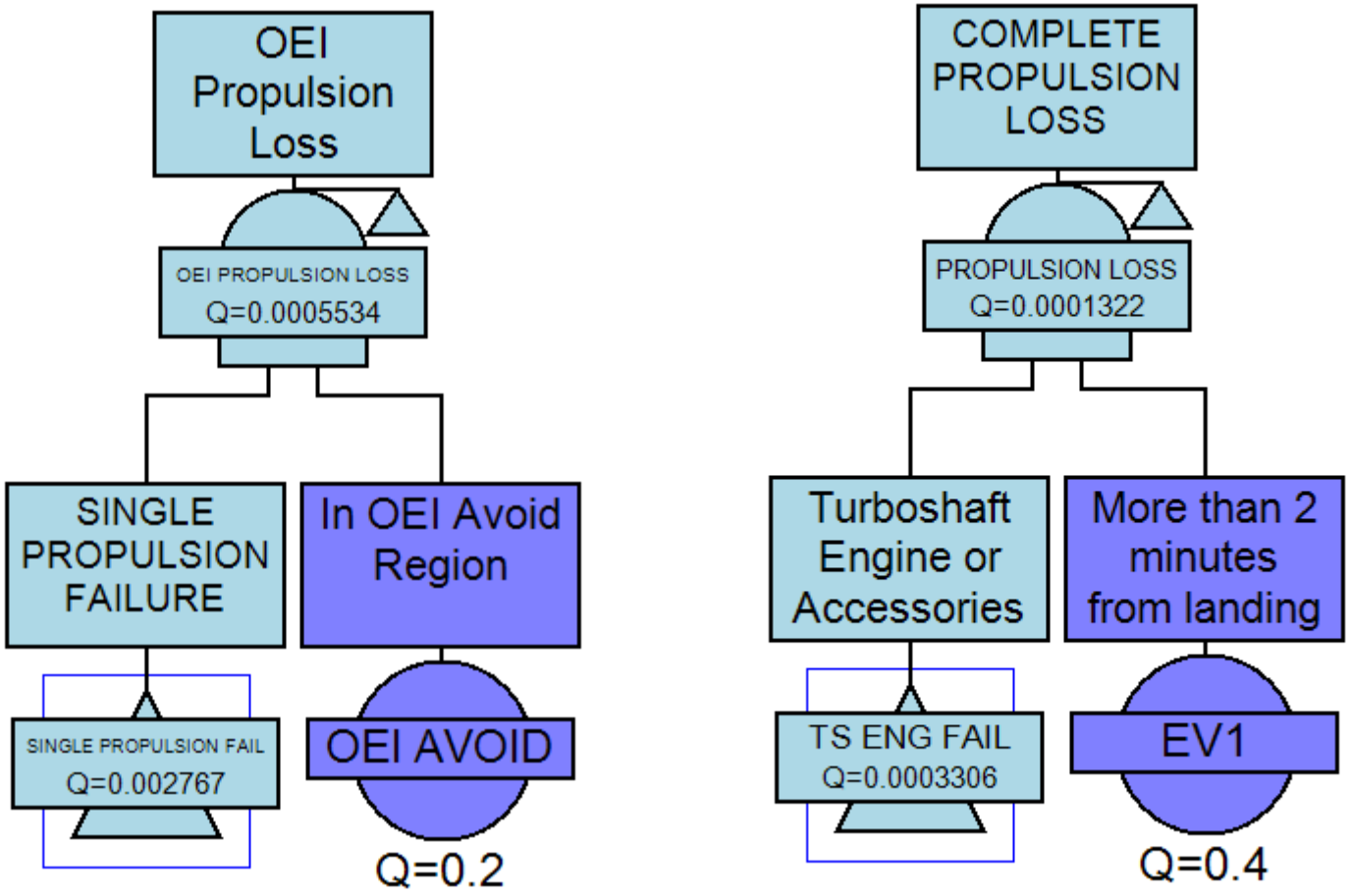
APPENDIX C TILT-WING FAULT TREE DIAGRAM

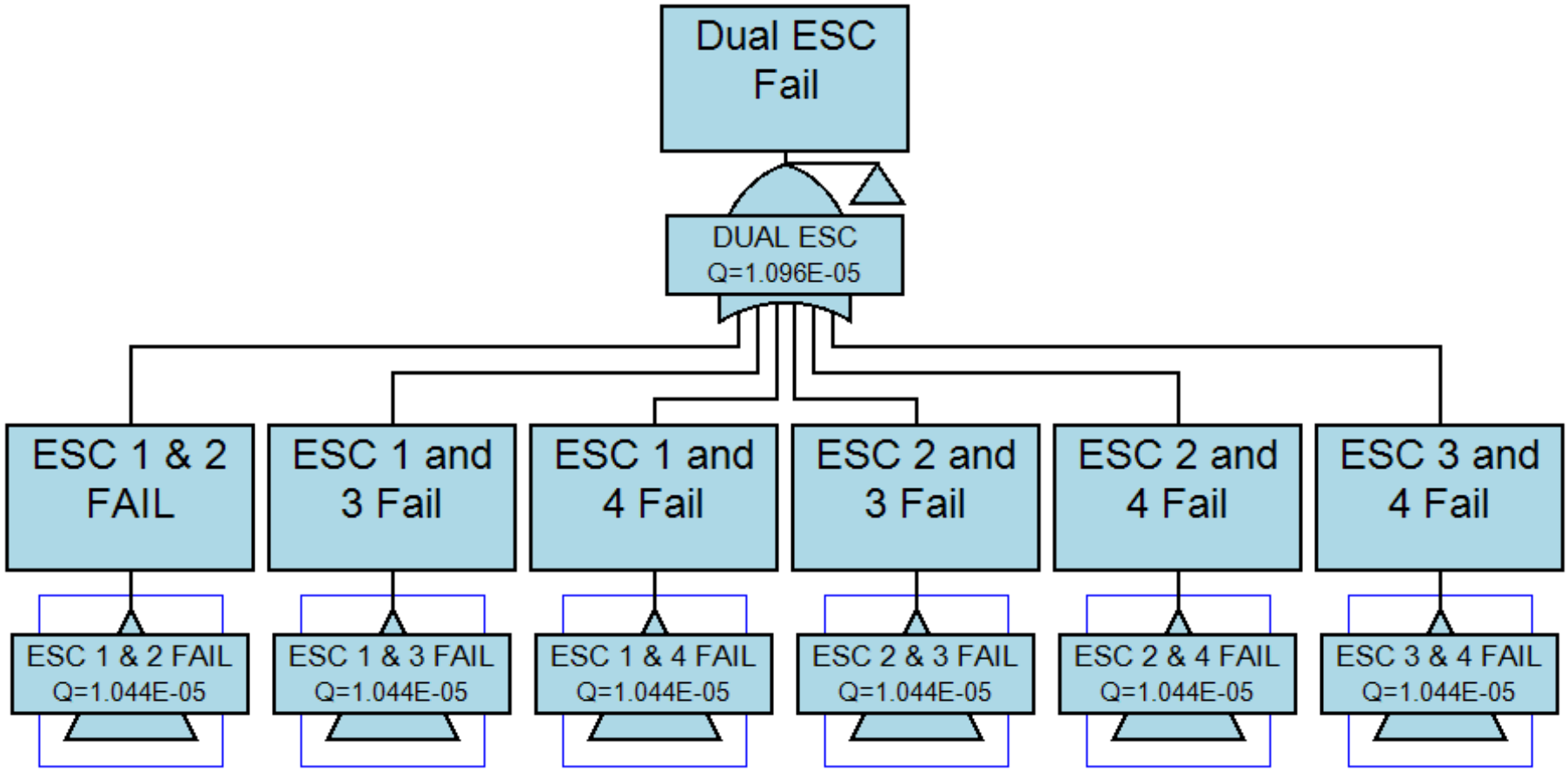


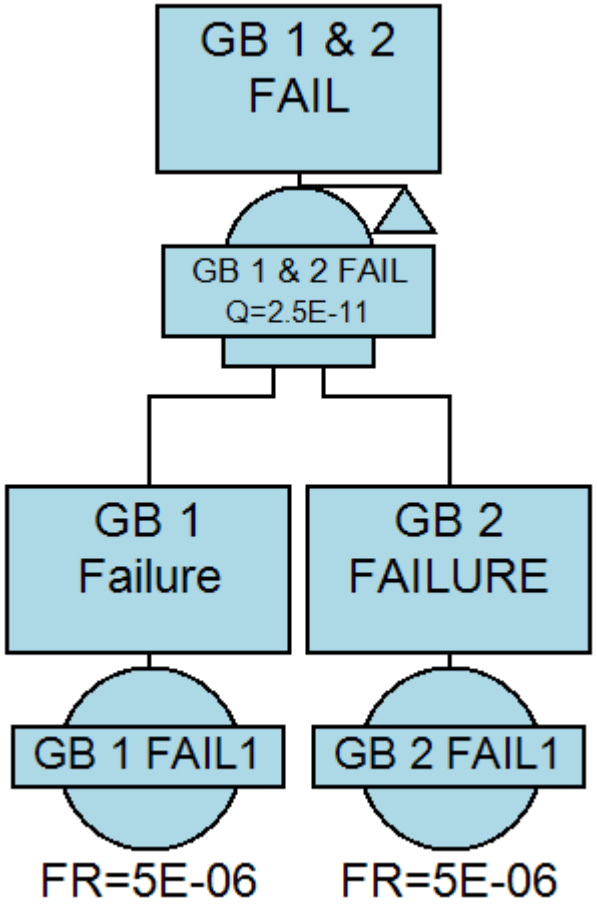

LOSS OF POWER TRANSMISSION
LOSS OF PROPULSION
Q=0.000696
Dual electric motor failure
Dual Gearbox Fail
OEI Propulsion Loss
COMPLETE PROPULSION LOSS
Dual ESC Fail
DUAL FAILURE
Q=1.029E-06
DUAL GB FAIL
Q=1.5E-10
OEI PROPULSION LOSS
Q=0.0005534
PROPULSION LOSS
Q=0.0001322
DUAL ESC
Q=1.096E-05


Dual electric motor failure
DUAL FAILURE
Q=1.029E-06
Dual Motor 1-2 Fail
Dual Motor 1-3 Fail
Dual Motor 1-4 Fail
Dual Motor 2-3 Fail
Dual Motor 2-4 Fail
Dual Motor 3-4 Fail
DUAL MOTOR 1-2
Q=1.714E-07
DUAL MOTOR 1-3
Q=1.714E-07
DUAL MOTOR 1-4
Q=1.714E-07
DUAL MOTOR 2-3
Q=1.714E-07
DUAL MOTOR 2-4
Q=1.714E-07
DUAL MOTOR 3-4
Q=1.714E-07

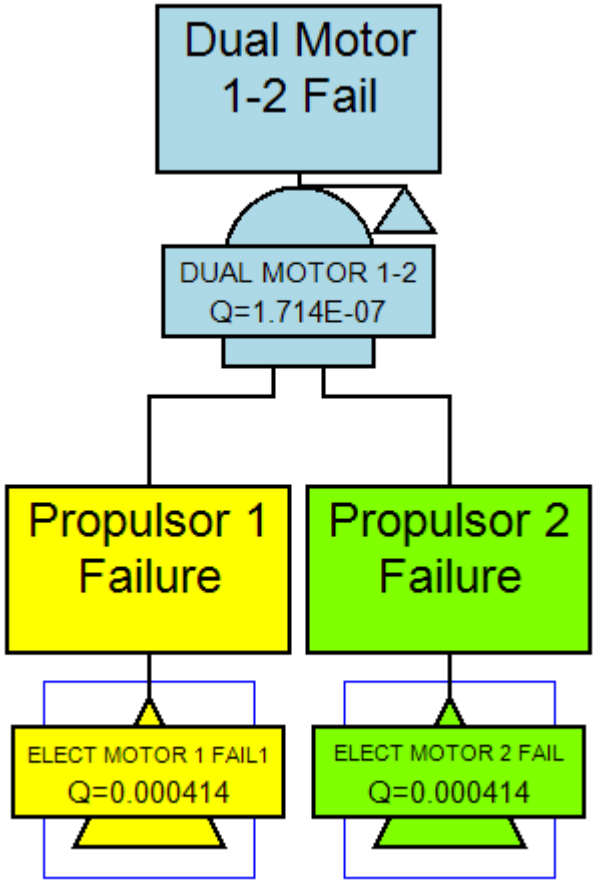

Dual
Gearbox Fail
DUAL GB FAIL
Q=1.5E-10
GB 1 & 2
FAIL
GB 1 & 3
FAIL
GB 1 & 4
FAIL
GB 2 & 3
FAIL
GB 2 & 4
FAIL
GB 3 & 4
FAIL
GB 1 & 2 FAIL
Q=2.5E-11
GB 1 & 3 FAIL
Q=2.5E-11
GB 1 & 4 FAIL
Q=2.5E-11
GB 2 & 3 FAIL
Q=2.5E-11
GB 2 & 4 FAIL
Q=2.5E-11
GB 3 & 4 FAIL
Q=2.5E-11


OEI Propulsion Loss
OEI PROPULSION LOSS
Q=0.0005534
SINGLE PROPULSION FAILURE
In OEI Avoid Region
SINGLE PROPULSION FAIL
Q=0.002767
OEI AVOID
Q=0.2
COMPLETE PROPULSION LOSS
PROPULSION LOSS
Q=0.0001322
Turboshaft Engine or Accessories
More than 2 minutes from landing
TS ENG FAIL
Q=0.0003306
EV1
Q=0.4

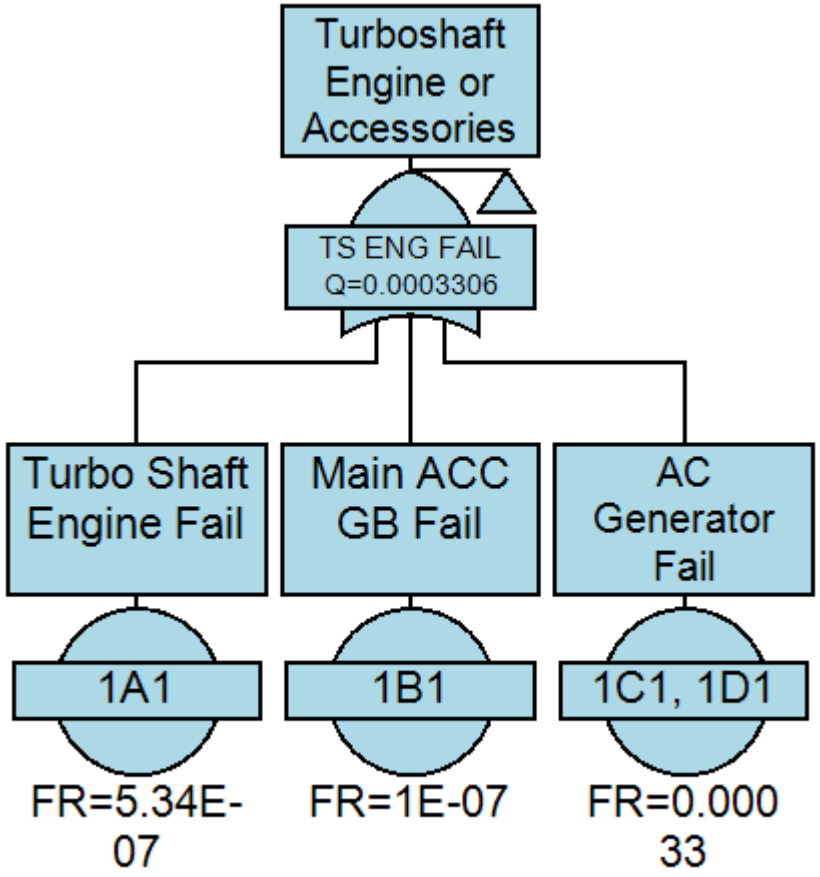

Dual ESC Fail
DUAL ESC
Q=1.096E-05
ESC 1 & 2 FAIL
ESC 1 and 3 Fail
ESC 1 and 4 Fail
ESC 2 and 3 Fail
ESC 2 and 4 Fail
ESC 3 and 4 Fail
ESC 1 & 2 FAIL
Q=1.044E-05
ESC 1 & 3 FAIL
Q=1.044E-05
ESC 1 & 4 FAIL
Q=1.044E-05
ESC 2 & 3 FAIL
Q=1.044E-05
ESC 2 & 4 FAIL
Q=1.044E-05
ESC 3 & 4 FAIL
Q=1.044E-05

