

**AN INTEGRATED FRAMEWORK TO EVALUATE
OFF-NOMINAL REQUIREMENTS AND RELIABILITY
OF NOVEL AIRCRAFT ARCHITECTURES IN EARLY
DESIGN**

A Thesis
Presented to
The Academic Faculty

by

Mayank Bendarkar

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Aerospace Engineering

Georgia Institute of Technology
May 2021

Copyright © 2021 by Mayank Bendarkar

**AN INTEGRATED FRAMEWORK TO EVALUATE
OFF-NOMINAL REQUIREMENTS AND RELIABILITY
OF NOVEL AIRCRAFT ARCHITECTURES IN EARLY
DESIGN**

Approved by:

Professor Dimitri Mavris, Advisor
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Simon Briceno
Jaunt Air Mobility

Dr. Nicholas Borer
Aeronautics Systems Analysis Branch
NASA Langley Research Center

Professor Daniel Schrage
School of Aerospace Engineering
Georgia Institute of Technology

Dr. Elena Garcia
School of Aerospace Engineering
Georgia Institute of Technology

Date Approved: 09 April 2021

To my parents & my teachers...

ACKNOWLEDGEMENTS

There are many people to thank as my graduate school journey comes to a close. Pursuing a Ph.D. has been one of the most challenging and fulfilling endeavors I have undertaken, and it would not have been possible without their support.

First and foremost, I want to thank my advisor and guru, Prof. Dimitri Mavris, without whose constant support and guidance none of this would be possible. I also want to thank him for providing me with the freedom and stability to choose a topic that interested me greatly, while sharing his insights and experience to help me explore my path. I will be forever grateful for everything he has done and continues to do for me. I would also like to express my sincere gratitude to the members of my thesis defense reading committee - Dr. Simon Briceno, Dr. Nicholas Borer, Dr. Elena Garcia, and Dr. Daniel Schrage. I want to thank Dr. Briceno for providing me a research home in his division at ASDL, his mentorship, and constant support and encouragement while I worked on my thesis. I am grateful to Dr. Nicholas Borer for providing great opportunities to conduct research related to certification and safety which helped motivate and shape this dissertation, and for providing invaluable feedback on different technical aspects of it. I would like to thank Dr. Elena Garcia for being one of the first persons to trust in my capabilities, for providing me opportunities and mentorship as a new graduate student. I am also grateful to her for pushing me to stay on track and steering me in the right direction during our weekly meetings leading up to the defense. I want to thank Dr. Daniel Schrage for his feedback and comments that have helped improve this dissertation greatly.

My Ph.D. journey has been made enjoyable (and even possible!) by my friends and colleagues during my time as a graduate student. I want to thank all of them,

and ask for their forgiveness if I miss naming anyone. I would like to start by thanking Tejas Puranik, Dushhyanth Rajaram, and Ameya Behere for being close friends, and for our long chats on anything and everything. I would also like to thank Darshan, Manish, and Arturo for being close buddies and helping me clear the qualifiers; Evan Harrison for being my co-TA and a good friend. I would like to thank Darshan and Evan for sharing their expertise in developing 6-DoF models and for being co-authors with me; Imon Chakraborty, Jiacheng (Albert) Xie, and Yu Cai for being great colleagues and co-authors. These past few years have allowed me to create new friends and strengthen old friendships. I would like to thank Achyut Panchal, Indranil Karandikar, Pushkar Godbole, Raunak Bhattacharyya, Aditya Pophale, Suyash Vidwans, Ketan Patwardhan, and Kaivalya Bakshi for being my close friends and for all the fun times together. I would also like to thank Shantanu Thakar, among my oldest friends for the great discussions and fun times we've had.

I would like to express my fond appreciation and gratitude to Urna Nandi, without whom I couldn't have reached this milestone. Her constant love, encouragement, and support even during stressful times inspired me to keep making progress and ultimately complete this dissertation. Finally, I cannot express in words the gratitude I have for my mother Saroj Bendarkar, and father Vasant Bendarkar. While my failings might be my own, whatever I have achieved till now is because of them. Their unwavering love, support, encouragement, and sacrifices have made it possible for me to focus on my education and personal growth. Having spent the past decade studying Aerospace Engineering, I can finally say to them, "*I'm done with college!*". I would also like to thank my brother Tejas Bendarkar, sister-in-law Saloni, and my extended family for their support and encouragement.

Mayank Bendarkar

Atlanta, GA

April, 2021

TABLE OF CONTENTS

DEDICATION	iii
ACKNOWLEDGEMENTS	iv
LIST OF TABLES	xi
LIST OF FIGURES	xiv
SUMMARY	xviii
I MOTIVATION	1
1.1 Introduction	1
1.2 A Paradigm Shift to Novel Aircraft Architectures and Technologies	2
1.3 Trends in Aviation Safety	5
1.4 A System Safety Perspective	7
1.5 Summary	10
II BACKGROUND AND LITERATURE REVIEW	13
2.1 The Aircraft Conceptual Design Process	13
2.1.1 Aircraft Architecting	16
2.1.2 Requirements Definition	19
2.2 Basic Concepts	22
2.2.1 Definitions	22
2.2.2 Safety Requirements	23
2.2.3 Reliability	26
2.3 Safety Assessments: The Current Paradigm	28
2.3.1 The Safety Assessment Process	32
2.3.2 The Safety Assessment Analysis Methods	37
2.3.3 Probability Models	46
2.3.4 Summary and Observations	47
2.4 Reliability and Safety Assessments: State of the Art	50

2.4.1	Methods	50
2.4.2	Reliability in Preliminary System Design	52
2.4.3	Optimization and System Safety	55
2.4.4	Treatments of Uncertainty	57
2.5	Summary of Observations	60
III	RESEARCH FORMULATION	63
3.1	Research Objective	63
3.2	Research Area 1	65
3.3	Research Area 2	74
3.4	Research Area 3	80
3.5	Developed Framework	82
3.6	Test Problem Definition	83
IV	EXTENDED C-FHA AND PERFORMANCE-BASED MULTI- STATE ANALYSIS	89
4.1	Methods	91
4.1.1	Extension to C-FHA	91
4.1.2	Performance-based Multi-state Analysis	96
4.2	Safety Metrics	99
4.2.1	Metrics from Flight Operations	101
4.2.2	Metrics from Safety Analysis Literature	105
4.2.3	Summary of Implemented Safety Metrics	106
4.3	Safety Related Off-Nominal Requirements	107
4.3.1	Experiment 1.2	108
4.3.2	Benchmark Results	111
4.3.3	The T-DEP Aircraft Models	113
4.3.4	C-FHA Results	121
4.3.5	Performance-based Multi-state Analysis Results	142
4.3.6	Summary of Experiment 1.2	148

4.4	Unit Level Allocation	149
4.4.1	Experiment 1.3	150
4.4.2	Network-based Bottom-up Analysis	151
4.4.3	The T-DEP Bottom-up Network Analysis	156
4.4.4	Component Reliability Allocation Results	159
4.4.5	Summary of Experiment 1.3	163
4.5	Chapter Summary	164
V	A BAYESIAN PROBABILITY AND DECISION FRAMEWORK WITH MULTISTATE EXTENSION	167
5.1	A Bayesian Probability Framework	169
5.1.1	Basic Principles	169
5.1.2	Failure Rate Distributions - A Bayesian Approach	170
5.1.3	Experiment 2.1	174
5.1.4	Benchmark Component Failure Rates	176
5.1.5	Bayesian Component Posteriors	178
5.1.6	Bayesian Posterior Results - A family of curves	184
5.1.7	Summary of Experiment 2.1	186
5.2	A Bayesian Decision Framework	187
5.2.1	Experiment 2.2	190
5.2.2	Benchmark Results	191
5.2.3	Loss Functions	191
5.2.4	Bayesian Expected Loss Results	194
5.2.5	Summary of Experiment 2.2	196
5.3	Multi-state Reliability	197
5.3.1	A Multi-state Network Reliability Approach	198
5.3.2	Experiment 2.3	202
5.3.3	Multi-state Reliability Results	202
5.3.4	Summary of Experiment 2.3	207

5.4	Chapter Summary	209
VI	THE INTEGRATED FRAMEWORK - SENSITIVITIES AND TRADE STUDIES	212
6.1	Unit Level Importance	215
6.1.1	Experiment 3.1	215
6.1.2	Reliability of Complex Systems	216
6.1.3	Multi-state Component Importance Measures	218
6.1.4	Multi-state Component Importance Results	223
6.1.5	Summary of Experiment 3.1	227
6.2	Trade-studies	229
6.2.1	Experiment 3.2 - Resized Vertical Tail (VT)	230
6.2.2	Results - Resizing the VT	231
6.2.3	Summary of Experiment 3.2	234
6.2.4	Experiment 3.3 - Resized VT + Oversized Cruise Inverters	235
6.2.5	Results - Resizing the VT + Cruise Inverters	236
6.2.6	Summary of Experiment 3.3	239
6.3	Chapter Summary	240
VII	CONCLUDING REMARKS	244
7.1	Detailed Summary of Findings	246
7.1.1	Research Area 1: Identification, characterization, and allocation of safety related off-nominal requirements	246
7.1.2	Research Area 2: Gaps in the treatment of uncertainty in failure rates	249
7.1.3	Research Area 3: Sensitivities and Trade-studies	251
7.2	Contributions	254
7.3	Recommendations for Future Work	258
APPENDIX A	— PHYSICAL ARCHITECTURE MATRIX OF ALTERNATIVES	261
APPENDIX B	— T-DEP DELPHI MODEL	262

APPENDIX C	— COMPONENT FAILURE DATA	271
APPENDIX D	— COMPONENT IMPORTANCE	276
REFERENCES	280
VITA	295

LIST OF TABLES

1	NASA ERA targets [164]	1
2	Quantitative Part 23 Allowable Failure Rate for Different Failure Conditions [8]	24
3	Potential safety metrics for RQ 1.1	71
4	System states, minimal cut sets, and probability for Fig. 30	99
5	Summary of implemented safety metrics for the T-DEP problem . . .	107
6	X-57 Power system hazard characterization [144]	112
7	X-57 Power system failure scenarios [52]	112
8	T-DEP aircraft wing geometry	114
9	T-DEP aircraft vertical tail geometry	114
10	T-DEP aircraft stabilator geometry	116
11	Mass build-up of T-DEP aircraft	116
12	Mass properties of T-DEP aircraft	116
13	T-DEP right engines locations relative to CG in the flight dynamics body-fixed reference frame (x-forward, y-right, z-down)	117
14	High-lift motors thrust dependence on V_{EAS} [81]	118
15	Estimated lateral aerodynamic coefficients of the T-DEP	120
16	Polynomial drag coefficients for different flap and high lift propulsor settings for the T-DEP	121
17	Summary of hazard severity for continuous thrust loss for the T-DEP	138
18	Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted) . . .	146
19	Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	146
20	System states resulting from component failures	154
21	Bottom-up analysis: T-DEP power architecture unique system level failure states and severity using C-FHA results	156

22	Bottom-up analysis: T-DEP power architecture unique system level failure states and severity using performance-based multistate 6-DoF analysis	158
23	Mot-01 subsystem critical flow method weights	162
24	Component failure rate requirement allocation	164
25	Benchmark compliance results	191
26	Generic loss function $L(X, a)$	192
27	Loss function $L(X, a)$ for decision maker D	193
28	Probability of meeting failure rate requirements for Bayesian analysts	194
29	Expected loss and compliance finding using Analyst A's posteriors . .	195
30	Expected loss and compliance finding using Analyst B's posteriors . .	196
31	T-DEP aircraft resized VT geometry	230
32	Estimated lateral aerodynamic coefficients of the T-DEP with resized VT	230
33	Resized VT: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)	231
34	Resized VT: $\Delta \tan(\gamma_{max})$ (%) and Δ ERM under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)	232
35	Resized VT: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	233
36	Resized VT: $\Delta \tan(\gamma_{max})$ (%) under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	233
37	Resized VT: Δ ERM under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	233
38	Larger VT + CM-Inv: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	236
39	Larger VT + CM-Inv: Δ ERM and $\Delta \tan(\gamma_{max})$ (%) under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)	238

40	Larger VT + CM-Inv: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)	238
41	Larger VT + CM-Inv: $\Delta \tan(\gamma_{max})$ (%) and Δ ERM under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)	238
42	Multi-state Component Importance Measures	257
43	Commercial aircraft architecting alternatives (Adapted from Ref. [101])	261
44	Configuration component buildup for the X-57 [55]	267
45	Coefficients for computing downwash angle [55]	270
46	Battery failure data	271
47	Electric Motor failure data	272
48	Motor Inverter failure data	273
49	Traction Power Bus failure data	274
50	Switch failure data	275
51	Resistor failure data	275

LIST OF FIGURES

1	Schematic CO_2 emissions reduction roadmap [88] (Source: IATA) . . .	2
2	Example Novel Aircraft Concepts	5
3	Commercial flight accident statistics [90]	6
4	GA Accidents between 2008 - 2017 (Source: NTSB [136])	7
5	GA accident statistics (Source: NTSB [136])	9
6	Cost, knowledge, and freedom with design stages [122]	14
7	Aircraft conceptual design process [154]	15
8	A notional constraint analysis plot for the F-86	21
9	The reliability bathtub curve	27
10	Interplay between ARP 4761 and ARP 4754 [6]	29
11	Generic RTA Architecture (Adapted from Ref. [10])	30
12	The System V & V diagram in the context of safety and aircraft design (Adapted from ARP4754 [6])	31
13	Relationship between FHAs and FTAs (Adapted from ARP 4761 [4])	35
14	Basic building blocks for FTA (Adapted from [64])	39
15	Steps for building a FTA (Adapted from [64])	40
16	(a) Blocks in series (b) Blocks in parallel	41
17	Example Markov Analysis for a three component non-repairable system	43
18	Notional plot of the extended C-FHA process	67
19	Notional plot of the multistate performance based safety assessment process	68
20	Notional uncertainty propagation during the C-FHA process	74
21	Overview of Research Area 1	75
22	Overview of Research Area 2	80
23	Overview of Research Area 3	82
24	Integrated Framework to Evaluate Off-Nominal Requirements & Reli- ability of Novel Architectures in Early Design	84

25	Test problem concept and architecture	87
26	From traditional loss to Taguchi loss (adapted from [25])	92
27	Notional hazard severity - from traditional FHA to Continuous FHA	93
28	Notional plot of the extended C-FHA process	94
29	Notional plot of the multi-state performance based safety assessment process	97
30	An example system with two sources and three terminal components in network representation	97
31	Summary of energy metrics utilized in GA flight data analysis (Adapted from Ref. [150])	103
32	Characterizing safety related off-nominal requirements	109
33	T-DEP aircraft traction power system	110
34	Traditional FHA - loss of thrust hazard severity	111
35	DELPHI framework (Credit: Refs. [34, 161])	113
36	The X-57 aircraft geometry using OpenVSP [133]	115
37	Ratio of TOFL required to available at 2356 ft under continuous thrust degradation	124
38	Ratio of TOFL required to available at sea-level ft under continuous thrust degradation	125
39	Ratio of TOFL required to available at 10,000 ft under continuous thrust degradation	125
40	T-DEP C-FHA results using TOFL metric under thrust degradation	127
41	n_{max} , ϕ_{max} for the T-DEP in nominal conditions	129
42	Thrust loss resulting in $n_{max} = 1$ for the T-DEP	130
43	Thrust loss resulting in $\phi_{max} \leq 30^\circ$ for the T-DEP	131
44	Thrust loss resulting in $\phi_{max} \leq 45^\circ$ for the T-DEP	132
45	C-FHA hazard severity for the T-DEP aircraft due to thrust degrada- tion using n_{max} , ϕ_{max} metrics	133
46	MPCG under thrust degradation scenarios at takeoff for the T-DEP .	135
47	MPCG under thrust degradation scenarios at cruise for the T-DEP .	137

48	C-FHA hazard severity due to thrust degradation using MPCG (γ_{max}) metrics	139
49	Summary of C-FHA hazard severity due to thrust degradation for the T-DEP aircraft using the different safety metrics discussed	140
50	Summary of C-FHA allowable failure rate allocation to thrust degradation for the T-DEP	141
51	T-DEP multistate T_a/T_{max} in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)	142
52	T-DEP multistate T_a/T_{max} in cruise configuration. Colored by C-FHA hazard severity from Fig. 49(b)	142
53	T-DEP asymmetric loss of thrust multi-state failures	143
54	T-DEP multistate asymmetric thrust loss in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)	148
55	Allocating aircraft level requirements to the unit level	151
56	An example system with two sources and three terminal components in network representation	152
57	Cruise motor required failure rate with time	160
58	Mot-01 subsystem failure rate determination	161
59	Procedure used to answer research question 2	168
60	Guidelines for selecting the Likelihood and Prior distributions (adapted from [58])	171
61	Bayesian failure rate posteriors for the two analysts	185
62	Notional Integrated Risk Assessment - Probability of meeting component failure rate requirements	189
63	An example system with two sources and three terminal components in network representation	199
64	T-DEP multi-state λ_{req} in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)	203
65	T-DEP multi-state λ_{req} in cruise configuration. Colored by C-FHA hazard severity from Fig. 49(b)	203
66	T-DEP asymmetric multi-state λ_{req} in takeoff configuration. Colored by asymmetric thrust loss hazard severity from Fig. 54	203

67	Multi-state failure rates for the two Bayesian analysts for takeoff C-FHA hazards colored by compliance finding	204
68	Multi-state failure rates for the two Bayesian analysts for cruise C-FHA hazards colored by compliance finding	205
69	Asymmetric loss of thrust – multi-state failure rates for the two Bayesian analysts for takeoff. Colored by compliance finding	206
70	Integrated Framework to Evaluate Off-Nominal Requirements & Reliability of Novel Architectures in Early Design	214
71	Multi-state importance metrics for Catastrophic failure conditions (Analyst B)	223
72	Multi-state importance metrics for Hazardous failure conditions (Analyst B)	225
73	Multi-state importance metrics for Major failure conditions (Analyst B)	226
74	Multi-state importance metrics for Minor failure conditions (Analyst B)	227
75	Resized VT + Oversized Cruise Inverters: T-DEP asymmetric multi-state λ_{req} in takeoff configuration. Colored by asymmetric thrust loss hazard severity from Fig. 54	237
76	Resized VT + Oversized Cruise Inverters: Asymmetric loss of thrust – multi-state failure rates for the two Bayesian analysts for takeoff. Colored by compliance finding	237
77	Overview of the Research Formulation	247
78	Integrated Framework to Evaluate Off-Nominal Requirements & Reliability of Novel Architectures in Early Design	252
79	DELPHI framework (Credit: Refs. [34, 161])	262
80	Multi-state importance metrics for Catastrophic failure conditions (Analyst A)	276
81	Multi-state importance metrics for Hazardous failure conditions (Analyst A)	277
82	Multi-state importance metrics for Major failure conditions (Analyst A)	278
83	Multi-state importance metrics for Minor failure conditions (Analyst A)	279

SUMMARY

The world of aviation is moving towards novel aircraft architectures and technologies as a result of a push towards higher efficiency, lower operating costs, and lower emissions. One of the barriers to the development of future concepts is the uncertainty related to their reliability and the safety risk they pose. It is paramount for aircraft designers to have the capability to quantify safety-related off-nominal requirements and reliability earlier in the design stage in a manner that allows exploration of the architectural space before degrees of freedom are locked down by design decisions.

In the traditional paradigm, system safety and reliability for an aircraft are generally quantified in the detailed design stage when most of the design decisions have been made. In the conceptual and preliminary design stage, traditional techniques rely on heuristics, experience, and historical data to assess system safety and reliability requirements. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new concepts. Additionally, a dearth of available reliability data results in poor treatment of epistemic and aleatory uncertainty for such novel concepts. This motivates the overall objective of the current work.

The overarching objective of this dissertation is to develop a framework that will enhance the safety assessments of novel aircraft physical architectures and technologies in early design by identifying, characterizing, and allocating off-nominal requirements, enabling compliance decision making under uncertainty, all while informing design trade studies with the information generated.

For the first research area in this dissertation, the developed framework utilizes

system performance models to evaluate system response to off-nominal operating states. Towards that end, Continuous-FHA (that considers the magnitude of functional degradation) is extended to consider the number of terminal, function-satisfying components lost in a failure mode. This extended C-FHA is developed for conceptual level analysis and demonstrated on a test distributed electric propulsion (T-DEP) aircraft inspired by the X-57. When additional design information is available, a preliminary 6 degrees of freedom (6-DoF) model is utilized in a performance-based multi-state analysis framework to evaluate the aircraft's response in different failure states. Combining the results of these conceptual and 6-DoF analyses with certification requirements or engineering judgement allows the characterization of hazard severity at the aircraft system level. Additionally, a network-based bottom-up algorithm is demonstrated along with the Critical Flow Method to allocate reliability requirements at the component level.

To deal with epistemic and aleatory uncertainty while assessing unit level failure rates, a Bayesian probability approach is utilized. The Bayesian framework allows subject matter expert opinion to be encoded in the failure rate models through prior distributions that capture epistemic uncertainty. This framework also enables the evaluation and propagation of alternative models generated by different subject matter experts to decision makers, leading to a more comprehensive treatment of uncertainty as compared to utilizing traditional measures of central tendency (point estimates). A Bayesian decision theoretic approach provides a mathematically backed framework for compliance finding. It utilizes the expected loss principle to minimize the posterior expected loss for any component while making a compliance decision. Such a method makes full use of the uncertainty encoded in Bayesian failure rate posteriors to provide a loss value for different compliance actions to decision makers, who can then make an informed choice. This thesis contributes a modified Monte-Carlo algorithm to estimate multi-state reliability of complex systems while utilizing

the Bayesian failure rate posteriors previously generated.

Finally, the developed tools, techniques, and methods are combined into an integrated framework with the capability to perform trade studies informed by safety and reliability considerations for novel aircraft architectures. A system reliability sensitivity study of the T-DEP aircraft architecture to components' reliability is evaluated using specially modified multi-state component importance measures. These measures help identify which components have the highest impact on improving or decreasing the aircraft system reliability, as well as the general sensitivity of the system reliability to the component reliability. To demonstrate how the developed integrated framework might be used to perform design trade studies, two trade-studies are conducted based on observations made from results of the first two research areas of this dissertation. These include resizing the vertical tail and over-sizing the cruise motor-inverters of the T-DEP aircraft to improve its performance in asymmetric loss of thrust scenarios. It is found that while over-sizing the vertical tail helps improve the aircraft's performance in asymmetric loss of thrust scenarios slightly, over-sizing the cruise motor inverter results in a much bigger benefit.

Providing a systematic, performance-based framework that enhances the safety assessment of novel aircraft architectures, and informs the conceptual and preliminary stage design trade-studies with safety-related off-nominal requirements is the defining contribution of this dissertation. It supports the main research objective of the present work with an example demonstration on a test distributed electric propulsion (T-DEP) aircraft inspired by NASA's X-57. The developed framework is expected to support the ability to more quickly explore the architectural and design space for novel aircraft architectures and technologies while bringing safety-related off-nominal considerations into early design.

CHAPTER I

MOTIVATION

1.1 *Introduction*

The last decade has witnessed a demand for air passenger services grow with a long-term average of over 5% in terms of revenue passenger miles (RPK) [97]. To mitigate the impact of this growth in aviation on the environment, as well as to maximize the economic benefit that can be achieved from added efficiency and performance, NASA Environmentally Responsible Aviation (ERA) project has suggested aggressive goals through the $N+$ program as shown in Table 1 [164]. The target for $N + 1$ generation was a reduction in the fuel burn by over 30% relative to a B737 with a CFM56 engine. Additionally, the aviation industry is committed to achieve a 50% reduction in its CO_2 emissions by 2050 over a 2005 baseline [88] (See Fig. 1). A push towards *cleaner* aircraft concepts is also visible in General Aviation (GA). As the current aircraft concepts and architectures mature and reach technology saturation, new technologies and revolutionary (as against evolutionary) aircraft architectures will have to be developed to achieve these targets in a time-bound manner as seen in figure 1.

Table 1: NASA ERA targets [164]

Technology Benefits	Technology Generations (TRL 4-6)		
	N+1 (2015)	N+2 (2020)	N+3 (2025)
Noise	- 32 dB	- 42 dB	- 71 dB
LTO NOx Emissions (below CAEP 6)	-60%	-75%	-80%
Aircraft Fuel/Energy Consumption (rel. to 2005 best in class)	-33%	-50%	-60%

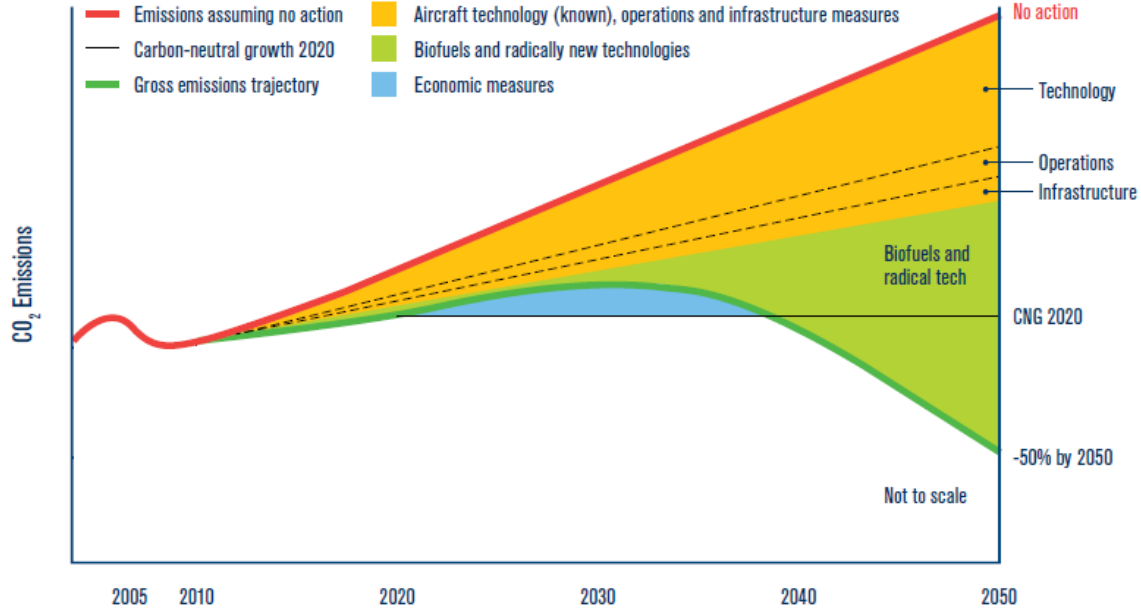


Figure 1: Schematic CO_2 emissions reduction roadmap [88] (Source: IATA)

1.2 A Paradigm Shift to Novel Aircraft Architectures and Technologies

Aircraft are typically designed to comply with different type certification requirements put forth by the Federal Aviation Administration (FAA) in the US. Aircraft type certifications occur under 14 CFR Part 23 (Normal Category Airplanes), Part 25 (Transport Category Airplanes), Part 27 (Normal Category Rotorcraft), and Part 29 (Transport Category Rotorcraft). Aircraft operations are certified under another set of rules which typically include 14 CFR Part 91 (General), Part 135 (Commuter and On-Demand), and Part 121 (Domestic, Flag, and Supplemental). General Aviation (GA) is an unofficial blanket term applied to certain types of Part 91 and 135 operations. It accounts for more than 90% of the registered civil aircraft fleet in the US [24]. An estimated 65% of GA flights annually are for business or other purposes that cannot be served by commercial flights [24], with a large proportion of these aircraft being design certified as normal category airplanes or rotorcraft.

Normal category airplanes (14 CFR Part 23) comprise the vast majority of GA

operations. Most of these utilize a piston engine as the primary power source with mechanically linked control surfaces, and very little secondary power drawn for instrumentation. The certification rules for this part were overhauled recently by the FAA in Amendment 64 [72], where earlier prescriptive requirements were replaced with performance-based requirements. These changes are intended to maintain the same level of safety associated with 14 CFR Part 23 Amendment 63 while establishing a higher level of safety for loss of control and icing [72]. The prescriptive means of compliance that used to be contained within the rules and associated advisory circulars (ACs) are now being ported over to a number of different consensus standards from the aviation community [73]. This new approach leverages the idea that the means of compliance (MoCs) developed from consensus standards organizations can be more agile than federal rule-making, thus enabling faster adoption of new technologies for these aircraft [35, 38]. Due to their size and scale, along with the enabling changes to their regulatory framework, this segment is slated to receive a big boost with the advent of novel architectures, technologies, and concepts of operations.

However, Part 23 is not unique in its push towards adoption of novel aircraft architectures and technologies. For transport category airplanes (14 CFR Part 25), traditional aircraft architectures largely feature mechanical, hydraulic, and pneumatic secondary power drawn from a power source like an internal combustion engine or a turbine engine whose primary function is to generate thrust. These conventional subsystem architectures are inherently inefficient due to a significant energy wastage associated with extracting bleed-air from the engines, and due to the bulkiness of the hydraulic systems [50]. To improve fuel efficiency over technologically saturated conventional concepts, a lot of research has been carried out to electrify aircraft architectures [36, 50, 75, 91, 103, 109, 115, 148, 175]. There are two general directions for aircraft electrification – electrification of the primary propulsive power, or of the secondary power extraction.

An *All-Electric Aircraft* (AEA) is one where the secondary power extractions (that drive conventionally pneumatic or hydraulic subsystems) are fully electrified. When partial electrification of these subsystems is achieved, the aircraft is termed *More-Electric*. These can be considered evolutionary concepts where new technologies are incorporated into a traditional system architecture. The More-Electric Aircraft (MEA) concept is one where the subsystems, including the Environmental Control System (ECS), flight controls, landing gear actuation and braking among others, consume secondary power that is solely electric in nature and represents an evolutionary leap towards novel technologies. Studies on quantification of subsystem electrification on fuel burn in MEA architectures suggest initial benefits of around 3-5% [32,88,151]. Subsystem electrification has already started in commercial aviation, with Airbus A380 introducing electric actuators for several flight controls in parallel to hydraulic actuators resulting in a weight savings of about 450 kg [51,169]. The Boeing 787 has already achieved a *bleedless* architecture, by using electric power for the cabin environmental control system (ECS) and the wing ice protection system (IPS). As subsystem electrification technologies mature, these benefits are expected to keep growing.

While these technology improvements continue, they will not be enough. The big improvements needed to meet aggressive future goals from Fig. 1 are expected to come from revolutionary architectures. The term *hybrid-electric* is usually applied to aircraft with partial electrification of primary propulsive power, while complete electrification of the same is called an *electric* aircraft. These can further be integrated with novel architectures like distributed propulsion to generate truly revolutionary architectures that are needed to meet the NASA ERA targets given in table 1.

The maturation of electrical power systems technologies, are at the heart of this push towards the development of various revolutionary concepts. These are not restricted to a particular design or operational certification category. They can be

found spread among 14 CFR parts 23, 25, 27, 29 for their design certification or parts 91, 121, and 135 for their operations. Novel concepts involving Urban/Advanced Air Mobility (UAM/AAM) use architectures such as electric vertical take-off and landing (e-VTOLs), and technologies such as distributed electric propulsion (DEP) which are being developed in every design and operational certification categories. Thus, novel concepts are diverse not only in terms of their certification requirements, but also in terms of their aircraft architectures, with some examples shown in Figure 2.