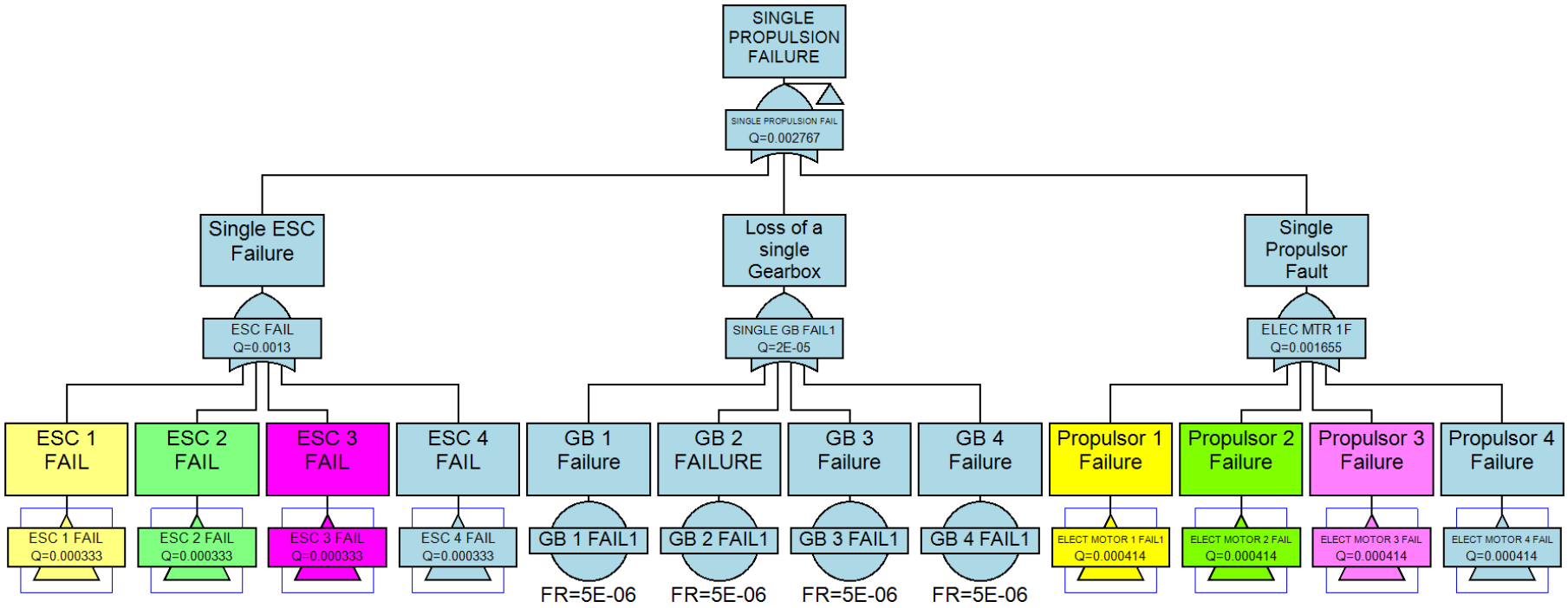


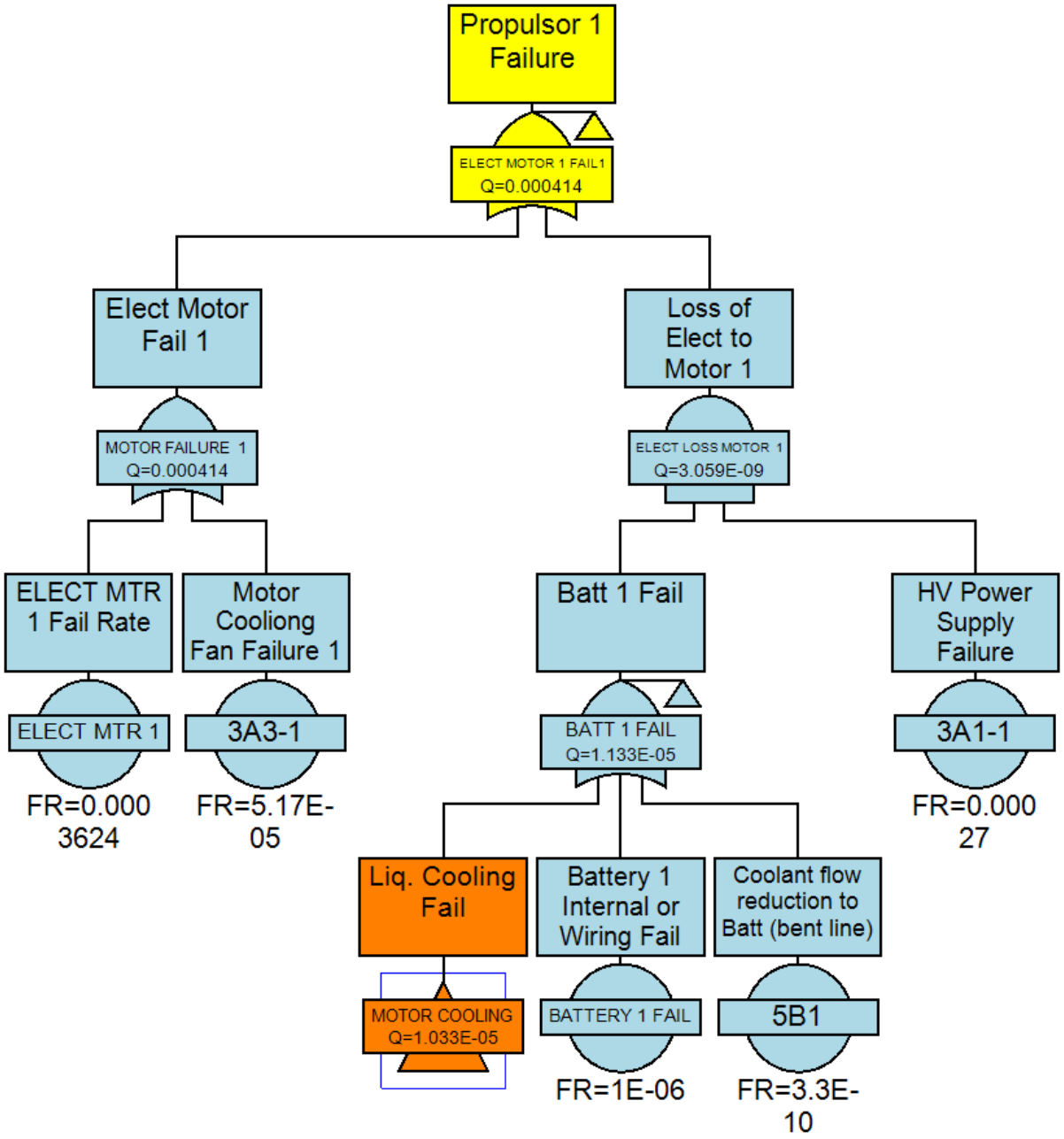
Note: "Dual Gear Box (GB) 1 & 2 Fail" is representative of all "Dual GB X & Y Fail" events in Appendix C.



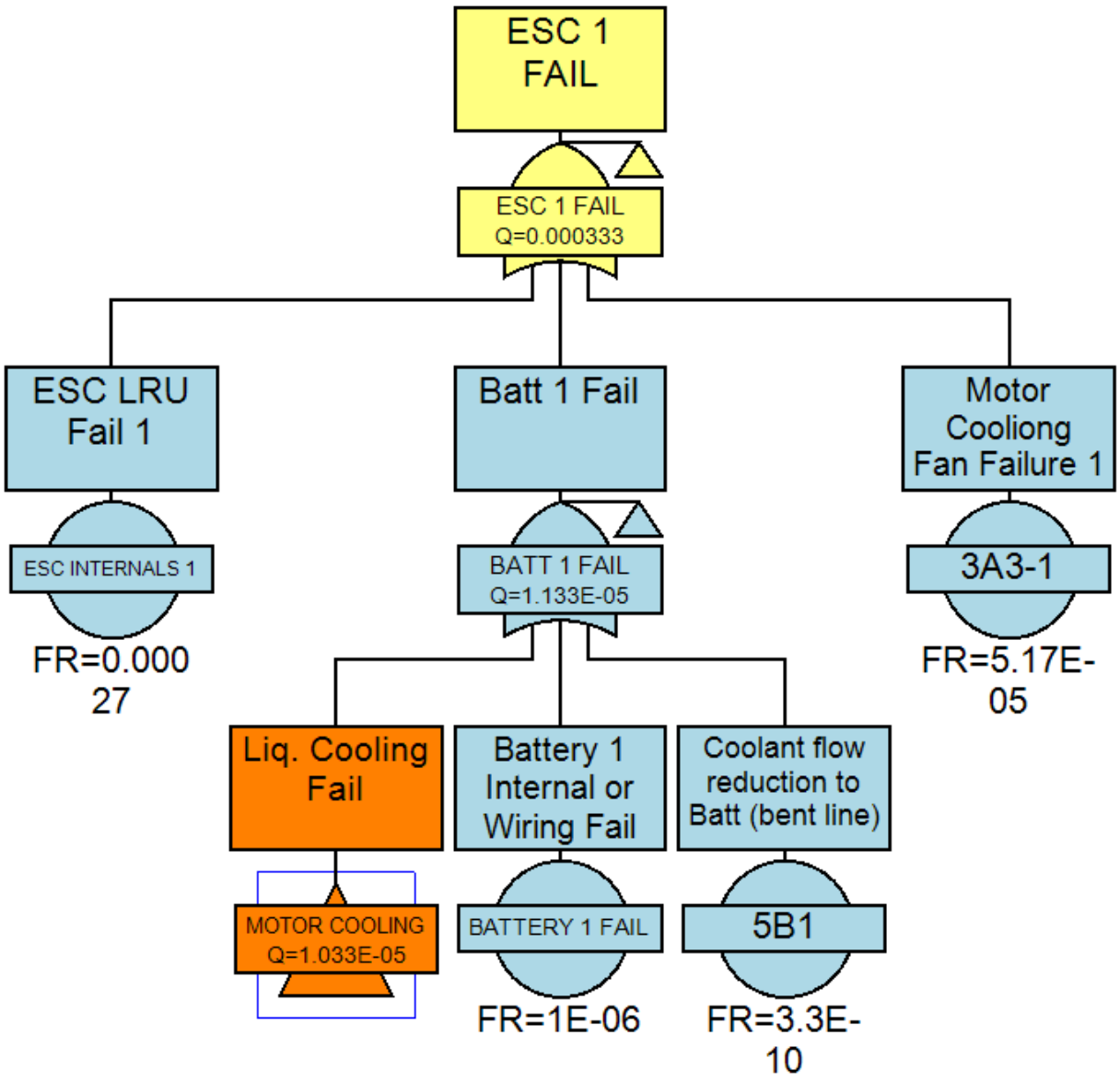
Note: "Dual Motor 1-2 Fail" is representative of all "Dual Motor X-Y Fail" events in Appendix C.


Turboshaft Engine or Accessories
TS ENG FAIL
Q=0.0003306
Turbo Shaft Engine Fail
Main ACC GB Fail
AC Generator Fail
1A1
1B1
1C1, 1D1
FR=5.34E-07
FR=1E-07
FR=0.00033

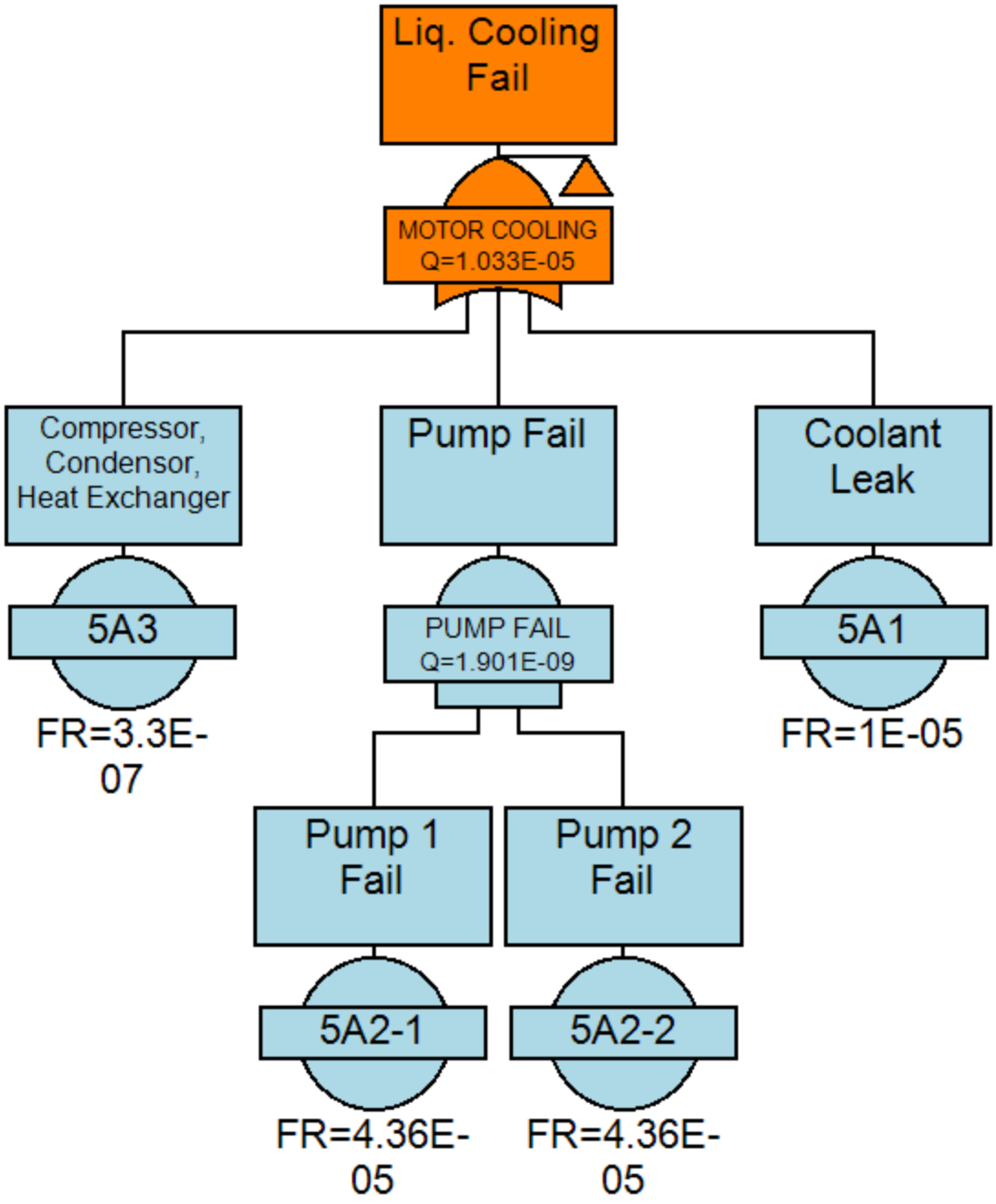

SINGLE PROPULSION FAILURE
SINGLE PROPULSION FAIL
Q=0.002767
Single ESC Failure
Loss of a single Gearbox
Single Propulsor Fault
ESC FAIL
Q=0.0013
SINGLE GB FAIL1
Q=2E-05
ELEC MTR 1F
Q=0.001655
ESC 1 FAIL
ESC 2 FAIL
ESC 3 FAIL
ESC 4 FAIL
GB 1 Failure
GB 2 FAILURE
GB 3 Failure
GB 4 Failure
Propulsor 1 Failure
Propulsor 2 Failure
Propulsor 3 Failure
Propulsor 4 Failure
ESC 1 FAIL
Q=0.000333
ESC 2 FAIL
Q=0.000333
ESC 3 FAIL
Q=0.000333
ESC 4 FAIL
Q=0.000333
GB 1 FAIL1
GB 2 FAIL1
GB 3 FAIL1
GB 4 FAIL1
FR=5E-06
FR=5E-06
FR=5E-06
FR=5E-06
ELECT MOTOR 1 FAIL1
Q=0.000414
ELECT MOTOR 2 FAIL
Q=0.000414
ELECT MOTOR 3 FAIL
Q=0.000414
ELECT MOTOR 4 FAIL
Q=0.000414



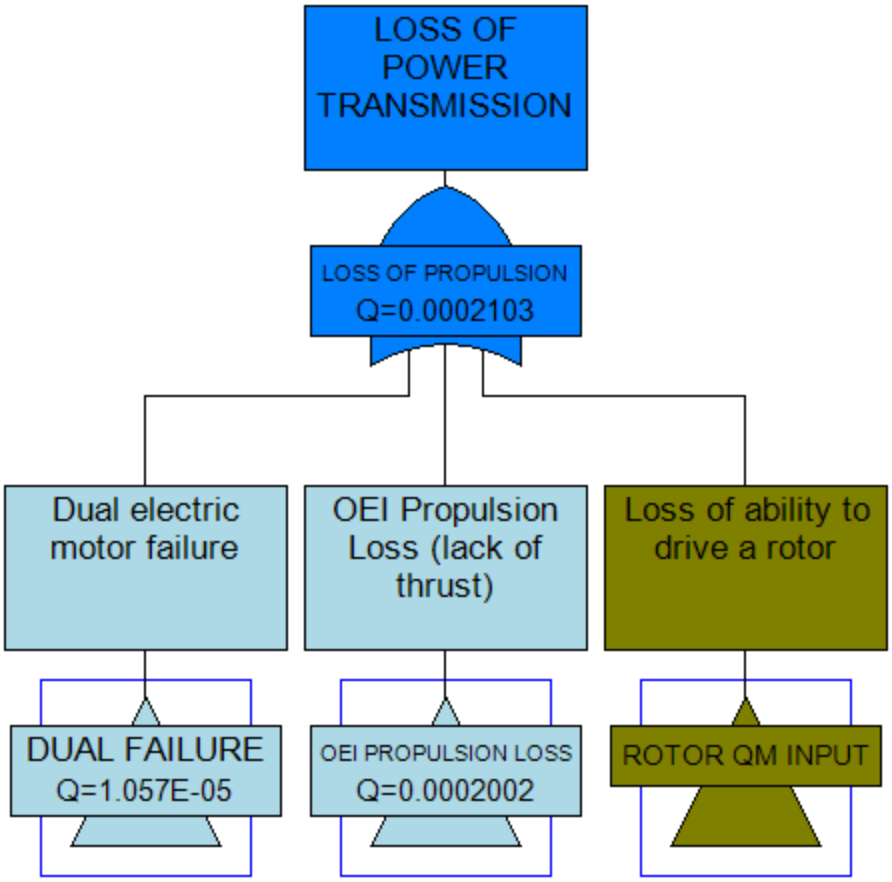
Note: "Propulsor 1 Failure" is representative of all "Propulsor X Failure" events in Appendix C.

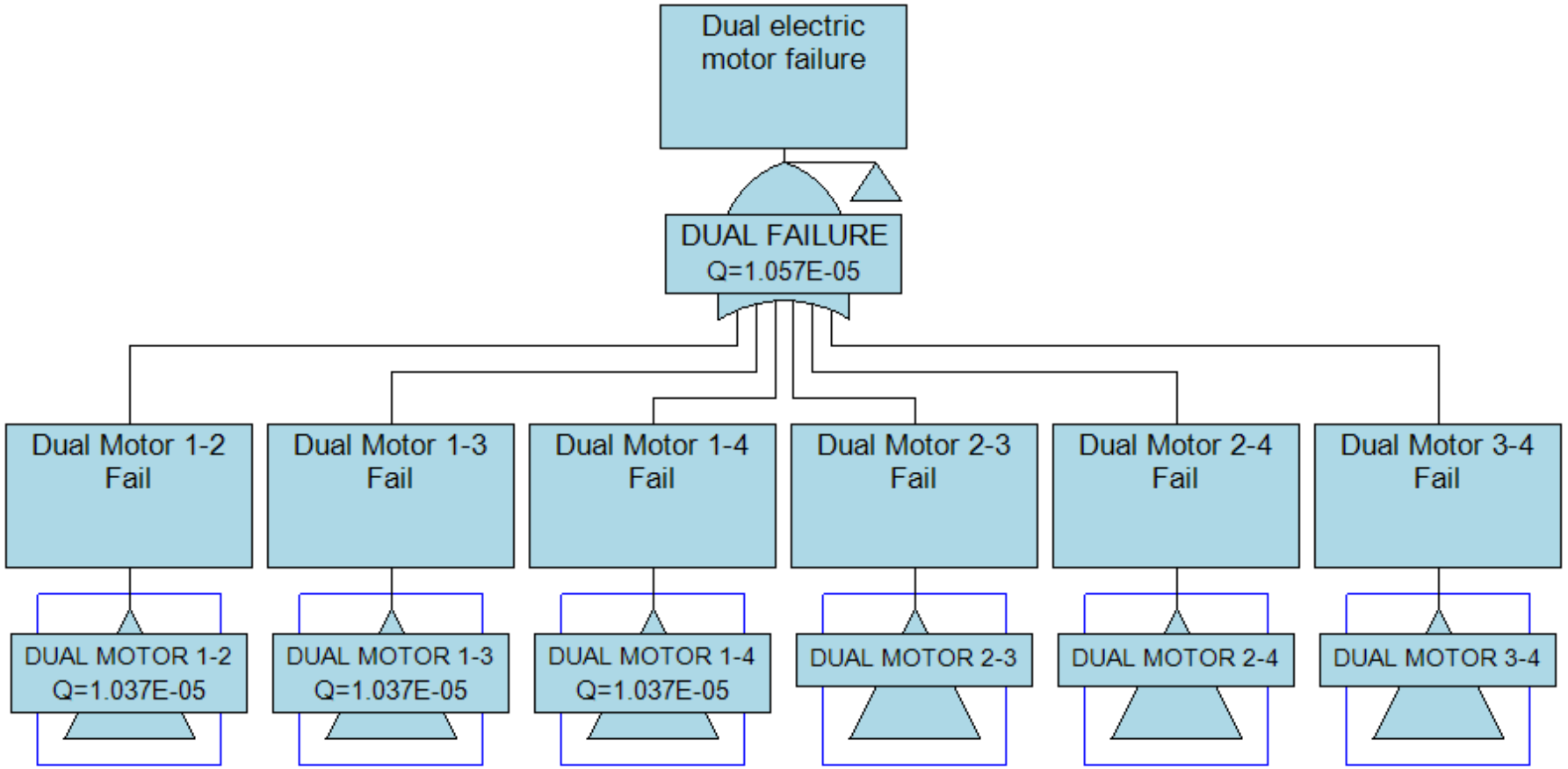


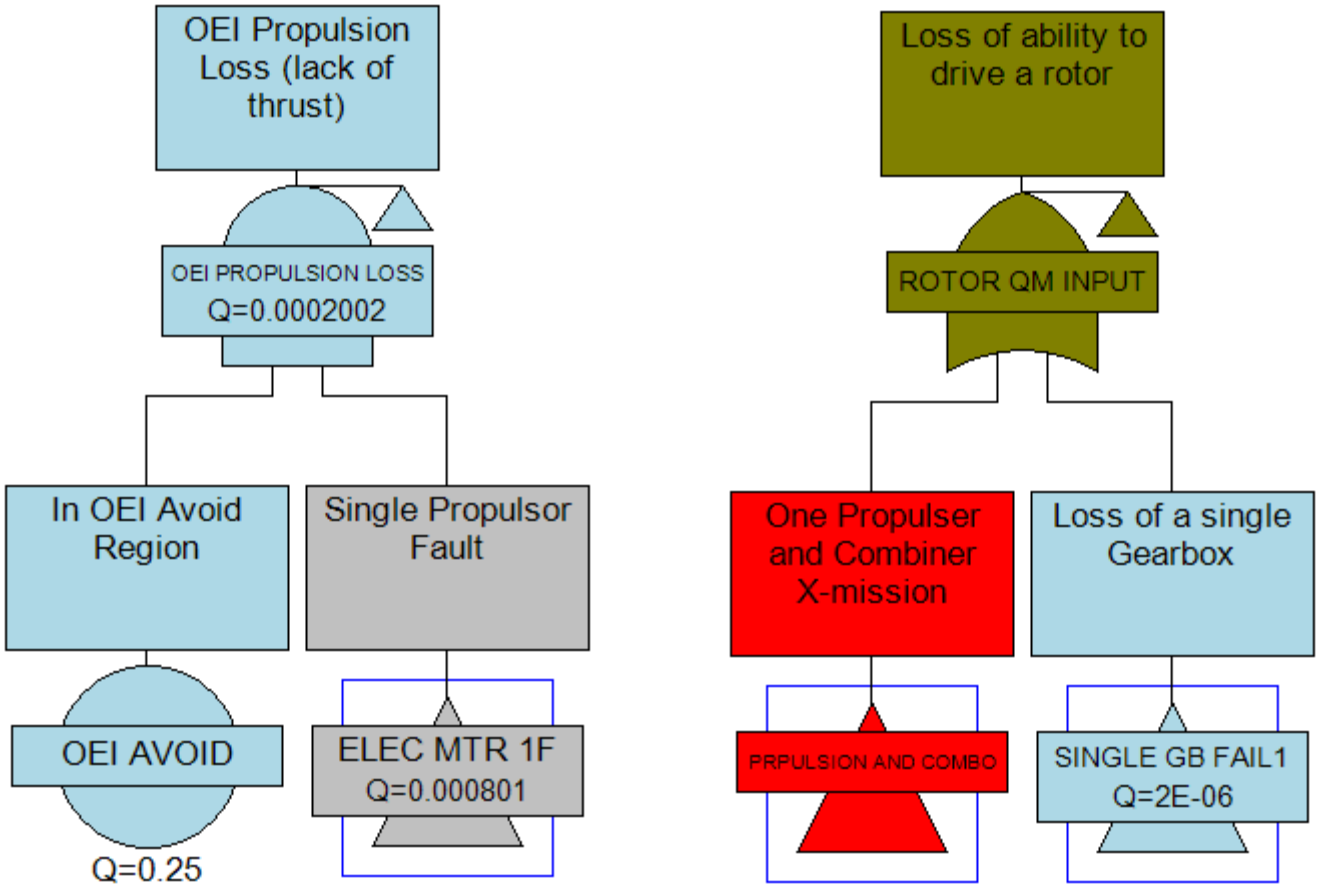
Note: "ESC 1 Fail" is representative of all "ESC X Fail" events in Appendix C.

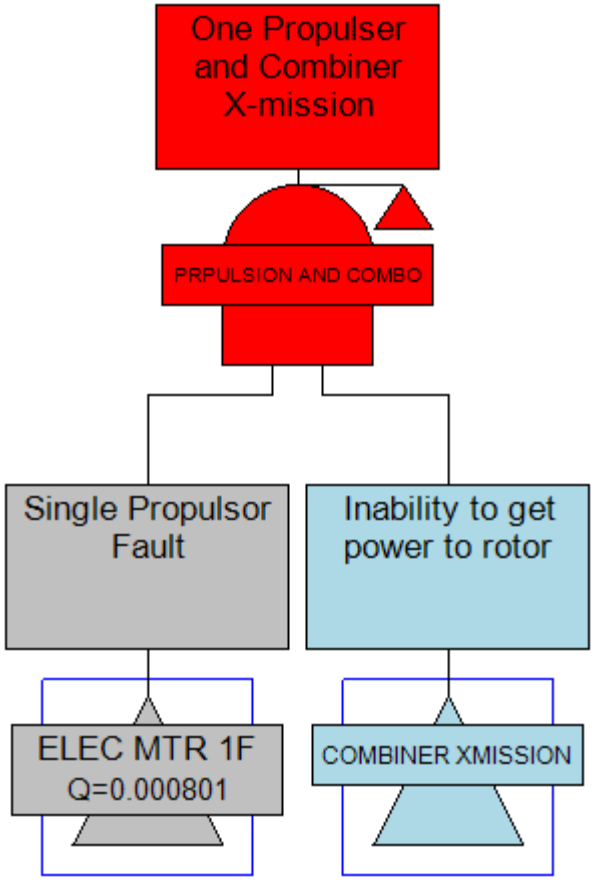

Liq. Cooling Fail
MOTOR COOLING Q=1.033E-05
Compressor, Condensor, Heat Exchanger
Pump Fail
Coolant Leak
5A3
PUMP FAIL Q=1.901E-09
5A1
FR=3.3E-07
FR=1E-05
Pump 1 Fail
Pump 2 Fail
5A2-1
5A2-2
FR=4.36E-05
FR=4.36E-05

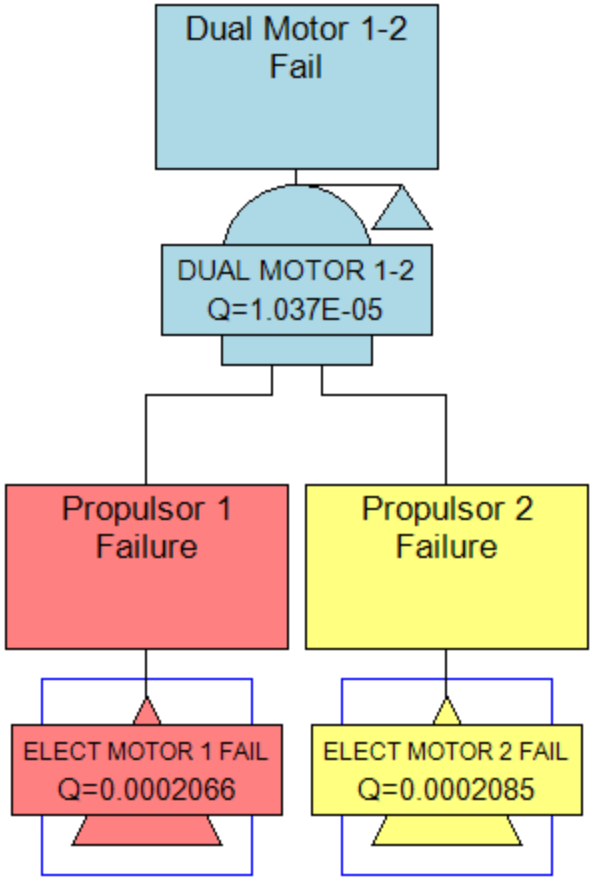
APPENDIX D QUAD-ROTOR FAULT TREE DIAGRAM


LOSS OF POWER TRANSMISSION
LOSS OF PROPULSION
Q=0.0002103
Dual electric motor failure
OEI Propulsion Loss (lack of thrust)
Loss of ability to drive a rotor
DUAL FAILURE
Q=1.057E-05
OEI PROPULSION LOSS
Q=0.0002002
ROTOR QM INPUT

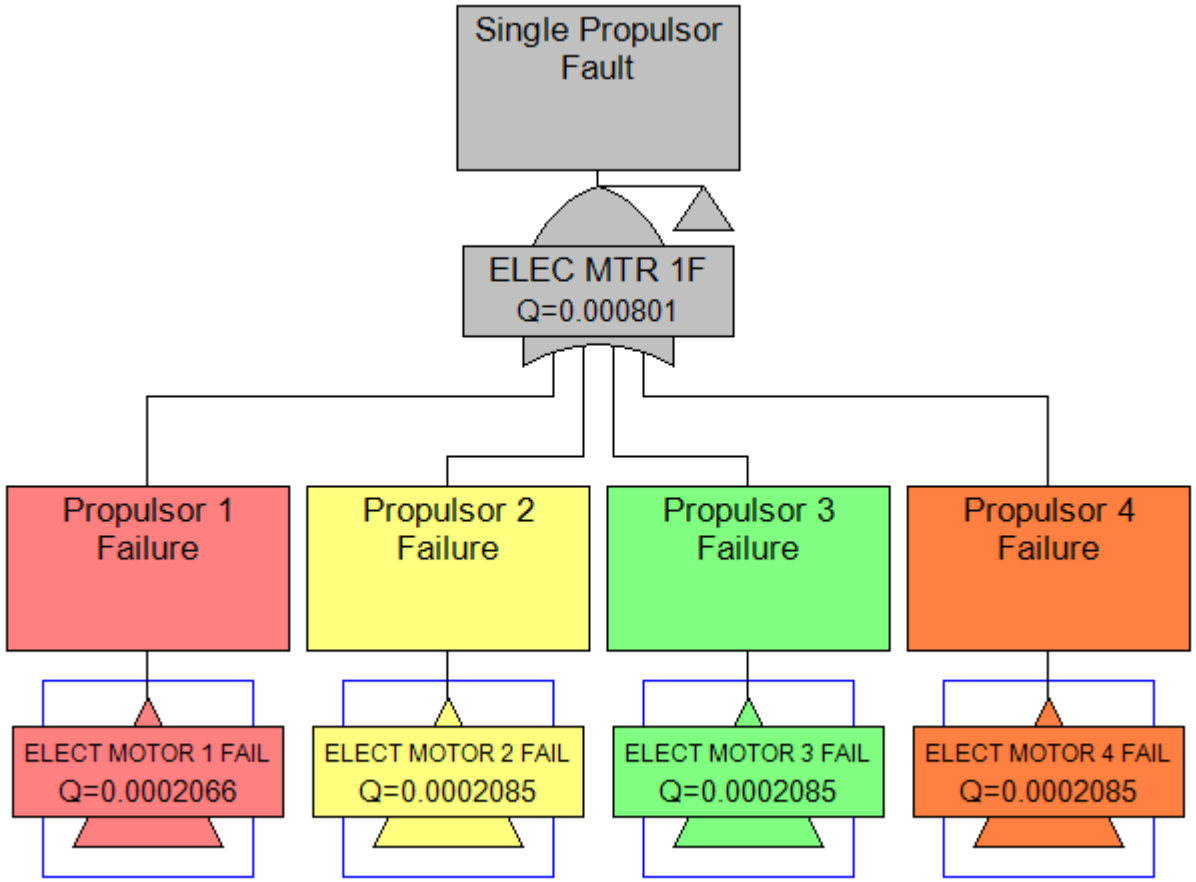

Dual electric motor failure
DUAL FAILURE
Q=1.057E-05
Dual Motor 1-2 Fail
Dual Motor 1-3 Fail
Dual Motor 1-4 Fail
Dual Motor 2-3 Fail
Dual Motor 2-4 Fail
Dual Motor 3-4 Fail
DUAL MOTOR 1-2
Q=1.037E-05
DUAL MOTOR 1-3
Q=1.037E-05
DUAL MOTOR 1-4
Q=1.037E-05
DUAL MOTOR 2-3
DUAL MOTOR 2-4
DUAL MOTOR 3-4

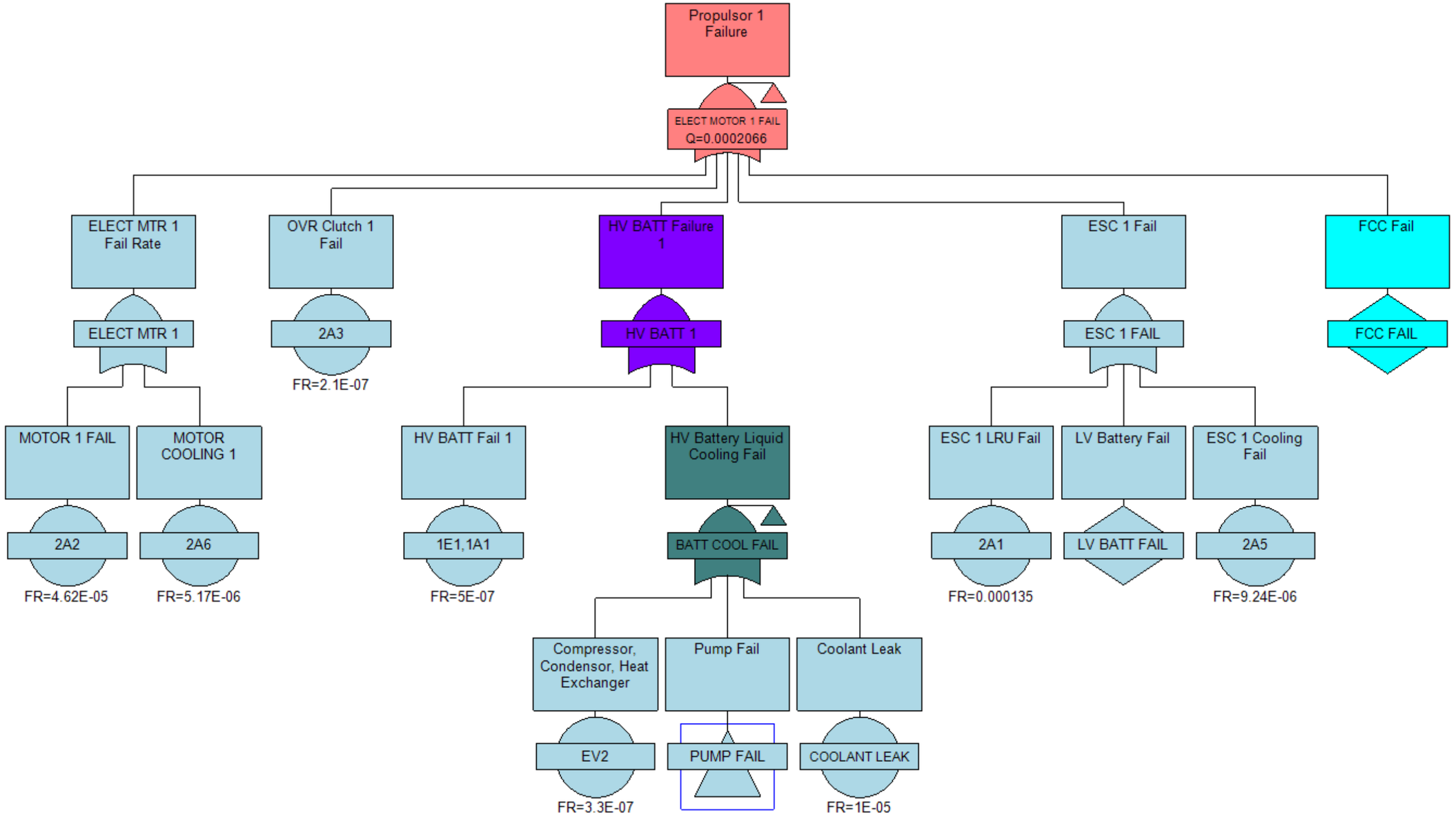

OEI Propulsion Loss (lack of thrust)
OEI PROPULSION LOSS
Q=0.0002002
In OEI Avoid Region
Single Propulsor Fault
OEI AVOID
Q=0.25
ELEC MTR 1F
Q=0.000801
Loss of ability to drive a rotor
ROTOR QM INPUT
One Propulser and Combiner X-mission
Loss of a single Gearbox
PRPULSION AND COMBO
SINGLE GB FAIL1
Q=2E-06



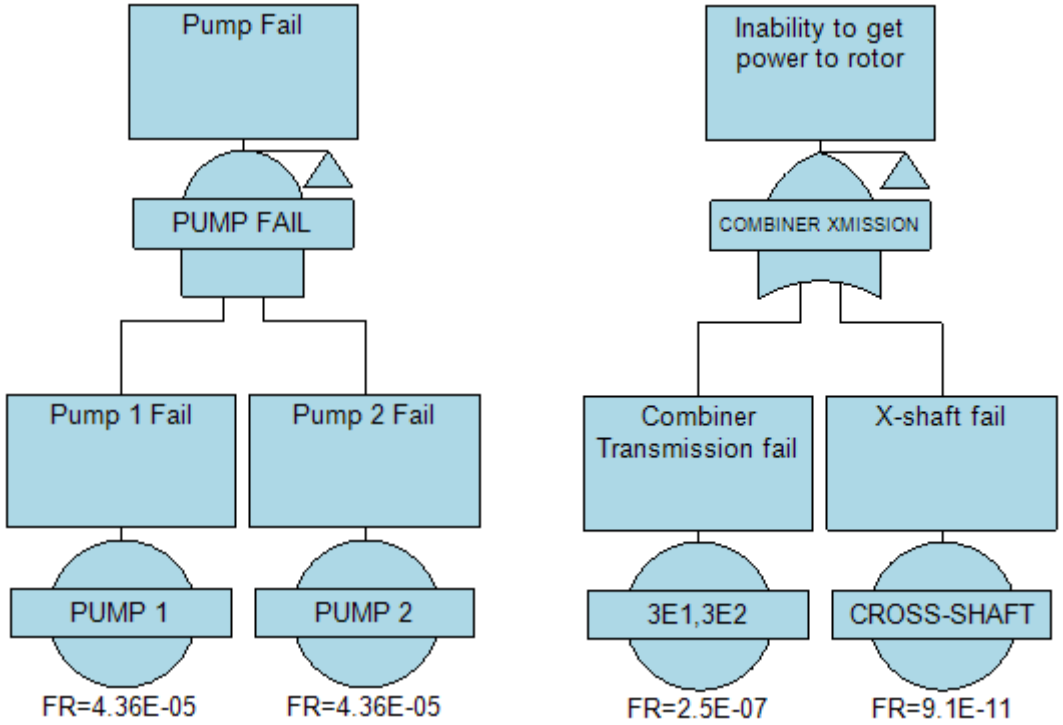


Note: "Dual Motor 1-2 Fail" is representative of all "Dual Motor X-Y Fail" events in Appendix D.

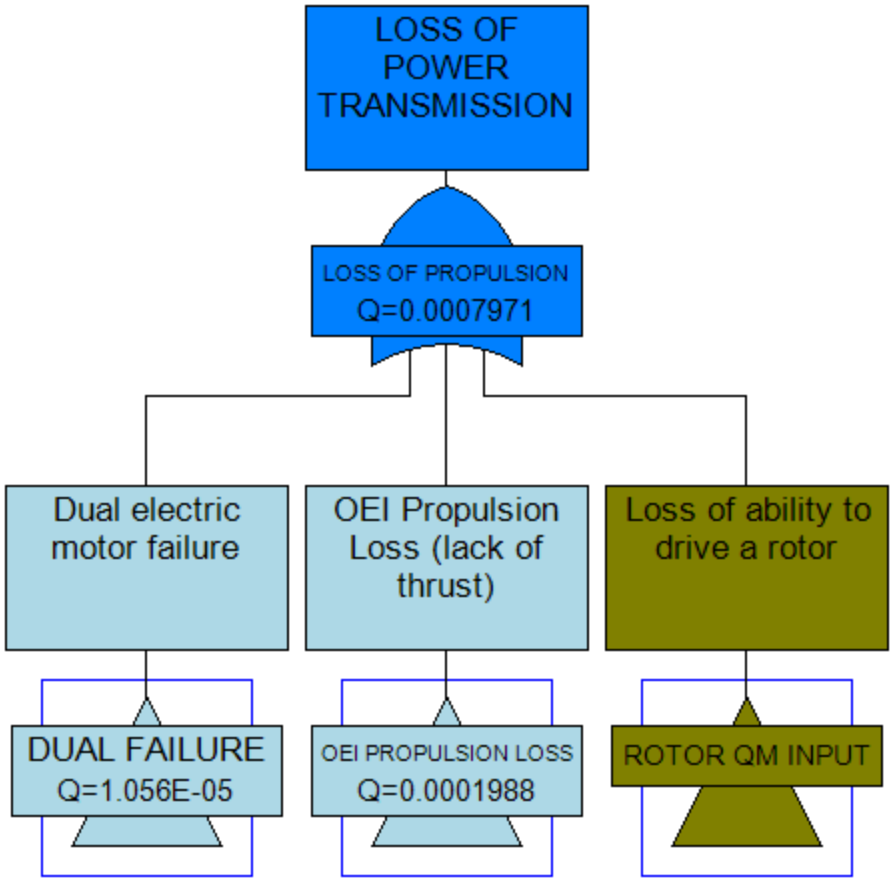

Single Propulsor Fault
ELEC MTR 1F
Q=0.000801
Propulsor 1 Failure
Propulsor 2 Failure
Propulsor 3 Failure
Propulsor 4 Failure
ELECT MOTOR 1 FAIL
Q=0.0002066
ELECT MOTOR 2 FAIL
Q=0.0002085
ELECT MOTOR 3 FAIL
Q=0.0002085
ELECT MOTOR 4 FAIL
Q=0.0002085