(a) Volocopter (Credit [14])



(b) Joby Aviation (Credit [13])



(c) Jaunt Air Mobility (Credit [12])



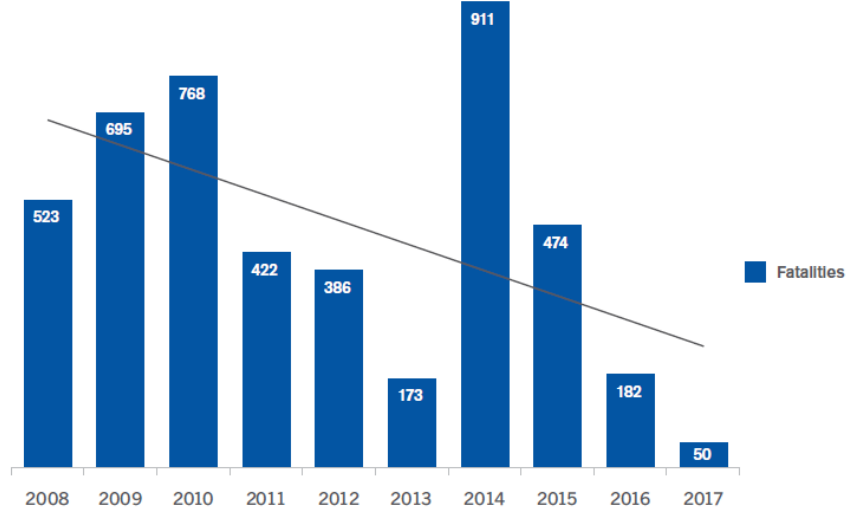
(d) NASA X-57 (Credit NASA)

Figure 2: Example Novel Aircraft Concepts

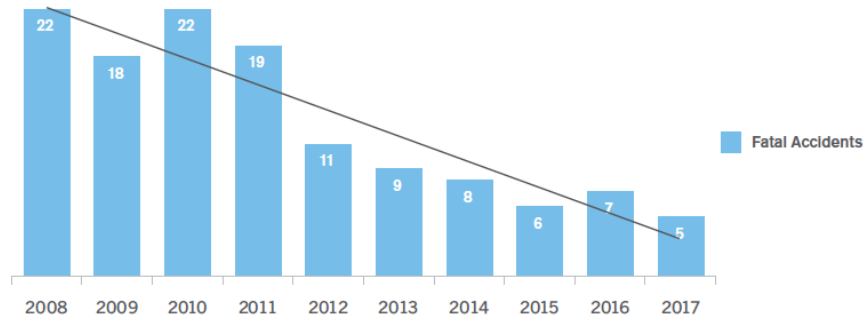
1.3 Trends in Aviation Safety

Aviation remains one of the safest modes of transportation accounting for $< 1\%$ of the annual transportation fatalities in 2017 [135]. For scheduled commercial flights, there has been a general trend of a lower number of fatalities and fatal accidents over

the past decade as seen in Figure 3. Runway safety events are the overall leading cause of all types of accidents, while loss of control in flight and operational damage are both significant contributors [90].



(a) Fatalities in scheduled commercial flight



(b) Fatal accidents in scheduled commercial flight

Figure 3: Commercial flight accident statistics [90]

However, within civil aviation, GA accounted for over 93% of accidents, 96% of fatal accidents, and 95% of fatalities in 2017 [136]. Figure 4 shows the number of fatal and overall accidents in GA between 2008 - 2017. While accident rates and fatalities for GA have marginally gone down over the years, they are still an order of magnitude higher than commercial flights.

While accident rates are slowly going down, global commercial operations are expected to grow by 2.5% per year in terms of revenue passenger miles flown [74].

The GA fleet is expected to remain stable year over year, with GA hours flown expected to grow by 0.7% annually. This is because the growth in turbine, rotorcraft, and experimental hours is expected to more than offset a decline in fixed wing piston hours in GA [74]. The potential revitalization of GA due to the advent of novel architectures and Con Ops means that the demand for improving the safety of aircraft is ever increasing.

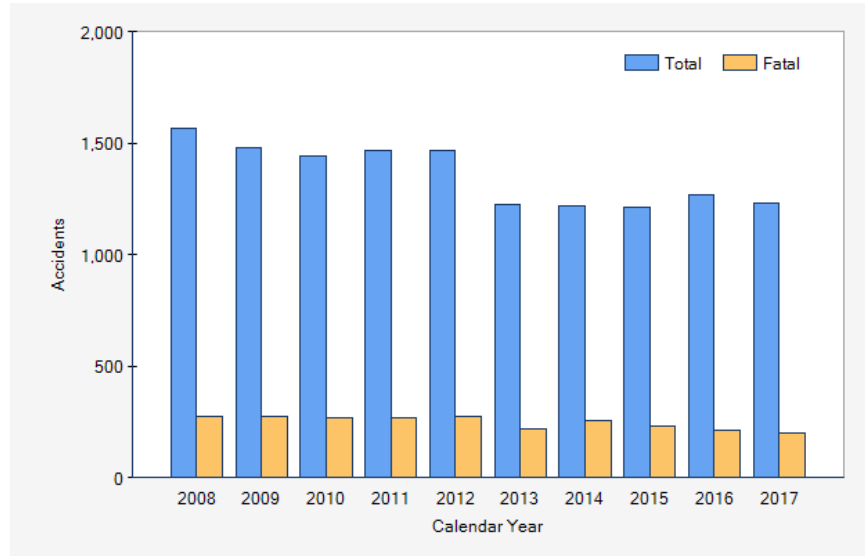


Figure 4: GA Accidents between 2008 - 2017 (Source: NTSB [136])

1.4 A System Safety Perspective

On January 7, 2013, a Japan Airlines Boeing 787-8 auxiliary power unit battery caught fire while it was parked at a gate. A similar incident involved the main battery of a B787 operated by Nippon Airways on January 16, 2013. While the rate of occurrence of such an event was estimated at 1 in 10 million flight hours, two had occurred in less than 52000 flight hours at the time of these incidents. An investigation by the National Transportation Safety Board (NTSB) listed “incorrect assumptions in safety assessments” as one of the reasons for these incidents [134].

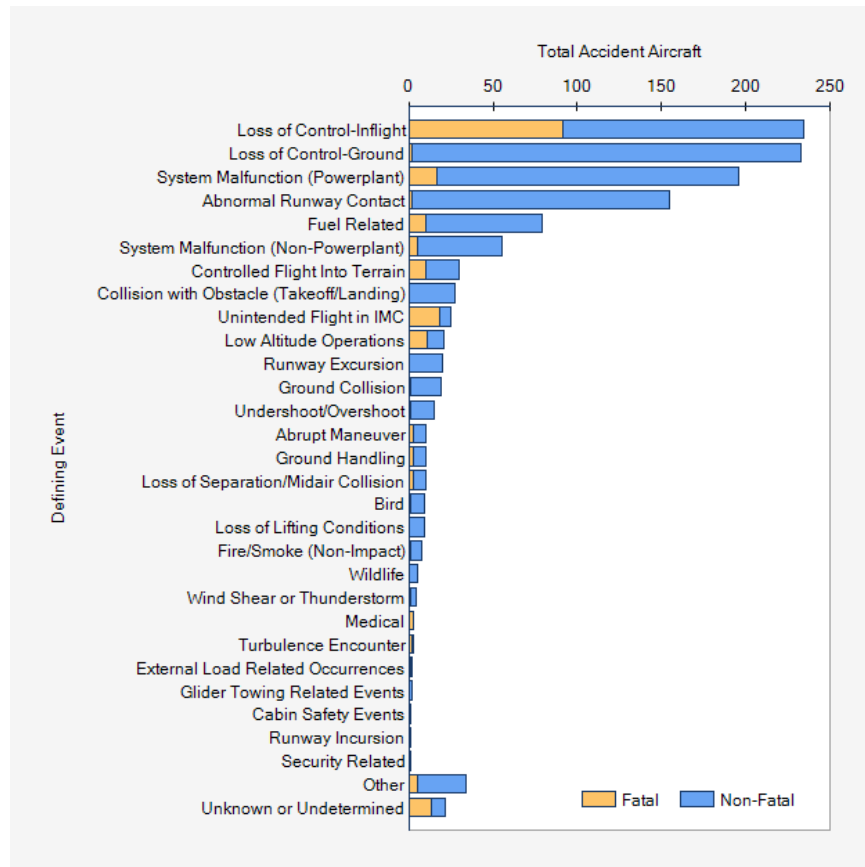
In March 2019, B737 MAX aircraft were grounded worldwide following two fatal crashes less than five months apart. The cause is suspected to be an automatic flight

control feature - the Maneuvering Characteristics Augmentation System (MCAS) forcing both the aircraft into a dive following erroneous data from a single Angle of Attack (AoA) sensor [40]. The introduction of the larger CFM LEAP-1B engines, with bigger nacelles required them to be positioned further ahead on the wing of the B737 MAX. The MCAS was originally introduced to mitigate the aerodynamic effect of this change [39].

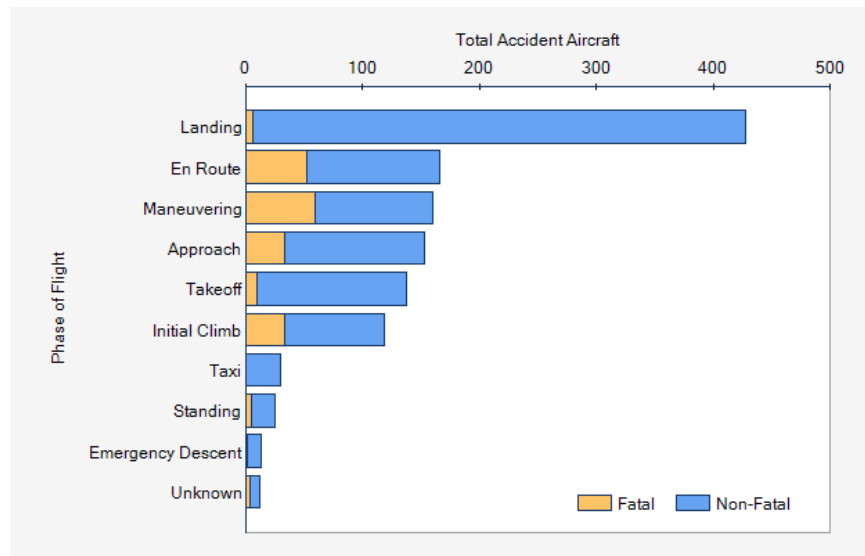
Safety on GA side continues to lag behind that of commercial aviation as previously discussed. Figure 5 provides a breakdown of GA accident statistics by flight phase and major causes. As can be seen, powerplant and non-powerplant system malfunctions are some of the biggest contributing events to GA accidents, both fatal and non-fatal. While the landing phase is the most critical in terms of the number of accidents, the initial climb, en-route, and maneuvering phases of flight are when the maximum number of fatal accidents occur. Novel aircraft architectures and concepts of operation carry with them an uncertainty related to the off-nominal operational risk they pose. It can be argued that aircraft designers would do well to include requirements related to such risks early in the design phases.

The above-mentioned accident cases and statistics highlight the importance of safety assessments in aircraft design. However, it is difficult to perform accurate safety assessments of novel aircraft architectures and technologies because of the inherent uncertainties associated with them. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new concepts. Thus to enable a rapid transition towards novel architectures and technologies, it is paramount for aircraft designers to have the capability to quantify system safety risk earlier in the design phases to help mitigate avoidable surprises once the aircraft is already built.

Historically, analyses to determine system safety and reliability are performed during the detailed design phase of aircraft design. By this time, numerous design



(a) Causes of GA accidents



(b) GA accidents by phase of flight

Figure 5: GA accident statistics (Source: NTSB [136])

decisions have been made and degrees of freedom locked down. As will be established in later chapters, the current methods to estimate safety and reliability at the conceptual and preliminary design stages are limited when it comes to application to revolutionary architectures, and hence cannot be applied effectively while exploring the design and architectural space. The goal of this thesis is to incorporate off-nominal requirements pertaining to system safety and reliability in conceptual and early preliminary design while allowing a more comprehensive treatment of uncertainty and informing design trade studies.

1.5 Summary

The world of aviation is moving towards novel aircraft architectures and technologies as a result of a push towards higher efficiencies, lower operating costs, and lower emissions. This can be seen in the development of novel aircraft concepts, operations, and technologies like UAM, e-VTOL, and a general push to implement electrified architectures. While these novel concepts and architectures are required to achieve aggressive targets in fuel efficiency and emissions, their development and implementation faces obstacles in terms of uncertainty regarding the reliability and safety risk they pose. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new concepts. Even when Original Equipment Manufacturers (OEMs) have preferred to take a cautious approach by introducing new technologies in a step-wise manner in commercial aircraft, recent incidents have reiterated the need to do so in a safe manner. This need is therefore felt even more strongly in the case of revolutionary designs that are likely to be introduced. In order to speed up the process of introduction of novel aircraft architectures and technologies, it is paramount for aircraft designers to have the capability to quantify off-nominal requirements earlier in the design phases

in a manner that provides a better treatment of uncertainty in light of limited knowledge and experience with these concepts, and informs trade studies before degrees of freedom are locked down by design decisions. These observations provide a high-level rationale to motivate the overall research objective of this thesis:

Research Objective:

Develop a framework that will enhance safety assessments of novel aircraft physical architectures and technologies in early design by

1. identifying off-nominal requirements,
2. allocating them to the system and component level,
3. enabling compliance decision-making while addressing both epistemic and aleatory uncertainties, and
4. informing design trade-studies.

A detailed background and literature survey to inform the gaps leading to the stated research objective is given in the following chapter. The rest of this thesis is organized as follows:

- Chapter 2 presents the background and literature review of the existing methods for safety and reliability assessment from various domains along with some observations and gaps found
- Chapter 3 presents the research questions and states the hypotheses while also providing an overview of the developed framework and the test problem utilized throughout this thesis

- Chapters 4, 5, and 6 provides details of the developed framework, along with results of experiments conducted to validate the hypotheses
- Chapter 7 contains the conclusions, contributions of this thesis with avenues for future research

CHAPTER II

BACKGROUND AND LITERATURE REVIEW

As discussed earlier, off-nominal requirements generally postulated during the conceptual design stage may not be complete or correct for novel or revolutionary architectures. These can act as potential show-stoppers if not considered earlier in the design phase. This chapter provides some background into the ideas and concepts to help focus the discussion from the motivations seen previously towards observations that will inform the research direction that follows in this thesis. This chapter begins by providing an overview of the aircraft design process, focusing on the tasks of requirements identification and aircraft architecting. The traditional means of incorporating off-nominal requirements into design are discussed, while bringing the focus on safety and reliability related off-nominal requirements. Next, some basic concepts of aircraft safety and risk analysis are explained for readers unfamiliar with this field. This is followed by a discussion on the current paradigm of safety assessments, and how its processes and methods are used during the aircraft design phases to inform and verify off-nominal requirements that result from architecting. Finally, the state of the art in safety and risk analysis is explored. All throughout this chapter, observations are made regarding the limitations posed by the current paradigm with regards to novel aircraft concepts, as well as any potential enablers that may hint at the appropriate direction to be taken to achieve the research objective of the present work.

2.1 The Aircraft Conceptual Design Process

Aircraft are complex systems characterized by large, multidisciplinary architectures, the design process of which is traditionally broken down into three phases - conceptual, preliminary, and detailed design. The conceptual design phase is generally considered

the most critical of the three due to the high levels of cost committed and design freedom locked in early on under limited knowledge. This is visible in Figure 6 shown by solid lines for the cost committed, knowledge available, and design freedom available. This is because early decisions impact future considerations of materials, labor, manufacturing, as well as the complete life cycle of the aircraft. Most recent research efforts therefore have been to buckle these trends by incorporating design for affordability and probabilistic techniques to increase the knowledge available earlier in the design phases, while maintaining design freedom and reducing cost committed. This is generally achieved by resorting to inexpensive first principles analyses or techniques like surrogate modeling to conduct design trade-offs [122].

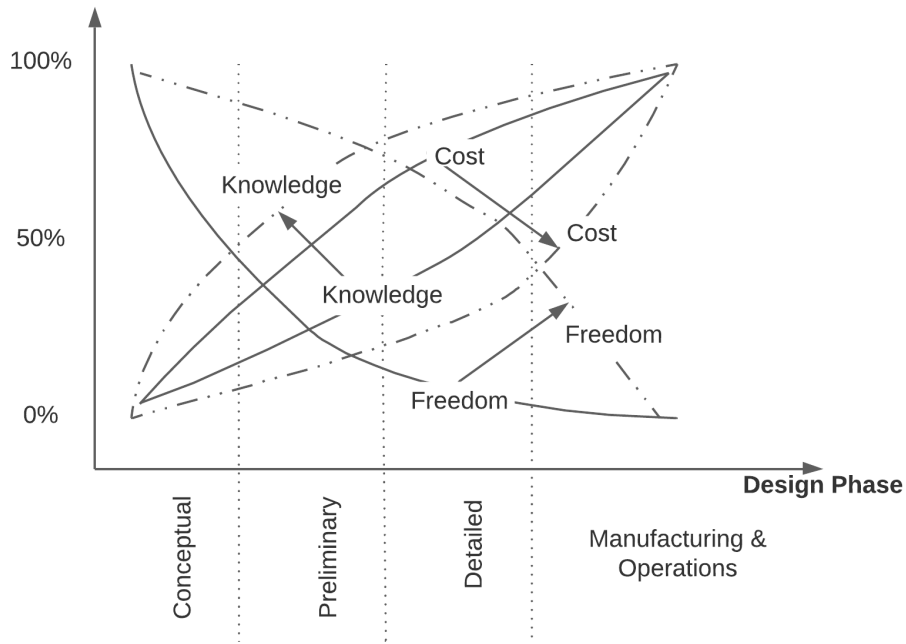


Figure 6: Cost, knowledge, and freedom with design stages [122]

The conceptual design stage generally includes three major steps of (i) defining the problem, (ii) generating alternatives, and (iii) down-selecting alternatives [158, 168]. The problem definition phase is when most of the customer requirements are generated. Conceptual design then investigates whether these requirements can be viably met by one or more high-level solutions that consider an overall understanding

of the basic functions the systems need to fulfil. This typically involves performing numerous concept studies drawing on the knowledge and experience of the design team to generate multiple alternatives. Filters or metrics are then used to down-select alternatives that are then considered for further development. Due to the limited knowledge available at this stage, it is difficult to identify all the detail necessary to architect a system. Therefore, aircraft conceptual design has traditionally primarily focused on geometry, weights, aerodynamics, propulsion, and structures [42]. While the emphasis on subsystems, architecture, and controls might be low, these disciplines can be included at this stage.

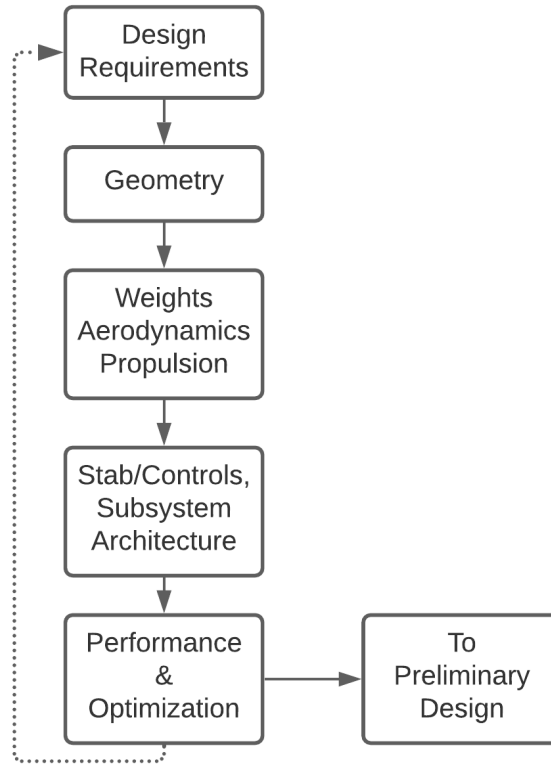


Figure 7: Aircraft conceptual design process [154]

Figure 7 shows a typical aircraft conceptual design process adapted from Raymer [154]. It begins with a set of design requirements that must be met. These can include parameters like payload, range, takeoff and landing performance, speed, and also any potential standard specifications. An initial geometry is then defined, followed by

sizing the aircraft to meet the mission requirements by estimating its weight and aerodynamic or propulsive performance. This process can be iterated until desired convergence, following which considerations of subsystems, stability, and controls can be brought in. Finally, performance is evaluated and optimized depending on the design objectives. It is at this stage that multiple possible alternatives are considered and evaluated. These are then down-selected using metrics of interest to proceed with preliminary design, where configuration and some of the additional details like lofting, structural design are fixed, and higher fidelity analyses are conducted. Modifications to this process for evolutionary designs involve incorporating technologies that affect aerodynamic, propulsive, or structural assumptions, and utilizing physics-based analyses to inform the sizing and performance instead of historical data. When it comes to design of revolutionary or novel concepts, defining design requirements, and conceptual architecting are two of the most important areas.

2.1.1 Aircraft Architecting

Architecting is the process by which solutions are defined to satisfy system requirements. The International Organization for Standards defines architecture design as a process to synthesize solutions that satisfy system requirements and explore multiple implementation strategies at an appropriate level of detail [92].

An architecture, on the other hand, can be considered as a fundamental defining characteristic of any complex system and can have an immense impact on its performance. There is no common definition for a system architecture, with each discipline providing its own depending on the perspective in which it is used. Jakkola and Thalheim state that a system architecture represents the conceptual model that defines the structure, behavior, and more views of a system [93]. IEEE 1471 defines architecture as a fundamental organization of a system embodied in its components, their relationships, and to the environment [11]. The International Council of Systems

Engineering (INCOSE) prefers this definition for its own work. System architecture is also defined by Whitney et al. as an abstract description of the entities of a system and the relationships between them [173]. Maier uses the term “architecture” in the sense of a fundamental or unifying system structure defined in any system dimension or view [118]. While talking about systems integration, Sage and Lynch define architecture in relation to the structure properties of the system, which may include components, interrelationships, and principles and guidelines under which the system is used [158]. They also distinguish between the systems’ functional architecture, physical architecture, and implementation architecture. ‘Architecture’ in the present work refers mainly to physical architectures and not functional or logical ones.

During conceptual design, aircraft architectures are often predefined or certainly assumed. This makes it easier for the designer to select a physical implementation to satisfy the desired functions. Conceptual designers must decide on the choice of lifting surfaces, control surface locations, propulsion systems, subsystems, payload storage geometry, etc. [157]. In the traditional paradigm, several of these choices end up being static, for e.g. a cantilever monoplane wing, separate horizontal and vertical empennage surfaces, single cylindrical fuselage, and a tricycle landing gear arrangement. Therefore, the majority of architecting decisions in the conceptual design phase of traditional architectures are about the number and location of the engines, the position of the wing, and empennage configuration [86]. When coming up with a derivative (e.g. extended range versions) or evolutionary (e.g. MEA) design, a fixed architectural scheme is assumed with modified energy storage or subsystems. In a review of architectural decisions of 157 aircraft from the DC-3 to the 787, Kellari et al. [101] state,

Aircraft designers have increasingly made the same architectural decisions, while realizing performance gains in component technologies rather than from major architectural innovations... Current improvements in

performance with this dominant architecture may be reaching the stage of diminishing returns.

Coming up with derivative or evolutionary designs, therefore, may restrict the performance improvement possible from an aircraft.

2.1.1.1 Novel Aircraft Architectures

In the light of the above, the definition of a ‘novel architecture’ is of particular interest in this thesis. Unfortunately, very little literature was found on this definition.

Definition 2.1.1 (Novel Aircraft Architecture). *A novel aircraft architecture is loosely defined here as one which differs significantly from the traditional paradigm mentioned above in its physical implementation to fulfil at least one aircraft level function.*

For instance, a novel architecture may differ in its choice of physical implementation to satisfy any aircraft function ‘*Generate Thrust*’ (distributed electric propulsion), or ‘*Generate Lift*’ (lift augmented compound helicopters/ hybrid wing body) among others. The possibilities for these concepts is as large as the combinatorial space of alternatives for implementing the aircraft functions itself. Appendix A provides the matrix of alternatives for traditional architecting solutions. The space for novel architectures is likely to be even larger.

On the technology front, revolutionary technologies (e.g. turbo-electric, propulsion airframe integration, active flow control) are expected to be implemented in novel architectural concepts. They promise a significant improvement, but also require creative and innovative architecture definition. These novel architectures can introduce complex interactions between the components which in turn result in previously unknown additional requirements at the system and component level.

2.1.2 Requirements Definition

The first step in the design process in Figure 7 is generating design requirements. This is conducted through requirements analysis, which is a means of generating desired attributes that a system must meet, and is carried out prior to any definition of the system functions, functional architecture, or physical architecture. At this stage, emphasis is placed on the end goals of a system, and not on how those are achieved. David Hay cautions against confusing requirements analysis with system design, stating that the prior concerns only with the problem space (what), and not the solution space (how) [84].

The requirements analysis preceding aircraft design considers primarily safety, cost, performance, regulations and standards, and environmental conditions among others. These are then grouped into mission, project, environmental, customer, interface, and non-functional requirements [114]. Also called the concept of operations (ConOps), this provides a description of aircraft level functions and sizing scenarios in terms of the mission and constraints. The Department of Defense distinguishes between three different views of requirements: operational, functional, and physical [114]. Operations determine the magnitude, duration, and environment of the platform level requirements, which must then be fulfilled by the aircraft in the functional view. The physical view focuses on the physical solutions (physical architecture) to meet the functions. Therefore, the platform-level requirements are analyzed and generated independently of the aircraft architecture. This means these requirements can be allocated differently to the aircraft systems and components depending on which functional and physical architectural solutions are considered [26].

One class of requirements not considered so far are “Emergent” requirements. In his Ph.D. thesis, Armstrong states [26],

Some requirements do not exist and cannot be predicted until product definition takes place

Emergent requirements are not defined through a decomposition of requirements obtained during the analysis phase. In fact, emergent requirements cannot be identified during traditional requirements analysis, since they result from the systems' 'emergent' behavior - a result of complex interactions between the elements of its architecture. While some aircraft function level safety requirements may be defined prior to the definition of a physical architecture, most system safety and reliability requirements fall into the category of 'emergent'. All such safety and reliability requirements are of particular interest in this thesis.

The traditional source of generating aircraft level requirements is the aircraft mission. Each phase presents constraints that must be satisfied by the aircraft which in turn drive the conceptual sizing loop given in Figure 7. However, off-nominal operations often drive system sizing critical requirements. These are architecture specific and inherently emergent as discussed earlier. The traditional approach to generate aircraft requirements is explored next, followed by literature on identifying safety-related requirements.

2.1.2.1 Traditional Aircraft Design Requirements Identification

Requirements identification in typical aircraft conceptual design process begins with a design mission. Each mission phase presents unique requirements on the primary flight functions (thrust, lift) that can drive aircraft attributes. Considering all the different phases together poses requirements on the energy storage which drives sizing. In addition to mission phases, information regarding means of takeoff or landing may be necessary. Traditional sizing determines the aircraft's gross weight by using aircraft scaling parameters. An energy-based constraint analysis by Mattingly is typically used which relates the thrust-to-weight ($\frac{T_{SL}}{W_{TO}}$) and wing loading ($\frac{W_{TO}}{S}$) at sea-level takeoff using Eq. 1 [121].

$$\frac{\alpha}{\beta} \frac{T_{SL}}{W_{TO}} = \frac{1}{\beta} \frac{qS}{W_{TO}} \left\{ K_1 \left(\frac{n\beta}{q} \frac{W_{TO}}{S} \right)^2 + K_2 \left(\frac{n\beta}{q} \frac{W_{TO}}{S} \right) + C_{D0} + C_{DR} \right\} + \frac{P_s}{V} \quad (1)$$

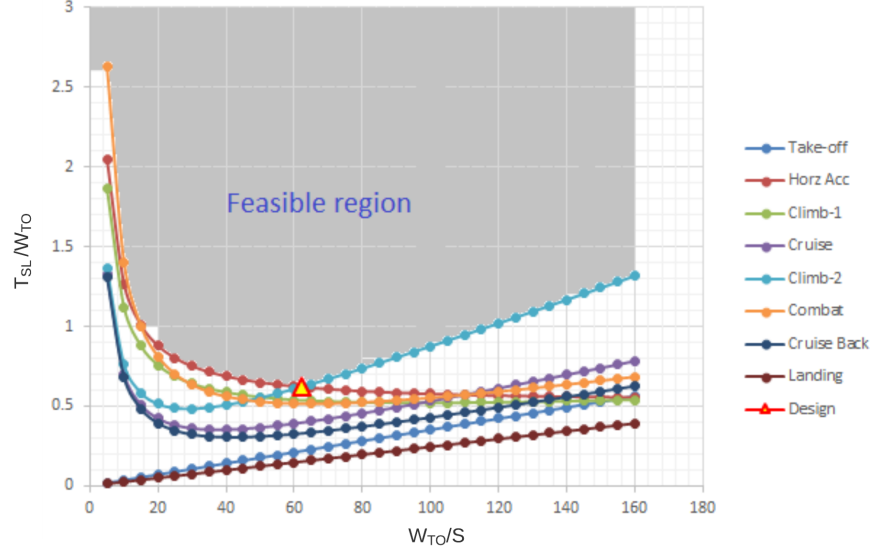


Figure 8: A notional constraint analysis plot for the F-86

Solving for Eq. 1 for different mission phases generates constraints on the thrust-to-weight ratio and wing loading. A notional plot showing these constraints for an example mission for the F-86 aircraft is shown in Fig. 8. The more critical of these constraints restrict the design solutions and drive aircraft level requirements for thrust and lift. Next, gross weight is iterated upon by determining the aircraft level energy storage requirements using historical information, as well as appropriate range and endurance equations for appropriate phases of flight.

Limited consideration is given to off-nominal scenarios in the traditional conceptual design process. Often, critical off-nominal scenarios are postulated based on historical experience designing similar aircraft concepts. For instance, a reserve mission is included in design missions to account for off-nominal conditions. Conditions like one-engine-out or ETOPS¹ (Extended Range Twin-Engine Operations) postulated by regulatory requirements often end up becoming the driving cases for propulsion requirements [68, 69]. These scenarios, in particular, can be easily included in the previously mentioned constraint analysis by modifying Eq. 1 appropriately.

The second kind of off-nominal scenarios are presented from identifying critical

¹informally called Engines Turn Or Passengers Swim

failure cases. This lies under the domain of safety analysis, which is typically carried out in the detailed design stage after the physical architecture has been defined and frozen. Such scenarios often impact the requirements imposed on the aircraft architecture and its components. The goal of such analysis is to verify that the architecture can meet reliability requirements and is safe. In the early stages, this effort focuses on identifying critical failure modes and incorporating redundancy to meet fail-safe design requirements [66]. These are typically determined based on previous experience with similar architectures. However, with novel aircraft concepts, where architectures may be unknown, flexible, or simply revolutionary, such processes of identifying safety requirements may not succeed. The off-nominal scenarios postulated may be wrong or incomplete. Thus, more exploratory approaches are necessary that do not assume failure modes or their criticality. We can draw the following observations from the discussions so far:

Observation: *Most aircraft safety and reliability requirements are emergent and depend on the physical architecture definition*

Observation: *Off-nominal scenarios have the potential to pose significant sizing and architecture specific requirements at the system level*

2.2 Basic Concepts

2.2.1 Definitions

The definitions of a few recurrent terms used commonly in literature in the context of reliability and safety assessment are provided here [4, 6, 130].

External Event – *“An occurrence which has its origin distinct from the aircraft or the system being examined, such as atmospheric conditions (e.g., wind gusts/shear, temperature variations, icing, lightning strikes), operating environment (e.g. runway conditions, conditions of communication, navigation, and surveillance services), cabin*

and baggage fires, and bird-strike. The term is not intended to cover sabotage.”

Failure – *“A loss of function or a malfunction of a system or a part thereof.”*

Hazard – *“A condition resulting from failures, external events, errors, or combinations thereof where safety is affected..”*

Redundancy – *“Multiple independent means incorporated to accomplish a given function..”*

Reliability – *“The probability that a system or item will perform a required function under specified conditions, without failure, for a specified period of time..”*

Risk – *“The combination of the frequency (probability) of an occurrence and its associated level of severity.”*

Safety – *“The state in which risk is acceptable.”*

2.2.2 Safety Requirements

As discussed earlier, novel aircraft concepts and architectures are expected to be developed across the spectrum of different airworthiness categories. Regardless, each of these parts have a requirement to ensure the safety risk of equipment and systems remains acceptable.