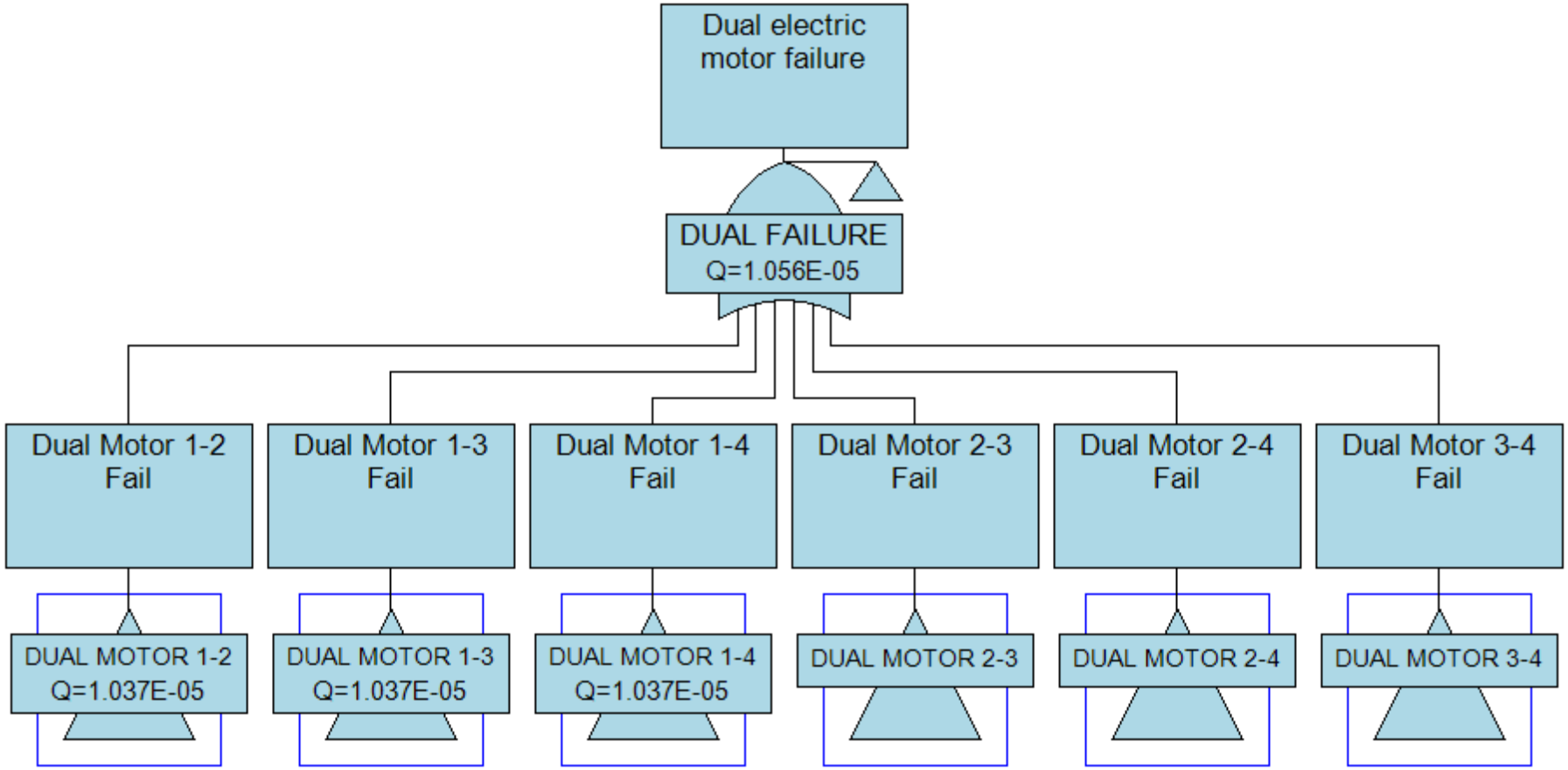


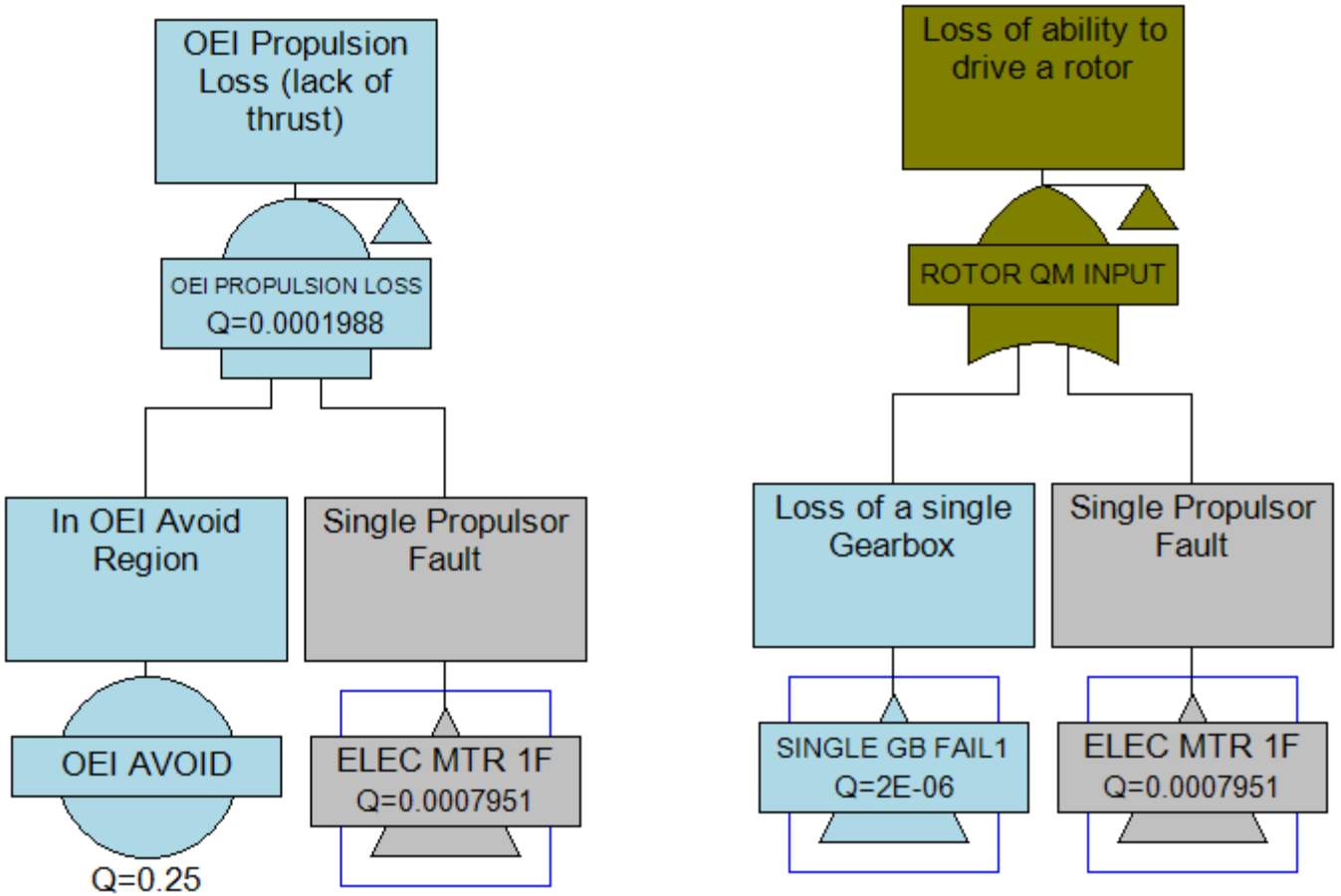
Note: "Propulsor 1 Failure" is representative of all "Propulsor X Failure" events in Appendix D.

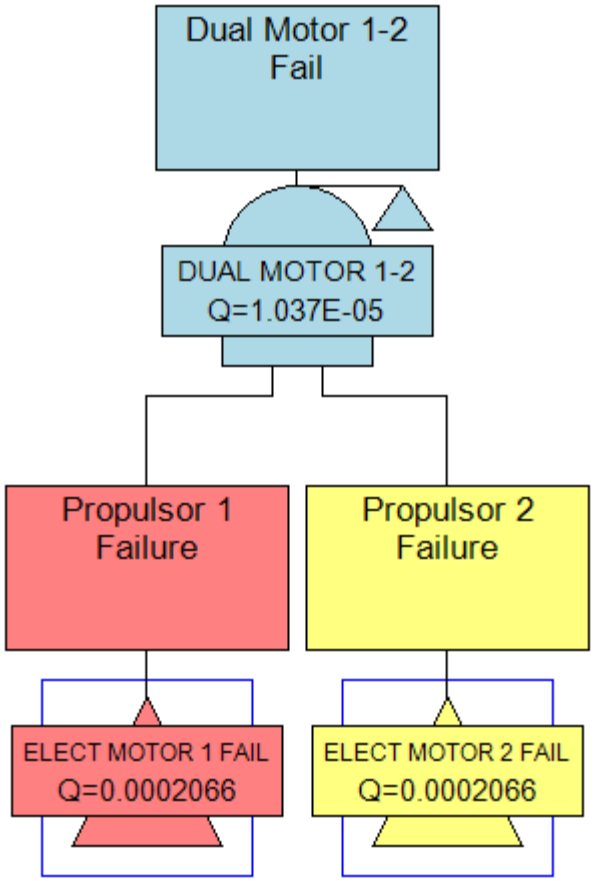

Pump Fail
PUMP FAIL
Pump 1 Fail
Pump 2 Fail
PUMP 1
PUMP 2
FR=4.36E-05
FR=4.36E-05
Inability to get power to rotor
COMBINER XMISSION
Combiner Transmission fail
X-shaft fail
3E1,3E2
CROSS-SHAFT
FR=2.5E-07
FR=9.1E-11

APPENDIX E ALTERNATE CONFIGURATION – QUAD-ROTOR WITHOUT INTERCONNECTING SHAFTS

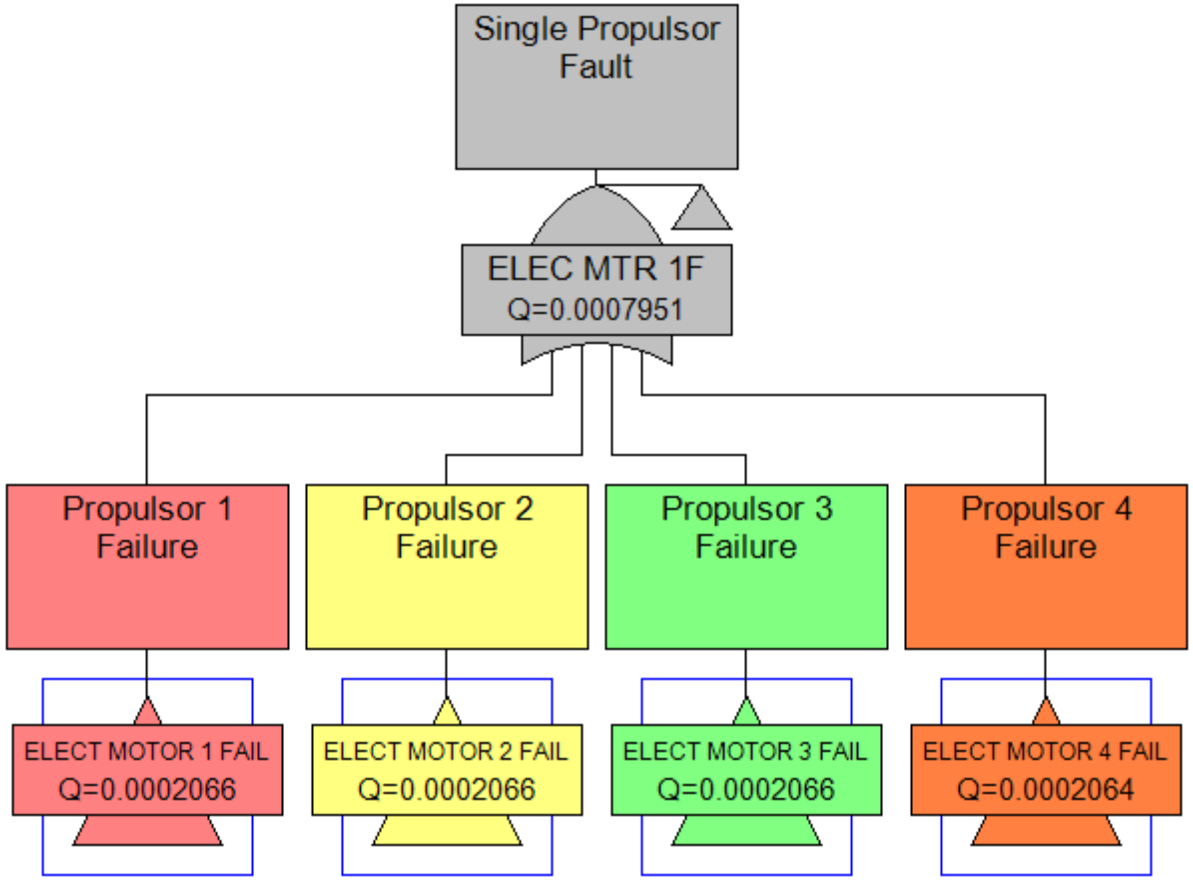

LOSS OF POWER TRANSMISSION
LOSS OF PROPULSION
Q=0.0007971
Dual electric motor failure
OEI Propulsion Loss (lack of thrust)
Loss of ability to drive a rotor
DUAL FAILURE
Q=1.056E-05
OEI PROPULSION LOSS
Q=0.0001988
ROTOR QM INPUT

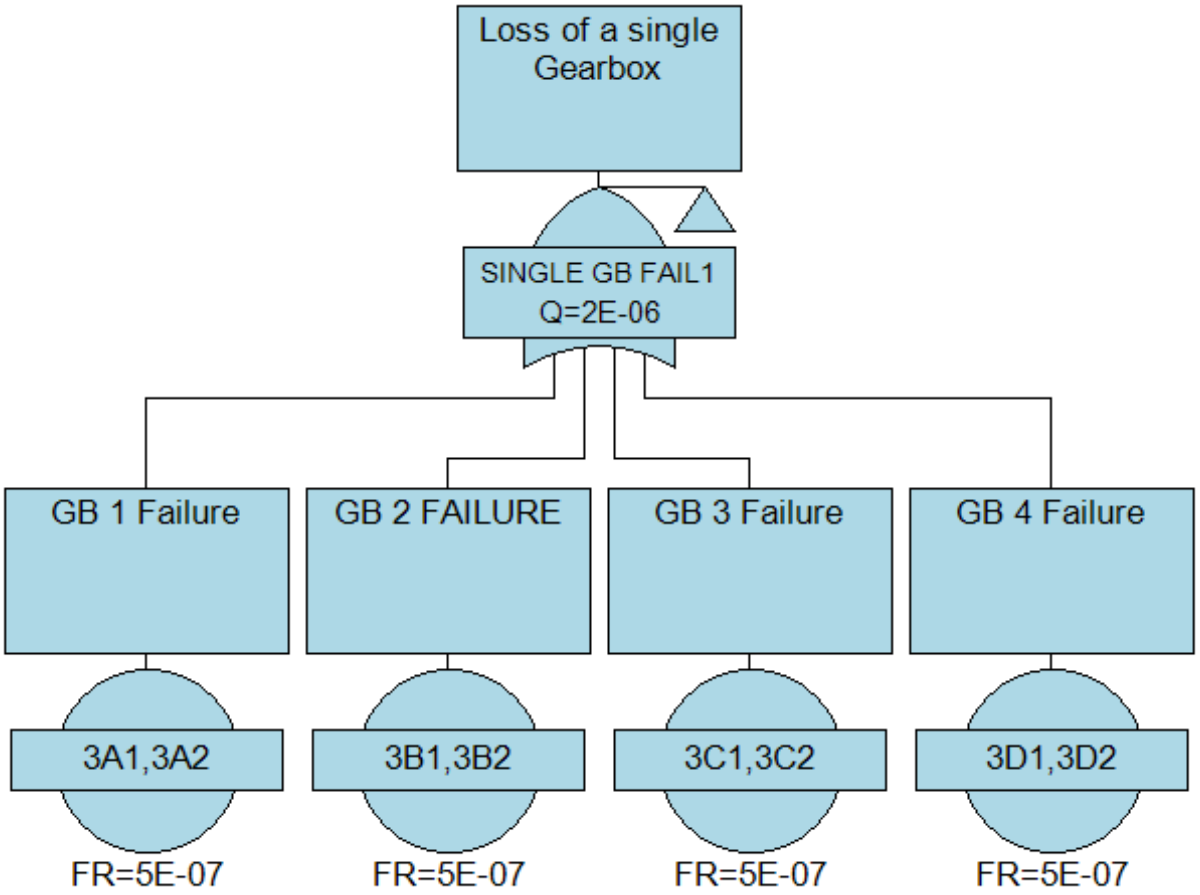

Dual electric motor failure
DUAL FAILURE
Q=1.056E-05
Dual Motor 1-2 Fail
Dual Motor 1-3 Fail
Dual Motor 1-4 Fail
Dual Motor 2-3 Fail
Dual Motor 2-4 Fail
Dual Motor 3-4 Fail
DUAL MOTOR 1-2
Q=1.037E-05
DUAL MOTOR 1-3
Q=1.037E-05
DUAL MOTOR 1-4
Q=1.037E-05
DUAL MOTOR 2-3
DUAL MOTOR 2-4
DUAL MOTOR 3-4

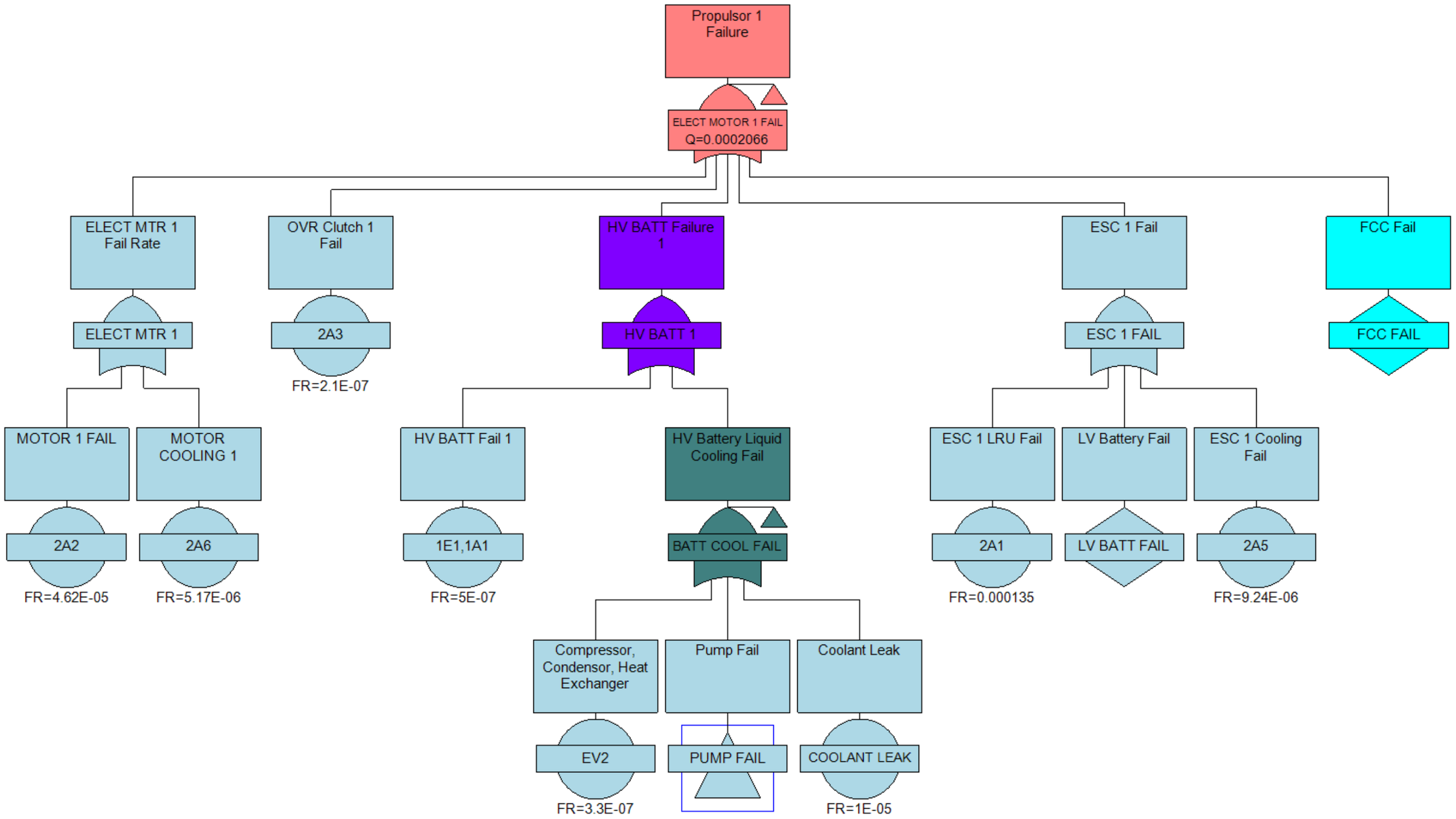

OEI Propulsion Loss (lack of thrust)
OEI PROPULSION LOSS
Q=0.0001988
In OEI Avoid Region
Single Propulsor Fault
OEI AVOID
Q=0.25
ELEC MTR 1F
Q=0.0007951
Loss of ability to drive a rotor
ROTOR QM INPUT
Loss of a single Gearbox
Single Propulsor Fault
SINGLE GB FAIL1
Q=2E-06
ELEC MTR 1F
Q=0.0007951



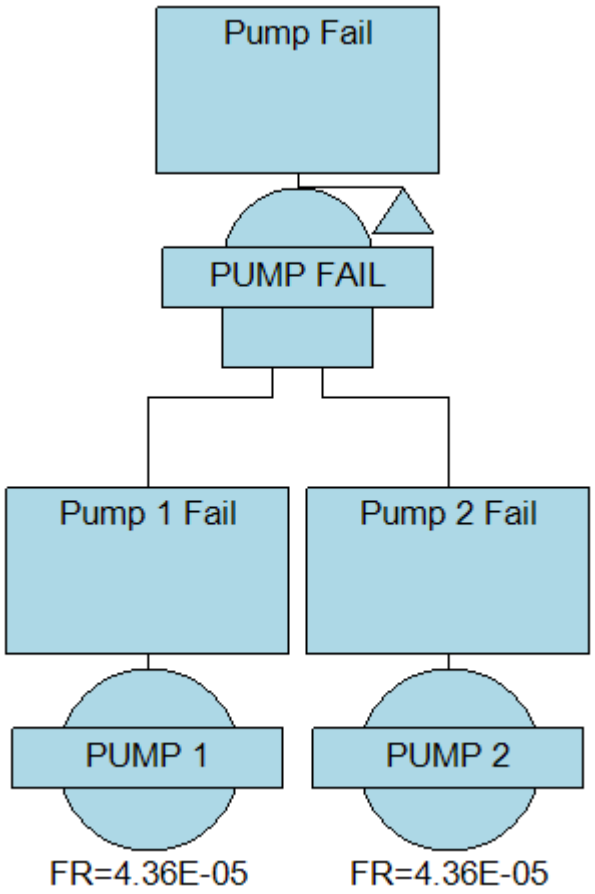
Note: "Dual Motor 1-2 Fail" is representative of all "Dual Motor X-Y Fail" events in Appendix E.


Single Propulsor Fault
ELEC MTR 1F
Q=0.0007951
Propulsor 1 Failure
Propulsor 2 Failure
Propulsor 3 Failure
Propulsor 4 Failure
ELECT MOTOR 1 FAIL
Q=0.0002066
ELECT MOTOR 2 FAIL
Q=0.0002066
ELECT MOTOR 3 FAIL
Q=0.0002066
ELECT MOTOR 4 FAIL
Q=0.0002064

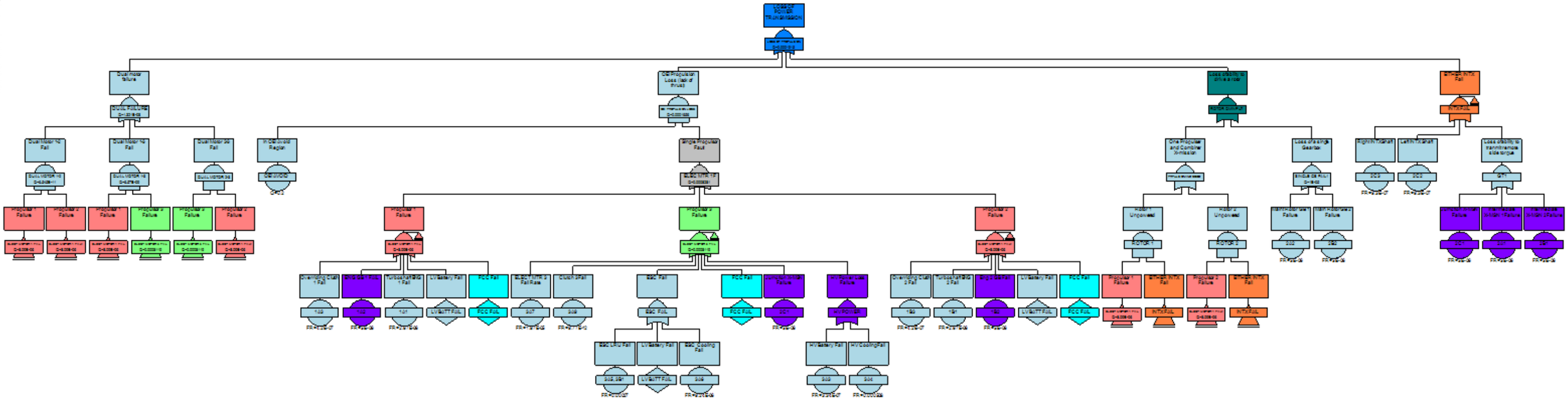

Loss of a single Gearbox
SINGLE GB FAIL1
Q=2E-06
GB 1 Failure
GB 2 FAILURE
GB 3 Failure
GB 4 Failure
3A1,3A2
3B1,3B2
3C1,3C2
3D1,3D2
FR=5E-07
FR=5E-07
FR=5E-07
FR=5E-07

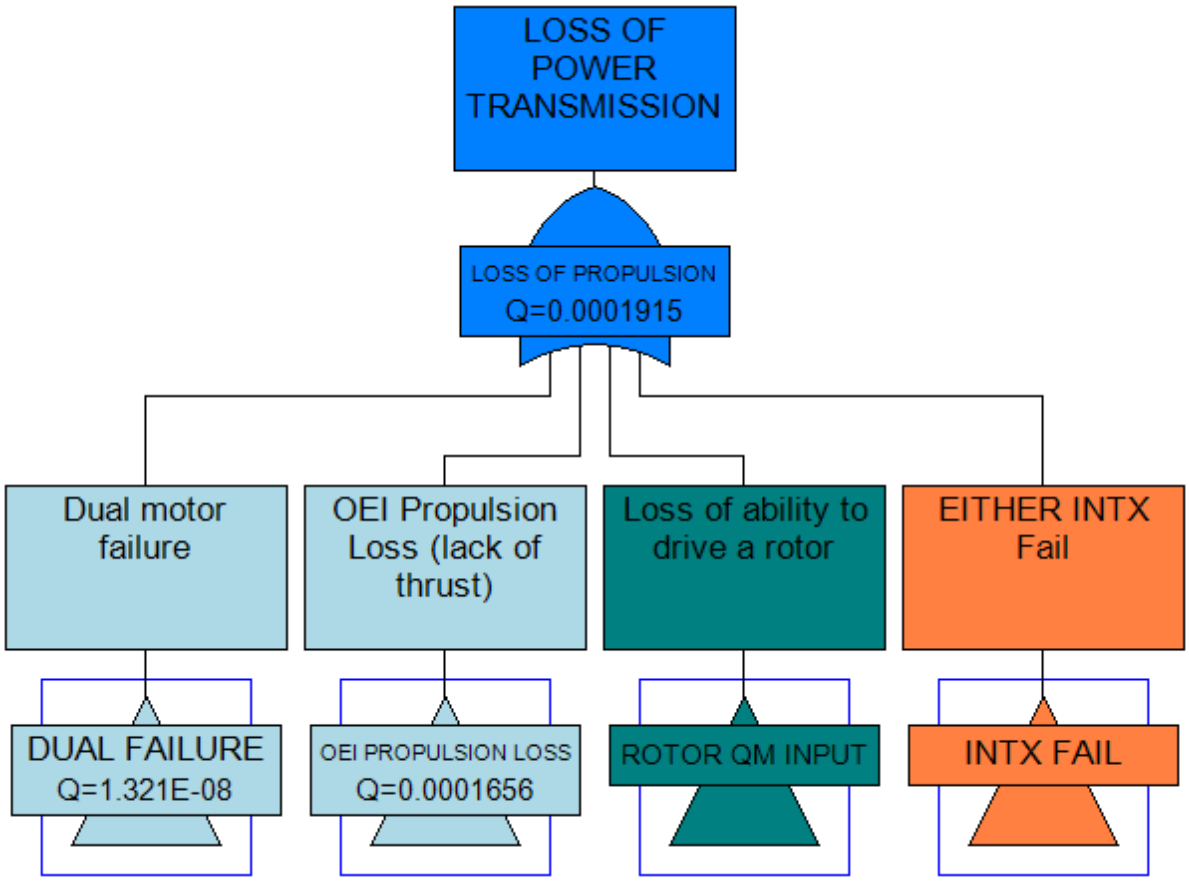


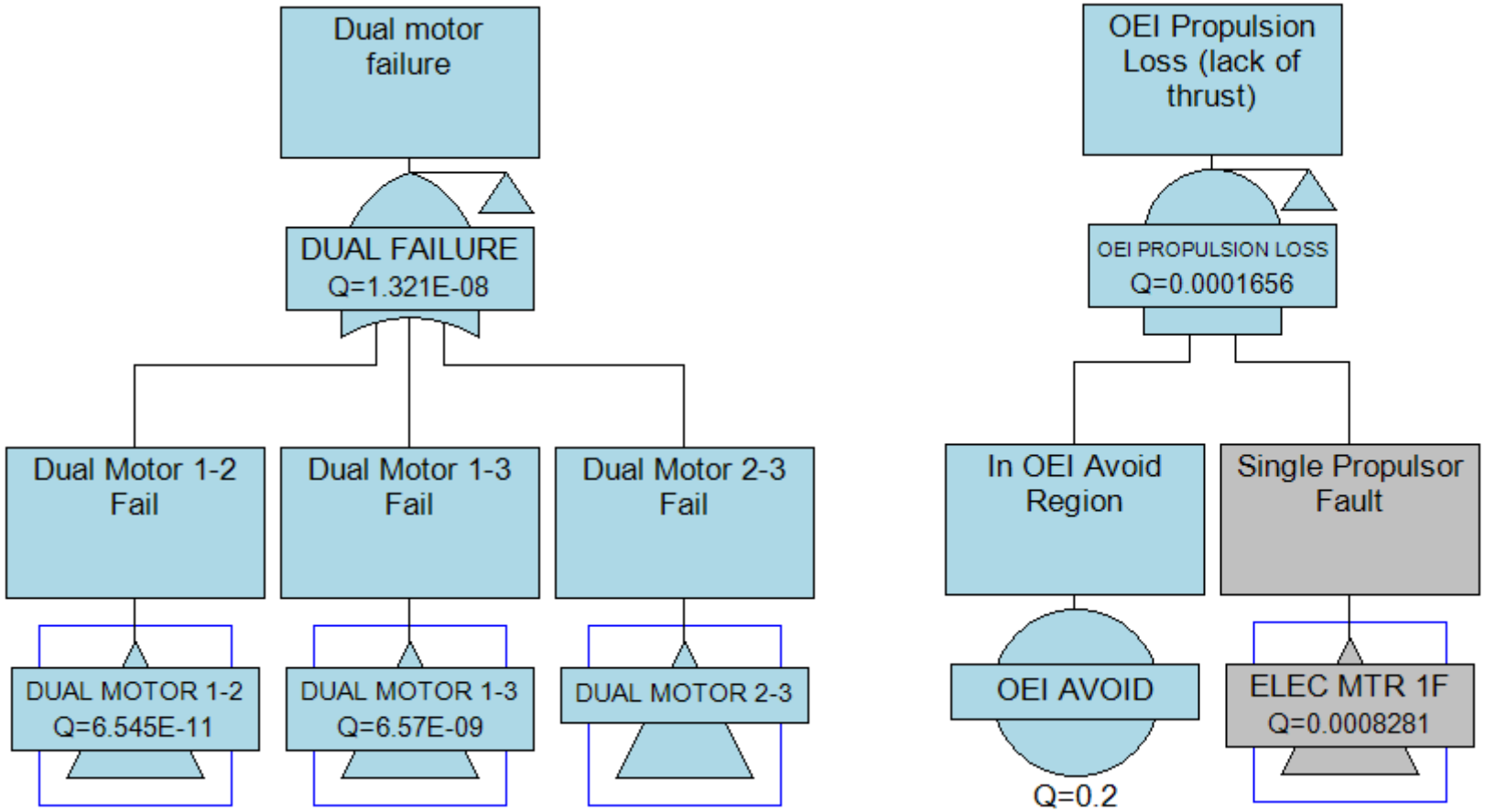
Note: “Propulsor 1 Failure” is representative of all “Propulsor X Failure” events in Appendix E.

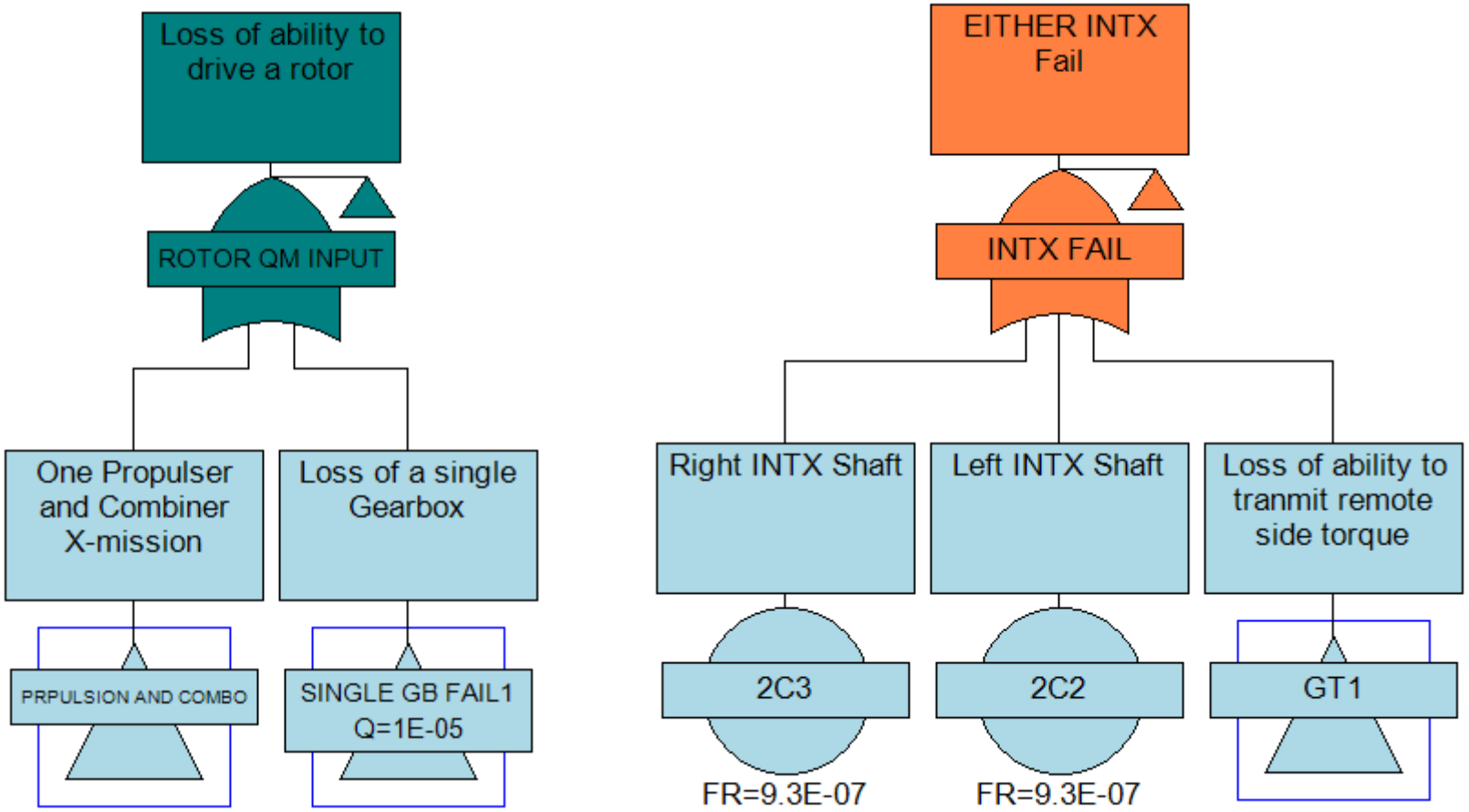

Pump Fail
PUMP FAIL
Pump 1 Fail
Pump 2 Fail
PUMP 1
PUMP 2
FR=4.36E-05
FR=4.36E-05

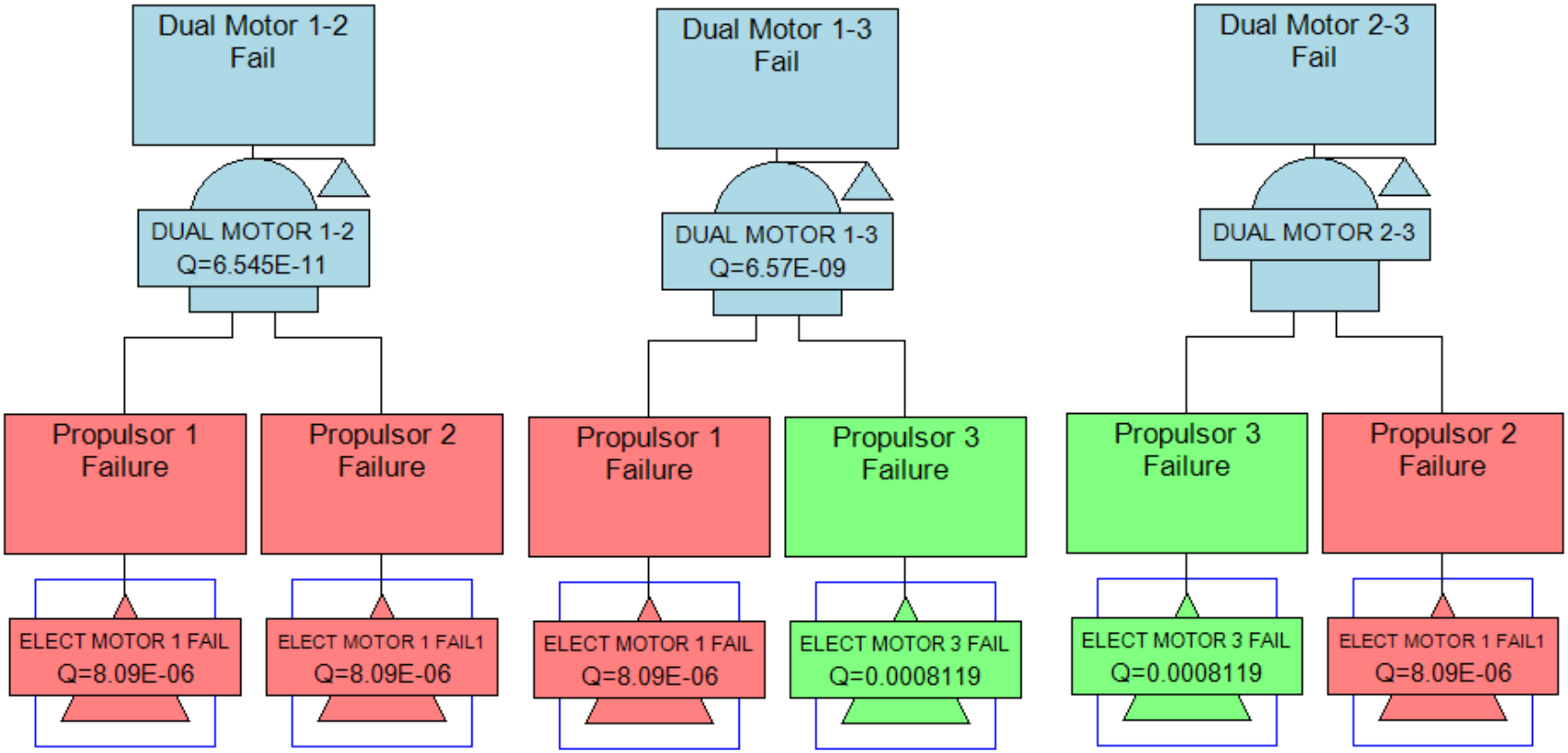
APPENDIX F LATERAL-TWIN FAULT TREE DIAGRAM