For normal category aircraft, the Federal Aviation Administration (FAA) implemented a new set of performance-based rules in Title 14 of the Code of Federal Regulations (CFR) Part 23 amendment 64 in 2017 [72] to ensure safety in an evolving paradigm. Compliance with these rules can now be shown using means of compliance information provided by approved consensus standards such as those developed by ASTM Committee F44 on GA aircraft [27,73]. In contrast, the 14 CFR Part 25 regulations remain prescriptive in nature. In the normal category (Part 23), of particular interest in this thesis is 14 CFR 23.2510 that is the prime drivers for the assignment of reliability requirements to aircraft equipment, systems, and installations by requiring them to have [72]

Table 2: Quantitative Part 23 Allowable Failure Rate for Different Failure Conditions [8]

Assessment Level	Failure Condition Classification				
	Negligible	Minor	Major	Hazardous	Catastrophic
I	No Probability Requirement	$<10^{-3}$	$<10^{-4}$	$<10^{-5}$	$<10^{-6}$
II		$<10^{-3}$	$<10^{-5}$	$<10^{-6}$	$<10^{-7}$
III		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-8}$
IV		$<10^{-3}$	$<10^{-5}$	$<10^{-7}$	$<10^{-9}$

“a logical and acceptable inverse relationship between the average probability and severity of failure conditions.”

The safety risk is generally quantified as a combination of two entities - the probability of a failure, and the severity associated with it [4]. The probability of a failure is the frequency with which it can be expected to occur, and is generally quantified using historical data [130]. The severity denotes the impact of a failure and is generally classified into multiple categories depending on whether said failure puts life or property in harm’s way. Generally speaking, severity is defined as [128]:

1. **Catastrophic** when there is a chance of multiple fatalities and/or a total loss of the aircraft,
2. **Hazardous** when a failure may result in serious injuries or some loss of life,
3. **Major** when there is a significant reduction in safety or functional capability of the aircraft, with expected continuation of safe flight, and
4. **Minor** when there may be little loss of safety margins but no expected injuries or damage.

Table 2 shows the relationship between failure probability and severity of failure conditions for normal category aircraft [8]. These pose reliability requirements at the aircraft level in terms of allowable probabilities of transitioning from a nominal flight

to the failed, off-nominal conditions. These are what can be called, safety requirements at the most basic level. These requirements, in turn, can pose requirements on the architecture in terms of system capacity and redundancy needed from the different elements.

The basic safety requirements mentioned above change slightly for transport category aircraft. Advisory Circular (AC) 25.1309-1A requires that major failure conditions be improbable ($< 10^{-5}$), while catastrophic failures are extremely improbable ($< 10^{-9}$). Additionally, unlike 14 CFR 23.2510, AC 25.1309-1A requires a fail-safe design concept, where the following basic objectives apply [66]:

1. “In any system or subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.
2. Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.”

The intent of safety assessments in the concept design stage then can be summarized as ensuring that any system under consideration poses no worse than an acceptable level of risk by allocating reliability requirements at the system and component level. These requirements are often inversely proportional to the consequences of failures.

2.2.3 Reliability

Reliability has many definitions with most of them converging on a similar intent. SAE ARP 4761 defines reliability as [4]

“The probability that a system or item will perform a required function under specified conditions, without failure, for a specified period of time..”

It can be considered an attribute of the system that depends on the functional and physical architecture including the components and their interactions. Mathematically, it can be defined as a function $R(t)$ which represents the probability of success for an item in a given time interval $(0, t)$. By definition, the failure probability is the complement of the reliability, and is also termed the cumulative distribution function [130]:

$$F(t) = 1 - R(t) \quad (2)$$

The probability density function (pdf), also called failure density $f(t)$, is the first derivative of $F(t)$.

$$f(t) = \frac{dF(t)}{dt} \quad (3)$$

$f(t)$ shows the frequency of failures at any specified time (t) in number per unit time [130]. A conditional failure rate $\lambda(t)$ denotes the probability of an item failing between $(t, t+\Delta t)$ given that it has survived until time t . The failure rate is considered as the most basic measure of reliability, and describes the distribution of failure time just as well as $f(t)$ or $F(t)$ [130].

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \quad (4)$$

Over the lifetime of a large population of items, a reliability bathtub curve characterizes the failure rate as shown in Fig. 9. The three phases shown include [130]

1. **A Decreasing Failure Rate Phase** also called as the burn in phase, when weak components fail early and design and processes are refined

2. **A Constant Failure Rate Phase** also called the useful life phase, when components fail randomly but at an approximately constant failure rate
3. **An Increasing Failure Rate Phase** also called the wear out phase, when ageing components fail because of degradation mechanisms

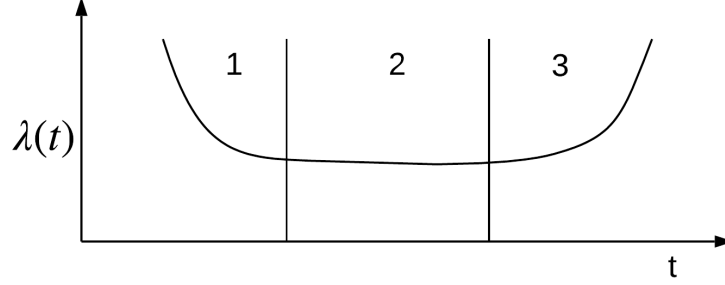


Figure 9: The reliability bathtub curve

Under the constant failure rate phase, the failure rate λ is assumed to be a constant. In such a scenario, reliability becomes

$$\lambda = \frac{-\frac{dR}{dt}}{R(t)}$$

$$R(t) = e^{-\lambda t} \quad (5)$$

$$F(t) = 1 - e^{-\lambda t} \quad (6)$$

$$f(t) = \lambda e^{-\lambda t} \quad (7)$$

It is evident that such an assumption leads to an exponential distribution of the failure density function as seen from Eq. 7. Apart from the exponential distribution, the Weibull distribution is also commonly used to describe component reliability. A Weibull distribution with the scale parameter η , and the shape parameter β is given by:

$$R(t) = e^{(\frac{-t}{\eta})^\beta} \quad (8)$$

The above provided definitions and equations form the basis for determining system reliability, and hence safety. When risk assessments at the system level allocate

functionality requirements at the component level, the criticality of failures acts as constraints on component reliability.

2.3 Safety Assessments: The Current Paradigm

Before we can discuss traditional and state-of-the-art in safety assessments or risk analysis, we must answer the following questions: i) “What is risk?”, and ii) “What makes it acceptable?”. Risk and its estimation, typically involves providing answers to the following three questions: i) what can go wrong?, ii) how likely is it?, and iii) what is the consequence? In one of the seminal works on quantitatively defining risk, Kaplan and Garrick suggest a ‘*set of triplets*’ idea – where risk is denoted by a triplet of i) scenario, ii) likelihood, and iii) consequence, to answer the three questions given above [100]. In determining what constitutes an “acceptable risk”, they pose two difficulties with the problem itself – one minor and one major. The ‘Minor’ difficulty is that risk is not linearly comparable – two different risks cannot always simply be compared². The ‘Major’ difficulty, which also serves as the answer to this underlying question, is that risk cannot be considered in isolation, but only in combination with the costs and benefits of the alternatives attendant to it. Thus, once we decide to fly, we must accept some inherent risk, with a baseline given by the risk posed by concepts and technologies available to us today. It is with this understanding that we proceed with the task of estimating and comparing (to make a decision on compliance) the risks posed by novel aircraft concepts and architectures. For the discussion that follows, we revert to a ‘*hazard severity & probability*’ paradigm to assess risk and make it comparable. A hazard is typically considered as a ‘*source of danger*’, which combined with the likelihood of precipitating it into damage or loss, gives us the risk [100].

Many different system safety and reliability standards have been developed by

²e.g. consider the famous Trolley problem [76, 94, 167] and the risks posed to the persons on the tracks

different agencies [4, 6, 59, 70]. Of these, SAE Aerospace Recommended Practice (ARP) 4761 and ARP 4754 are widely used to conduct system safety analysis and design assurance in order to comply with the relevant regulatory requirements. While ARP 4761 focuses on guidelines and methods of performing the safety assessments of aircraft, ARP 4754 looks at the development of aircraft systems along with validation of requirements and verification of design implementation for certification and product assurance [4,6]. The interplay between the two is shown in Figure 10 [6].

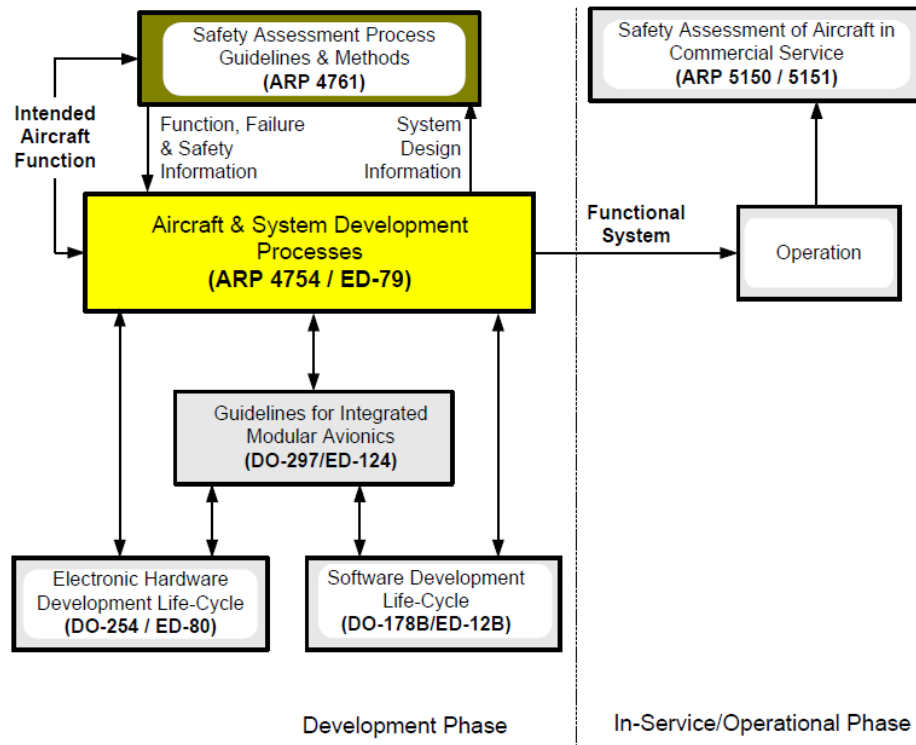


Figure 10: Interplay between ARP 4761 and ARP 4754 [6]

There are two key aspects to the safety assurance of novel aircraft concepts – i) software and electronic hardware development assurance, and ii) hardware reliability assessment. The prior aspect is important given that most of these novel concepts involve some elements of autonomy and non-deterministic methods (like artificial intelligence). To ensure compliance with airworthiness regulations, consensus standards DO-178C for software and DO-254 for airborne electronic hardware are used in

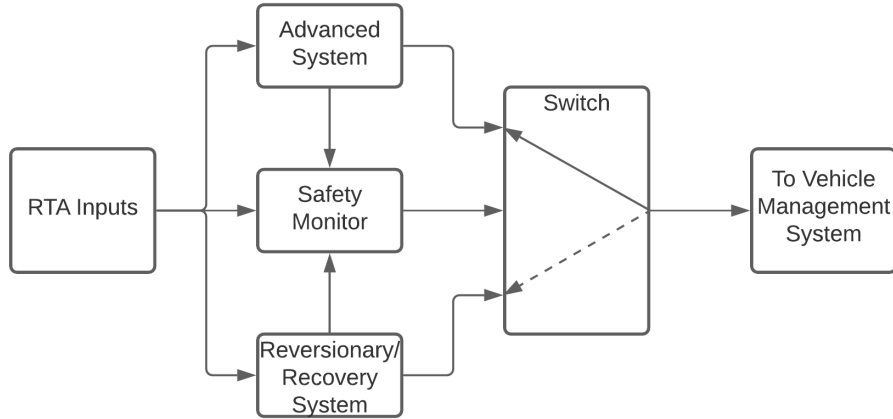


Figure 11: Generic RTA Architecture (Adapted from Ref. [10])

the traditional paradigm [10]. Both these standards provide development assurance processes to gain confidence that development errors have been eliminated. Reliability is another concept that may be used to gain equivalent confidence in a system. However, these do not provide a cost-effective path to certifying the complex non-deterministic methods required for advanced autonomy [10]. A direct requirement of assuring a function satisfied by software using non-deterministic methods may involve an enormous number of test cases. The Run-Time Assurance (RTA) concept utilizes one or more safety monitors along with assured recovery control functions to ensure safety for a novel non-deterministic control software. The complex system of interest may not be assured but the reversionary/recovery system is assured using traditional methods. The novel software/electronic system function is thus prevented from ‘*doing the wrong thing*’ by a safety monitor that switches control from the new system to the recovery system if needed [10]. Such a generic RTA architecture is shown in figure 11. While important in its own right, the development and real-time assurance of novel flight critical software and related electronic hardware is beyond the scope of the present work.

Instead, the present work focuses on the second aspect of design-time assurance which involves hardware reliability of novel aircraft physical architectures. System

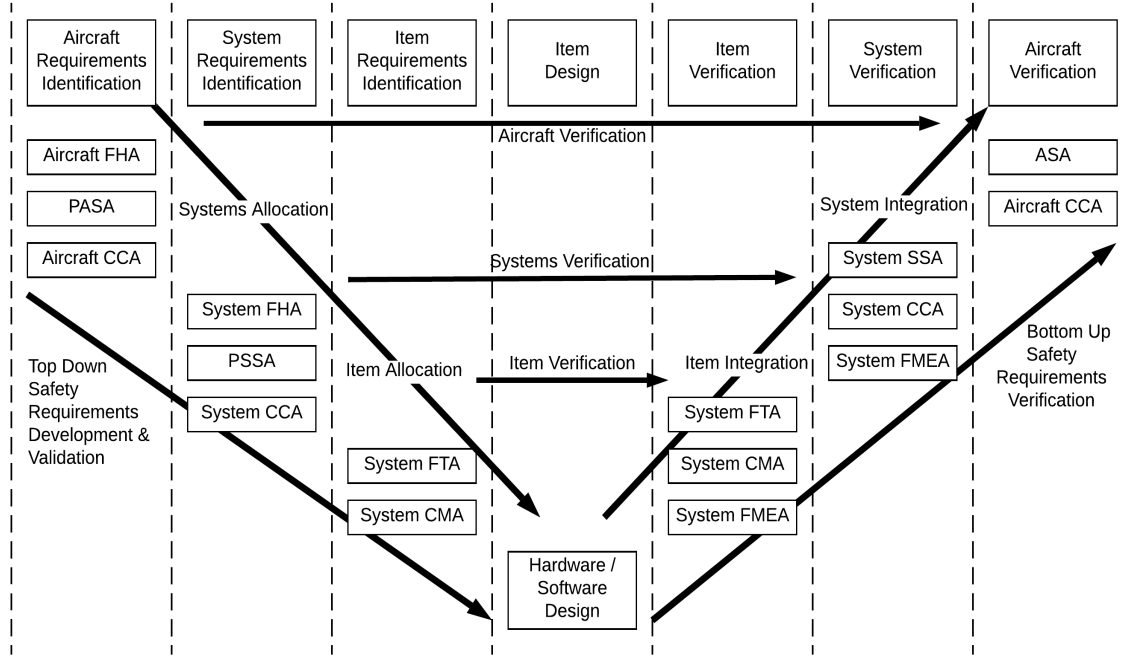


Figure 12: The System V & V diagram in the context of safety and aircraft design (Adapted from ARP4754 [6])

safety assessment processes of these are generally carried out in parallel to the development effort. Figure 12 shows a systems engineering ‘V’ in the context of safety and aircraft design. It shows that safety and reliability requirements are allocated to the item or component level following a hierarchical decomposition of aircraft functions and architecture. Safety requirements are initially functionally decomposed at the aircraft level. The system level requirements are generated by a *flow-down* of the aircraft level functions to the system level. The analyses conducted at this level include both aircraft and system level Functional Hazard Analysis (FHA), Common Cause Analysis (CCA), and a Preliminary System Safety Assessment (PSSA). In terms of the aircraft design timeline, these correlate well with the conceptual and preliminary design phases. The present work focuses on enhancing the safety assessments of novel aircraft physical architectures at these stages. This corresponds to the upper part of figure 10 and the first two vertical sections of figure 12. As the design matures, Fault Tree Analysis (FTA) is conducted at the aircraft and system level. As the aircraft is

built, these analyses and the requirements generated are verified, thus travelling back up the ‘V’.

ARP 4761 partitions the safety assessment practice into two top-level groups - i) the safety assessment process, and ii) the safety assessment analysis methods [4].

2.3.1 The Safety Assessment Process

The intent of the safety assessment process is to generate safety-related off-nominal requirements and verify that they are met during the aircraft development activities. It provides a methodology to systematically evaluate the aircraft throughout its design process to identify hazards, allocate requirements, and complete verification. The safety assessment process begins at conceptual design as is seen in Figure 12 where functional requirements are generated and hazards assessed. As the design evolves, the changes are reassessed, leading to further changes, leading to a loop that must be iterated until convergence. Finally, verification activities continue well past detailed design where flight tests may be conducted to provide the necessary evidence.

2.3.1.1 Functional Hazard Assessment (FHA)

ARP 4761 defines Functional Hazard Assessment (FHA) as [4]

“a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity”

An FHA is conducted at the aircraft level in conceptual design. It is meant to identify and classify failure conditions associated with aircraft level functions and combinations of functions [4]. While the aircraft level FHA is high level and qualitative, once an architecture is defined and aircraft functions assigned to subsystems, a system level FHA is conducted. The failure modes considered in a FHA are dependent on the mission phase. The output of the FHA is used as a starting point for conducting a PSSA (explained later) [4].

FHA usually involves multiple steps, including identification of all the functions of an aircraft, description of failure conditions associated with them, determination of the effects of those conditions, classifying them according to their severity (see table 2), and assigning requirements at the lower level [4]. FHA usually takes a tabular form as shown in Fig. 13.

Traditional FHA utilizes the fact that the functional decomposition of an aircraft is likely to remain the same (irrespective of what configurations or technologies are implemented) to keep the implementation and behavioral spaces independent while characterizing hazards [26]. Thus, an advantage of such a functional analysis is that it provides an understanding of system functionality, interconnection between functions, and a base for further reliability and system safety analysis. However, traditional FHA usually results in only two discrete types of functional requirements – (i) *Availability* (e.g. the loss of function), and (ii) *Integrity* (e.g. malfunction) [83]. Additionally, wrong assumptions, for instance in performance models or criteria, can lead to wrong conclusions [95]. Here lies its limitation when it comes to novel aircraft concepts and architectures. Novel concepts may not have discrete functional failures, and their consequences may not be well understood due to a lack of historical precedent and data. Qualifying a function failure merely as a *loss of function* or *malfunction* may not provide a complete picture for such concepts. As Armstrong demonstrates in his Ph.D. thesis [26]

“Assumptions regarding the relationship between function loss and hazard severity employed during traditional FHA bias architecture design and lead to inaccurate estimation of unit level requirements.”

Finally, the traditional tabular approach is slow and time consuming since it requires an analyst to evaluate every unique aircraft architecture manually – greatly limiting the scope for conducting trade studies in conceptual design.

Observation: *Traditional FHA allocates hazard values to discrete losses of function or malfunction*

2.3.1.2 Preliminary System Safety Assessment (PSSA)

The PSSA process as defined in ARP 4761 is a systematic top down approach to determine how failures in a proposed system architecture can lead to the functional hazards identified by FHA, and how the corresponding requirements can be met [4]. The PSSA is concerned with analyzing proposed system architectures to validate the safety of the proposed system design and to identify derived safety requirements (DSR) to guide further development [54]. For each aircraft or system functional failure identified in the FHA, the PSSA addresses the failure conditions through a qualitative or quantitative analysis as required [4]. The quantitative tools utilized to verify safety requirements being met by the aircraft and system architecture include fault trees and reliability block diagrams among others, both of which will be explained later. The system FHA and the aircraft Fault Tree Analysis (FTA) are the two main inputs to the PSSA process. The FTA may also be supplemented by a Common Cause Analysis (CCA), which establishes system level requirements like redundancy, separation, and independence in system architecting. The output of the PSSA process is intended to identify effects of component failures, reliability budgets, Development Assurance Levels (DALs), and any additional architectural features needed to meet aircraft and system safety objectives [4].

Figure 13 shows an overview of the relationship between FHA and FTA in conceptual and preliminary aircraft design. FTA, which forms an important part of Preliminary System Safety Assessment (PSSA) is verified using a Failure Modes, Effects, and Criticality Analysis (FMECA) by postulating failure mechanisms at the component level, and the addition of failure probability data available [128]. These are discussed in the section that follows. As the design progresses from the conceptual

phase to the preliminary design phase, functional safety assessments are followed by physical assessments that focus on the physical layout, while validating any redundancy and independence assumptions made. Finally, operational safety requirements are generated out of unusual scenarios, with unsatisfactory results being fed back into the design process [83].

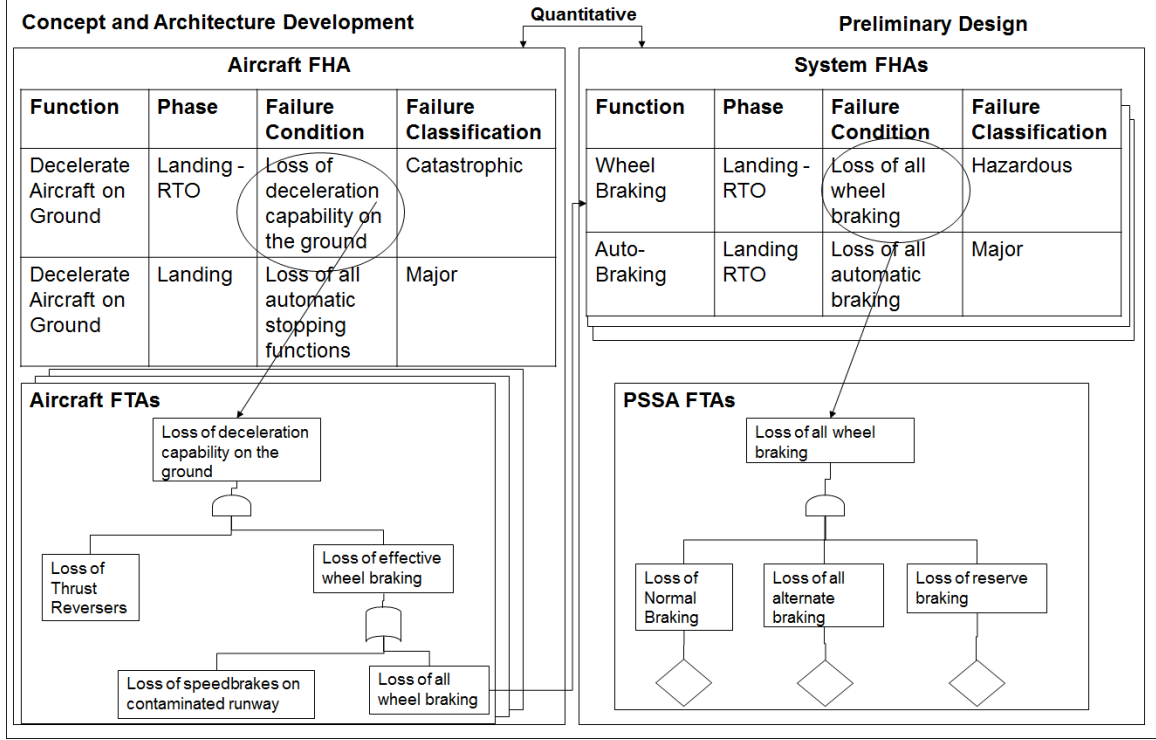


Figure 13: Relationship between FHAs and FTAs (Adapted from ARP 4761 [4])

While the intent of the PSSA process is to enable validation of system safety requirements earlier in the design phases, it does have quite a few shortcomings as reported by Dawkins et al. [54]. They state:

“There is a genuine conundrum in doing PSSA. To meet its objectives we want to do PSSA early and thus influence the design, but we will then be faced with the cost of updating the PSSA at each design change. Conversely, by waiting until the design is “stable” we will save money in PSSA, but lose the ability to influence the design cheaply. What is

needed is a “lightweight” way of doing PSSA early on, which becomes more rigorous as the design matures.”

System design and safety teams are often at loggerheads, since the responsibility for making trade-offs between different objectives lie with the designers, while it is the safety perspectives that give better insight into effective designs [54].

Additionally, there is uncertainty with how the PSSA process should be used with modifications and evolution of aircraft and systems. Sometimes, the smallest of changes may necessitate a re-analysis of system safety, and the effort required to implement such a change becomes proportional to the size of the system, not the size of the change [54].

Observation: *Traditional PSSA limits the scope for conducting trade studies in conceptual design*

2.3.1.3 System Safety Assessment (SSA)

A system safety assessment (SSA) is a comprehensive evaluation of the aircraft and its systems to prove that all safety requirements are met. Therein lies the difference between a PSSA and SSA. While both use similar methods, the prior evaluates the proposed architecture to identify safety requirements, whereas the latter provides evidence to verify that those requirements have been met by the final architecture [4].

The SSA process flow is generally represented through succeeding levels of verification. The right side of Figure 12 denotes these upward hierarchical verification levels where hardware reliability requirements, architectural requirements, and hardware and software Development Assurance Levels are verified against the safety requirements generated from the PSSA process. Various analysis methods like FTA, CCA, Failure Models, Effects, and Criticality Analysis(FMECA), Markov Analysis (MA)

among others are utilized in this effort to support the failure rates and modes considered and verify that safety objectives are met. Some of these analysis methods are discussed next.

Overall, it can be seen that the current paradigm seeks to identify hazards early in the design process and percolate corresponding qualitative or quantitative safety requirements downstream. Washington et al. [172] summarize the outcome of the system safety assessment process as four related sets F (not to be confused with failure probability defined earlier), C , Λ , and O where:

1. F is the set of n identified failure conditions $f_1 - f_n$
2. C is the set of severity c_i assigned to each failure condition f_i
3. Λ is the set of failure rate λ_i of each failure condition f_i , and
4. O is the set of failure rate objective o_i associated with f_i and its severity c_i , as given by AC 25.1309-1A or table 2

2.3.2 The Safety Assessment Analysis Methods

Once FHAs and/or PSSAs are completed, airplane and system functional designs or architectures are proposed to meet the generated safety requirements. The verification of functional designs takes the form of numerical analyses [83]. There are two broad classes of numerical analysis methods prescribed for this task:

1. Top-down Methods:

- Fault Tree Analysis (FTA)
- Reliability Block Diagram (RBD)
- Markov Analysis

2. Bottom-up Methods:

- Failure Modes and Effects Analysis (FMEA)
- Failure Modes, Effects, and Criticality Analysis (FMECA)
- Event Tree Analysis (ETA)

In addition to these, a Common Cause Analysis (CCA) is conducted to test the assumption of independence between functions, systems, or components. A brief overview of some of these is provided next.

2.3.2.1 Fault Tree Analysis (FTA)

FTA was originally invented in Bell Labs by H. Watson and Allison B. Mearns. It was later used by Dave Haasl of the Boeing company who recognized the power of this method to conduct quantitative safety analysis [64]. FTA is one of the most widely accepted, graphical, logic and probability based method for system safety assessment. It is a top-down method where an analyst begins with a single top level hazard and determines its root cause and probability of occurrence by recursively finding all single fault or failure combinations at the immediate lower level which could cause said hazard [4,64]. Such a recursive analysis continues till a primary event – one which cannot be broken down further is uncovered. These primary events may be internal or external in nature. In reality, however, FTAs are conducted to a level suitable for the phase of design and knowledge available at that point. For instance, during preliminary aircraft design, aircraft level events may be broken down to failures in subsystems or components and then stopped, thus treating these subsystem failures as primary events.

Figure 14 shows the basic building blocks for the FTA. The graphical fault tree is constructed using four basic building blocks [64] – (i) Basic Events, (ii) Gate Events, (iii) Conditional Events, and (iv) Transfer Events. Ericson defines three principle concepts to construct a fault tree using these basic blocks [64]:


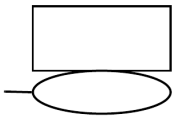
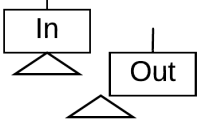
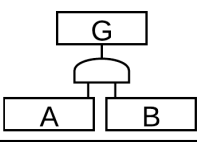
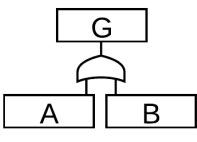
Symbol	Type	Description
	Node - Text Box	Contains text for all FT nodes. If it is a primary failure, it is called a basic event
	Condition Event	A condition restriction or probability
	Transfer Event	Indicates where a branch or sub-tree is marked for same usage elsewhere in the tree.
	AND Gate	Output occurs only if all inputs occur together $P_G = P_A \cdot P_B$
	OR Gate	Output occurs only if at least one of the inputs occur $P_G = P_A + P_B - P_A \cdot P_B$

Figure 14: Basic building blocks for FTA (Adapted from [64])

1. The I-N-S concept – Involves answering the question “What is immediate (I), necessary (N), and sufficient (S)”
2. The SS-SC concept – If a fault is caused due to component failure, classify it as a “state-of-the-component” (SC) fault, otherwise classify it as a “state-of-the-system” (SS) fault
3. The P-S-C concept – Involves answering the question “What are the primary (P), secondary (S), and command (C) causes of the event?”

The creation of a fault tree using these building blocks and concepts is shown in Fig. 15. Using such a construction, the top level hazard probability can be determined based on primary event / component failure probabilities. An example of the aircraft and system level FTA can be seen in Fig. 13.

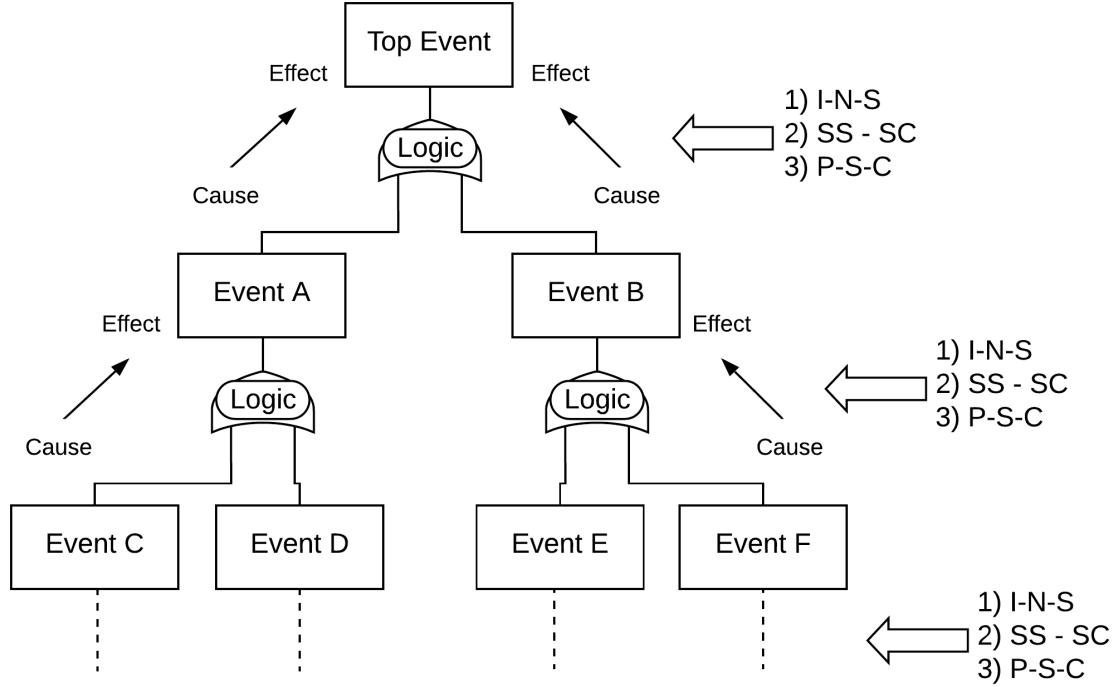


Figure 15: Steps for building a FTA (Adapted from [64])

An important time and cost saving feature of the FTA method is that only the system elements or components contributing directly to the top level hazard are analyzed. FTA can be used to (i) verify design compliance with DSR, (ii) Identify safety deficiencies that may be missed, (iii) Establish preventive measures to eliminate or mitigate such deficiencies, (iv) Identify common failure modes, and to (v) Establish system design requirements when working with fail-safe qualitative requirements [4, 64].

While FTA is a very powerful method and is widely used, it does have certain drawbacks. To start, while ARP 4761 considers FTA, dependence diagrams, and Markov analysis as equivalent, FTA cannot express repair and recovery strategies like Markov analysis. At the same time, FTA can support an upward propagation of probabilities, not the top-down allocation required for PSSA [54]. It requires an analyst with experience and understanding of FTA as well as the system being analyzed to conduct a FTA. With a logical structure, a FTA can become intractably

large and time consuming for complex systems. This means whenever an aircraft architecture changes, developed FTAs will have to be re-evaluated, in most cases manually, thus limiting the scope to conduct trade studies before design freedom is restricted.

2.3.2.2 Reliability Block Diagrams (RBD)

The RBD is an inductive, function and dependence driven approach where the system is divided into blocks that represent system elements [25,95]. It is also described as a success-oriented network, that allows an exhaustive search for pathways of success [95]. The structure of the RBD defines the logical interaction of component reliability by arranging them in series and parallel.

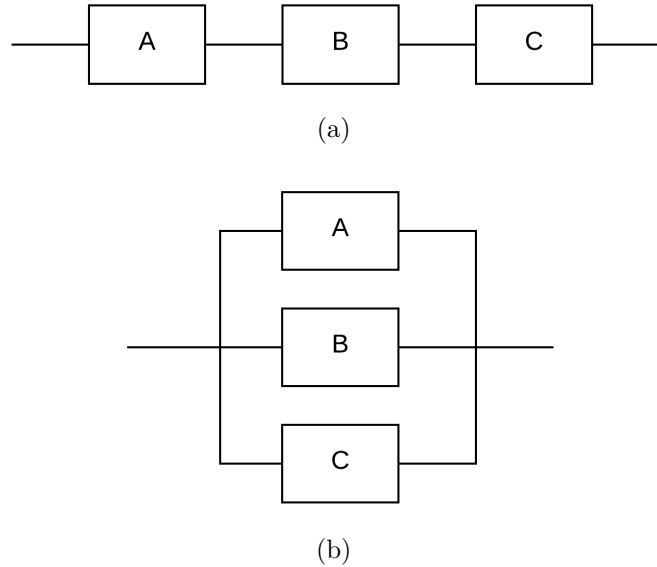


Figure 16: (a) Blocks in series (b) Blocks in parallel

Consider the series and parallel systems shown in Fig. 16 with the assumption that component failures are independent. When the components are in series, a failure in any combination of components will result in system failure. Thus, the system failure

probability and reliability are given as:

$$\begin{aligned}
F_S &= F_A + F_B + F_C + F_{AB} + F_{AC} + F_{BC} + F_{ABC} \\
&= (1 - R_A) + (1 - R_B) + (1 - R_C) + (1 - R_A)(1 - R_B) + (1 - R_A)(1 - R_C) \\
&\quad + (1 - R_A)(1 - R_C) + (1 - R_B)(1 - R_C) + (1 - R_A)(1 - R_B)(1 - R_C) \\
&= 1 - R_A \cdot R_B \cdot R_C \\
R_{S,series} &= R_A \cdot R_B \cdot R_C
\end{aligned} \tag{9}$$

When the components are in parallel, the failure probability and reliability are given as:

$$\begin{aligned}
F_S &= F_A F_B F_C \\
&= (1 - R_A)(1 - R_B)(1 - R_C) \\
R_{S,parallel} &= 1 - (1 - R_A)(1 - R_B)(1 - R_C)
\end{aligned} \tag{10}$$

RBD can be a powerful tool in determining system reliability. When components can be assumed to belong to a constant rate phase, the reliability (R) as a function of failure rate (λ) is given by Eq. 5 repeated here for convenience:

$$R(t) = e^{-\lambda t}$$

Thus, when the reliability is to be determined for a system shown in Fig. 16 in terms of component failure rates (failures/unit time) under a constant failure rate assumption, Eq. 5,9,10 give:

$$R_{S,series} = e^{-(\lambda_A + \lambda_B + \lambda_C)t} \tag{11}$$

$$R_{S,parallel} = 1 - (1 - e^{-\lambda_A t})(1 - e^{-\lambda_B t})(1 - e^{-\lambda_C t}) \tag{12}$$

As can be seen, placing components in parallel increases reliability of the system due to redundancy, while placing components in series decreases reliability. In general, the RBD correlates well with the physical relationship between system components

and can help quantify reliability levels of aircraft and system architecture during PSSA. However, as systems get complex, the equations to compute reliability using RBDs get complex, leading to a reduced utility for aircraft conceptual design, when exploration and trade studies of complex systems are of interest.

2.3.2.3 Markov Analysis

Markov Analysis (MA) models system failure as a stochastic process where the system state (S^s) is modeled with transition probabilities (λ) and repair rate (μ). The evolution of the system state, therefore, is a function of both time, and probabilities (λ, μ). Typically, the process of system transition is discrete in the state-space, and continuous in the time-space, and is typically called a chain. When a system state at time $t + \Delta t$ as a result of failure transitions is only dependent on its state at time t , this process is called *Markovian*. The system state can then be represented as:

$$S^s(t + \Delta t) = fn(S^s(t), \lambda^s(t), \mu^s(t)) \quad (13)$$

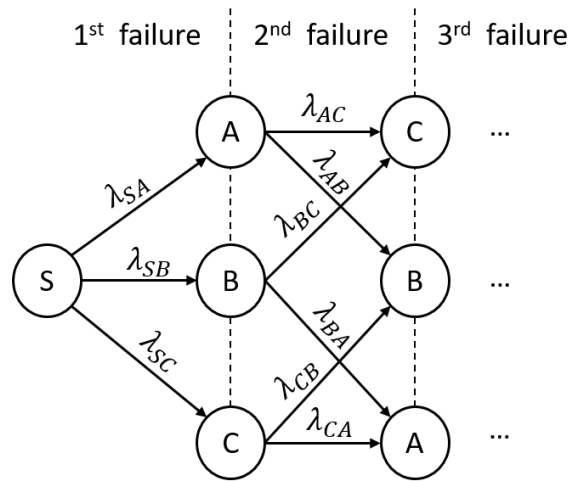


Figure 17: Example Markov Analysis for a three component non-repairable system

During the constant failure rate phase as shown in Fig. 9, the system transition probabilities (component failure rates) depend not on t , but only on Δt . This assumption results in a steady state stochastic process with the corresponding Markov

process being called ‘homogeneous’. In such a case, the probabilities λ and μ are given by the inverse of the Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) respectively, and are called failure rates and repair rates respectively [16]. Typically for aerospace applications, failure duration and their impacts are visible within the mission being flown when a component fails. Thus, aircraft failures can be considered non-repairable to evaluate their effect in terms of severity.

Figure 17 shows a Markov chain created for failure analysis of a three component non-repairable system from Fig. 16. Beginning in state S at time t where all components are functioning, the probability that the system leaves S in time Δt is given by

$$P_{S \rightarrow} = (\lambda_{SA} + \lambda_{SB} + \lambda_{SC})\Delta t \quad (14)$$

When component states are binary (working or failed), the total number of system failure states can be 2^N , where N is the number of components. A similar analysis for all the other states provides a system of first order linear differential equations that can be solved rapidly. MA provides an efficient means of stochastically modeling the failure state transitions of a complex system, without having to perform Monte Carlo analysis [16]. However, each failure state involving multiple components can be reached in multiple paths (for e.g. system state with components A, B failed can be reached if A fails first and B second, or vice-versa. Thus, the total number of chains and states explored in Markov analysis can explode with the number of components. To deal with this intractability, two assumptions can be made - i) Trim the MA by assuming component independence, so only one chain is considered leading to any system state (e.g. A first, B second); and/or ii) Truncate the MA to only consider a limited number of failures at once. When the individual component reliability is high as is the case in aircraft systems, the probability of multiple failures at once is exceedingly low. Thus, the Markov chains can be trimmed to only consider one or two component failures at once without losing much fidelity.

2.3.2.4 *Failure Modes, Effects, and Criticality Analysis (FMECA)*

ARP 4761 defines Failure Modes and Effects Analysis (FMEA) as [4]

“an inductive or a bottom-up method of identifying the failure modes of a system, item, or function and determining the effects on the next higher level of the design.”

As seen in Fig. 12, FMEA is conducted when the design of an aircraft transitions from the preliminary to the detailed stages, and more knowledge on system architecture and components is available. When combined to support a quantitative method like the FTA or Markov analysis, that can assign criticality to the failures postulated, FMEA is also called FMECA. In this bottom-up analysis, a certain component failure or initiating condition is postulated, and its effect on the system is determined. The output of such an analysis is an FMECA worksheet that documents (i) the component or function postulated to fail, (ii) identified failure modes and failure rates, and (iii) effects of the failure (directly and/or at the next higher level) [4].

An advantage of this method is that it offers a systematic review of all components in an aircraft architecture and identifies failure modes and their effects. The output of FMEA can be used in conjunction with FTA and RBD to inform the criticality of such component failures [95].

Similar to FTA, an FMECA is time consuming. In fact, it only covers a single failure at a time in a tabular manner. It also requires sufficient detail regarding aircraft architecture and components, and thus cannot be used for design-space exploration before degrees of freedom are locked down. Additionally, for a complex system, such an analysis can become prohibitively expensive.

2.3.2.5 *Common Cause Analysis (CCA)*

Many times during quantitative analysis using the methods discussed above, independence between system functions or components is assumed. While this tends to

simplify calculations, it is important to verify these assumptions. CCA provides tools to identify dependencies or external events that may cause multiple failures and is subdivided into three types [4].

1. *Zonal Safety Analysis (ZSA)* is performed on each zone of the aircraft with the objective to ensure any components are installed properly and do not cause unwanted interference with other systems under failure.
2. *Particular Risks Analysis (PRA)* is used to identify events that can impact safety but are outside the system, such as hail, bird strikes, lightning etc. The intent is to show that such risks are either eliminated or acceptable.
3. *Common Mode Analysis (CMA)* is performed to verify that different AND events postulated in FTAs are indeed independent.

2.3.3 Probability Models

While most of the above described processes or methods can be used to qualify hazard severity, they need to be combined with probability theory to provide quantifiable failure requirements, or to determine the actual failure probability. Failure rates are generally estimated by looking at available data and trying to determine summary statistics like the mean, median, or mode of the data, along with confidence intervals. Sometimes, patterns of failure are represented by probability distributions, and the parameters estimated using available sample data. The probability theory and models utilized in traditional aircraft safety assessment literature is what is known as the ‘*frequentist*’ approach by modern statisticians. In this approach, probabilities are informed purely by available data, where any uncertainty is reduced by increasing the number of data points.

Such a ‘*frequentist*’ approach, suggested by ARP 4761, cannot comprehensively address uncertainty in input data and models [172]. Uncertainty is generally classified into two categories [146]:

- **Epistemic Uncertainty** (Greek ‘*episteme*’: knowledge) is also called knowledge-based uncertainty that results from incomplete knowledge or understanding about fundamental phenomenon. This uncertainty is significant in situations where not enough evidence or data is available.
- **Aleatory Uncertainty** (Latin ‘*alea*’ : game of dice) is the second type of uncertainty and relates to the inherent randomness or stochasticity of a system that is not reducible.

The ‘*frequentist*’ approach can only take aleatory uncertainty into account through data that is available [146]. ARP 4754 and 4761 suggest making conservative assumptions to deal with this downside and manage uncertainty better [4, 6, 172]. However, with novel aircraft concepts and architectures, data available are insufficient and epistemic uncertainty is large, thus rendering existing ‘*frequentist*’ probability models unsuitable [58, 172].

Observation: *Traditional methods for conducting safety assessments are unsuitable for dealing with the large uncertainty associated with novel concepts.*

2.3.4 Summary and Observations

The intent of the safety assessments is to ensure that any aircraft or system under consideration poses no more than an acceptable level of risk. The current paradigm is largely based on SAE ARP 4761 and 4754, which act as established guides for performing safety assessments [4, 6, 73].

A functional hazard assessment (FHA) is performed at the aircraft and system level under preliminary aircraft safety assessment (PASA) followed by a preliminary system safety assessment (PSSA). These generally correlate with aircraft conceptual and preliminary design stages. A benefit of the FHA is that it keeps functional and behavioral spaces independent while characterizing hazards [25]. This allows the

aircraft level assessment to be conducted before design degrees of freedom are locked down by keeping it independent of architectural details. However, traditional FHA is a tabular approach in which assumed discrete functional failures are assigned a discrete hazard severity. This assumption may not be valid for novel aircraft concepts. Also, the FHA process is slow and time consuming, requiring an analyst to analyze every unique configuration manually for the system level FHA, thus limiting the scope for conducting trade studies during early design.

A fault tree analysis (FTA) is a powerful method and is widely used. However, it supports an upward propagation of failure probabilities, not the downward required for PSSA. It is generally constructed manually, can get intractably large, and needs to be re-created with any change in system design. This also restricts its usefulness earlier in the design phase.

Reliability block diagrams (RBDs) can determine system reliability using simple logical relationships and correlates well with the physical relationship between system components. This technique can be combined with certain aspects of network theory to enable exploration of the architecture space as is described later.

Markov analysis models the transitions of system failure states as Markov chains, and benefits from the well established mathematical framework to support it. It provides an advantage over some of the other methods discussed so far in exploring the scenario tree of system failure states. However, MA suffers from the cost of explosion of the state-space for complex problems with a large number of components.

A failure modes, effects, and criticality analysis (FMECA) offers a systematic review of all components, along with the failure modes and their effects at the aircraft level. It can also be used in conjunction with FTA or RBD to inform the criticality of such failures. However, this method is time consuming, takes a tabular form, and cannot be used for conducting design trade studies efficiently.

Observation: *The traditional safety assessment processes and methods used in preliminary design phases limit the scope for exploration of the design and architecture space*

Additionally, novel aircraft concepts and architectures may not have discrete functional failures, and the severity (consequences) of such failures may not be well understood. Consider for instance a distributed electric propulsion (DEP) architecture that is being considered for some novel GA concepts. Instead of traditional scenarios regarding loss of thrust, the DEP is likely to have a range of thrust degradation scenarios (0% to 100% thrust degradation depending on how many propulsors lose power or fail). Since there is no historical precedent, the current approaches fall short in qualifying the severity of functional degradation and can potentially result in incorrect functional hazard severity allocation. A hypothesis demonstrated by Armstrong [25] in his Ph.D. thesis thus becomes another observation of interest here:

Observation: *Assumptions regarding the relationship between functional loss and hazard severity during traditional PSSA can lead to inaccurate estimation of component level requirements for novel aircraft concepts and architectures*

On the aspect of computing failure probability, the current approach uses either summary statistics or probability models whose parameters are estimated from data samples to represent patterns of failure. For conventional systems and architectures, where large quantities of data are available over multiple decades, this approach has proved to be quite useful to ensure air transportation remains one of the safest means of travel. However, this ‘*frequentist*’ approach cannot address uncertainty well, especially in the absence of available data. For novel aircraft concepts and architectures, data is insufficient and epistemic uncertainty is large, making the existing approach unsuitable.

Observation: *Traditional approaches to model failure probability are insufficient to address the large uncertainties associated with novel aircraft concepts and architectures*

2.4 Reliability and Safety Assessments: State of the Art

In light of the previous observations, a literature review was conducted to identify the state of the art in reliability and safety assessment processes and methods to identify alternatives and promising techniques. This section is broadly divided into four parts. The first part looks at the improvements made in methods for conducting safety assessments. The second looks at reliability and safety studies conducted in the context of system design. The third part looks at informing system design trade-studies and optimization using safety and reliability considerations, while the fourth looks at treatments of uncertainty in the state of the art.

2.4.1 Methods

Hazard and operability study (HAZOP) is a method similar to FHA, but uses a design view of the system instead of functional requirements one for failure identification. [18]. HAZOP was originally used for analyzing processes or operations, with a focus on a flow of materials through a chemical plant [25]. While HAZOP has a larger set of guide-words than FHA, it is limited in its ability to respond quickly and accurately to a redesign or alternate configurations [18, 25].

Amongst all the methods used for safety assessments, FTA has probably received the most attention in terms of research interest and improvements suggested. Ruijters and Stoelinga published a survey on the state of the art in modeling FTA [155]. They note that a “wild jungle” of different FTA techniques now exists, including standard fault trees (FTs), as well as extensions like dynamic, repairable, and extended FTs. Standard FTs, also called static FTs (SFTs) are the most basic fault trees as explained

in the previous section. They can be analyzed qualitatively and quantitatively and have some commercial tools available for ease of implementation [155]. Dynamic FTs (DFTs) include a temporal sequence of information that cannot be handled by SFTs. Due to the inclusion of a temporal element, the qualitative and quantitative analysis of DFTs is different from SFTs [155]. Repairable FTs are used when reliability is computed over a long period of time with the possibility of repairing or replacing failed components [155]. However, in aircraft applications, failures cause an immediate dynamic response in the order of seconds because of which the assumption of repairability is invalid, making repairable FTs less preferred [61]. Finally, Fuzzy FTs are proposed to be used where precise data are not available, and decisions need to be made from vague information. Fuzzy set theory has proven useful when experts cannot provide exact numerical values for component failure probabilities, and instead give their opinion in linguistic terms [98]. Despite all these developments in FTAs, a typical FTA remains architecture specific and requires time and manual effort to conduct for every system under consideration. They also require experience in postulating safety critical events or hazards, which may be lacking for novel architectural or operational concepts.

Observation: *Advances in the state-of-the-art safety methods like HAZOP or FTA variants have not improved identification and classification of hazards for novel concepts, nor improved the ease of conducting design trade studies with safety considerations*

Since FTAs require a lot of modeling effort, the field of Model Based Dependability Analysis (MBDA) has developed to explore how dependability information can be synthesized from system models automatically [98]. Papadopoulos and others looked at automating the generation of FTAs and FMEAs [138, 139, 141, 142]. In a tool they

developed called Hierarchically Performed hazard Origin & Propagation Studies (HiP-HOPS), FTAs and FMEAs can be generated automatically once the corresponding system Simulink model is annotated with component failure information. Additionally, the tool provides optimization capability by automatically changing the system topology [140, 143]. Walker et al. extended HiP-HOPS to include a temporal aspect to the generated FTAs [171], while Kabir et al. extended the method to conduct dynamic analysis using Petri nets and Bayesian belief networks that provide a better treatment of uncertainty [99].

While the tools developed to automate the generation of FTAs, and enable design optimization by letting the optimizer change the system topology are quite powerful, one must note that (i) they were developed over almost a decade of research, and (ii) the tools are limited to using MATLAB Simulink models annotated with failure data to give meaningful results. For the safety assessment of novel aircraft concepts and architectures, these techniques do not address the limitations in the generation of safety critical off-nominal requirements.

Observation: *Model Based Dependability Analysis (MBDA) techniques show promise in automating safety analyses and enabling architectural space exploration and optimization*

2.4.2 Reliability in Preliminary System Design

Numerous studies have been conducted in the recent past to look at the reliability and safety of novel aircraft architectures and systems early in the design phase. Safety and reliability considerations while designing an aircraft electrical system have been of interest for a long time [111]. Due to the large number of components electrified, certain studies suggest restricting analyses to components considered safety critical -

flight surface actuators, fuel pumps, and generators [41]. Due to the lack of operational experience of MEA architectures, a combination of FTA, Markov analysis, and Bayesian analysis is suggested [166], as against the traditional paradigm [159].

For novel concepts and architectures in non-aerospace applications, safety assessment techniques in literature have focused on the traditional paradigm. While looking at an integrated power system for an electric ship, Menis et al. utilized FTAs and FMEA tables to analyze the causes and effects of faults and/or failures occurring in an integrated power system component [124]. On a similar study on a direct methanol fuel cell, Deodath et al. conducted extensive quantitative FTA and FMEA analysis to determine system reliability under different failure states [56]. In both these studies, like many others [87], a fixed system architecture was analyzed with no considerations of informing design trade-studies.

Within the aerospace domain, numerous studies have been conducted for safety assessment of novel architectures or technologies. Hasan et al. [82] integrated hardware reliability with a simulation of flight operations to measure safety improvements due to deployment of new technologies. Hemm et al. [85] conducted a safety assessment of ground automation-controlled and ground automation-augmented concepts under two abnormal conditions. Both these studies utilized modeling and simulation tools to gain additional knowledge regarding hazard severity and probabilities while focusing on the operational safety paradigm. Otherwise, they utilized traditional techniques like FTAs to analyze failure scenarios and their relationship to system-wide risk. Papathakis et al. [145] demonstrated a safety system design process used while building technology demonstrators in the form of electric propulsion aircraft test-beds where a system safety workgroup was established to assess hazard severity, probabilities, and design to eliminate or mitigate hazards. Woodham et al. utilized a Model-Based Safety Analysis (MBSA) method to address safety challenges associated

with NASA’s FUELEAP³ project [174]. In it, an aircraft level FHA was conducted using SysML hazard blocks, with the intent of relating hazard conditions to initiating events and possible mitigations like design modifications [174]. These last two studies relied on expert opinions to conduct a safety assessment using traditional tabular structures for representing safety risk.

Observation: *Traditional methods continue to be the dominant approach for conducting safety assessments for novel system architectures*

One of the problems with determining the safety risk and reliability of novel aircraft concepts and architectures lies in determining the severity of failures because there is little historical data or precedent to inform the analyst. In such a situation, an approach that utilizes system performance and dynamic models, along with multi-state reliability theory seems to show promise. Multi-state reliability is a relatively recent concept in reliability theory where both system and components are allowed to assume more than two levels of performance. In a review article, Yingkui and Jing [176] look at the latest methods, computational approaches, and optimization of multi-state system reliability. In a study that utilizes system models to determine the effects of component failure on critical functions, Borer et al. [44] evaluated two critical portions of proposed NASA Lunar Surface Systems. When physical components were mapped to system critical functions, a direct simulation of component dependencies (power, thermal, etc.) resulted in the identification of cascading failures and allowed the determination of architectural features that drive system loss probability [44]. Dominiguez-Garcia et al. [61] proposed a methodology that uses a behavioral model for system performance and dynamics with artifacts to model component failure, along with Markov chains for modeling the different configurations (states) a system can adopt under component failures to enable dynamic performance and reliability

³FUELEAP - Fostering Ultra-Efficient Low-Emitting Aviation Power

evaluation of fault-tolerant systems. In a case study on a lateral-directional flight control system of a fighter aircraft, they demonstrated that using a quantitative system behavioral model allowed them to assess the “*degree of failure*” along with degraded system operational modes [61]. In a multi-state design approach to analyze twin-engine aircraft performance robustness, Agte et al. [15] determined the effect of changing aircraft geometry, control gains, and component failure rates on expected aircraft performance to inform availability. They showed how making small changes in aircraft design variables can improve performance and help optimize the aircraft for nominal conditions, but can end up hurting performance in off-nominal conditions by decreasing expected performance or availability across system lifetime [15].

Observation: *Optimizing aircraft design parameters for nominal conditions can worsen performance in off-nominal conditions and lead to lower availability across system lifetime*

Observation: *Multi-state reliability assessment methods that utilize system performance and behavioral models show promise while determining hazard severity for novel aircraft concepts and architectures*

2.4.3 Optimization and System Safety

There have been some studies that try to include aircraft design and architectural optimization while considering safety and reliability requirements. In a Ph.D. thesis, Johansson [95] suggested using Markov analysis as the best approach to model reliability in early design phases, after looking at reliability methods like RBD, event trees, Markov analysis, and Petri nets. She then applied a genetic algorithm to optimize for system safety and reliability while minimizing development cost by finding the optimal vendor for each piece of equipment [95]. It is important to note that a

fixed system architecture was considered in this optimization. In another study by the same author, three fixed fuel system architectures were analyzed with the aim to inform the selection of the best alternative in a multi-attribute sense [96].

Campbell [48] in her PhD thesis developed a methodology to architect a power distribution system of turbo-electric aircraft while allocating redundancy. The redundancy allocation was optimized using particle swarm optimization to meet system level reliability requirements. However, the reliability requirement was based on a single simplistic hazard of having enough motors operational for take-off, while failure rate estimation was carried out through historical data [48].

Armstrong [25] in his thesis developed the method to identify off-nominal operational requirements based on risk and reliability during the conceptual design phase. In it, traditional functional hazard analysis and system safety analysis was expanded to consider the magnitude of function loss, instead of the discrete functional loss scenarios suggested by the current paradigm. The result pertinent to the current work was the development of Continuous FHA (C-FHA) where severity of functional failures are expressed as a continuous function of the magnitude of function loss, and Analog PSSA where failure probability requirements are expressed as a continuous function of the magnitude of function loss [25]. These ideas regarding C-FHA and Analog PSSA will be discussed further later in the current work.

While Armstrong did not conduct optimization of the system architecture, he evaluated the system safety risk for a conventional and more electric baseline and optimized for the *load-shedding* strategies since such off-nominal considerations were shown to drive system requirements [25].

Observation: *Informing the trade-studies during the aircraft design process with reliability considerations has received limited attention in the aircraft design community*

2.4.4 Treatments of Uncertainty

As established earlier, uncertainty is of two primary types – *aleatory* uncertainty refers to inherent randomness in the system, while *epistemic* uncertainty refers to uncertainty due to lack of knowledge. For novel aircraft concepts and architectures, the aleatory uncertainty is large due to the lack of available data. Additionally, because of the limited knowledge and experience available for these aircraft, the epistemic uncertainty is large too. As explained in the summary of Sec. 2.3, the traditional approach, also called the *frequentist* approach is unable to comprehensively address these uncertainties [172]. Additionally, there are difficulties in demonstrating a given reliability requirement when the available data are limited. When failure is assumed to follow an exponential distribution (constant failure rate), Bonis [43] observes the following two conditions must be met:

1. To ensure the lower confidence limit is at least equal to required reliability, the observed reliability value must be much higher than required, and
2. In order to avoid endless testing, the designed Mean Time Between Failure (MTBF) must be several times the required MTBF

As can be anticipated, such requirements can lead to significant over-design of the system, or worse – a reduction of confidence levels for demonstrating reliability requirements (a risky option). Under such seemingly impossible options, an alternate approach to the treatment of uncertainty in failure rates lies in the paradigm of *Bayesian* inference. While the field is old, the current work refers to the work of Dezfuli et al. [58] who define Bayesian inference as:

“A process of inference using Bayes’ theorem in which information is used to newly infer the plausibility of a hypothesis.”

While the *frequentist* approach uses data to determine failure probabilities, a *Bayesian*

approach utilizes information, including models, data, and subject matter expert opinions among others [58]. The utility of the Bayesian approach can be attested to when one considers that numerous industries consider these techniques standard [1, 58, 79, 80, 102]. Additional details on the theory behind Bayesian inference will be provided in later chapters.

Kelly and Smith [102] conducted a Bayesian risk analysis of the space shuttle based on O-ring data collected prior to the ill-fated launch of the Challenger in July 1986. The intent of this analysis was to include a better treatment of uncertainty in the data by allowing uncertainties in observable launch parameters such as temperature to be propagated through the model. An et al. [21] proposed a Bayesian framework to address the epistemic and aleatory uncertainty in the input variables, as well as meta-model uncertainty that arises from the approximation of the response function while performing reliability analysis. Two case studies are provided where input uncertainties are managed through a posterior predictive distribution to evaluate failure probability, while the meta-model uncertainties are quantified using a Gaussian process or Kriging model [21]. Youn and Wang [177] proposed a Bayesian reliability based design optimization (RBDO) approach to optimize a use case while dealing with uncertainty. Banghart et al. [28] applied a Bayesian network to a field dataset to develop a predictive method capable of predicting failure of several important components as compared to traditional reactive methods. Luxhøj [116] implemented a Bayesian belief network in an aviation system risk model that combines the use of a human error taxonomy and case based scenarios to assess a relative risk intensity metric. In a non-aerospace application, Ewing et al. [65] tried to estimate a marine energy converter drive train reliability under a lack of specific reliability data. They developed a Bayesian updating framework using high fidelity onshore wind failure data to form the prior distributions of the unknown parameters of a Weibull component failure model and updated those with the next 6 months of failure data [65].

A NASA handbook by Dezfuli et al. [58] aims to provide engineers and scientists an analytical structure for combining data and information from various sources to generate estimates of parameters of uncertainty distributions used in risk and reliability models. All readers interested to learn more about the Bayesian inference method and its uses in probabilistic risk assessment are directed to this document. Washington and Clothier [172] utilized some elements from this NASA handbook to present a Bayesian approach to showing compliance to system safety requirements for unmanned aircraft systems. Their reason for choosing a Bayesian approach remains similar to every other so far – a better treatment of both levels of uncertainty, especially when available data are scarce.

Another approach to address uncertainty is using Fuzzy set theory. It is especially used to deal with semantic variables where linguistics can cause ambiguity in the true value. Oztekin and Luxhøj [137] proposed a hybrid fuzzy-Bayesian approach for safety assessment of unmanned aircraft operations in the presence of uncertainty and vagueness. Suresh et al. [165] presented a comparative study of probabilistic and fuzzy methodologies for the evaluation of top level uncertainty in a fault tree (FT). In a study that applies fuzzy FTs to patient safety risk in healthcare, Komal [104] states that fuzzy FTs are used when:

1. Clear boundaries between success and failure states of the system do not exist,
2. A lack of sufficient data, and resulting uncertainty means the failure probability cannot be calculated precisely, and
3. There is subjective evaluation of reliability.

It is apparent that a Bayesian approach suits the problem of dealing with limited data and knowledge associated with novel architectures and technologies better than any other.

Observation: *Bayesian inference techniques are widely used in nuclear and space industry to better characterize aleatory and epistemic uncertainty in probabilistic safety assessment*

2.5 Summary of Observations

The observations of this chapter have been summarized here for easy reference. They serve to identify the shortcomings in the current paradigm related to identifying safety related off-nominal requirements for novel architectures and technologies and incorporating them earlier in the aircraft design process to inform design trade-studies. Some observations from the state of the art serve to identify potential enablers to solve some of the shortcomings and to guide the direction of the search for a solution for the research objective. These observations have been divided into three top level groupings as shown below.

Observations Group 1: Characterizing safety related off-nominal requirements for novel aircraft architectures

1. *Off-nominal scenarios have the potential to pose significant sizing and architecture specific requirements at the system level*
2. *Most aircraft safety and reliability requirements are emergent and depend on the physical architecture definition*
3. *Traditional methods continue to be the dominant approach for conducting safety assessments for novel system architectures*
4. *Traditional FHA allocates hazard values to discrete losses of function or malfunction*

5. *Assumptions regarding the relationship between functional loss and hazard severity during traditional PSSA can lead to inaccurate estimation of component level requirements for novel aircraft concepts and architectures*
6. *Multi-state reliability assessment methods that utilize system performance and behavioral models show promise while determining hazard severity for novel aircraft concepts and architectures*

Observations Group 2: Treatment of uncertainty in available data and models

1. *Traditional approaches to model failure probability are insufficient to address the large uncertainties associated with novel aircraft concepts and architectures*
2. *Bayesian inference techniques are widely used in nuclear and space industry to better characterize aleatory and epistemic uncertainty in probabilistic safety assessment*

Observations Group 3: Incorporating safety requirements in early design

1. *The traditional safety assessment processes and methods used in preliminary design phases limit the scope for exploration of the design and architecture space*
2. *Informing the trade-studies during the aircraft design process with reliability considerations has received limited attention in the aircraft design community*
3. *Optimizing aircraft design parameters for nominal conditions can worsen performance in off-nominal conditions and lead to lower availability across system lifetime*
4. *Model Based Dependability Analysis (MBDA) techniques show promise in automating safety analyses and enabling architectural space exploration and optimization*

The observations made above will help guide the direction of research in this thesis. Along with any additional ones made during the course of implementation and analysis, they inform the foundation upon which this dissertation is based.

CHAPTER III

RESEARCH FORMULATION

Building on the arguments, observations, and gaps identified in the previous chapter, this chapter will focus on formulating the problem at hand and explaining the proposed approach. This will involve coming up with an overall research objective, along with certain requirements and broad research areas that must be addressed by any proposed solution. These will lead to the formulation of specific research questions that seek to tackle deficiencies identified, which when answered, will seek to meet the overall research objective. A set of hypotheses will be built based on observations from literature, or original research conducted by the author to answer these research questions. Any background necessary to understand the corresponding hypothesis will be provided as needed. When any hypothesis leads to additional questions, an attempt is made to duly identify them and answer them based on knowledge of prior art. If such questions need to be tackled separately to completely test the parent hypothesis, these questions become secondary research questions. Secondary hypotheses are then proposed to answer such questions.