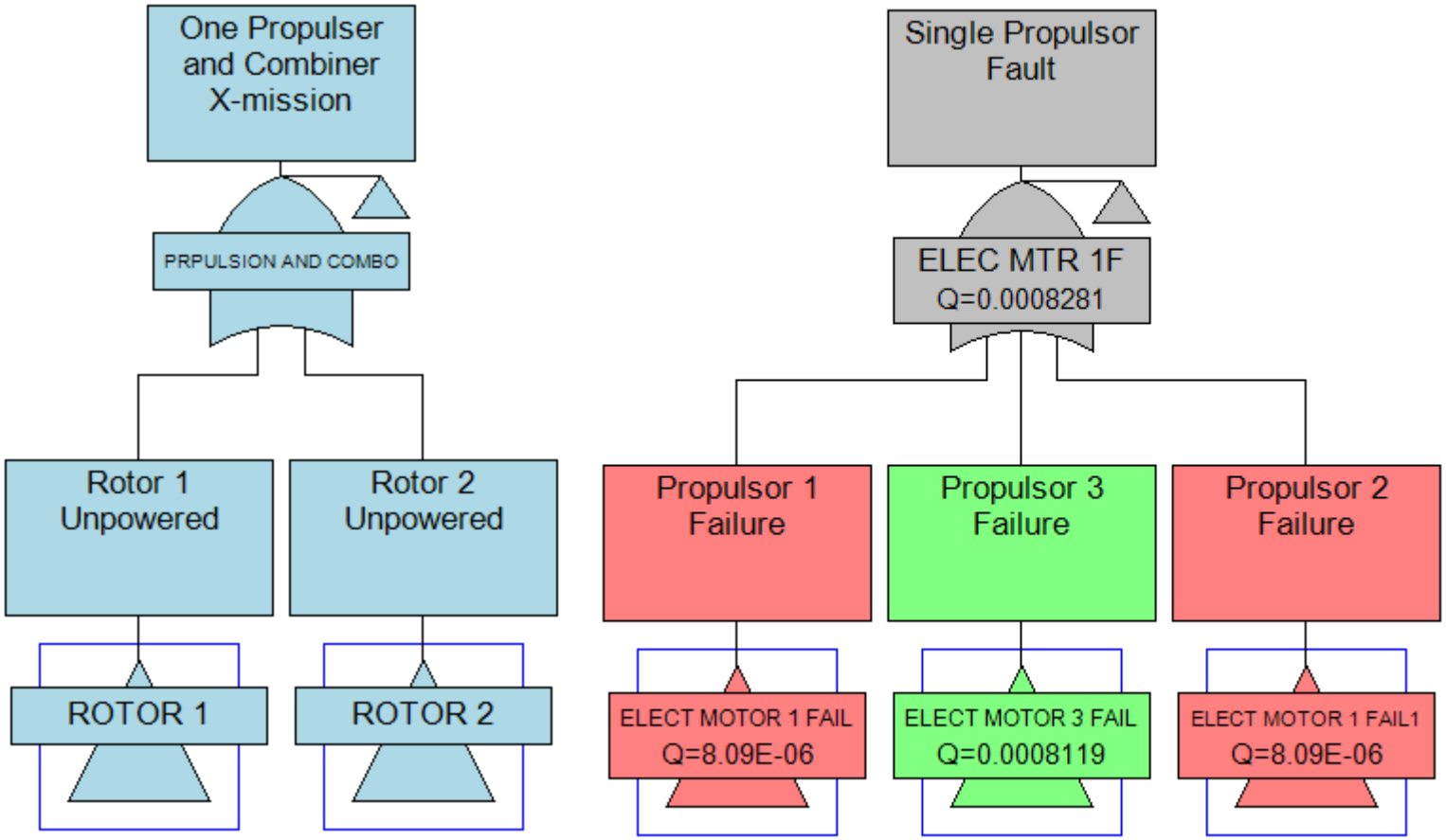


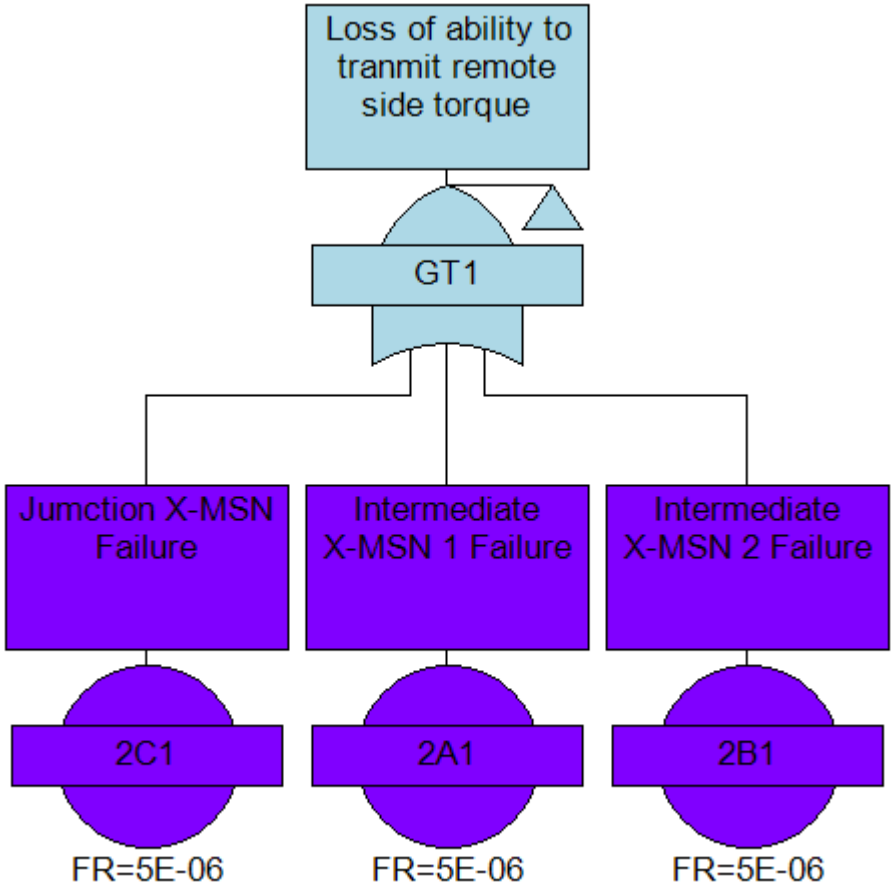

LOSS OF POWER TRANSMISSION
LOSS OF PROPULSION
Q=0.0001915
Dual motor failure
OEI Propulsion Loss (lack of thrust)
Loss of ability to drive a rotor
EITHER INTX Fail
DUAL FAILURE
Q=1.321E-08
OEI PROPULSION LOSS
Q=0.0001656
ROTOR QM INPUT
INTX FAIL

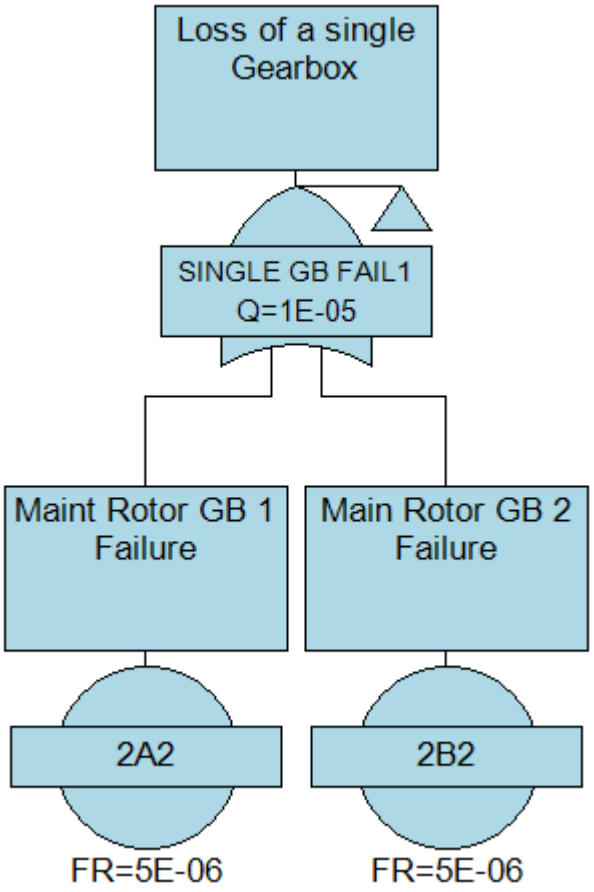

Dual motor failure
DUAL FAILURE
Q=1.321E-08
Dual Motor 1-2 Fail
Dual Motor 1-3 Fail
Dual Motor 2-3 Fail
DUAL MOTOR 1-2
Q=6.545E-11
DUAL MOTOR 1-3
Q=6.57E-09
DUAL MOTOR 2-3
OEI Propulsion Loss (lack of thrust)
OEI PROPULSION LOSS
Q=0.0001656
In OEI Avoid Region
Single Propulsor Fault
OEI AVOID
Q=0.2
ELEC MTR 1F
Q=0.0008281

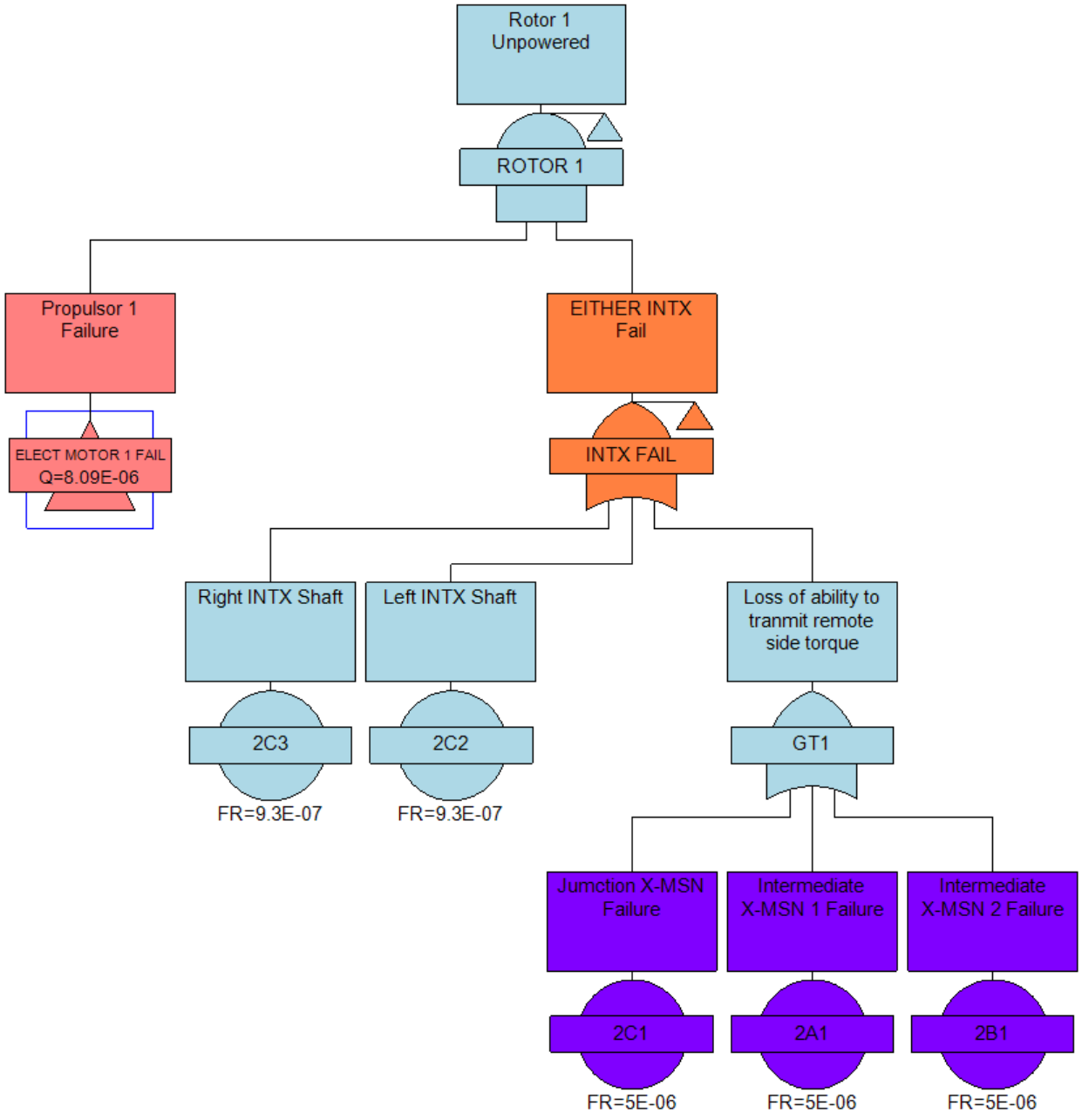

Loss of ability to drive a rotor
ROTOR QM INPUT
One Propulser and Combiner X-mission
Loss of a single Gearbox
PRPULSION AND COMBO
SINGLE GB FAIL1
Q=1E-05
EITHER INTX Fail
INTX FAIL
Right INTX Shaft
Left INTX Shaft
Loss of ability to tranmit remote side torque
2C3
2C2
GT1
FR=9.3E-07
FR=9.3E-07

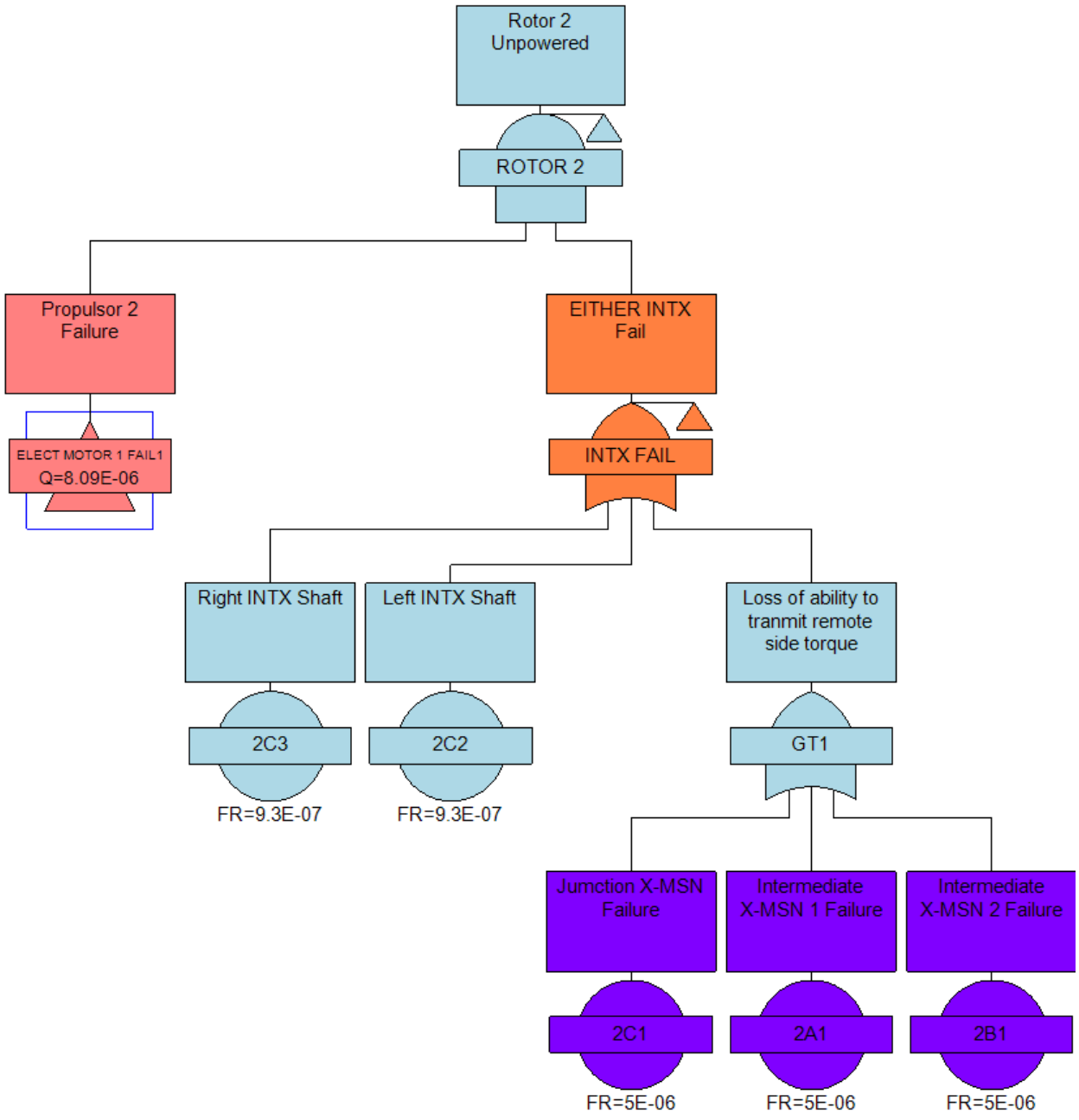

Dual Motor 1-2 Fail
DUAL MOTOR 1-2
Q=6.545E-11
Propulsor 1 Failure
Propulsor 2 Failure
ELECT MOTOR 1 FAIL
Q=8.09E-06
ELECT MOTOR 1 FAIL1
Q=8.09E-06
Dual Motor 1-3 Fail
DUAL MOTOR 1-3
Q=6.57E-09
Propulsor 1 Failure
Propulsor 3 Failure
ELECT MOTOR 1 FAIL
Q=8.09E-06
ELECT MOTOR 3 FAIL
Q=0.0008119
Dual Motor 2-3 Fail
DUAL MOTOR 2-3
Propulsor 3 Failure
Propulsor 2 Failure
ELECT MOTOR 3 FAIL
Q=0.0008119
ELECT MOTOR 1 FAIL1
Q=8.09E-06