3.1 Research Objective

Based on the motivation and observations stated in chapters 1 and 2, a need to enhance the safety assessment of novel aircraft architectures can be established. This leads to the overall research objective of this thesis which was stated in chapter 1.5, and is restated here.

Research Objective:

Develop a framework that will enhance safety assessments of novel aircraft physical architectures and technologies in early design by

1. identifying off-nominal requirements,
2. allocating them to the system and component level,
3. enabling compliance decision-making while addressing both epistemic and aleatory uncertainties, and
4. informing design trade-studies.

This research objective talks about enhancing safety assessments for novel architectures and technologies. It is important to pause here and restate the definition of novel aircraft architectures and technologies used in this thesis (See Def. 2.1.1.1) before proceeding.

Definition 3.1.1 (Novel Aircraft Architecture). *A novel aircraft architecture is loosely defined here as one which differs significantly from the traditional paradigm mentioned above in its physical implementation to fulfil at least one aircraft level function.*

The stated research objective can be realized by addressing the four enumerated requirements listed in it. In this thesis, the research objective is thus broken down into three parts for this purpose. The first research area focuses on methods for the identification and characterization of safety related off-nominal requirements at the aircraft level for novel architectures, followed by methods to allocate these requirements at the system and component level. The second research area focuses on addressing the large uncertainty due to the limited data and experience with novel concepts while

enabling decision making. The third research area integrates the framework consisting of the outcomes of the first two and uses it to demonstrate its applicability to informing design trade-studies. These three research areas will be discussed next.

3.2 Research Area 1

This research area focuses on addressing the gaps found in observations group 1 from chapter 2.5. Risk assessment is an exercise in the imagination of failure. As noted earlier, novel aircraft architectures and technologies carry with them an uncertainty related to the off-nominal risk they pose. The limitations and off-nominal operational considerations postulated during the traditional safety assessments may not be correct or complete for these.

Research Question 1

Observations group 1 in chapter 2.5 alludes to multiple problems in identifying, characterizing, and allocating off-nominal requirements for novel aircraft architectures using traditional methods. Traditional methods require designers or analysts to assess individual architectures manually creating the FHA/FMEA tables and FTs. The FHA process assumes discrete functional loss which may not be valid for novel aircraft architectures and technologies. Analysts have to determine safety critical scenarios and estimate the severity of hazards, both of which are usually conducted manually through subject matter expert opinions for a given architecture. These are then fed back into design to allocate failure rate requirements at the component and subsystem level. It may be difficult to determine the hazard severity due to limited prior knowledge of failures associated with novel architectures. As a result, hazards may be identified or characterized with large uncertainty. All of these considerations lead to the first research question (RQ 1):

Research Question 1:

What method or group of methods can enable identification, characterization, and allocation of safety related off-nominal requirements for novel aircraft architectures and technologies in the conceptual and preliminary design stage?

Resultant Requirements Any solution to this research question must satisfy the following requirements to be considered complete.

Requirements:

1. *Generation of off-nominal / safety critical scenarios and corresponding hazards*
2. *Estimation of hazard severity under different scenarios*
3. *Allocation of reliability requirements to components and subsystems*
4. *Treatment of uncertainty in models while estimating hazard severity*

A solution to satisfy the first requirement must allow for the generation of off-nominal/hazardous scenarios, while the second requirement requires the solution to have the capability to estimate the hazard severity under said conditions. Finally, we require the solution to be able to allocate reliability requirements generated from the corresponding hazard severity to the components and subsystems. The focus on *improved treatment of uncertainty* in the last requirement is intended for the solution to operate in an environment with little knowledge and experience, as will be found in the design of novel concepts.

Formulation of Hypothesis 1

The primary goal of this research area is to identify or develop a method or a combination of methods that provide a better identification, characterization, and allocation of safety related off-nominal requirements at the system and component level for novel aircraft architectures and technologies. As such, it should be able to deal with the uncertainty due to a lack of knowledge and experience while dealing

with novel concepts and their failures. In observations group 1 from chapter 2.5, it was noted that multi-state reliability assessment techniques that utilize system performance and behavioral models show promise in answering research question 1. However, the multi-state reliability methods discussed in literature [15,16,61] all rely on detailed system models to quantify system performance under off-nominal operating conditions. For case studies involving aircraft, a six degree of freedom (6-DoF) model was created that can quantify aircraft dynamic response to different failures. While promising when preliminary design knowledge is available, the intent of research question 1 is to estimate risk related requirements in the aircraft conceptual design phase as well. Therefore, another method is needed that can work in the conceptual stage and is generalizable with respect to the varying physical implementations of novel architectures.

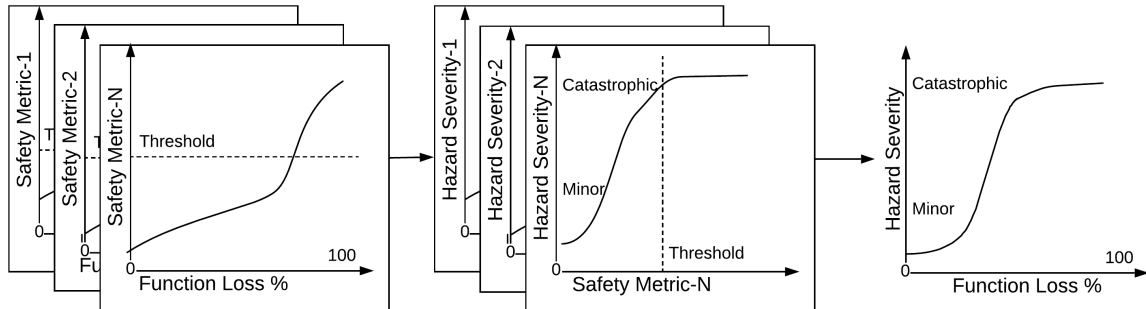


Figure 18: Notional plot of the extended C-FHA process

The functional decomposition of a novel system architecture or technology is likely to remain similar to a conventional system even if the implementation varies drastically between the two. Thus, a method based on loss of function to characterize hazards can be expected to be generalizable regardless of the physical implementation of the aircraft concept. While traditional FHA with its discrete function loss assumption might not suit novel concepts well, the current work utilizes an extension of the Continuous FHA developed by Armstrong [25] in his Ph.D. thesis for the conceptual design stage. This is shown through a notional plot in figure 18. At a high level,

a continuous degradation in the aircraft's functions is postulated, with the effect of such conditions quantified using 'safety metrics' of interest. These safety metrics are ones that can ideally be linked to the severity of the underlying hazards. Once numerous such metrics are computed for a given aircraft level function under different scenarios of degradation, aircraft level continuous function loss can be allocated hazard severity.

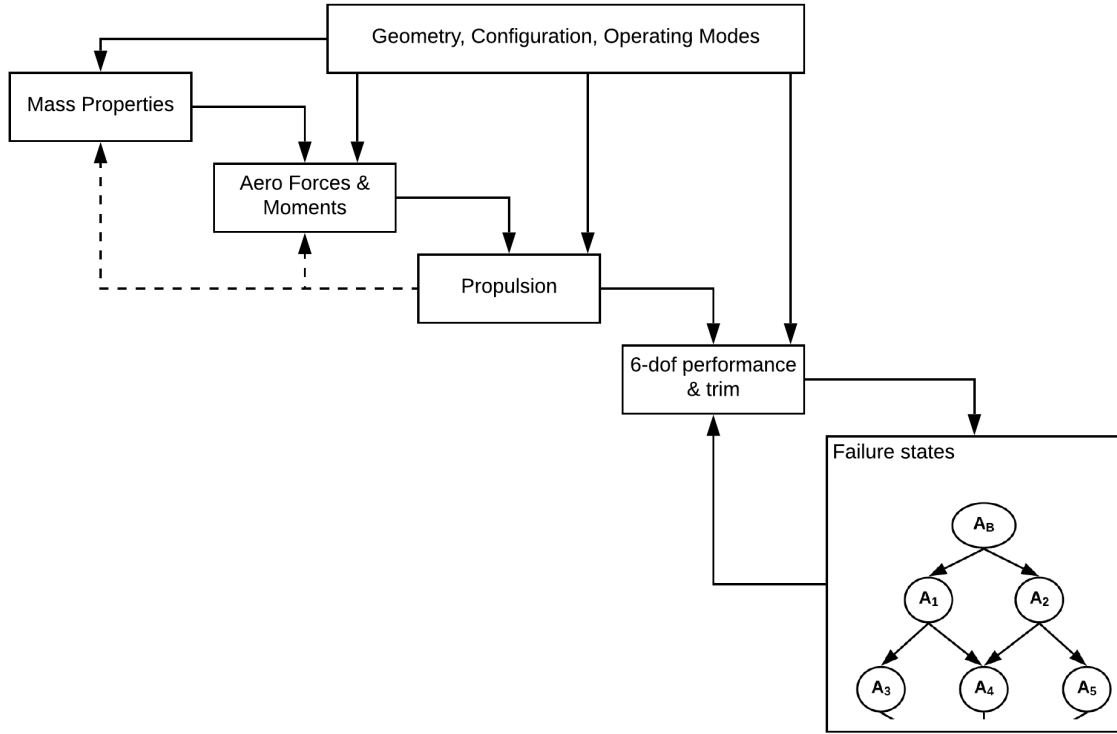


Figure 19: Notional plot of the multistate performance based safety assessment process

Novel aircraft architectures are likely to have different off-nominal operational modes compared to traditional predefined scenarios. In network reliability theory, this is known as a multistate reliability problem, where each component and the system as a whole may have different operational states depending on which node or edge has failed. Thus, the traditional point reliability problem of ensuring compliance of a binary system is replaced with a problem of ensuring that every system state is in compliance with reliability requirements. This piece of the puzzle is solved using a

method similar to multistate system safety assessment using aircraft performance as proposed by Agte [16], and Dominguez-Garcia et al [61]. Figure 19 shows a notional process to conduct a multistate performance based analysis of the system. A preliminary 6-DoF model of the aircraft is created in the early preliminary design stage using available geometry and estimated mass properties and aero-propulsive loads. Different failure states of the system are simulated using this model to obtain trim solutions while capturing safety metrics of interest. These are then used to infer the hazard severity of the different states.

Hypothesis 1: *A hybrid approach utilizing Continuous FHA during conceptual sizing and multistate performance models during preliminary sizing, along with suitable safety metrics and reliability allocation methods, will yield more accurate identification and allocation of off-nominal requirements (than traditional safety analysis methods) for novel aircraft architectures and technologies*

Research Questions 1.1 and 1.2

Two questions immediately follow based on the notional plots in figures 18, 19, and Hypothesis 1. The earlier section explained how extended C-FHA and the multistate performance-based method are facilitated by appropriate safety metrics. However, these methods assume the existence of certain ‘safety metrics’ that can be used to characterize the different off-nominal conditions in terms of their hazard severity. The following two obvious questions can thus be asked, (i) “What are these metrics?”, and (ii) “How can they be used?”. Research question 1 is therefore further decomposed into RQ 1.1 and 1.2 at this stage as follows:

Research Question 1.1:

What metrics can be used with the methods given in hypothesis 1 to identify off-nominal requirements in the conceptual and preliminary design phase?

Research Question 1.2:

How can safety related off-nominal requirements be identified and allocated at the system level during conceptual and preliminary design phases using the previously defined safety metrics?

Formulation of Solutions for RQ 1.1 and RQ 1.2

There is no one-size-fits-all answer to RQ 1.1. A degradation in different functions can have different consequences on the safe operation of the aircraft. For instance, a transport aircraft, whether conventional or all-electric, will have to provide thrust as well as enough fresh air in the pressurized cabin. The failures of these two have different consequences, but both can lead to catastrophic hazards. While a degradation in thrust during take-off may be characterized by multiple metrics such as ‘*required Takeoff Field Length (TOFL)*’ or ‘*climb gradient*’, the function ‘*provide fresh air*’ might only have ‘*available mass flow*’ as a single metric to characterize hazard severity under degradation scenarios.

A thorough literature search conducted with the intent of identifying suitable safety metrics resulted in a few possible solutions. When it comes to quantitative safety analysis of flight operations, literature abounds with metrics for programs like Flight Operational Quality Assurance (FOQA) [67] and Flight Data Monitoring (FDM) [47]. While common and widespread in transport category (14 CFR Part 25) aircraft, metrics and tools to conduct such statistical flight data analyses on normal category (Part 23) airplanes have been of interest in literature. Puranik [150]

Table 3: Potential safety metrics for RQ 1.1

Performance Models	Degraded Function	Safety Metrics
Conceptual	Provide Thrust	TOFL, Max Potential Climb Gradient, ϕ_{max}, n_{max}
Preliminary 6 DoF	Provide Thrust	Max Climb Gradient Aircraft States Aircraft Controls

requires that safety metrics pertinent to GA flight data analysis have three qualities – (i) Parsimony, in terms of the number of metrics defined, as well as the amount of recorded or generated data required to define them; (ii) Safety relevance, to map how these metrics help identify anomalous events; and (iii) Generalizability – to ensure metrics remain comparable across a wide spectrum of GA aircraft classes and operations.

While most of the research to identify metrics that correlate with safety deals with aircraft operations, the intent of this thesis is to identify an appropriate subset of these to be used during conceptual and preliminary sizing to aid safety by design. This requires that these metrics be computed with the limited information or models available in the corresponding phases of design, along with identifying appropriate thresholds which signify deviation from safe performance. Thus, RQ 1.1 is answered through a combination of a literature survey, downselection, and rationalization without the need for an explicit hypothesis for the same. The details of these are provided Ch. 4.2. A brief overview of the metrics implemented in this dissertation is provided in table 3.

Research question (RQ) 1.2 poses a question about the identification and allocation of requirements to the system level using previously defined safety metrics. The solution for this stems from hypothesis 1, where the two methods - an extended C-FHA and multistate performance based safety analysis, are used for this purpose.

However, both these methods rely on appropriate system performance models that can quantify the safety metrics under off-nominal operations. Combined with pre-defined thresholds on these safety metrics using values suggested from certification rules, or just plain logic, these performance models can be used to make a determination of hazard severity of different off-nominal scenarios. Thus, hypothesis 1.2 is stated as follows:

Hypothesis 1.2: *If the identified safety metrics are quantified under off-nominal scenarios using appropriate system performance models, then identification and allocation of safety requirements at the system level can be completed with greater resolution and accuracy than traditional methods*

Research Question 1.3

RQs 1.1 and 1.2 decompose the first research question and deal with the first two requirements posed when RQ 1 was first defined in chapter 3.2. The present research question deals with requirement 3 stated under RQ 1 - the need to allocate hazard severity and allowable failure rate probability to the subsystem and component level.

Research Question 1.3:

How can the identified aircraft level off-nominal requirements be allocated to the unit level?

Formulation of Hypothesis 1.3

The output of hypothesis 1.2 is expected to be a hazard severity allocation to the ‘multistate’ novel aircraft architecture characterized by multiple unique failure states for a given function. For novel aircraft concepts that fall under 14 CFR Part 23 (Normal Category), each hazard severity has an associated maximum allowable failure rate requirement imposed by the FAA and is given in table 2. These requirements

are imposed at the top level and need to be allocated to the component level for any system. This is accomplished in the present work by using a network reliability algorithm that automates a bottom-up analysis to determine the effect of component failures on the platform level functions. A rough idea of how this algorithm works is stated here, along with further details provided in Ch. 4.4. The overarching idea is to determine system level failure states by considering a single component failure at a time. Once a set of all system level failure states is obtained, single component failures that lead to the same state are combined into a logical ‘OR’ statement. The allowable failure probability of the system in the given state, as computed from hypothesis 1.2, is therefore a sum of the individual component probabilities that result in the said state. These are then allocated using a reliability allocation method. This method assumes that component failures are independent of one another and that the probability of multiple components failing at once is much less than the probability of any one component failing.

At the end of the allocation exercise, it is expected that all components of a system architecture will have allowable probability requirements (or reliability requirements) allocated.

Hypothesis 1.3: *If unit level failures are mapped to system level failure states, the allowable failure rate requirements generated at the system level can be allocated to the unit level*

A Note on Uncertainty

Hypothesis 1 which combines extended C-FHA and multistate performance based severity assessment, relies on available performance models to determine the effects of functional degradation on safety metrics in order to characterize hazards and allocate failure rate requirements to the unit level. The last requirement to be satisfied to

completely answer research question 1 needs a quantification of uncertainty due to modeling assumptions. This is accomplished by completing the process laid out under chapter 3.2 for different modeling assumptions and is shown notionally in Fig. 20.

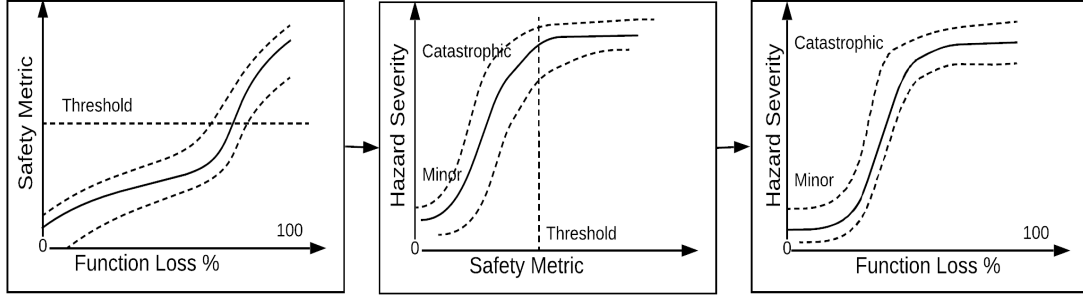


Figure 20: Notional uncertainty propagation during the C-FHA process

Since the safety metrics are computed from functional degradation scenarios using available performance models, the uncertainty in model inputs can be propagated using the same models. This can be achieved by representing modeling uncertainty by distributions in input variables. The resultant output will be a distribution in the safety metrics of interest, which can be used to determine hazard severity by designers as shown notionally in Fig. 20.

Figure 21 provides an overview of the research formulation of research area 1.

3.3 *Research Area 2*

Observation group 2 from chapter 2.5 is concerned with the large uncertainty in quantitative risk assessments of novel aircraft architectures primarily due to the lack of data and experience. The goal of this research area is to provide a solution to this problem using some enablers found in literature.

Research Question 2

It was noted earlier that traditional methods are unable to provide a complete treatment of epistemic uncertainty due to the traditional ‘*frequentist*’ approach. Additionally, the aleatory uncertainty, which is best reduced with abundant data, is

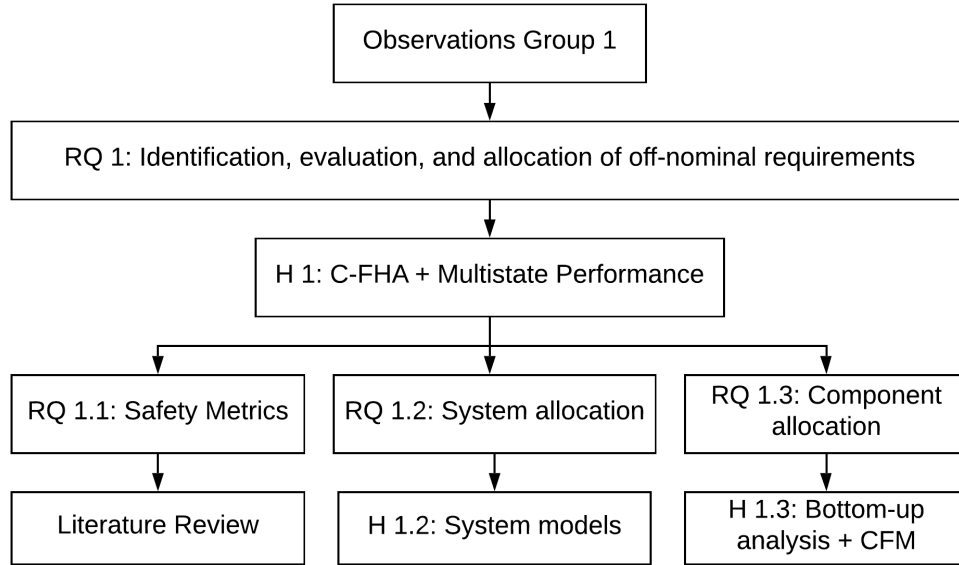


Figure 21: Overview of Research Area 1

large for novel technologies. This leads to the following research question (RQ):

Research Question 2:

What method or group of methods can allow estimation of unit and system reliability - accounting for both epistemic and aleatory uncertainty under scarcity of available data, while also providing a mathematically defensible framework for compliance decision making?

Resultant Requirements It is clear that any solution that tries to answer RQ 2 must account for both aleatory as well as epistemic uncertainty under a scarcity of available data. Additionally, it requires the solution to provide a *mathematically defensible* framework for *compliance decision making*. Thus, the resultant requirements to be met by any potential solution for RQ 2 are as follows:

Requirements:

1. *Ability to estimate unit level probabilities under scarcity of available data*
2. *Explicit treatment of epistemic and aleatory uncertainty*

3. *A mathematically defensible framework for compliance decision making*

4. *Estimation of multistate system reliability*

Research Question 2.1

A solution under consideration can be shown to answer research question 2 if and only if it can meet the requirements above. These requirements can be further grouped into three broad categories. The first deals with the ability to estimate unit level probabilities while providing a thorough treatment of uncertainty under scarce data (requirements 1,2 above). These two can therefore be restated as a smaller research question:

Research Question 2.1:

What method or group of methods can allow estimation of unit level reliability while accounting for both epistemic and aleatory uncertainty under scarcity of available data?

Formulation of Hypothesis 2.1

There are two schools of thought when it comes to defining probability - the ‘*frequentist*’ (objective) and the ‘*Bayesian*’ (subjective). A Bayesian approach of estimating probability allows for the treatment of both epistemic and aleatory uncertainty even when available data is limited. Kaplan and Garrick argue that when faced with insufficient data, there is no choice but to use a Bayesian approach [100]. Instead of only using data, a Bayesian approach relies on using information - which includes data, models, and other available information like subject matter expert (SME) knowledge [58]. Furthermore, a Bayesian inference model can be continuously updated as additional information becomes available. Bayesian inference techniques for safety and reliability assessment have been applied to numerous problems in literature [21, 28, 43, 177] and are considered mature and mathematically sound for the

purpose. The utility of this approach can be attested to when one considers that numerous industries consider these techniques standard [1, 79, 80, 102]. Hypothesis 2.1 is therefore stated as follows:

Hypothesis 2.1: *Utilizing a Bayesian probability framework to model unit level failure rates results in a more comprehensive treatment of both epistemic and aleatory uncertainty under scarcity of available data.*

Research Question 2.2

Once unit level reliability requirements have been allocated using hypothesis 1.3 and Bayesian failure rate posteriors are obtained, the next obvious step is to complete a compliance finding for each component of the architecture of interest. The traditional means of completing this step involves utilizing a point probability value for every component, along with a point probability requirement as stated in table 2. The benefit of a Bayesian framework over a traditional frequentist approach is that it provides a ‘*probability of frequency*’ [100]. A probability distribution (of failure rate for instance), has intrinsic meaning in quantifying uncertainty. This is lost when a simple point estimate is taken of it. Therefore, the next logical question to be asked pertains to whether an advantage of the Bayesian probability framework can be taken when it comes to compliance decision making - so as to not throw away all the gains made in quantifying uncertainty in failure rates by reverting to a point estimate. This is stated as research question 2.2:

Research Question 2.2:

How can mathematically defensible compliance decisions be made without losing the gains made in quantifying uncertainty?

Formulation of Hypothesis 2.2

Compliance finding is often an exercise in decision making under uncertainty. Washington et al. [172] suggest using a Bayesian decision framework for this purpose alongside generated Bayesian probability estimates. Bayesian inference provides a mathematical framework for measuring uncertainty while making decisions using Bayesian probability theory. Input to such a framework are the unit failure rate posteriors which provide the degree of belief in the failure rates of components, along with any requirements on said components. In a Bayesian decision theoretic setup, an action space $a \in A$ represents actions to be taken (in this context: $A = \{\text{'compliant'}, \text{'non - compliant'}\}$). Every action comes with a loss (opposite of utility), which is given by a loss function $L(\theta, a)$. The loss function depends not only on the compliance action taken but also on the (unknown) true state of the component. This true state is estimated using the posterior distribution obtained from hypothesis 2.1. The idea behind a Bayesian decision framework is to minimize the expectation of this loss function with respect to the component posterior failure rate. A decision action a^* (also called Bayes' action), that minimizes this expected loss, is chosen as a compliance action for the given component. Further details of this method are given in Ch. 5.2. Hypothesis 2.2 can thus be stated as follows:

Hypothesis 2.2: *If the posterior expected loss using suitable loss functions can be determined for system components, then the action that minimizes such an expected loss would inform the compliance action to be taken under uncertainty*

Research Question 2.3

With hypotheses 2.1 and 2.2, the part of research question 2 that deals with estimating unit level probabilities under a scarcity of data while characterizing epistemic and aleatory uncertainty, as well as a mathematically defensible framework for unit

level compliance making is complete. All that remains is the requirement to estimate the multistate reliability of novel architectures at the system level. This final research sub-question, once answered, will completely satisfy the requirements necessary to provide a solution for research question 2.

Research Question 2.3:

What method can allow the estimation of multistate system reliability while accounting for both epistemic and aleatory uncertainty under scarcity of available data?

Formulation of Hypothesis 2.3

As stated earlier, novel aircraft concepts are expected to have physical architectures that satisfy at least one aircraft level function using non-traditional solutions (see definition 2.1.1.1). As a result, it can be assumed, without loss of generality, that such configurations will not have the traditional binary failure states for a function or system of interest (operating/failed). Instead, these architectures are likely to have multiple terminal components providing a given function. Consider a distributed electric propulsion aircraft for example. The task of providing thrust is divided between multiple electric propulsors, instead of the traditional usual two. When multiple components help satisfy a system level function, their failures result in the system having multiple failure states. Thus, novel aircraft architectures are likely to have multiple failure states in certain functions of interest. In literature, reliability assessment of systems with multiple failure states falls under the domain of multi-state systems. Multi-state network reliability theory is one of the most developed in this field and therefore, the most promising to provide a solution to the problem at hand. Within the multi-state network reliability paradigm, numerous methods exist to estimate the reliability (analogous to failure rate) of a complex system in its various states [176]. While additional details have been provided in chapter 5.3, a modified Monte Carlo approach seems promising and robust [176]. Therefore, hypothesis 2.3 can be stated

as:

Hypothesis 2.3: *A multistate network reliability approach utilizing Monte Carlo simulations, suitably adjusted to work with Bayesian failure rate posteriors will provide accurate estimation of the system level reliability under uncertainty.*

Figure 22 provides an overview of the research formulation of research area 2.

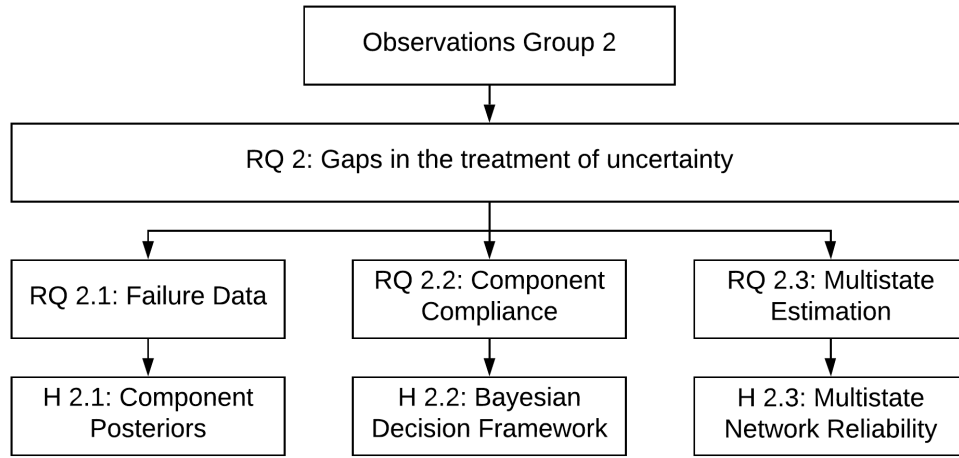


Figure 22: Overview of Research Area 2

3.4 Research Area 3

The intent of research area 3 is to integrate the tools and methods discussed so far into a framework that allows better incorporation of safety related off-nominal considerations into early design stages for novel aircraft architectures.

Research Question 3

The chief takeaway from observation group 3 in chapter 2.5 is the limited scope to incorporate safety related off-nominal requirements into the aircraft design loop during the early design phases. In the overarching research objective of the present thesis, research areas 1 and 2 focus on (i) identifying the off-nominal requirements for novel architectures, (ii) allocating them to the system and component level, and

(iii) enabling compliance decision making at the system and component level under uncertainty. The last remaining objective is utilizing the developed framework to inform design trade studies during the preliminary design stage. With that in mind, research question 3 (RQ 3) is stated as follows:

Research Question 3:

How can design trade studies for novel aircraft architectures and technologies be conducted in early design while incorporating safety related off-nominal scenarios?

Formulation of Hypothesis 3

The resultant framework is intended to integrate the methods utilized to identify and characterize off-nominal hazards with the multi-state reliability assessment and compliance process to evaluate the safety of a novel aircraft architecture. Results from component and system level compliance decision making can be fed back into the design loop, where alternatives can be evaluated. This can be in terms of targeted resizing or re-architecting of the system to improve compliance finding. Providing designers with results of a what-if analysis to make such safety-risk informed decisions is the end goal of the present work. To this end, an integrated framework to evaluate off-nominal requirements and reliability of novel aircraft architectures and technologies is provided in Ch. 3.5.

Hypothesis 3: *The integrated framework given in figures 24 or 70 enables design trade studies while incorporating safety related off-nominal requirements and reliability of novel aircraft architectures in early design*

Figure 23 provides an overview of the research formulation of research area 3.

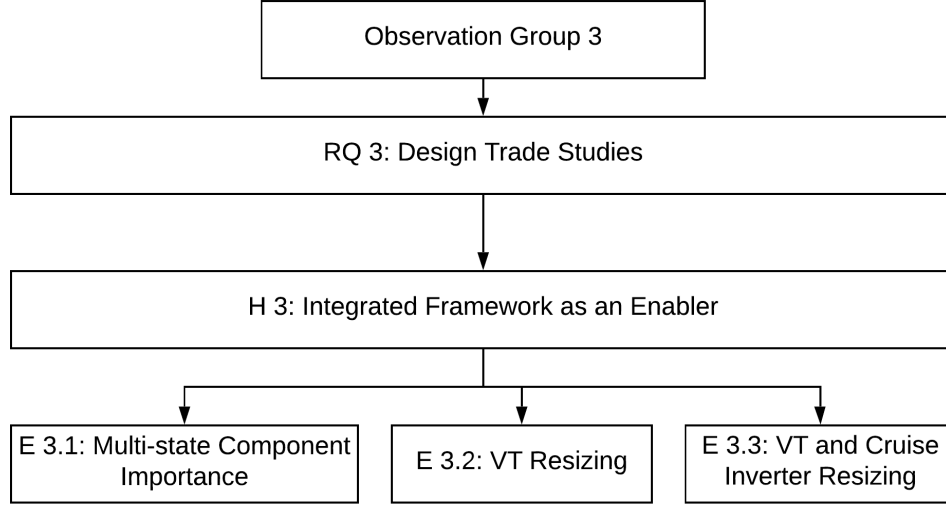


Figure 23: Overview of Research Area 3

3.5 Developed Framework

An overview of the developed framework is provided in figure 24. It is assumed in Fig. 24 that the configuration has been sized – this includes the weight breakdown including mass properties, geometric definitions including wing and other areas including locations of control surfaces if any, architecture definition that includes any redundancy considerations for the internal energy flows of the systems, any available aerodynamics and propulsion models, and finally, any available subsystem sizing details. Depending on the stage of design (conceptual/preliminary), the first task then is to identify a set of appropriate safety metrics of interest for the given architecture. For the conceptual level analysis, adequate models are developed for the functions of interest to characterize the effect of functional degradation on safety metrics. These may include models that can characterize the take-off, climb, cruise, and landing performance in the conceptual design phase. When additional knowledge is available in early preliminary design, this performance model library can be expanded to include aircraft trim and dynamic considerations under off-nominal operating states that the architecture may find itself in. The purpose of these models is to quantify

the change in safety metrics of interest (see Table 3) under functional or component loss scenarios. These metrics are compared with their allowable thresholds that are established based on regulatory requirements, or subject matter expert suggestions to obtain system level functional or multistate availability requirements. These are passed on to the next module to compute component level requirements. A bottom-up network algorithm computes the requirements allocated to the components, followed by a Bayesian safety and decision making framework. The system level multistate reliability is computed along with system level multistate compliance findings. The outputs of the compliance findings are translated to the final part where unit level importance metrics are quantified as an exercise in sensitivity analysis to the component failure rate posteriors. Any geometric trade studies can be conducted by repeating the process after obtaining modified system models. At this stage, the framework can be used to inform design decisions, as well as close the loop to optimize the conceptual sizing using reliability information in a reliability based design optimization (RBDO) loop (beyond the scope of the present work). The outputs of which can be used to inform the late stage preliminary design and onward.