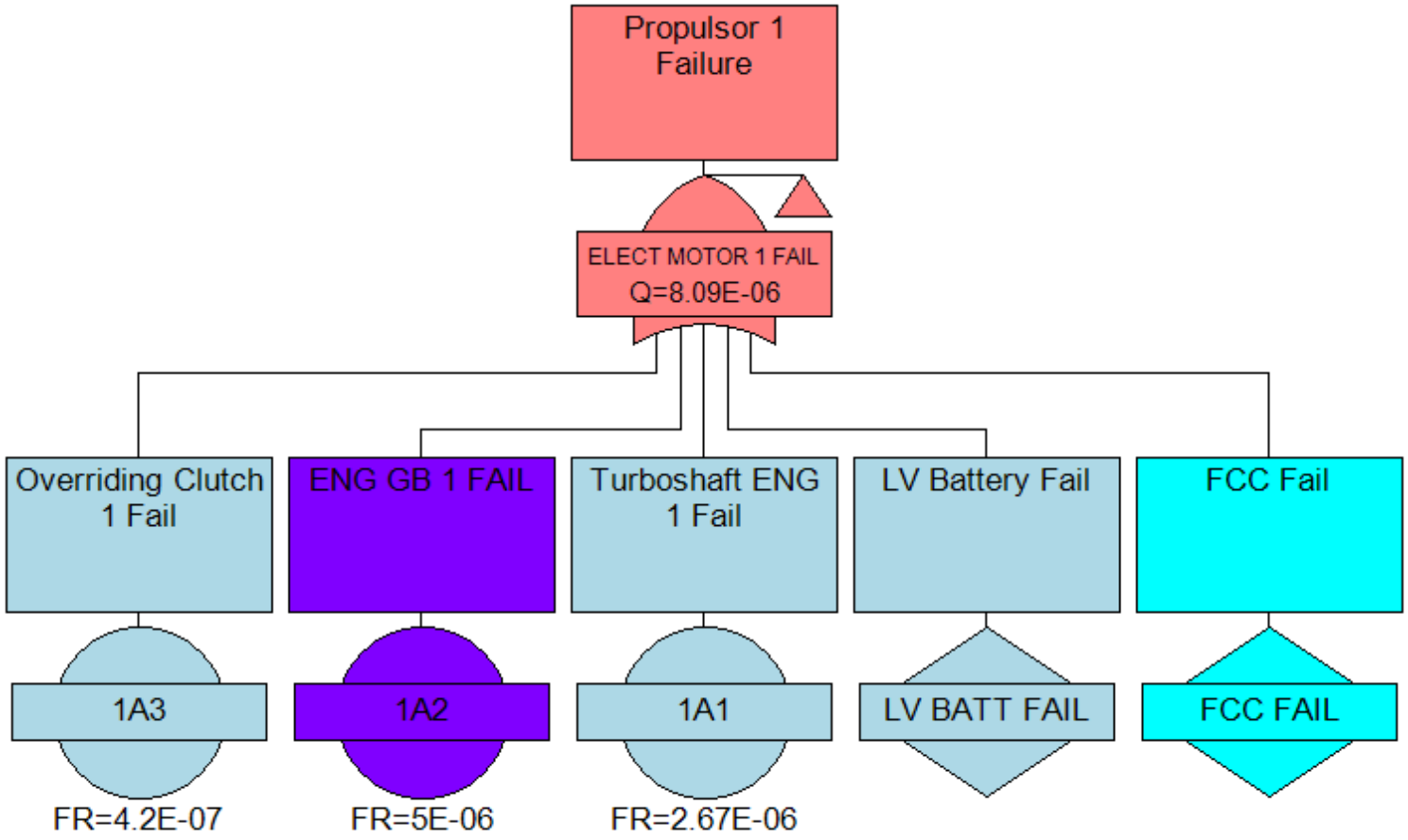

One Propulser and Combiner X-mission
PRPULSION AND COMBO
Rotor 1 Unpowered
Rotor 2 Unpowered
ROTOR 1
ROTOR 2
Single Propulsor Fault
ELEC MTR 1F
Q=0.0008281
Propulsor 1 Failure
Propulsor 3 Failure
Propulsor 2 Failure
ELECT MOTOR 1 FAIL
Q=8.09E-06
ELECT MOTOR 3 FAIL
Q=0.0008119
ELECT MOTOR 1 FAIL1
Q=8.09E-06

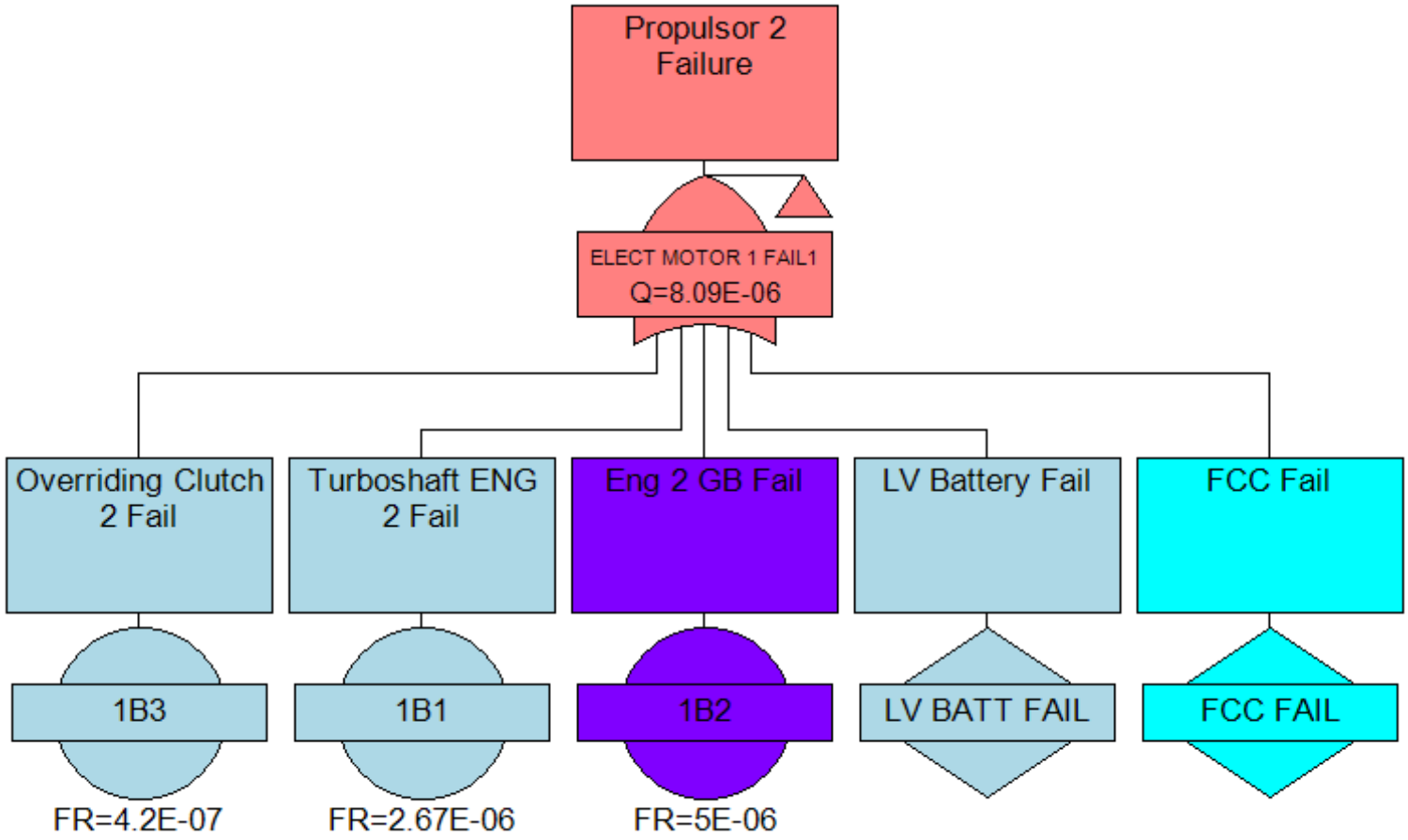

Loss of ability to tranmit remote side torque
GT1
Jumction X-MSN Failure
Intermediate X-MSN 1 Failure
Intermediate X-MSN 2 Failure
2C1
2A1
2B1
FR=5E-06
FR=5E-06
FR=5E-06

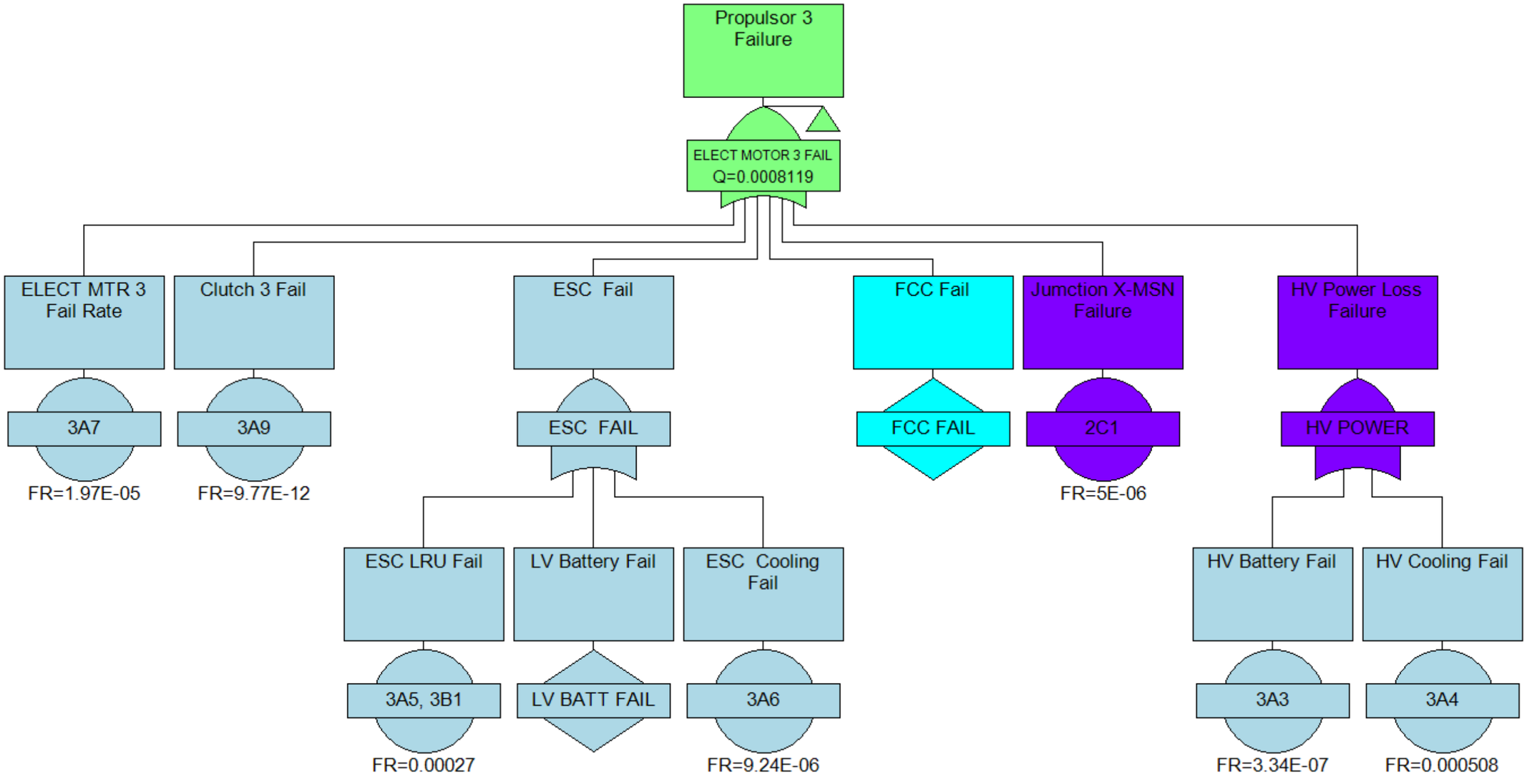

Loss of a single Gearbox
SINGLE GB FAIL1
Q=1E-05
Maint Rotor GB 1 Failure
Main Rotor GB 2 Failure
2A2
2B2
FR=5E-06
FR=5E-06


Rotor 1
Unpowered
ROTOR 1
Propulsor 1
Failure
ELECT MOTOR 1 FAIL
Q=8.09E-06
EITHER INTX
Fail
INTX FAIL
Right INTX Shaft
Left INTX Shaft
Loss of ability to
tranmit remote
side torque
2C3
2C2
GT1
FR=9.3E-07
FR=9.3E-07
Jumction X-MSN
Failure
Intermediate
X-MSN 1 Failure
Intermediate
X-MSN 2 Failure
2C1
2A1
2B1
FR=5E-06
FR=5E-06
FR=5E-06

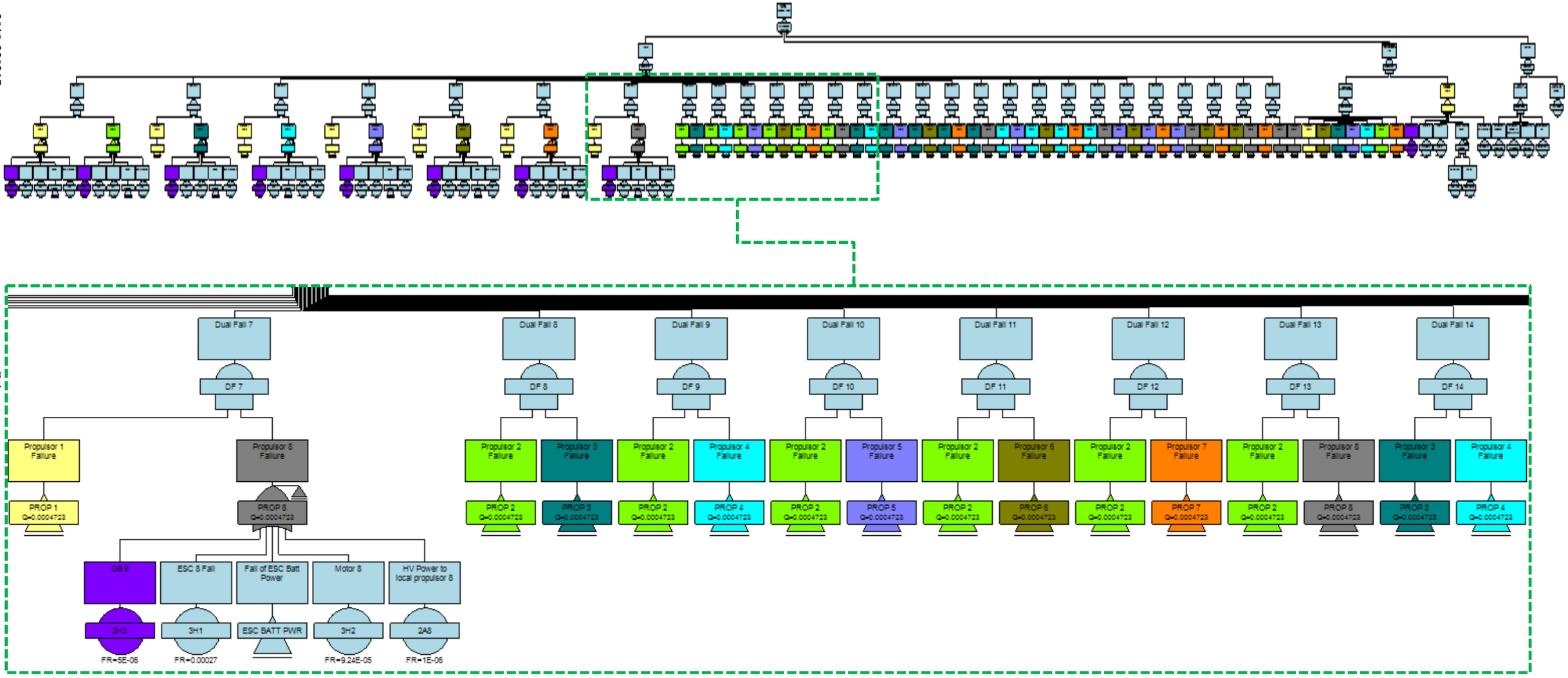

Rotor 2
Unpowered
ROTOR 2
Propulsor 2
Failure
ELECT MOTOR 1 FAIL1
Q=8.09E-06
EITHER INTX
Fail
INTX FAIL
Right INTX Shaft
Left INTX Shaft
Loss of ability to
tranmit remote
side torque
2C3
FR=9.3E-07
2C2
FR=9.3E-07
GT1
Jumction X-MSN
Failure
Intermediate
X-MSN 1 Failure
Intermediate
X-MSN 2 Failure
2C1
FR=5E-06
2A1
FR=5E-06
2B1
FR=5E-06

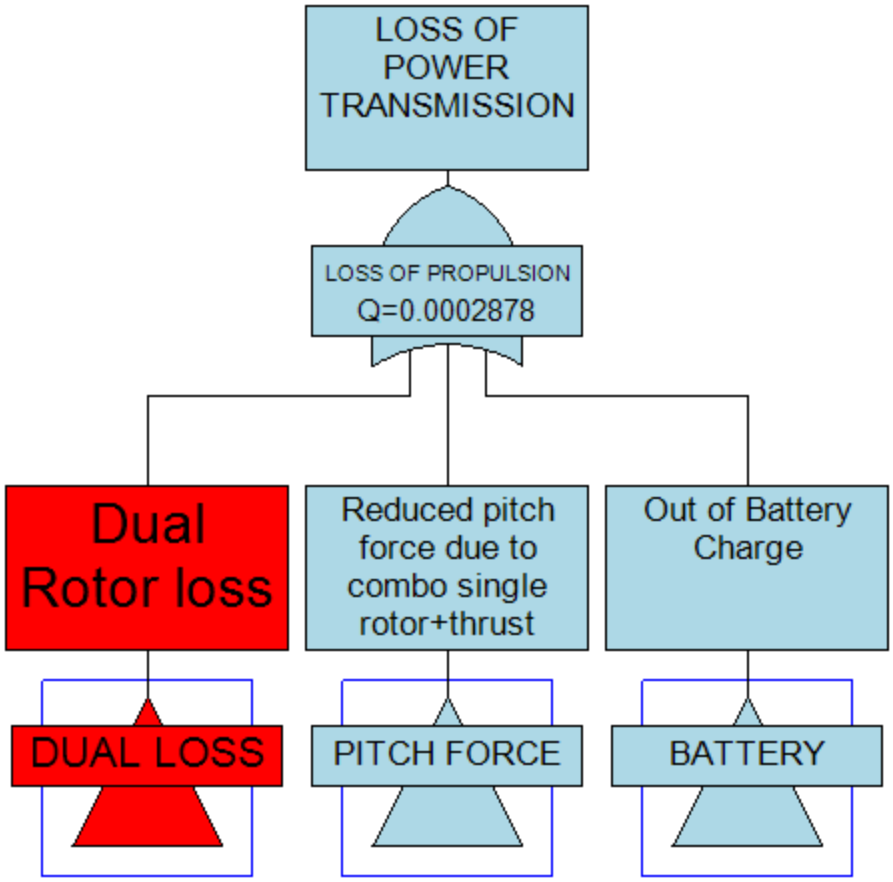

Propulsor 1 Failure
ELECT MOTOR 1 FAIL
Q=8.09E-06
Overriding Clutch 1 Fail
ENG GB 1 FAIL
Turboshaft ENG 1 Fail
LV Battery Fail
FCC Fail
1A3
1A2
1A1
LV BATT FAIL
FCC FAIL
FR=4.2E-07
FR=5E-06
FR=2.67E-06

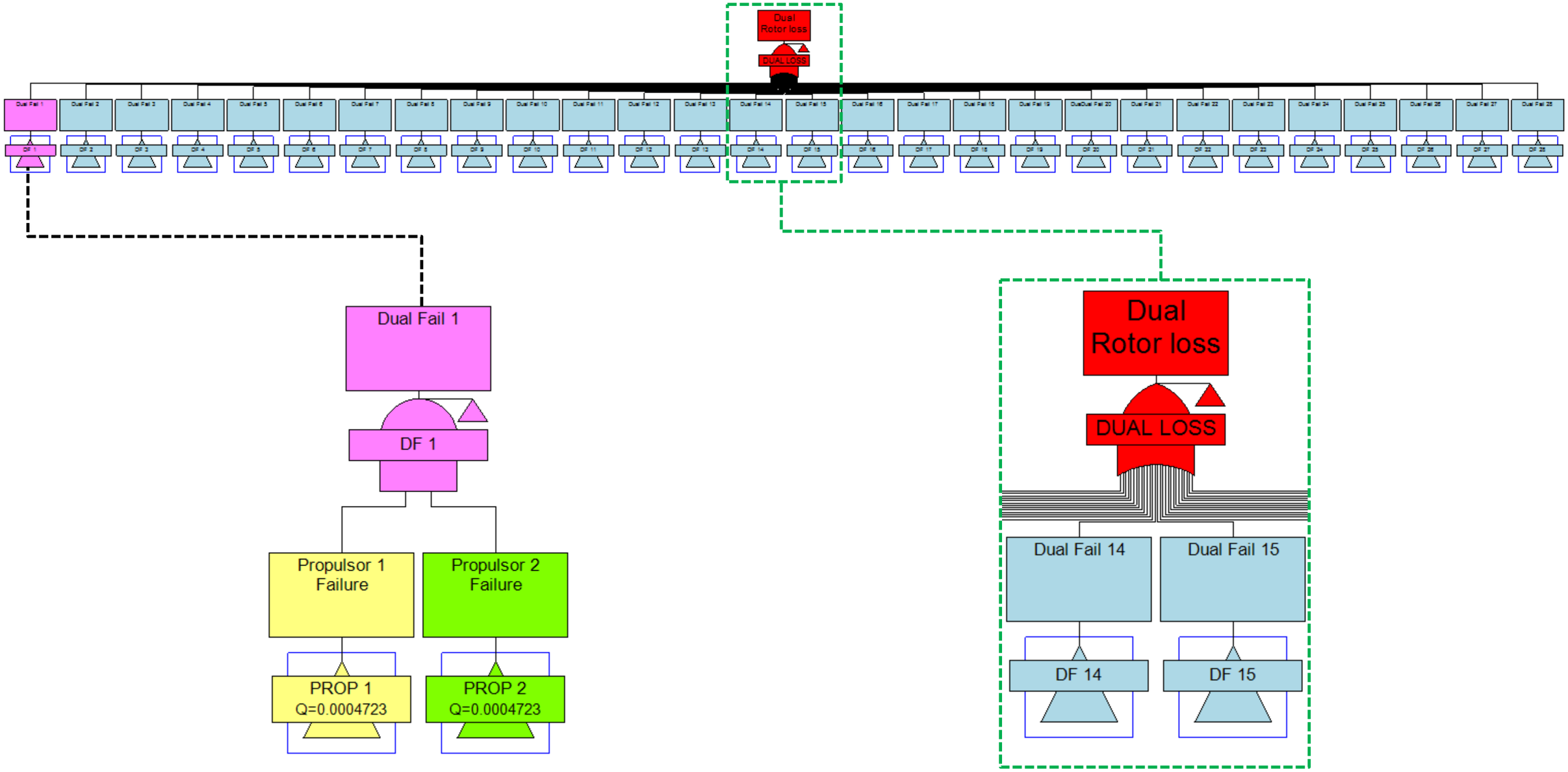

Propulsor 2 Failure
ELECT MOTOR 1 FAIL1
Q=8.09E-06
Overriding Clutch 2 Fail
Turboshaft ENG 2 Fail
Eng 2 GB Fail
LV Battery Fail
FCC Fail
1B3
1B1
1B2
LV BATT FAIL
FCC FAIL
FR=4.2E-07
FR=2.67E-06
FR=5E-06