3.6 Test Problem Definition

The framework developed in this work will be thoroughly demonstrated on a test problem. The intent of this section is to characterize the desired qualities in a test problem in order to utilize the results generated and verify all the hypotheses stated so far. It is important that the test problem maintain sufficient complexity and fidelity in order to characterize real life conceptual design problems, while also being simple enough so that the results do not get confounded with other emergent attributes of the system.

Problem Characterization

The integrated framework given in figure 24 needs to be demonstrated on a test

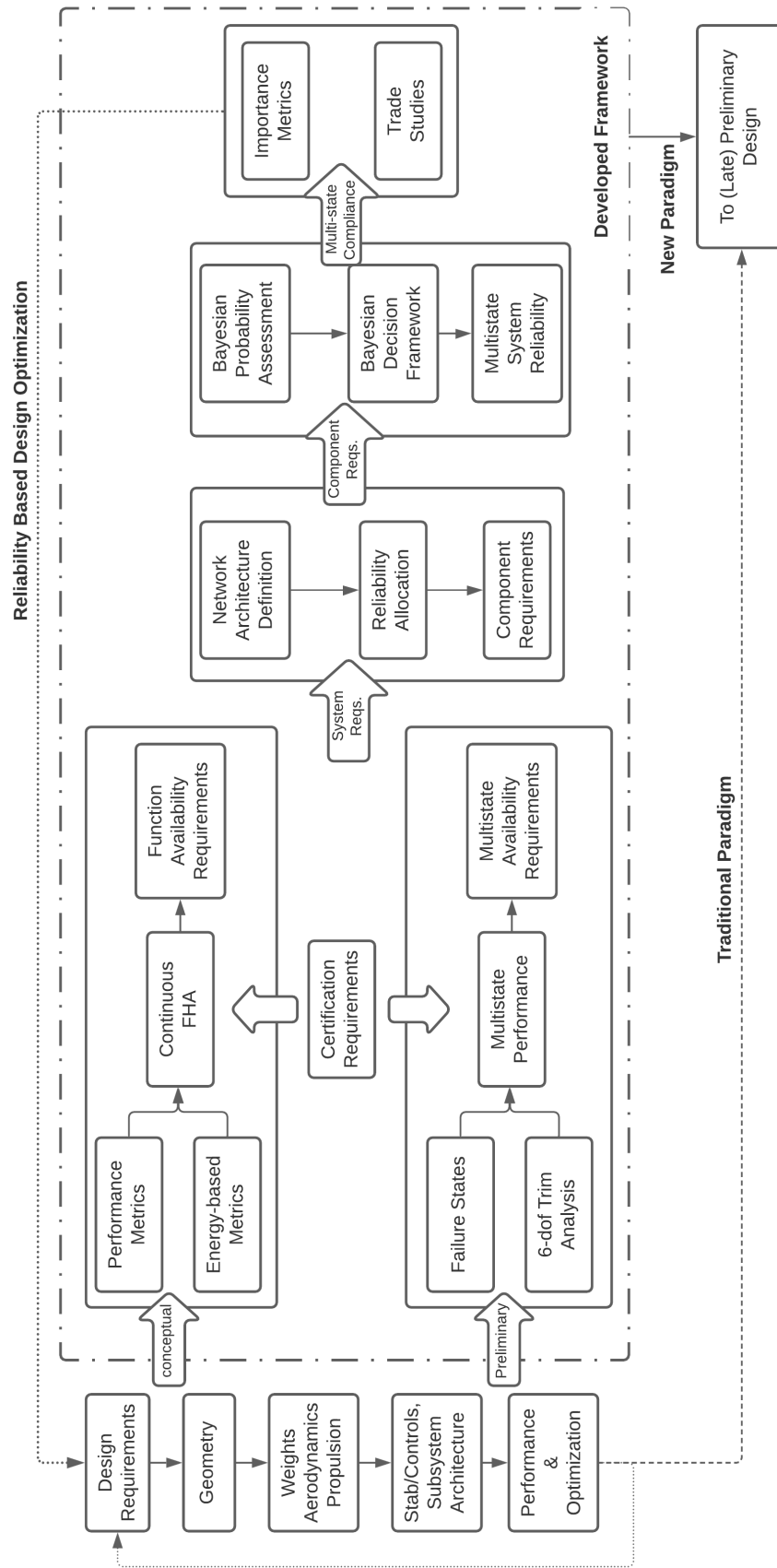


Figure 24: Integrated Framework to Evaluate Off-Nominal Requirements & Reliability of Novel Architectures in Early Design

problem that meets certain criteria. The research objective of this thesis is to enhance the current safety assessment paradigm for novel architectures and technologies. As discussed earlier, novel concepts have a lack of available data or relevant experience for safety assessments. Additionally, due to multiple terminal components utilized to satisfy a top level function in a novel architecture, traditional binary system failure states are replaced with multi-state failure considerations. Finally, the framework aims to inform the early preliminary aircraft design process, which places restrictions on the amount of detail available. Thus, a test problem used to demonstrate this framework needs to satisfy the following considerations:

1. Novel architecture according to definition 2.1.1.1
2. Insufficient safety data - large uncertainty
3. Complex architectural connectivity leading to multiple failure states
4. Design knowledge - conceptual to preliminary
5. Benchmarking results available for comparison

A Test Distributed Electric Propulsion (T-DEP) Aircraft

A test distributed electric propulsion architecture (T-DEP) aircraft inspired by the X-57 is chosen as a test-case aircraft to demonstrate the proposed method. The X-57 *Maxwell* is an experimental aircraft designed to demonstrate a 3.5 times aeropropulsive efficiency gain at a “high-speed cruise” flight condition for comparable general aviation aircraft by effectively utilizing propulsive airframe integration (PAI), made practical due to the progress made in electric propulsive powertrains [52]. To build the X-57, a Tecnam P2006T airframe is to be modified with a higher aspect ratio wing, with two main propulsive electric motors installed at the wingtips to power the cruise propellers. Another 12 electric motors in nacelle-pylons will power the

high lift propellers distributed across the wing leading edge. This Distributed Electric Propulsion (DEP) architecture is expected to provide a higher dynamic pressure during takeoff and landing while providing more efficient aero-propulsive performance during cruise. Overall, the X-57 is expected to achieve a five times lower energy use than the Tecnam P2006T [55].

It is easy to demonstrate that the T-DEP aircraft modeled on the X-57 meets the definition provided for novel aircraft architectures (see Def. 2.1.1.1). The distributed electric propulsors along with wing-tip cruise motors provide a novel architectural solution for the aircraft level function of ‘Provide Thrust’. Similarly, the twelve high lift propulsors also augment the aerodynamic characteristics, specifically the lift generated by the wing, and therefore act as high-lift devices (in addition to the presence of flaps). This provides a novel solution to the aircraft level function of ‘Provide High Lift’ during takeoff or landing, with wing flaps being the traditional choice of physical solution to provide that function.

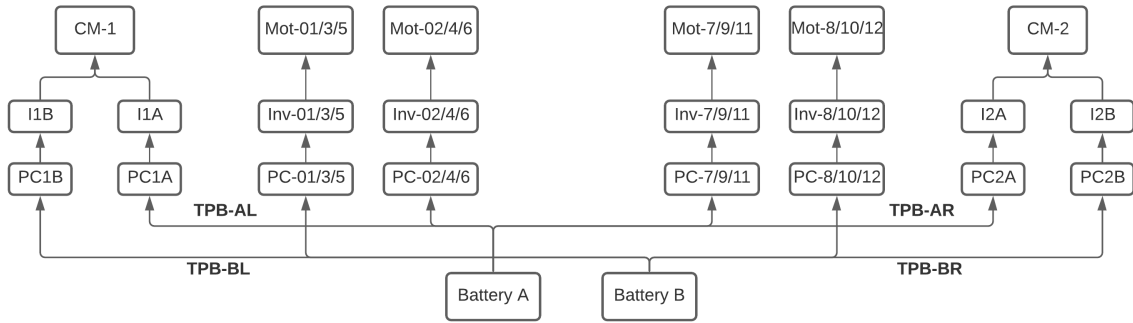
Being a novel DEP concept, there is limited data regarding the reliability of electrical systems of such an aircraft, leading to large uncertainty. The modeled T-DEP aircraft simplifies the design detail publicly available for the X-57, and can be considered to be at the preliminary stage (see Ref. [132] for details). In addition to the novel technologies being tested with the X-57 program, of interest in the present work are the tools and methods used to conduct a safety analysis of such transformational aviation concepts. Research in this direction available in literature points towards the utilization of traditional methods or early conceptual analyses to assess safety [52, 145, 147, 174].

The DEP architecture is the novel feature of the test aircraft considered in this dissertation. Having multiple propulsors, the effect of one or more propulsors failing must be considered to assess the safety of the aircraft. Each cruise motor can fail at either 50% thrust, or 0%, while each high lift motor has a binary failure mode. As a

result, the total number of failure states of the T-DEP aircraft propulsion architecture is $3^2 \cdot 2^{12} - 1 = 36861$. Discounting for symmetry in the XZ plane, these become 18431 unique failure states – a number large enough to cause difficulty in conducting a traditional safety analysis comprehensively. Therefore, the modeled aircraft, in particular, its traction power system architecture meets all the requirements stated under the problem characterization above and forms the test problem for the current work.



(a) The X-57 (credit: NASA)



(b) The T-DEP aircraft power system representative diagram (Adapted from Ref. [52])

Figure 25: Test problem concept and architecture

The simplified power system of the T-DEP aircraft is inspired by the X-57. Its components and connectivity are shown in figure 25 and have been adapted and simplified from Clarke et al. [52]. It has two main batteries, traction buses, pre-chargers, and inverters supplying 30 kW each (half of the required cruise power)

to the wing-tip cruise motors. Similarly, each battery bus supplies three high lift motors on either side of the wing, providing good redundancy. The X-57 traction power system has been designed using a combination of available standards and best practices since the traditional 14 CFR Part 23 and Part 25 provide little applicable guidance for electric power systems [52]. Clarke et al. [52] also performed a traditional safety analysis (FMECA¹) on this system, including all permutations of cruise or high lift motors failing. Since multiple failure modes of any component have the same effect at the system level, only single-point top level failure modes of the components were considered. Their results show two primary critical failure scenarios – (i) asymmetric thrust due to cruise motor failure, and (ii) in-flight battery fire. While the former results in an untrimmable yawing moment using the stock rudder, the latter can result in total power loss and catastrophic structural failure. Both of these are potentially unrecoverable for the pilot. Additionally, Ref. [52] provides a failure scenario matrix providing criticality of single component failures. These results will therefore be utilized to benchmark the performance of the severity assessment method presented in the current work.

Chapter 4 up next deals with the first research area in greater detail, while chapters 5, and 6 discuss the second and third research area in greater detail. The experiments conducted in this thesis are not discussed in the present chapter. Instead, they are discussed in the chapters that discuss the details of every research area. This is to allow sufficient discussion on designing the correct experiments for the research questions and hypotheses of interest while providing enough technical background on the test problem at hand.

¹Failure Modes, Effects, and Criticality Analysis

CHAPTER IV

EXTENDED C-FHA AND PERFORMANCE-BASED MULTISTATE ANALYSIS

This chapter presents the work on the first research area which deals with identification, characterization, and allocation of safety related off-nominal requirements. This particular research area is motivated by observations group 1 (see Ch. 2.5). To recap, it was discussed how traditional FHA considers the discrete loss of function or malfunction scenarios, while assumptions during traditional PSSA can lead to inaccurate estimation of off-nominal requirements. These issues are especially pertinent for novel aircraft architectures, where the imagination of failure might be limited due to lack of experience, and where traditionally postulated off-nominal scenarios might not capture the safety space accurately. These considerations led to the first research question (RQ), which is restated below:

Research Question 1:

What method or group of methods can enable identification, characterization, and allocation of safety related off-nominal requirements for novel aircraft architectures and technologies in the conceptual and preliminary design stage?

Literature to deal with identifying off-nominal conditions in novel concepts or technologies converges on the need to utilize system performance or dynamic models for this purpose. Methods in literature that take this approach to reliability can be broadly classified into five categories.

Model Based Dependability Analysis (MBDA) techniques synthesize dependability information from system models automatically [98, 99]. This is typically accomplished by automatically generating fault trees (FTs) and failure modes and effects analysis (FMEA) tables using system models that have been annotated with failure information, including the modes in which each component fails, and their probabilities [138, 139, 141, 142, 171]. While these help to automate the task of conducting analysis during the preliminary system safety assessment (PSSA), they do not explicitly deal with the challenges faced by novel technologies, viz. the lack of knowledge or experience regarding their off-nominal scenarios.

Dynamic Probabilistic Risk Assessment (DPRA) was developed over a decade between 1981 to 1992 to evaluate nuclear reactor safety [17, 20, 57]. It involves utilizing a dynamic-behavioral model of the system along with Markov chains to model the stochastic transitions that take place between system configurations as components fail. However, this method presumes a coupling between system dynamic variables and stochastic transitions between component failures - an assumption that is unnecessary given aircraft failure states pan out over time periods of seconds, and the probability of multiple components failing in that time duration is very small. This makes the mathematical formulation of DPRA needlessly complex for aircraft problems [61].

In fault tolerant computing systems, ‘Performability’ analysis deals with quantifying system performance degradation due to faults and their interactions with the overall system [29, 126]. Meyer coined the term ‘Performability’ to denote a unified treatment of performance and reliability while providing a probabilistic framework to jointly model the two [127]. In it, a reward, based on the system’s performance is assigned to every state of the Markov chain. While promising, this technique needs modifications in the reward function to deal with aircraft systems applications.

Armstrong proposed Continuous Functional Hazard Assessment (C-FHA) instead

of traditional FHA to explore the effect of the magnitude of function loss on hazard severity [25]. Since it works at a functional level, this method is well suited to be applied during the conceptual design phase, when not much is known in terms of the detailed subsystem architecture. While it was used to determine optimal load shedding schedules under degradation, it shows promise to be applied to novel concepts in the current work.

Finally, Domínguez-García and Agte developed a method to utilize elements of Performability analysis, viz Markov rewards models, but with reward functions given by differential equations related to aircraft performance metrics to model multistate system reliability using dynamic performance models [15, 16, 60, 61]. These methods utilize Markov Analysis and are therefore restricted by its limitations of an exponentially growing state-space as the size of the system being analyzed increases.

Of these five broad techniques that utilize system performance under off-nominal situations to infer hazard severity, the last two – C-FHA and multistate system performance analysis seem to fit the requirements generated from RQ 1 and provided in chapter 3.2. In their implementation in the present work, they are modified to better suit the research objective and are explained in the following sections.

4.1 Methods

4.1.1 Extension to C-FHA

The functional decomposition of a novel system architecture or technology is likely to remain similar to a conventional system even if the implementation varies drastically between the two. For example, an airborne system is likely to have a function “*Provide Thrust*” to overcome drag and translate, or “*Provide Lift*” to stay airborne irrespective of whether it is a conventional tube and wing aircraft, or a Distributed Electric Propulsion (DEP) concept. Traditional FHA utilizes this knowledge to keep implementation and behavioral spaces independent while characterizing hazards [26].

While traditional FHA considers discrete off-nominal scenarios like (i) Excess function, (ii) Loss of function, (iii) Incorrect operation of function, these scenarios might not be enough to explain off-nominal conditions faced by novel architectures. It can become important to differentiate between magnitudes of function loss in terms of continuous functional degradation.

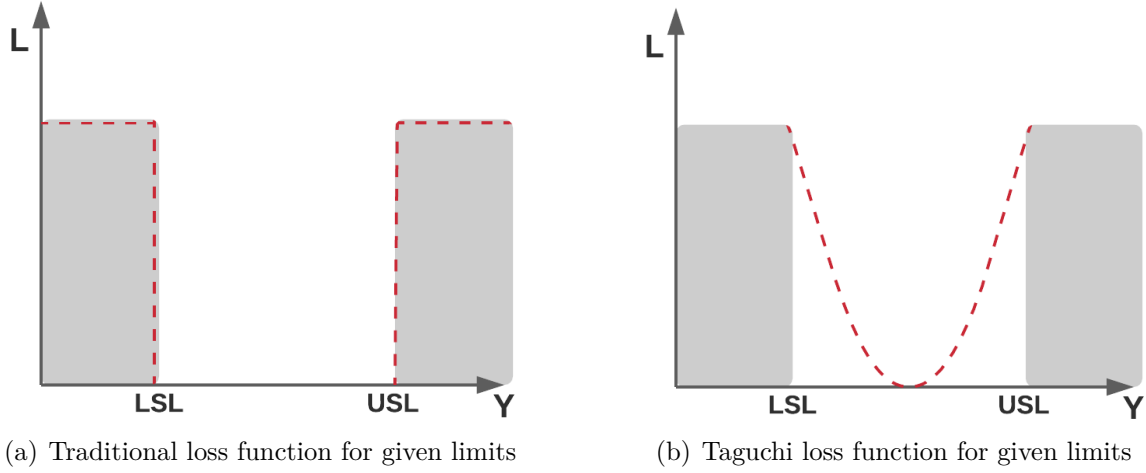


Figure 26: From traditional loss to Taguchi loss (adapted from [25])

Armstrong made a case for Continuous FHA (C-FHA) to assign a continuous hazard severity to a continuous functional degradation scenario [25] while looking at load shedding optimization under off-nominal scenarios. He compared the C-FHA approach to Taguchi’s loss function approach in quality control and robust design, where a traditional step loss function is replaced by a continuous one. This is represented notionally in figure 26. Taguchi’s idea was to minimize the loss of design variance in terms of cost, while Armstrong used a continuous representation of functional hazard to inform load shedding optimization by minimizing hazard risk for the more-electric aircraft [25].

The present work utilizes this approach in a different sense to optimizing the load shedding capability of the system. Novel architectures by definition, are likely to have unique solutions for satisfying aircraft level functions by definition. More often than not, this involves distributing the satisfaction of these functions to multiple terminal

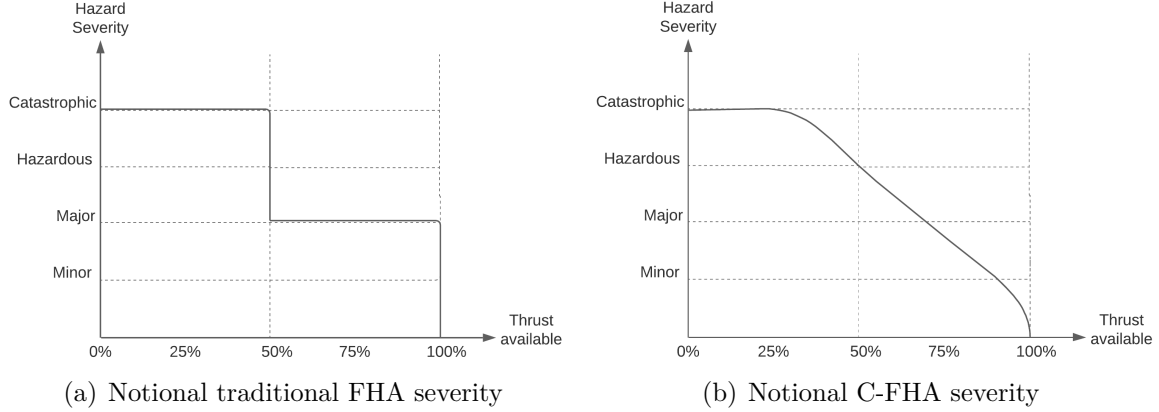


Figure 27: Notional hazard severity - from traditional FHA to Continuous FHA

components (energy sinks) as opposed to the traditional one or two. Therefore, a failure in a subset of these terminal components is likely to result in a near-continuous degradation in the function performed. For example, consider a distributed electric propulsion system with 16 propulsors. The satisfaction of the function ‘generate thrust’ is now the responsibility of 16 terminal propulsors, as against a traditional two. Losing 4 out of 16 propulsors may result in a 25% loss of thrust, while losing 8 out of 16 may result in a 50% loss of thrust. While both of these situations would fall under *Partial thrust loss* under the traditional FHA paradigm, both these situations will result in different system responses and hazard severity.

Continuous FHA allows the characterization of such continuous degradation scenarios by assigning a continuous hazard severity to them as is shown notionally by figure 27. Even within the case where 4 out of 16 propulsors fail, the system response may be different based on which specific propulsors fail. Four outboard propulsors failing on the same side of the wing are likely to cause a more severe hazard compared to two each failing symmetrically due to lateral stability considerations. C-FHA extends the traditional FHA to consider the magnitude of function loss while assessing an architecture.

The present work extends C-FHA to involve the number of terminal component

failures in evaluating the failure states and consequences of novel multistate architectures ¹. Once a hazard severity is defined as a result of continuous function degradation, the allowable failure rates necessarily follow an inverse trend (as is also seen in table 2 in chapter 1). This now means that reliability needs to be redefined as a multi-state reliability – in terms of the capability or probability of a system’s ability to perform a given degree of a function. In the above example of a distributed electric propulsion architecture, the probability of 8 out of 16 propulsors failing would generally be lower than the probability of 4 out of 16 failing. In such a case, the architecture will have a different probability of providing (reliability) 50% thrust as compared to its probability of providing 25% thrust.

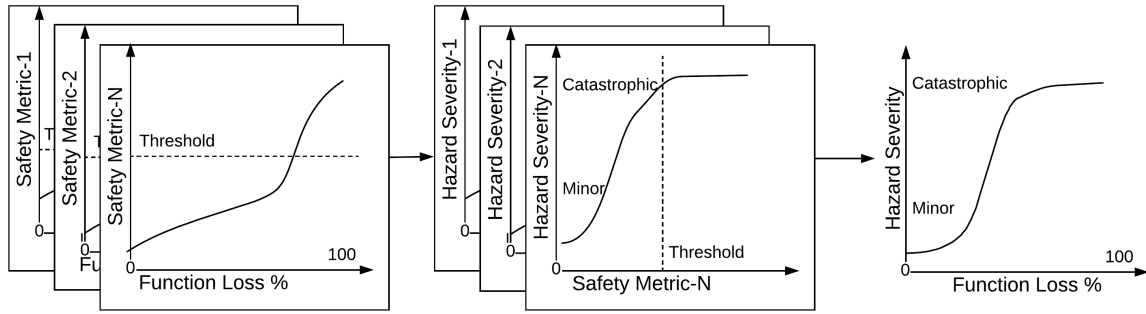


Figure 28: Notional plot of the extended C-FHA process

The extension to C-FHA in the present work can be notionally explained through Fig. 28. As a first step, the analyst establishes safety critical metrics of interest for different functions and different flight phases. Next, the effect of functional degradation scenarios on the established safety metrics is determined using appropriate performance or simulation models. Typically, every such metric is likely to have a threshold, which when crossed represents a safety concern. Therefore, the analyst is required to define continuous hazard severity as a function of variation in the established safety metrics. Decision makers can then utilize this knowledge to combine the different hazard severity curves into one *most conservative* hazard severity curve for

¹This approach has been demonstrated by the author in prior work [30,34]

the function under consideration for the flight phase of interest. This is shown in the first part of Fig. 28. This final hazard severity - function loss curve now provides a physics backed relationship between the two, as opposed to a heuristic and case-by-case approach provided by traditional FHA. Finally, this process must be repeated for a given function at each mission phase and expected off-nominal scenarios.

$$SM_i = Fn(F_{degraded}, A, Op) \quad (15)$$

$$H = Fn(SM_i, SM_{threshold}, A, Op) \quad (16)$$

$$Op = \{altitude, Mach, configuration, \dots\} \quad (17)$$

Thus, the safety metrics are computed as a function of degradation in aircraft function, aircraft architecture, and operational scenario as given in Eq. 15. When a threshold value for these safety metrics is established, it can be used alongside the computed metrics to determine the hazard severity given in Eq. 16. Such a C-FHA curve can be generated for every aircraft level function of interest under different flight conditions. Once these hazard severity curves are generated, the allowable failure rate requirements necessarily follow an inverse trend as mentioned earlier. These requirements are allocated to the aircraft at a functional level and need to be allocated down to the system and subsystem or component level – a problem that will be dealt with later. Selecting appropriate safety metrics, and defining hazard severity as a function of these safety metrics are the only two steps an analyst is required to perform manually *a priori* in the current method. However, it is important to note that hazard severity requirements eventually collapse from their continuous form to step functions mandated by regulations which designers have little power to change. They are generally categorized into four significant, discrete categories - i) Minor, ii) Major, iii) Hazardous, and iv) Catastrophic [8]. Therefore, even after using a continuous curve for hazard analysis, the final system level allocation must, due to

regulations, be discrete.

4.1.2 Performance-based Multi-state Analysis

C-FHA utilizes conceptual level system performance models to characterize hazard severity. When higher fidelity models and greater design knowledge is available, 6 degrees of freedom (6-DoF) system models can be used to inform the severity of off-nominal conditions. The second method in this thesis is inspired by the work of Domínguez-García and Agte who developed a method to utilize Markov chains to compute aircraft state transitions as one or more components fail [15,16,60,61]. They augmented the Markov reward functions with performance metrics from aircraft 6-DoF models to determine safe and unsafe aircraft characteristics for every system state identified in the Markov chains. While they generate results to estimate nominal and off-nominal states, they do not explicitly translate these performance characteristics into hazard severity and therefore reliability requirements. Instead, they identify system availability and unreliability as a function of time, while not dealing with the problem of requirements allocation at the system and component level.

Figure 29 was first introduced in chapter 3.2 and is reproduced here to provide a notional overview of what this method entails. A detailed model of the aircraft that combines aircraft geometry and configuration details with mass properties and aero-propulsive forces and moments to generate a 6-DoF trim analysis capability is developed for this method. The intent is to simulate each unique system state under consideration to determine the capability of the aircraft while maintaining trim conditions. These trim solutions are used in conjunction with engineering judgement and certification requirements to characterize the severity of different system states. Similar to C-FHA, this method seeks to quantify performance metrics of interest and compare them against a threshold to determine hazard severity. The difference is the utilization of higher fidelity (6-DoF) models to conduct trim analysis under failures.

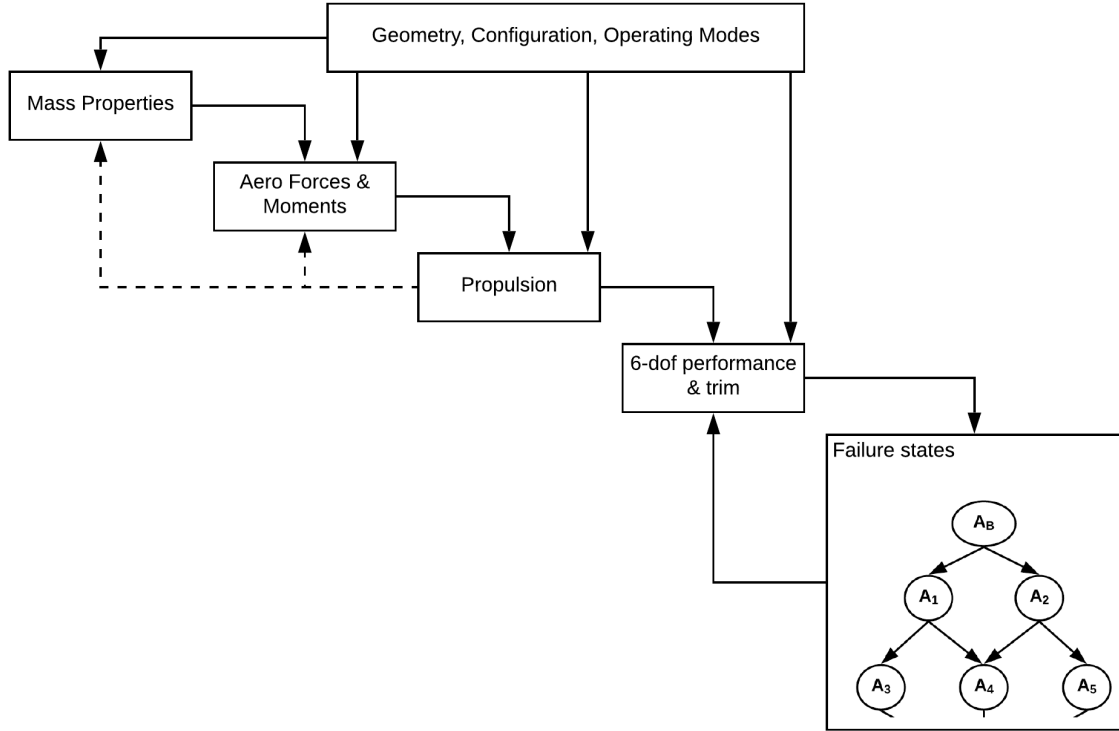


Figure 29: Notional plot of the multi-state performance based safety assessment process

Therefore, developing models that can simulate the system in its different states, and identifying metrics that can be used to characterize hazard severity are the two precursors to successfully implementing this method.

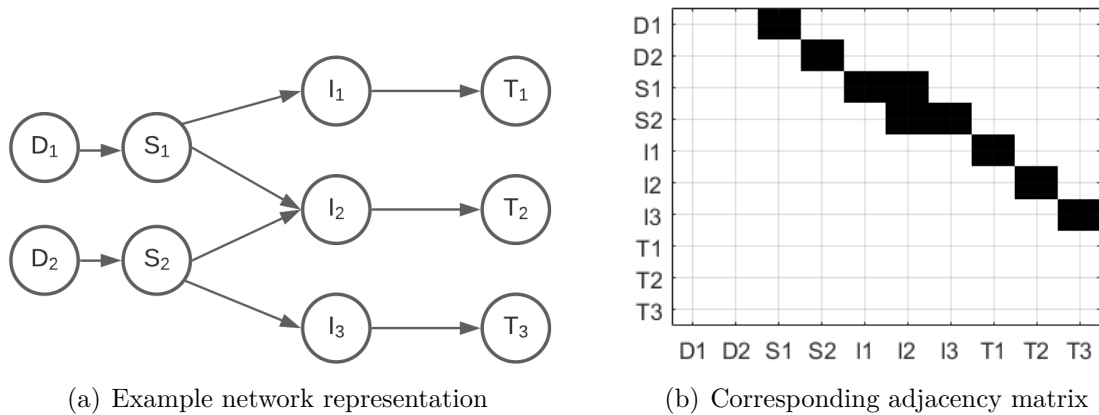


Figure 30: An example system with two sources and three terminal components in network representation

The last block in figure 29 denotes the system failure states identified and simulated using the generated 6-DoF aircraft model. In the present method, system states is a term borrowed from Markov analysis where different failure states are called Markov states. Presently, these states refer to failed system configurations when one or more of the terminal components that provide a system level function fail.

As an example, consider a system with two sources and three sinks as shown in figure 30(a). In an aircraft, these can be represented by batteries (sources of energy), and propulsors (sinks that satisfy system function ‘Provide Thrust’). Dummy components D_1 , D_2 have been added to the system for the purpose of computing system reliability as will be discussed in Ch. 5.3, and can be ignored in the following discussion. The system level function is provided by the three terminal components T_1 , T_2 , T_3 shown. The source components S_1 , S_2 redundantly supply the intermediate component I_2 , while I_1 and I_3 are supplied by a single source. Such a system architecture can be represented as a binary adjacency matrix as shown in figure 30(b), with dark spaces showing the positions of ‘1’s. At the system level, the function under consideration is being satisfied by just three terminal components - T_1 , T_2 , and T_3 . Assuming each of these has a binary operational state of operational or failed, a total of 7 unique failure states result at the system level function. These are given in the first column of table 4. The system states can be a result of different components, or a combination of components failing and is given by the second column. The corresponding probability of the system entering said failed states is given by the third column and is of interest in the problem of multi-state reliability calculation that will be discussed in Ch. 5.3. The idea of the last block in figure 29 is to identify such unique states so that they can be simulated by the aircraft 6-DoF model to obtain their trim performance. The obtained performance metrics are then used to determine the hazard severity for each one of these states.