Propulsor 3 Failure
ELECT MOTOR 3 FAIL
Q=0.0008119
ELECT MTR 3 Fail Rate
Clutch 3 Fail
ESC Fail
FCC Fail
Jumction X-MSN Failure
HV Power Loss Failure
3A7
3A9
ESC FAIL
FCC FAIL
2C1
HV POWER
FR=1.97E-05
FR=9.77E-12
FR=5E-06
ESC LRU Fail
LV Battery Fail
ESC Cooling Fail
HV Battery Fail
HV Cooling Fail
3A5, 3B1
LV BATT FAIL
3A6
3A3
3A4
FR=0.00027
FR=9.24E-06
FR=3.34E-07
FR=0.000508

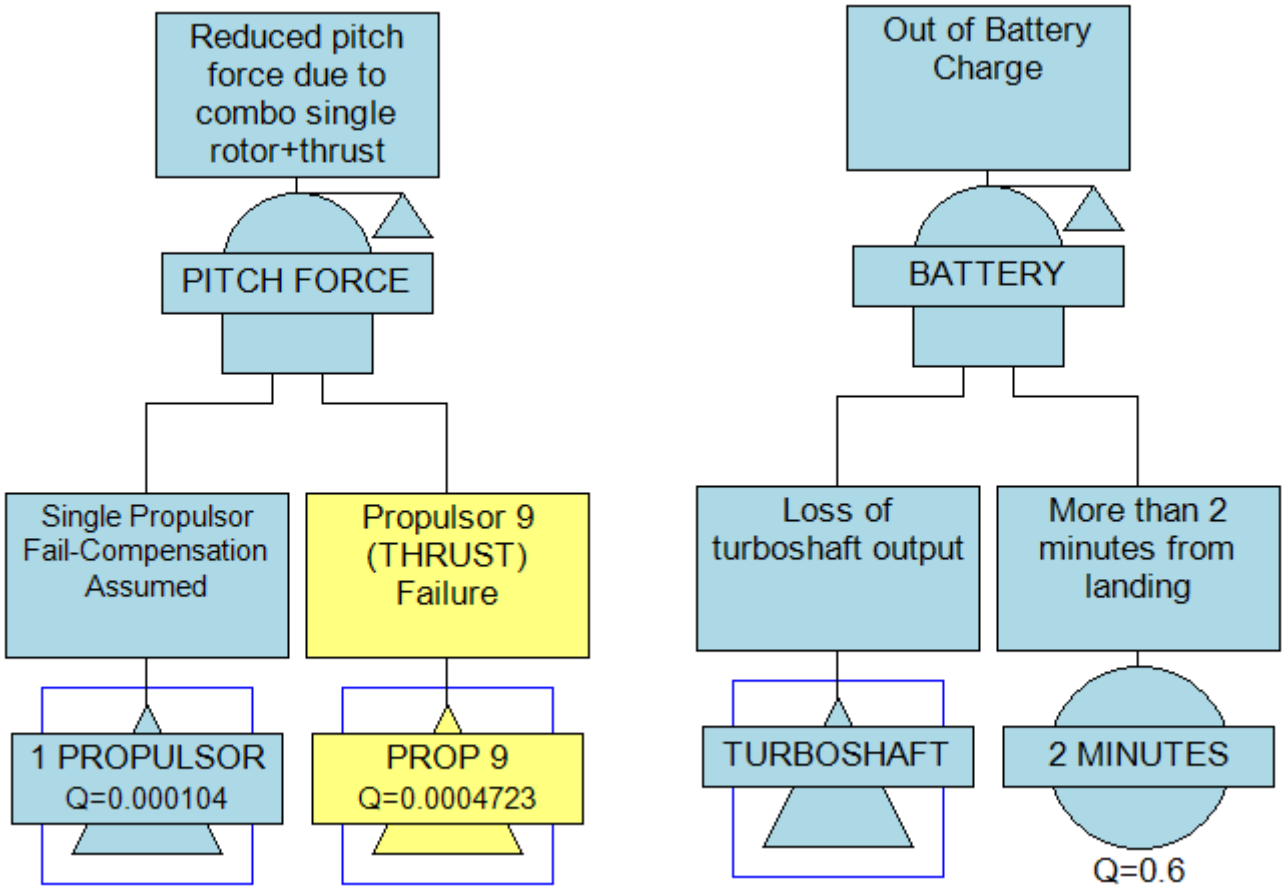
APPENDIX G LIFT+CRUISE FAULT TREE DIAGRAM



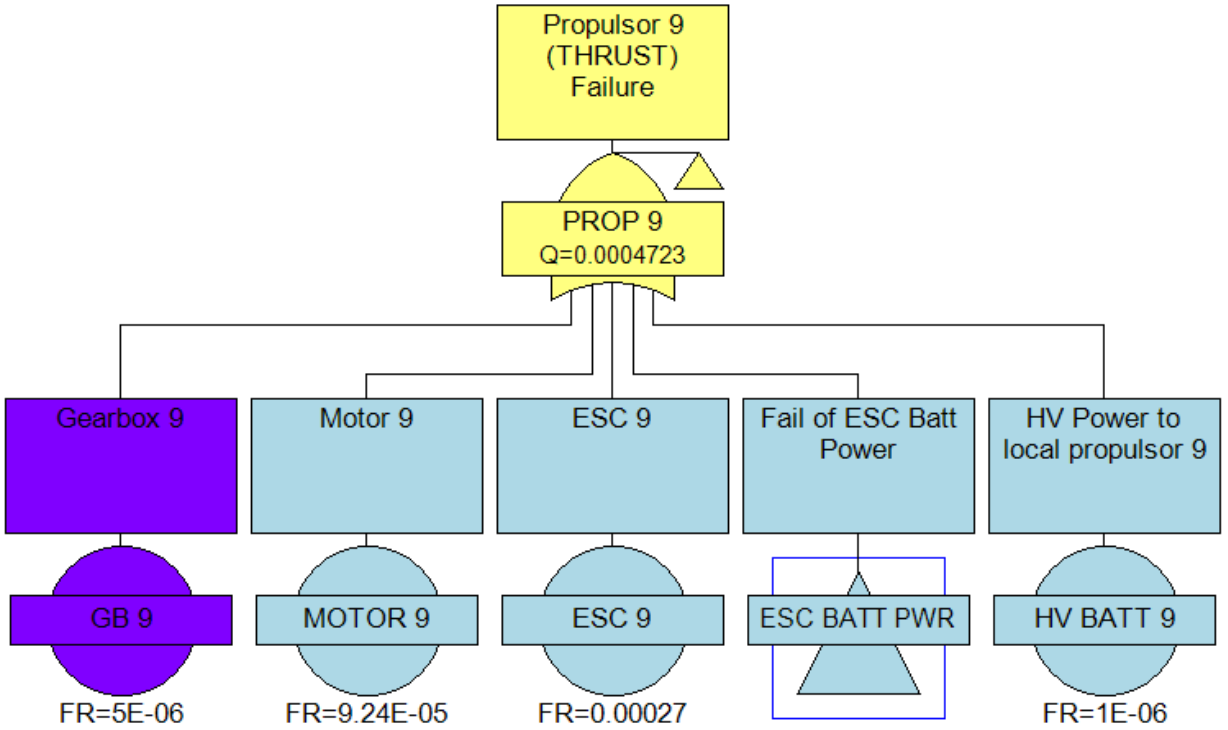

LOSS OF POWER TRANSMISSION
LOSS OF PROPULSION
Q=0.0002878
Dual Rotor loss
Reduced pitch force due to combo single rotor+thrust
Out of Battery Charge
DUAL LOSS
PITCH FORCE
BATTERY

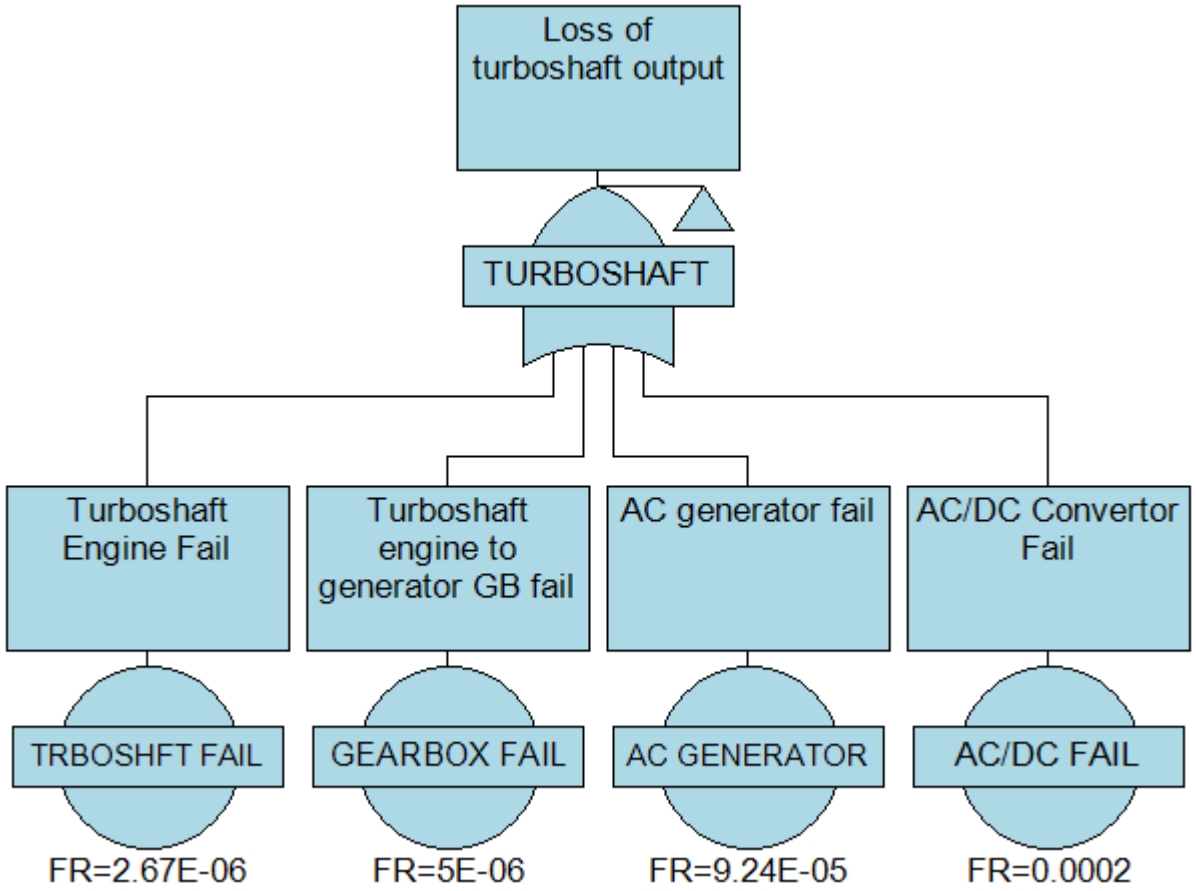


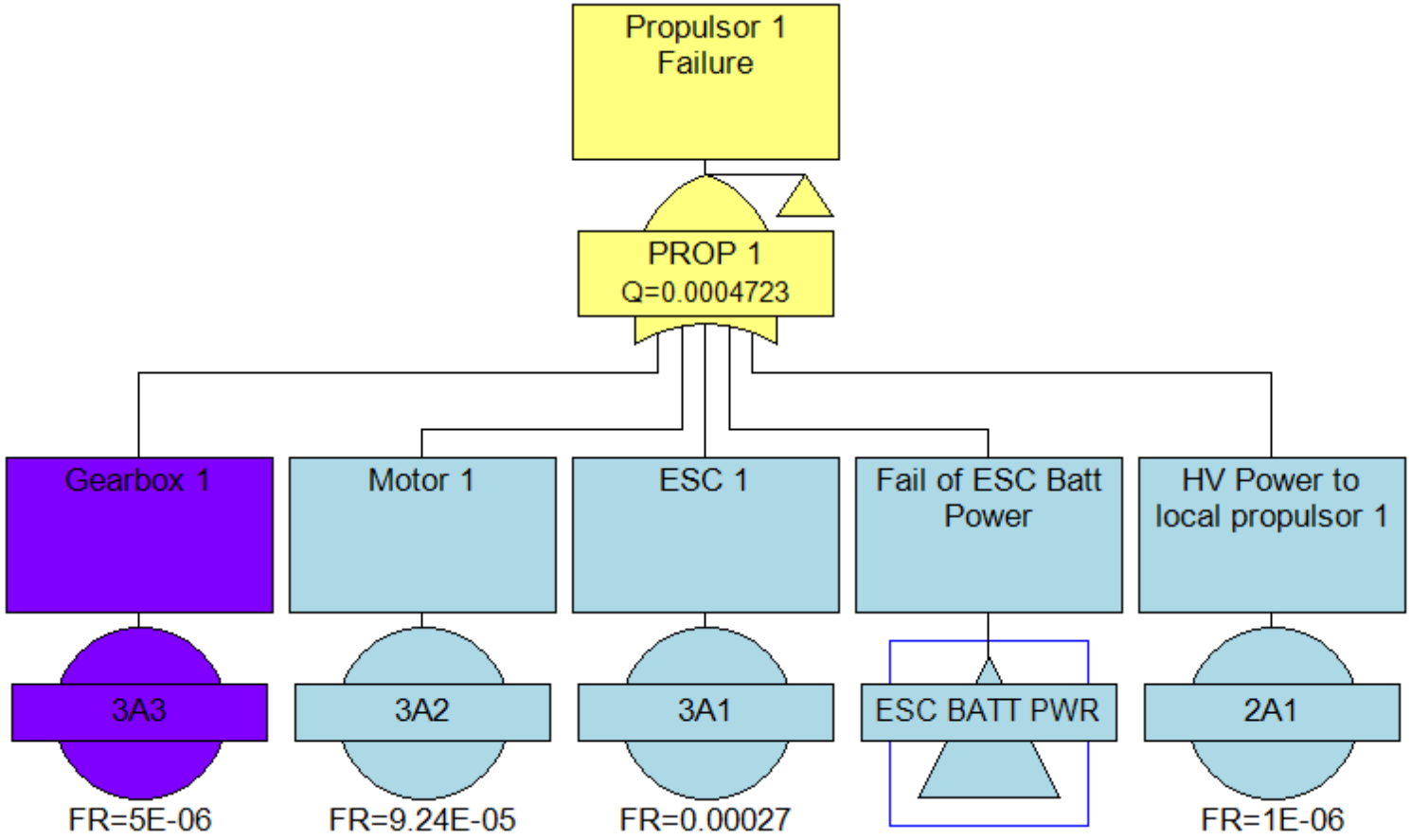
Note: "Dual Fail 1" is representative of all "Dual Fail X" events in Appendix G.
All "Dual Fail" events include the failure of all combinations of two (2) lifting propulsors, Propulsor 1 through Propulsor 8.


Reduced pitch force due to combo single rotor+thrust
PITCH FORCE
Single Propulsor Fail-Compensation Assumed
Propulsor 9 (THRUST) Failure
1 PROPULSOR
Q=0.000104
PROP 9
Q=0.0004723
Out of Battery Charge
BATTERY
Loss of turboshaft output
More than 2 minutes from landing
TURBOSHAFT
2 MINUTES
Q=0.6

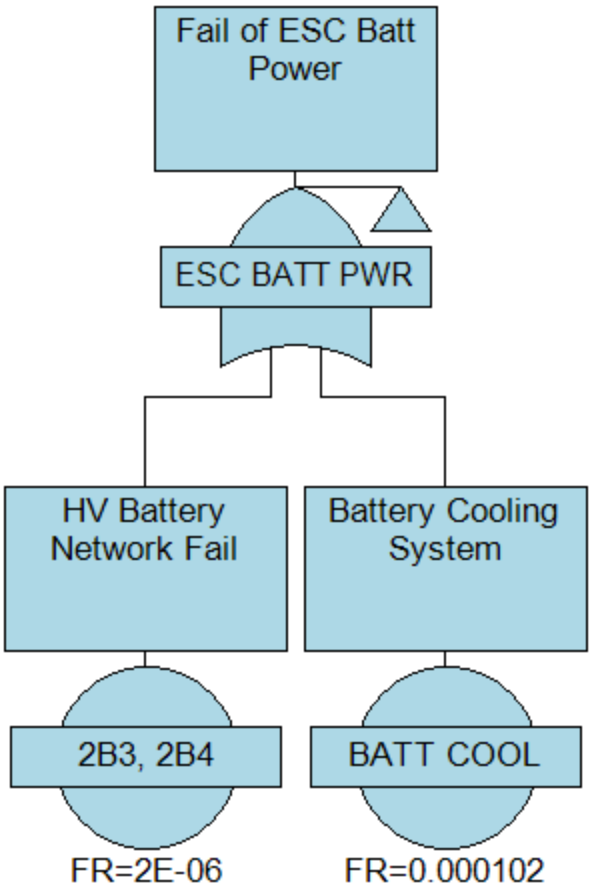
Single Propulsor Fail-Compensation Assumed
1 PROPULSOR
Q=0.000104
Propulsor 8 Failure
Propulsor 1 Failure
Propulsor 6 Failure
Propulsor 3 Failure
Propulsor 5 Failure
Propulsor 4 Failure
Propulsor 2 Failure
Propulsor 7 Failure
PROP 8
Q=0.0004723
PROP 1
Q=0.0004723
PROP 6
Q=0.0004723
PROP 3
Q=0.0004723
PROP 5
Q=0.0004723
PROP 4
Q=0.0004723
PROP 2
Q=0.0004723
PROP 7
Q=0.0004723


Propulsor 9
(THRUST)
Failure
PROP 9
Q=0.0004723
Gearbox 9
Motor 9
ESC 9
Fail of ESC Batt
Power
HV Power to
local propulsor 9
GB 9
MOTOR 9
ESC 9
ESC BATT PWR
HV BATT 9
FR=5E-06
FR=9.24E-05
FR=0.00027
FR=1E-06


Loss of turboshaft output
TURBOSHAFT
Turboshaft Engine Fail
Turboshaft engine to generator GB fail
AC generator fail
AC/DC Convertor Fail
TRBOSHFT FAIL
GEARBOX FAIL
AC GENERATOR
AC/DC FAIL
FR=2.67E-06
FR=5E-06
FR=9.24E-05
FR=0.0002



Note: "Propulsor 1 Fail" is representative of Propulsor 1 through Propulsor 8 events in Appendix G.


Fail of ESC Batt Power
ESC BATT PWR
HV Battery Network Fail
Battery Cooling System
2B3, 2B4
BATT COOL
FR=2E-06
FR=0.000102