Table 4: System states, minimal cut sets, and probability for Fig. 30

System states (T_i failed)	Causal factors	Probability
T_1	S_1 or I_1 or T_1	$p(S_1)+p(I_1)+p(T_1)$
T_2	I_2 or T_2	$p(I_2)+p(T_2)$
T_3	S_2 or I_3 or T_3	$p(S_2)+p(I_3)+p(T_3)$
$T_1 \& T_2$	$(S_1 \text{ and } I_2) \text{ or } (I_1 \text{ and } I_2)$ or $(S_1 \text{ and } T_2) \text{ or } (I_1 \text{ and } T_2)$ or $(T_1 \text{ and } T_2) \text{ or } (I_2 \text{ and } T_1)$	$p(S_1).p(I_2) + p(I_1).p(I_2)$ $+ p(S_1).p(T_2) + p(I_1).p(T_2)$ $+ p(T_1).p(T_2) + p(I_2).p(T_1)$
$T_2 \& T_3$	$(S_2 \text{ and } I_2) \text{ or } (I_3 \text{ and } I_2)$ or $(S_2 \text{ and } T_2) \text{ or } (I_3 \text{ and } T_2)$ or $(T_3 \text{ and } T_2) \text{ or } (I_2 \text{ and } T_3)$	$p(S_2).p(I_2) + p(I_3).p(I_2)$ $+ p(S_2).p(T_2) + p(I_3).p(T_2)$ $+ p(T_3).p(T_2) + p(I_2).p(T_3)$
$T_1 \& T_3$	$(I_1 \text{ and } I_3) \text{ or } (I_1 \text{ and } T_3)$ or $(I_3 \text{ and } T_1) \text{ or } (T_1 \text{ and } T_3)$	$p(I_1).p(I_3) + p(I_1).p(T_3)$ $+ p(I_3).p(T_1) + p(T_1).p(T_3)$
$T_1 \& T_2 \& T_3$	$(S_1 \text{ and } S_2) \text{ or } \dots$ (3x terms)	$p(S_1).p(S_2) + \dots$ (3x terms)

The first hypothesis considers the two methods discussed above and is restated here

Hypothesis 1: *A hybrid approach utilizing Continuous FHA during conceptual sizing and multistate performance models during preliminary sizing, along with suitable safety metrics and reliability allocation methods, will yield more accurate identification and allocation of off-nominal requirements (than traditional safety analysis methods) for novel aircraft architectures and technologies*

4.2 Safety Metrics

The extended C-FHA and multistate performance based methods both rely on the identification and evaluation of suitable metrics, termed ‘safety metrics’ to quantify hazards. This leads to the first research sub-question that is restated here:

Research Question 1.1:

What metrics can be used with the methods given in hypothesis 1 to identify off-nominal requirements in the conceptual and preliminary design phase?

As noted in chapter 3.2 under the formulation of solutions for research question 1.1, there is no one-size fits all answer for the appropriate safety metrics to be considered in the above mentioned methods. Novel concepts can vary in their novelty regarding the physical architectural solutions for different functions. Therefore, different metrics may have to be used depending on the architecture of interest.

The first quality that any metrics considered for this problem have is safety relevance. They must correlate well with safety for the mission segments they are considered. Additionally, it would be preferred if they provide not just a binary distinction of ‘safe’ versus ‘unsafe’, but also provide an understanding of the extent to which a condition is unsafe. Although different metrics may be used for different architectures, it would be favorable to have some homogeneity in their definition and use. As a second quality to have, it would be favorable if these metrics be as generalizable as possible. Due to the wide architectural diversity expected in novel aircraft concepts, it is important that the safety metrics identified be comparable across a wide range of aircraft sizes, architectures, and operations.

The test problem of interest in the present section is the T-DEP power systems architecture that provides power supply to the two cruise motors and the twelve distributed propulsors. For the present section, solutions to research question 1.1 are drawn from an extensive literature survey of criteria or metrics that are traditionally correlated with safety for the function ‘*Provide Thrust*’. Literature review for this exercise focuses on two broad areas – i) Metrics used in the safety analysis of flight operations, and ii) Metrics used in preliminary aircraft and system safety assessments using performance models.

4.2.1 Metrics from Flight Operations

Literature related to flight operations data analysis abounds, especially in commercial aviation, with metrics for programs like Flight Operational Quality Assurance (FOQA) [67] and Flight Data Monitoring (FDM) [47]. An unstable approach is a major cause of aircraft accidents (see fig 5). An unstable approach may lead to landing short, runway overruns, or hard landings. The FAA requires a stabilized approach to have a constant rate of descent and constant angle near the touchdown point, among other things [71]. These lead to stabilized approach criteria (SAC) that have been widely studied [129, 162]. Some of the important parameters in SAC, and summarized by Puranik [150] are

1. Descent altitude and profile
2. Airspeed
3. Rate of descent
4. Configuration settings
5. Power settings
6. Track angle

Exceedances are another set of criteria currently in use in the analysis of flight operations. It is the deviation of a parameter beyond a predefined threshold. When multiple parameter exceedances occur concurrently, it is called an Event. Typical flight parameters utilized for exceedance detection include [150].

1. Vertical speed
2. Bank angle
3. Pitch angle

4. Vertical g-loads
5. Oil temperature and pressure
6. Fuel quantity
7. Cylinder head temperature

It is clear from the above lists that not all these metrics satisfy the generalizability requirement. For instance, exceedances in oil pressure, fuel quantity, and cylinder head temperature are not applicable in most novel electric propulsion aircraft that are expected to form a bulk of novel architectures. Metrics like airspeed or rate of descent can be dependent on the size of the aircraft, and may not be comparable across the board. Energy based metrics are another class of metrics that solve this issue by providing a weight specific energy state characterization of the aircraft.

Energy Metrics

Originally used for fighter aircraft performance [46, 156, 178], energy metrics have been used in cockpit displays to improve pilot awareness [19, 77, 170], in trajectory optimization of unmanned vehicles [23], in energy based control systems [105, 107, 108] among numerous other studies. Puranik [149] suggested 19 energy metrics for retrospective safety analysis of flight operations during takeoff, approach, and landing. These typically include specific potential, kinetic, and total energy, their rates, and their errors with respect to a reference profile. Figure 31 provides an overview of these energy metrics.

The energy metrics given in figure 31 primarily compute the aircraft's weight specific mechanical energy, specific excess power, or its variants. Of these, when used during conceptual design, the specific mechanical energy metrics (kinetic/potential) are a function of the aircraft operational state and are assumed rather than calculated using flight data. Only the metrics that can be computed from performance models in the right column are relevant during conceptual design. If a simulator model that

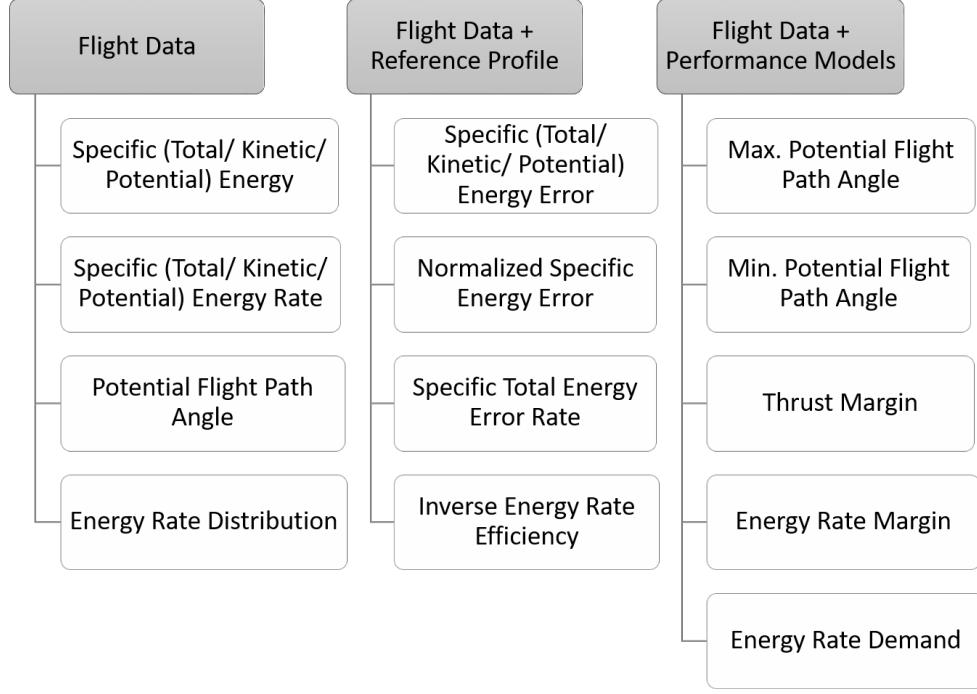


Figure 31: Summary of energy metrics utilized in GA flight data analysis (Adapted from Ref. [150])

can simulate the flight profile under off-nominal states is available, the complete set of metrics may be utilized. For the present work, it is assumed that a complete flight simulator is unavailable, and only a preliminary 6-DoF model to conduct aircraft trim analysis in the presence of failures is available. Some of these metrics are provided below to aid further discussion –

Maximum Potential Flight Path angle is a theoretical maximum flight path angle attainable by the aircraft under maximum available thrust at the current speed and configuration [150].

$$PFPA_{max} = \frac{T_{max} - D}{W} \quad (18)$$

In the present work, this metric can be computed for different system failure states and provides a surrogate for available specific excess power if the pilot were to apply maximum throttle. This is achieved by replacing the T_{max} term with a $T_{max,available}$ term to represent that maximum thrust available might not be equal to the aircraft's

theoretical maximum thrust post failure. $PFPA_{max}$ can then also be used in computing the climb gradient under different loss of thrust scenarios.

Maximum Potential Climb Gradient (MPCG) can be obtained from $PFPA_{max}$ in light of the test problem for this thesis - the T-DEP power architecture, as a more intuitive and direct metric that can be compared to certain certification requirements.

$$\gamma_{max} = \arcsin(PFPA_{max}) \quad (19)$$

Minimum Potential Flight Path Angle is a theoretical minimum attainable at ideal thrust computed at current configuration settings and velocity [150].

$$PFPA_{min} = \frac{T_{idle} - D}{W} \quad (20)$$

Thrust Margin (TM) is a term that computes the margin between currently required thrust to the maximum available at the current flight condition [150].

$$TM = 1 - \frac{T}{T_{max}} \quad (21)$$

While it provides an indicator of the percentage of available thrust being utilized in a given scenario, it does not directly provide a comparable insight into the capability of aircraft.

Energy Rate Margin (ERM) is a better indicator of the capability of an aircraft to get out of trouble caused due to a low energy state. To that extent, it provides a better metric than TM which does not tell much about its impact on the aircraft energy state. ERM is defined as the ratio of actual specific excess power (P_S) to the theoretical maximum specific excess power that is provided at maximum thrust [150].

$$ERM = \frac{W (\sin(\gamma_a) + \frac{\dot{V}_a}{g})}{(T_{max} - D)} \quad (22)$$

$$= \frac{W \sin(\gamma_{max})}{|T_{max, degraded} - D|} \quad (23)$$

In the present work, ERM is used under various loss of thrust scenarios. In such off-nominal conditions, T_{max} is replaced by $T_{max,degraded}$ to indicate it is the degraded maximum capability available to the aircraft. A value less than -1 indicates that the aircraft is rapidly losing energy height and has no means of making P_S positive or even 0 – a potentially catastrophic situation. Similarly, during takeoff or climb conditions, ERM is positive between 0 and +1. A value closer to +1 indicates that the aircraft is operating close to its maximum power setting available and has little room to improve performance further. Whereas, a case when $-1 < ERM < 0$ in climbing or cruise segment might indicate the aircraft is limited by the control authority/trim penalty and cannot fully utilize the thrust available post failure.

Energy Rate Demand (ERDm) denotes the maximum energy that can be dissipated by the aircraft at the current speed and configuration [150]. When descending, it is given by

$$ERDm = \frac{W(\gamma_c + \frac{\dot{V}_e}{g})}{T_{idle} - D} \quad (24)$$

and while climbing, it is given by

$$ERDm = \frac{W(\gamma_c + \frac{\dot{V}_e}{g})}{T_{max} - D} \quad (25)$$

This metric is typically between 0 and 1, and when greater than one represents that the commanded trajectory is untenable. A downside of this metric is that it requires a commanded (or reference) flight profile while descending or climbing. For the present analysis, such a commanded profile may not be available.

4.2.2 Metrics from Safety Analysis Literature

Studies that utilize system performance models to characterize aircraft safety are relatively rare in literature. In a case study of the lateral directional flight control system of a fighter aircraft, Dominguez-Garcia et al. [61] chose the sideslip angle, the body axis roll rate, the body axis yaw rate, and the body axis roll angle as

performance metrics to characterize hazards due to failures of different components. These correspond well to the aircraft state variables typically considered under the exceedance detection paradigm discussed above.

In a multistate design and performance robustness study by Agte et al. [15], expected specific excess power in a climbing turn was considered as the metric of interest to be evaluated for the nominal as well as off-nominal failure cases. The specific excess power is just one of many metrics already discussed while deliberating on ‘Energy Metrics’ above. In both these studies, detailed flight dynamics models, or 6-DoF models were utilized to map the response of failure cases in terms of metrics of interest.

While evaluating off-nominal requirements on the More Electric Aircraft architectures using optimal load-shedding, Armstrong utilized metrics like required takeoff field length (TOFL) and available range for loss of thrust, potable air mass flow for ECS failures, etc. for characterizing hazard severity [25].

In a study on reliability lunar surface systems, Borer et al [44] utilized system behavioral models to determine the degradation in system functions due to component failures. While the metrics they used apply for lunar systems and are not particularly relevant for novel aircraft architectures, they utilized side constraints on system performance (lower bounds on functional satisfaction) to determine if a system was failed.

4.2.3 Summary of Implemented Safety Metrics

The test problem of interest in the present work is T-DEP aircraft inspired by the X-57 Maxwell (see Ch. 3.6). Although it has a novel architecture for the functions of ‘provide thrust’ and ‘provide high lift’, the rest of the aircraft is a conventional tube and wing design with a conventional horizontal and vertical tail. As has been mentioned above, there is no one-size-fits-all set of metrics that can be utilized as

safety metrics for the safety framework provided in this thesis. Therefore, this section focused on identifying the metrics that would be best suited for the test problem in implementing the developed framework.

Table 5: Summary of implemented safety metrics for the T-DEP problem

Classification	Safety Metrics	Required Model Detail
Performance-based	$TOFL_{Req}$ Achievable Load Factor (n_{max}) / Bank Angle (ϕ_{max})	Conceptual
Energy-based	Maximum potential climb gradient (γ_{max}) Energy Rate Margin (ERM)	Conceptual
Exceedance detection Safety analysis literature	Altitude Airspeed Angles ($\gamma, \theta, \psi, \phi$) Throttle settings (τ_L, τ_R) Control Deflections (δ_r, δ_a)	Preliminary 6-DoF + Trim Analysis

Overall, research question 1.1 is answered by identifying and borrowing safety relevant metrics by conducting a thorough literature review. Table 5 provides a summary of the implemented metrics in this dissertation for research question 1.1.

4.3 *Safety Related Off-Nominal Requirements*

Having identified metrics suitable for the test problem of interest, the next research sub-question considers the problem of estimating them under off-nominal scenarios, and utilizing them to identify and characterize hazard severity.

Research Question 1.2:

How can safety related off-nominal requirements be identified and allocated at the system level during conceptual and preliminary design phases using the previously defined safety metrics?

The formulation of hypothesis 1.2 for this research question is given in chapter 3.2. Specifically, Continuous FHA and a performance-based multistate analysis were proposed as two methods to quantify the metrics provided in table 5. The methods themselves can be found in chapter 4.1. The idea is to utilize these methods to quantify system performance using the metrics discussed earlier and compare them to a threshold that is established using engineering judgement, or using regulatory requirements. In light of this, hypothesis 1.2 is restated here for convenience:

Hypothesis 1.2: *If the identified safety metrics are quantified under off-nominal scenarios using appropriate system performance models, then identification and allocation of safety requirements at the system level can be completed with greater resolution and accuracy than traditional methods*

The process followed to implement C-FHA and the multistate method is given in figure 32. A background is first provided into the available information and knowledge about the distributed electric propulsion (DEP) aircraft.

4.3.1 Experiment 1.2

The intent of the present section is to follow the process given in figure 32 to demonstrate that the two methods - C-FHA and Multistate Performance Analysis (see Ch. 4.1), provide a better identification and characterization of safety requirements than traditional methods. For that purpose experiment 1.2 is designed to test hypothesis 1.2.

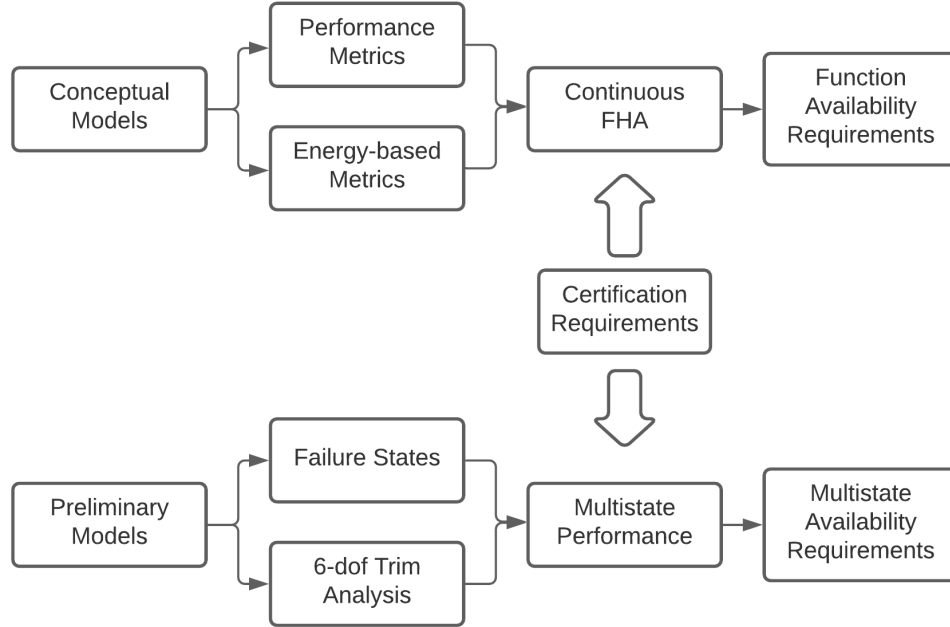


Figure 32: Characterizing safety related off-nominal requirements

4.3.1.1 Purpose of the Experiment

Research question (RQ) 1 was partitioned into three sub-questions in Ch. 3.2 to make it easier to demonstrate the truth value of hypothesis 1. In those partitions, RQ 1.2 deals with the first two requirements that were stated under RQ 1 – i) identification of safety related off-nominal scenarios and corresponding hazards, and ii) Estimation of safety requirements at the aircraft level. Hypothesis (H) 1.2 suggests that quantifying the down-selected safety metrics from Ch. 4.2.3 on the test problem should result in a more accurate allocation of safety requirements at the aircraft level compared to traditional methods. Thus, the following are the main objectives of this experiment:

1. Demonstrate the utility of safety metrics to identify and characterize hazards using the models discussed
2. Demonstrate that the resultant hazard severity allocation at the aircraft level provides a better resolution than traditional methods

4.3.1.2 Experiment Setup

In order to test H-1.2, two preconditions must be met - i) Hazards for the test problem identified from traditional methods must be characterized, and ii) Hazard severity results using the new methods and safety metrics must be generated. On comparing the two sets of results, a determination can be made about whether the new methods provide improved characterization of hazards.

The test problem of interest is the T-DEP traction power system architecture, which is a simplified version of the X-57 traction power architecture. Failures in this system affect the aircraft level functions of ‘Provide Thrust’ and ‘Provide High Lift’. A failure in the traction power system can result in either a symmetric degradation or an asymmetric degradation in these functions. Figure 33 that shows the T-DEP aircraft traction power system was first introduced in Ch. 3.6 and is reproduced below to aid the upcoming discussions.

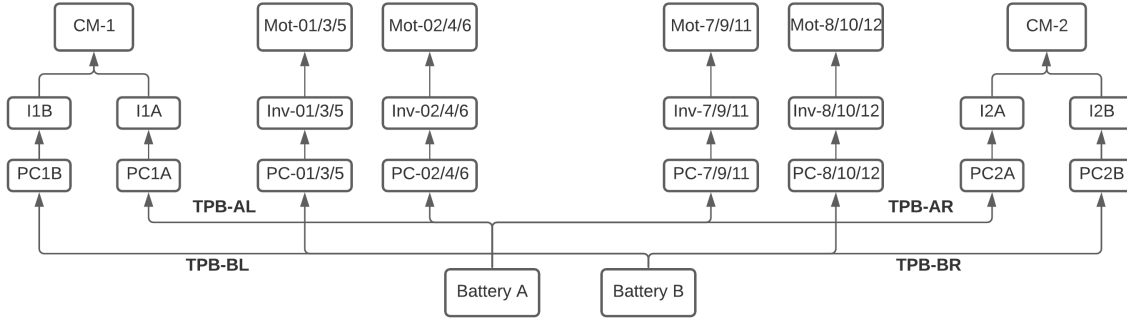


Figure 33: T-DEP aircraft traction power system

For the benchmarking case, results available in literature [52, 144] are utilized along with an assumed step function loss - hazard severity curve. For experiment 1.2, hazard severity for functional degradation is identified using C-FHA and compared against the benchmark FHA results. Additional results generated using the multi-state performance analysis method are also compared to results from literature as a benchmark. Upon comparison, it will be demonstrated that the methods proposed in this thesis provide a better resolution in identifying and characterizing hazards and

corresponding requirements compared to traditional approaches.

4.3.2 Benchmark Results

Traditional FHA typically recognizes a discrete loss of function to allocate hazard severity to the aircraft level. For the test aircraft, this is represented in the present work as three states for the function ‘Provide Thrust’ - i) Nominal, ii) Partial Loss of Thrust, and iii) Complete Loss of Thrust. These are allocated hazard severity of i) None, ii) Major, and iii) Catastrophic to serve as the benchmark functional hazard allocation, and is represented by figure 34.

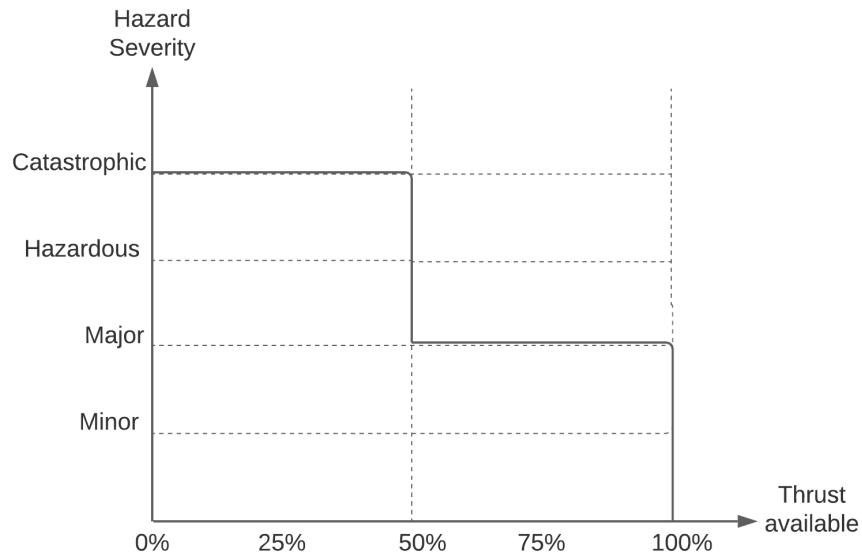


Figure 34: Traditional FHA - loss of thrust hazard severity

In addition, literature provides some results regarding the hazard severity of different failure conditions of the X-57 traction power system [52,144]. In a presentation on safety considerations for the X-57, Papathakis [144] classified five safety events relevant to the traction power system using severity categories from MIL-STD-882E [59]. These categories as per MIL-STD-882E are: I - Catastrophic, II - Critical, III - Marginal, IV - Negligible. For the present work, they are translated into the categories presented in table 2 as: I - Catastrophic, II - Hazardous, III - Major, IV - Minor. The identified hazards and their risk profile is provided in table 6.

Table 6: X-57 Power system hazard characterization [144]

Identified Hazard	Severity	Estimated Probability
Aircraft traction battery fire	Catastrophic	Remote
Traction bus failure	Catastrophic	Improbable
Symmetric loss of cruise propeller thrust (partial/total)	Hazardous	Improbable
Abrupt asymmetric thrust	Catastrophic	Remote
Failure of propulsor system	Catastrophic	Improbable

In a study on the X-57 traction power system, Clarke et al [52] provided a failure scenario matrix for the Mod-II and III architecture with no high lift propulsors (HLP) given here in table 7. The severity categories are stated as follows [52] – S: Land as

Table 7: X-57 Power system failure scenarios [52]

Failure Scenario	Severity
Single cruise motor	S
Single motor controller	M
Quad motor controller	S
Single traction bus	M
Quad traction buses	S
Single main battery	S
Dual main batteries	S

soon as possible, and M: Land as soon as practical. These results from literature visibly characterize failure scenarios as discrete loss of thrust events. They lend credence to the hazard severity assigned to loss of thrust, partial or complete given in figure 34. This discrete, step hazard allocation is therefore used as a benchmark to compare the results generated from the process given in figure 32 for experiment 1.2.

The next sections will provide some background on the conceptual performance and preliminary 6-DoF trim analysis models created in the present work to implement the methods given in chapter 4.1.

4.3.3 The T-DEP Aircraft Models

Both methods listed under chapter 4.1 require aircraft performance models to be established to estimate safety metrics of interest. Therefore, the T-DEP aircraft's models have been created for the purpose of this thesis at two levels of detail - i) conceptual to compute performance, and ii) 6-DoF preliminary to conduct trim analysis. Conceptual models utilized for the C-FHA method require information of only the aircraft weight, wing area, drag polar in different configurations, and thrust in different configurations at different velocities. The 6-DoF preliminary model, on the other hand, requires much more detailed definition of the geometry, mass properties, aerodynamic characteristics, and propulsive performance. This detailed model is explained below. The basic conceptual models will be explained when they are used. The preliminary 6-DoF model is developed utilizing publicly available data, and first order estimates where data is unavailable.

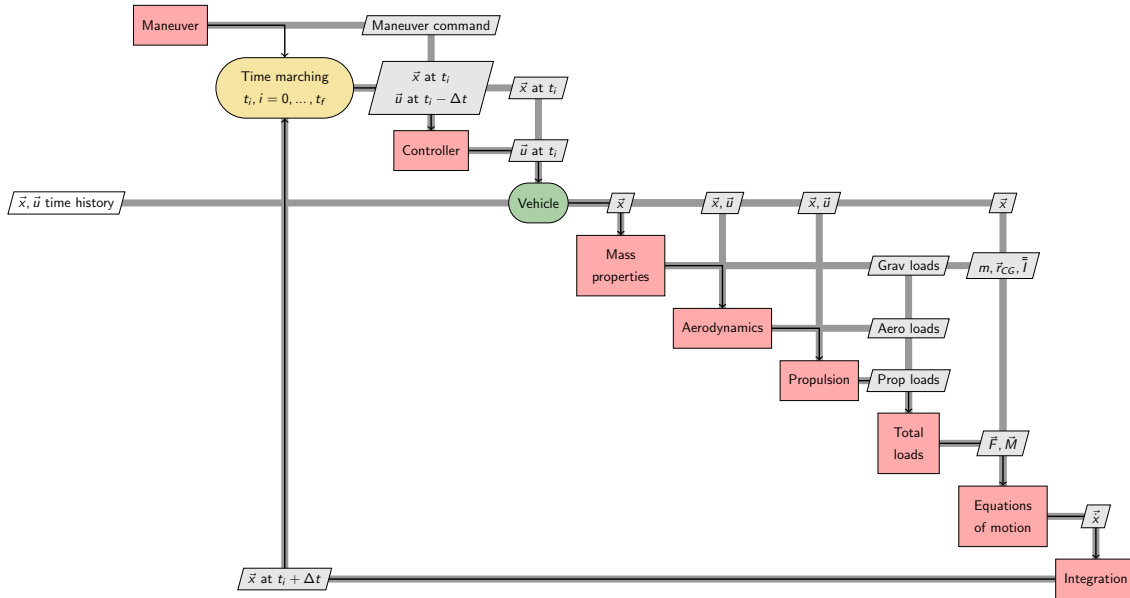


Figure 35: DELPHI framework (Credit: Refs. [34, 161])

The Dynamic Environment for Loads Prediction and Handling Investigation (DELPHI) framework developed as a flight dynamics simulation environment at the Aerospace

Systems Design Lab is used in this work for 6-DoF trim analysis [63, 78, 160, 161]. Developed as an object-oriented python code, DELPHI is intended to have the capability to simulate any aircraft model in any desired maneuver. A high-level view of DELPHI is shown in Fig. 35. Appendix B provides additional details of the simulation environment. Some pertinent details are provided in the following sections for completeness.

4.3.3.1 Geometry

Geometric details of the T-DEP aircraft are based on the publicly available X-57 OpenVSP model provided by NASA [133]. Figure 36 shows the three views of the publicly available OpenVSP common research model (CRM) of the X-57 Mod. IV. Important wing, horizontal stabilator, and vertical tail geometric details are given in tables 8, 9, and 10.

Table 8: T-DEP aircraft wing geometry

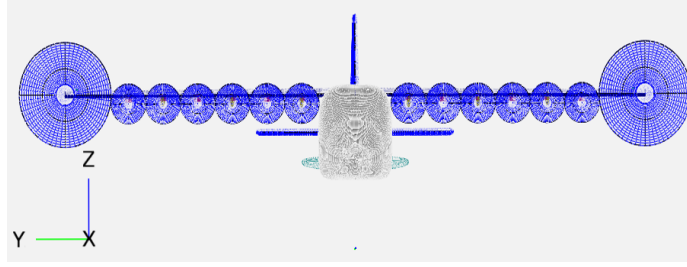
Parameter	Value	Unit
Planform area- S_{wing}	6.2	m ²
Wingspan- b_{wing}	9.64	m
Reference chord- c_{wing}	0.65	m
Aspect ratio- AR_{wing}	15	
Incidence angle	2	deg

Table 9: T-DEP aircraft vertical tail geometry

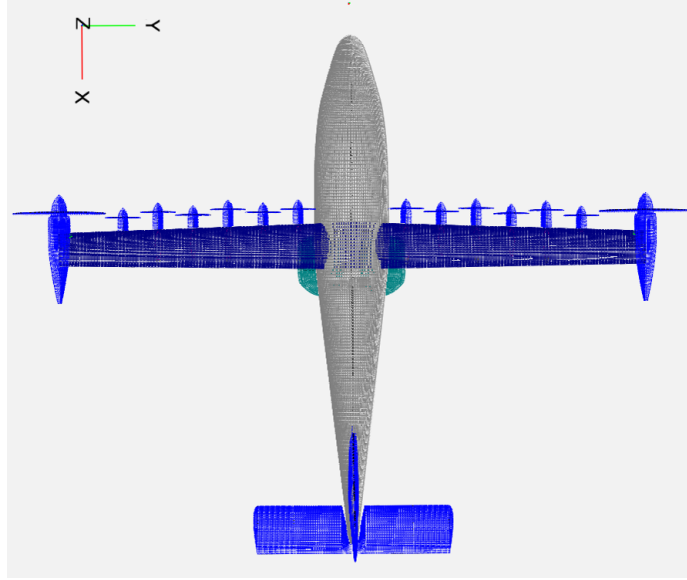
Parameter	Value	Unit
Planform area- S_{vt}	1.95	m ²
Span- b_{vt}	1.62	m
Reference chord- c_{vt}	1.44	m
Leading edge sweep	37.45	deg

4.3.3.2 Mass Properties

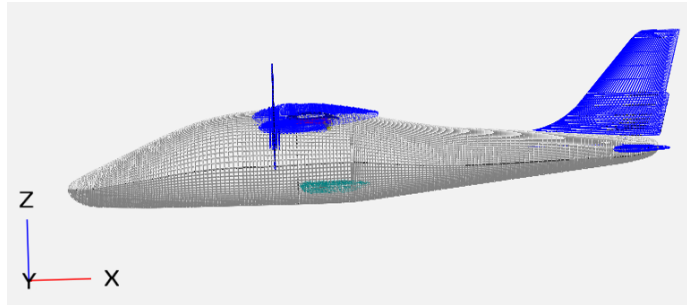
The mass properties of the T-DEP aircraft are built-up from the X-57's component mass properties that are obtained from literature, or estimated based on the Tecnam



(a) X-57 front view



(b) X-57 top view



(c) X-57 side view

Figure 36: The X-57 aircraft geometry using OpenVSP [133]

P2006T's component weight breakdown. Each cruise motor is assumed to have a mass of 117 lbs, while each high-lift motor is assumed to have a mass of 15 lbs [131]. The locations of the motors are obtained from the OpenVSP model and are given in table 13. The battery is assumed to be located at the wing quarter chord and to

Table 10: T-DEP aircraft stabilator geometry

Parameter	Value	Unit
Planform area- S_{stab}	2.45	m^2
Span- b_{stab}	3.14	m
Reference chord- c_{stab}	0.78	m

have a mass of 860 lbs [131]. Procedures and equations provided in Ref. [110] are utilized for computing inertia properties of the wing, empennage, and the fuselage (see Appendix B). The component mass build-up is given in Table 11, and the net aircraft mass properties are given in Table. 12.

Table 11: Mass build-up of T-DEP aircraft

Parameter	Value	Unit
$2 \times$ cruise motor	106.14	kg
$12 \times$ cruise motor	81.65	kg
Battery	390.08	kg
Empennage	27.3	kg
Fuselage	235.87	kg
Landing gear	61.15	kg
Wing	152.88	kg
$2 \times$ pilot	170	kg
Misc	135.7	kg
Total	1360.77	kg

Table 12: Mass properties of T-DEP aircraft

Parameter	Value	Unit
Weight	1360.77	kg
I_{xx}	4314.08	$kg.m^2$
I_{xy}	-232.85	$kg.m^2$
I_{xz}	-2563.29	$kg.m^2$
I_{yy}	18656.93	$kg.m^2$
I_{yz}	-62.42	$kg.m^2$
I_{zz}	22340.21	$kg.m^2$

4.3.3.3 Propulsion

The T-DEP aircraft's propulsion is modeled to be as close to that of X-57 as possible, with simplifications where necessary. The X-57 is based on the Tecnam P2006T which has been modified to test a distributed electric propulsive architecture. The propulsion architecture therefore treats every single cruise and high lift propulsors (HLP) as independent objects. The cruise motors can be throttled to control their thrust, while the HLPs can only be switched on or off. To accurately capture the impact of this novel architecture on the aircraft, a first principles physics based approach is utilized. Every propulsor is treated as a point object generating thrust at its location in its own axis, which is determined from the OpenVSP model. Moments of inertia of these motors and propellers are computed about the aircraft center of gravity (CG) using the parallel axis theorem. The locations of the different motors about the flight dynamics reference point are given by table 13. Appendix B provides additional details into the calculation of the propulsive moments of inertia. The RPM

Table 13: T-DEP right engines locations relative to CG in the flight dynamics body-fixed reference frame (x-forward, y-right, z-down)

Engine	x offset	y offset	z offset	Unit
Wingtip propulsor	0.33	4.82	-0.024	m
Distributed propulsor 1	0.39	0.89	0.11	m
Distributed propulsor 2	0.34	1.46	0.11	m
Distributed propulsor 3	0.39	2.04	0.11	m
Distributed propulsor 4	0.3	2.62	0.11	m
Distributed propulsor 5	0.35	3.19	0.11	m
Distributed propulsor 6	0.26	3.77	0.11	m

of the wingtip motors is controlled using the throttle setting τ . τ changes the RPM of the motors linear from minimum value of 0 to a maximum value of 2500. Thus, RPM ω as a function of the throttle (τ) is given by:

$$\omega = \omega_{min} + \tau(\omega_{max} - \omega_{min}) \quad (26)$$

The wingtip propellers are modeled with a diameter (d) of 1.524 meter, with a thrust coefficient (C_T) of 0.07. This is based on a thrust value of 511 N at 8000 feet and 2250 RPM [55]. The thrust produced by the motors at different throttle settings or altitude is then computed using:

$$T_{wingtip} = C_T \rho \omega^2 d^4 \quad (27)$$

where ρ is the density of the air. The dependence of the thrust on the altitude at which the aircraft is flying is taken into account through the density. It is assumed that there is no dependence of Mach number on C_T , since the X-57 flight envelop is in the low-subsonic region.

As stated earlier, the high-lift motors are controlled through binary on/off switches. When ON, the thrust they produce depends on the equivalent airspeed of the aircraft as given in Table 14 [81]. Above 93 KEAS, they do not produce any thrust.

Table 14: High-lift motors thrust dependence on V_{EAS} [81]

Velocity (KEAS)	0	17	24	31	38	58	64	70	76	84	93
Thrust (lbf)	0	10	20	30	40	50	40	30	20	10	0

4.3.3.4 Aerodynamics

No lateral aerodynamic data for the X-57 was found in literature at the time of writing this thesis. The T-DEP aerodynamic model is therefore decoupled into two parts- longitudinal, and lateral. The longitudinal aerodynamic model for this work is based on regressions that provide aerodynamic coefficients in the wind frame. These regressions are obtained by fitting linear polynomial equations through the digitized data from Deere et al. [55]. A component build-up approach is used where the aerodynamic coefficients of the entire aircraft are found by adding contributions of each component - wings, nacelles, pylons, stabilator, fuselage, and vertical tail. Appendix B provides additional details of the individual contributions of these lifting surfaces. The aerodynamic coefficients are given as a function of the following:

- States
 - Angle of attack: α
 - Sideslip angle: β
 - Angular rates: p, q, r
- Controls
 - Stabilator incidence angle: δ_s
 - Trim-tab deflection angle: δ_{tt}
 - Flap deflection angle: δ_f
 - Aileron deflection angle: δ_a
 - Rudder deflection angle: δ_r
 - High lift propeller blowing (boolean)

The lift coefficient is found as:

$$C_L(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{L_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{L_{\text{wing} + \text{tip-nacelle}}} + C_{L_{\text{flap}}} + C_{L_{\text{HLN}}} + C_{L_{\text{fuse+Vtail}}} + C_{L_{\text{stab}}} \frac{S_{\text{stab}}}{S_{\text{wing}}} \quad (28)$$

Note that the lift coefficient is assumed to not be affected by the sideslip angle. The drag coefficient is similarly found as:

$$C_D(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{D_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{D_{\text{wing} + \text{tip-nacelle}}} + C_{D_{\text{flap}}} + C_{D_{\text{HLN}}} + C_{D_{\text{fuse+Vtail}}} + C_{D_{\text{stab}}} \frac{S_{\text{stab}}}{S_{\text{wing}}} \quad (29)$$

The moment coefficient is found as:

$$C_m(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{m_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{m_{\text{wing} + \text{tip-nacelle}}} + C_{m_{\text{flap}}} + C_{m_{\text{HLN}}} + C_{m_{\text{fuse+Vtail}}} + C_{m_{\text{stab}}} \frac{S_{\text{stab}} c_{\text{stab}}}{S_{\text{wing}} c_{\text{wing}}} \quad (30)$$

The reader is directed to Appendix B for additional details of the component contributions.

Table 15: Estimated lateral aerodynamic coefficients of the T-DEP

	β	\hat{p}	\hat{r}	δ_a	δ_r
C_Y	-0.9905	-0.0813	0.8312	0.0054	0.2959
C_n	0.2616	0.0729	-0.3621	0.0132	-0.1466
C_l	-0.0106	-0.6620	0.2096	0.1667	0.0048

Since no publicly available lateral aerodynamic data for the X-57 was found, a Vortex Lattice Method (VLM) is used to estimate them. VLM is based on potential flow theory where the lifting surfaces are model as discretized vortex panels following Biot-Savart Law and Kutta-Joukowski Theory, while the non-lifting bodies are modeled as sources/sinks or doublets to enforce the non-penetrating condition. Due to its nature of linearization, VLM is able to quickly compute the stability and control derivatives. An open-source vortex lattice method software, AVL [62], is used in the present work to obtain the lateral aerodynamic coefficients. While limitations posed by a linearized estimation method while ignoring the effects of swirl and sidewash generated by multiple high-lift and wingtip propellers are acknowledged, the intent of the present work is to generate a quick estimate by utilizing data available in early-preliminary design stages. For that reason, the results generated are considered adequate for the purpose of the present research. The lateral aerodynamic coefficients from AVL are given in Table 15.

The net lateral coefficients are found as:

$$C_Y = C_{Y_\beta}\beta + C_{Y_p}\hat{p} + C_{Y_r}\hat{r} + C_{Y_{\delta_a}}\delta_a + C_{Y_{\delta_e}}\delta_e + C_{Y_{\delta_r}}\delta_r \quad (31)$$

$$C_l = C_{l_\beta}\beta + C_{l_p}\hat{p} + C_{l_r}\hat{r} + C_{l_{\delta_a}}\delta_a + C_{l_{\delta_e}}\delta_e + C_{l_{\delta_r}}\delta_r \quad (32)$$

$$C_n = C_{n_\beta}\beta + C_{n_p}\hat{p} + C_{n_r}\hat{r} + C_{n_{\delta_a}}\delta_a + C_{n_{\delta_e}}\delta_e + C_{n_{\delta_r}}\delta_r \quad (33)$$

where

$$\hat{p} = \frac{pb}{2V} \quad (34)$$

$$\hat{r} = \frac{rb}{2V} \quad (35)$$

Finally, the aerodynamic loads are computed from the coefficients as:

$$L = \bar{q}S_W C_L \quad (36)$$

$$D = \bar{q}S_W C_D \quad (37)$$

$$Y = \bar{q}S_W C_Y \quad (38)$$

$$l = \bar{q}S_W b C_l \quad (39)$$

$$m = \bar{q}S_W c C_m \quad (40)$$

$$n = \bar{q}S_W b C_n \quad (41)$$

The above loads are obtained in the wind-axis and are rotated to the body-fixed axis frame before being used in the equations of motion in DELPHI.

4.3.4 C-FHA Results

Continuous functional hazard assessment is intended to be performed during the conceptual design stage. For the T-DEP, this means obtaining a simple polynomial drag polar of the form.

$$C_D = C_{D_0} + K \cdot C_L^2 \quad (42)$$

Depending on whether the flaps are extended or retracted, and the high lift propulsors (HLP) are switched on or off, the aircraft has four different settings at which the drag polar is computed. The values of the constants are given in table 16.

Table 16: Polynomial drag coefficients for different flap and high lift propulsor settings for the T-DEP

	Flaps Retracted		Flaps Takeoff	
	HLP OFF	HLP ON	HLP OFF	HLP ON
C_{D_0}	0.01869	0.1097	0.04235	0.1104
K	0.043	0.03255	0.02781	0.02503

The function of interest for the test problem is ‘Provide Thrust’. Propulsion models given in chapter 4.3.3.3 are utilized to compute the amount of thrust available under different configurations at different velocities and altitudes.

4.3.4.1 Takeoff Field Length

Under a continuous degradation in thrust available, the Takeoff field length (TOFL) required for the aircraft to safety takeoff from a given runway is computed using the procedure given in Ref. [25]. For a successful takeoff, the TOFL is decomposed into (i) ground roll (s_g), (ii) rotation distance (s_R), and (iii) distance to climb and clear obstacle (s_{obs}) [22]. In the case of a critical thrust loss during takeoff before the decision speed V_D , the balance field length (BFL) includes the distance covered to accelerate from 0 to V_D , along with the distance required to brake to a stop.

$$\begin{aligned} ds &= V_\infty dt \\ &= \frac{d(V_\infty^2)}{2(\frac{dV_\infty}{dt})} \end{aligned} \quad (43)$$

$$\begin{aligned} \frac{dV_\infty}{dt} &= \frac{1}{m} (T - D - \mu_r(W - L)) \\ &= g \left(T/W - \mu_r - \frac{\rho_\infty V_\infty^2}{2(W/S)} (C_{D_0} + KC_L^2 - \mu_r C_L) \right) \end{aligned} \quad (44)$$

Substituting Eq. 43 into Eq. 44 gives,

$$s_{gV_1 \rightarrow V_2} = \int_{V_1}^{V_2} \frac{V_\infty}{g \left(T/W - \mu_r - \frac{\rho_\infty V_\infty^2}{2(W/S)} (C_{D_0} + KC_L^2 - \mu_r C_L) \right)} dV_\infty \quad (45)$$

$$s_{gV_1 \rightarrow V_2} = \int_{V_1}^{V_2} \frac{V_\infty}{g(K_T + K_A V_\infty^2)} dV_\infty \quad (46)$$

$$K_T = T/W - \mu_r \quad (47)$$

$$K_A = \frac{-\rho_\infty}{2(W/S)} (C_{D_0} + KC_L^2 - \mu_r C_L) \quad (48)$$

Eq. 46 gives the distance covered by the aircraft on the ground when accelerating from $V_1 \rightarrow V_2$ when a thrust T acts on it. In case of a failure just before decision speed, the distance covered till V_D is given by integrating Eq. 46 from 0 to V_D ,

$$s_{g1} = \frac{1}{2gK_A} \ln \left(\frac{K_T/K_A + V_D^2}{K_T/K_A} \right) \quad (49)$$

where K_T is evaluated at $V = 0.7 \cdot V_{TO}$ for the present case. To compute the decision speed of the aircraft, the ground roll for the braking phase is calculated by

assuming the pilot cuts the power upon failure and applies breaks. Thus, the thrust term in Eq. 47 is set to zero, and rolling friction coefficient $\mu_r = 0.02$ in Eq. 48 is replaced by the braking coefficient $\mu_B = 0.50$ [89].

$$s_{g_2} = \frac{1}{2gK_{AB}} \ln \left(\frac{K_{TB}/K_{AB}}{K_{TB}/K_{AB} + V_D^2} \right) \quad (50)$$

$$K_{TB} = -\mu_B \quad (51)$$

$$K_{AB} = \frac{-\rho_\infty}{2(W/S)} (C_{D_0} + KC_L^2 - \mu_B C_L) \quad (52)$$

Eq. 50 gives the distance needed to stop and aircraft from the decision speed while reducing thrust to zero and applying breaks. The Balanced Field Length (BFL) is given as,

$$BFL = s_{g_1} + s_{g_2} \quad (53)$$

For a given runway length, the speed at which the difference between runway length and BFL is zero can be obtained through a fixed point iteration. This speed is called the decision speed V_D , reaching which an aircraft has no choice but to continue take-off procedure. Thus, the critical safety case is when a loss of thrust occurs just after the decision speed. In such cases, the TOFL is given by,

$$TOFL = s_{g_1} + s_{g_{fail}} + s_R + s_{obs} \quad (54)$$

where $s_{g_{fail}}$ is the distance covered by the aircraft to reach the take-off velocity V_{TO} from V_D under a thrust degradation scenario. In such a scenario, the ground roll needed to continue the takeoff run and reach takeoff velocity is given by

$$s_{g_{fail}} = \int_{V_D}^{V_{TO}} \frac{V_\infty}{g(K_{TD} + K_A V_\infty^2)} dV_\infty \quad (55)$$

$$K_{TD} = (T/W)_{degraded} - \mu_r \quad (56)$$

Finally, the distance required to rotate and clear the obstacle is calculated using

equations provided by Anderson [22] as follows,

$$s_{rotate} = t_{rotate} V_{TO} \quad (57)$$

$$s_{obs} = R \sin(\theta_{obs}) \quad (58)$$

$$\theta_{obs} = \arccos(1 - h_{obs}/R) \quad (59)$$

$$R = 6.96 V_{stall}^2 / g \quad (60)$$

where the time to rotate is assumed to be 1 second for a small GA aircraft of the size of X-57, and the obstacle height is assumed at 50 feet.

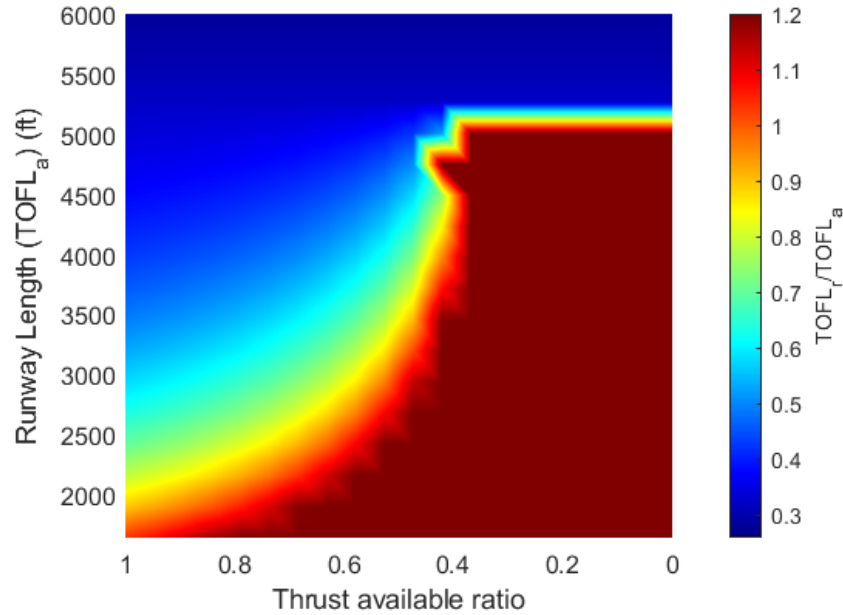


Figure 37: Ratio of TOFL required to available at 2356 ft under continuous thrust degradation

Figure 37 gives the ratio of TOFL required to available for different runway lengths (Y-axis) under a continuous thrust degradation scenario. The X-axis gives the thrust that is available as a ratio to the maximum under degradation. The upper limit of this ratio is truncated at 1.2 to keep the focus on the values near unity. The TOFL required is computed at an altitude of 2356 feet – the altitude of the Edwards Air Force Base in California from where the X-57 is expected to conduct its operations.

The regions where this plot shows a ratio of above unity are the regions where the T-DEP cannot safely takeoff or brake to a stop within the runway available.

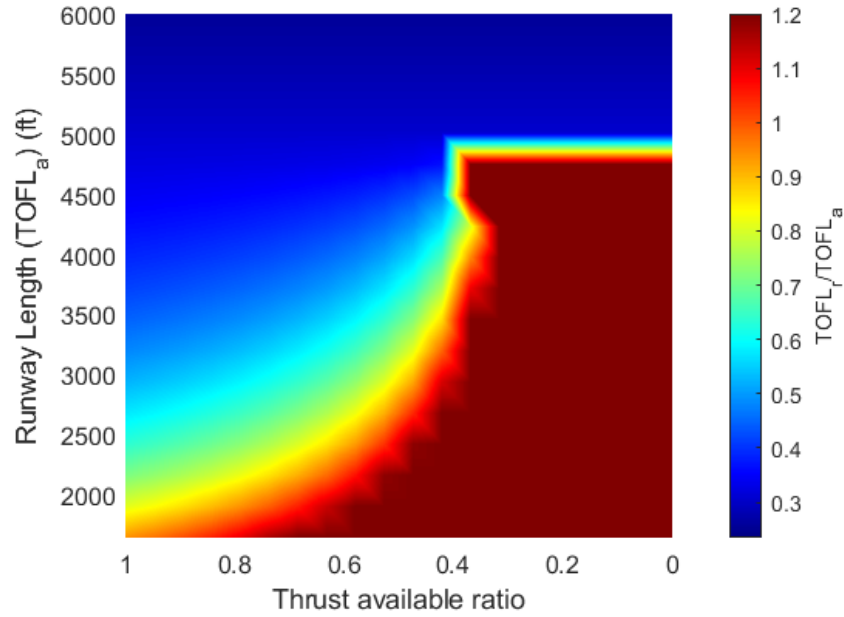


Figure 38: Ratio of TOFL required to available at sea-level ft under continuous thrust degradation

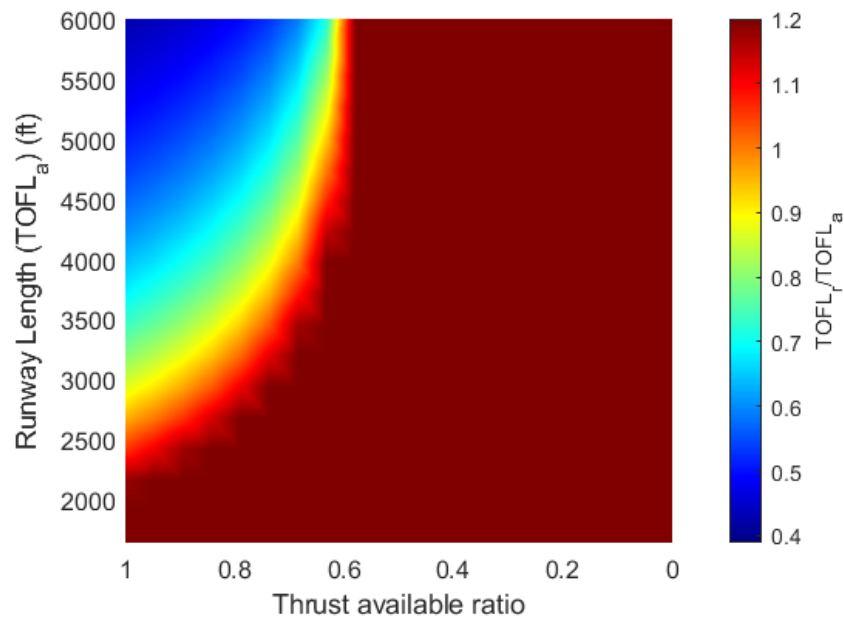
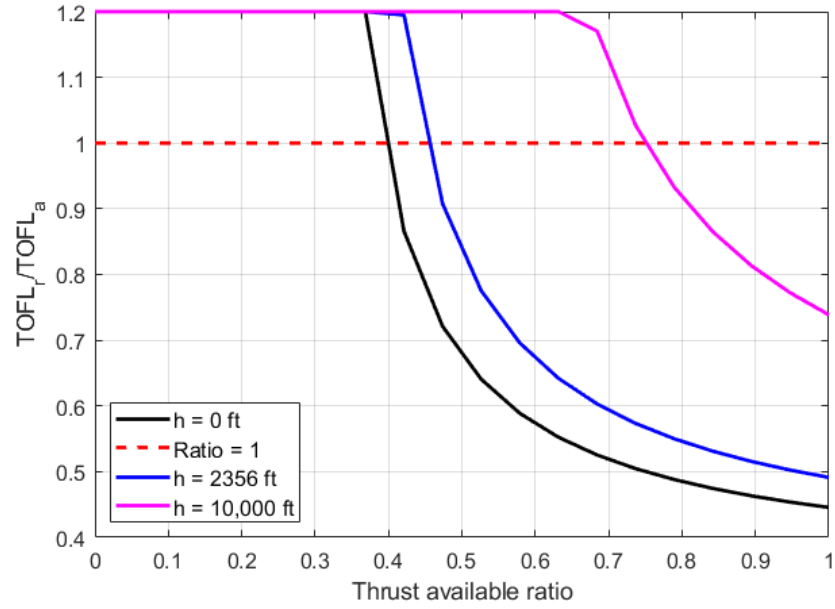


Figure 39: Ratio of TOFL required to available at 10,000 ft under continuous thrust degradation

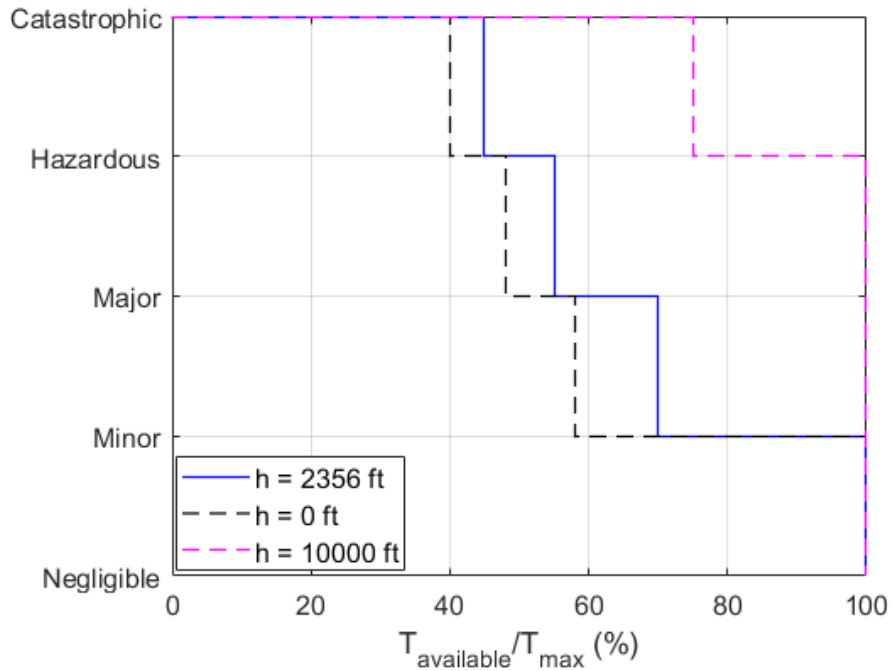
Determining the TOFL required from sea level to 10,000 ft (as required by 14 CFR 23.2105.b.1) results in figures 38 and 39. Taken together, these three figures can be used to estimate hazard severity as a consequence of continuous degradation in the function ‘Provide Thrust’.

While the Edwards AFB runways are renowned to be some of the longest (for the space shuttle), the intent of the present work is to conduct safety analysis for novel DEP architectures similar to the X-57 that will one day takeoff from regular GA airports. Therefore, a runway of 3400 feet, the lower end of a typical GA airport runway length is investigated next to determine the impact of thrust degradation on the T-DEP’s takeoff performance. Results of this runway length at the three altitudes mentioned above are given in figure 40(a).

The next step in C-FHA pertains to converting the safety metric (TOFL required) obtained as a consequence of degradation in thrust into aircraft level function - hazard relationship. This step is inherently subjective and must be guided by subject matter expertise or some guiding principles, either from regulatory requirements, or engineering judgement. For the three TOFL curves given in figure 40(a), the following heuristic is used to determine the hazard severity: i) $1 \leq \text{TOFL ratio}$ is catastrophic since the aircraft can neither continue takeoff nor stop within the runway available; ii) $0.7 \leq \text{TOFL ratio} \leq 1$ is rated hazardous; iii) $0.6 \leq \text{TOFL ratio} \leq 0.7$ is rated major; iv) $\text{TOFL ratio} \leq 0.6$ is rated minor. The resultant hazard severity - thrust loss curves are given in figure 40(b). It is important to note that this relationship between hazard severity and thrust loss for the T-DEP is valid only for the take-off configuration with flaps deployed and HLP powered on. The hazard severity - thrust loss curve given at 2356 ft altitude (blue) is considered as the thrust loss hazard curve going forward in this thesis. The curves given by airport altitudes of 0 ft and 10,000 ft present bounds on the hazard severity and serve to denote the uncertainty in the hazard severity - thrust loss relationship for the T-DEP while considering TOFL



(a) Ratio of TOFL required to available for a runway length of 3400 ft under continuous thrust degradation



(b) C-FHA hazard severity due to thrust degradation during takeoff

Figure 40: T-DEP C-FHA results using TOFL metric under thrust degradation

required as a safety metric of interest.

4.3.4.2 Maximum load factor and bank angle

A level turn is an important flight maneuver not only from an operational point of view but also from a safety point of view. An aircraft facing a sudden degradation in thrust might have to turn around to find a suitable location for an emergency landing. To that extent, the airplane's maximum attainable load factor and maximum attainable bank angle can be utilized as metrics in C-FHA analysis. Under a level turn, the aircraft must satisfy the following equations:

$$\phi = \cos^{-1}(1/n) \quad (61)$$

$$n = L/W \quad (62)$$

The load factor thus depends only on the bank angle, and the two can be considered together in the analysis that proceeds. As the load factor increases though, the aircraft has to generate more lift, which increases the drag (due to the lift induced drag). As a result, a greater amount of thrust is needed to overcome this drag increase during a level turn. This results in an upper limit being placed on the aircraft's load factor by the amount of thrust available to it [22]:

$$n_{max} = \left(\frac{\rho_{\infty} V_{\infty}^2}{2K(W/S)} \left((T/W)_{max} - \frac{1}{2} \rho_{\infty} V_{\infty}^2 \frac{C_{D_0}}{W/S} \right) \right)^{1/2} \quad (63)$$

Under a thrust degradation scenario, Eq. 63 can be modified as,

$$n_{maxdegraded} = \left(\frac{\rho_{\infty} V_{\infty}^2}{2K(W/S)} \left((T/W)_{degraded} - \frac{1}{2} \rho_{\infty} V_{\infty}^2 \frac{C_{D_0}}{W/S} \right) \right)^{1/2} \quad (64)$$

As is visible, the maximum load factor is dictated not only by the thrust available under degradation, but also by design parameters like wing loading, C_{D_0} , and K . While Eq. 64 seems to provide an upper limit on the load factor under thrust degradation, there is another consideration that constrains n_{max} . That stems from Eq. 62 – the wings can only produce lift until the maximum lift coefficient is reached. This constraint on the load factor generally applies at lower velocities and is given by [22],

$$n_{max} = \frac{1}{2} \rho_{\infty} V_{\infty}^2 \frac{C_{L_{max}}}{W/S} \quad (65)$$

Figure 41 shows the n_{max} , ϕ_{max} curves for the X-57 at nominal operations given by Eqs. 64, 65, 61. Also plotted on the second Y-axis (in blue) is the maximum bank angle achievable by the X-57 in the takeoff configuration. The takeoff plots are generated at 50 feet, while cruise plots are generated at 1500 feet altitude. The dotted lines show the trend-lines where n_{max} due to maximum thrust or maximum lift coefficient are larger than the other, and therefore untenable. Some observations

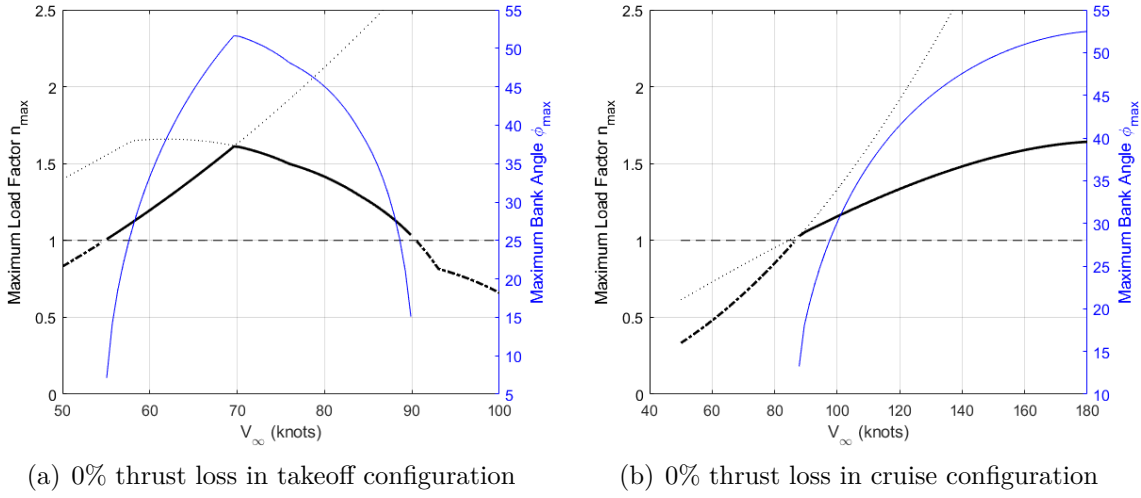


Figure 41: n_{max} , ϕ_{max} for the T-DEP in nominal conditions

can be immediately drawn from these nominal conditions. The T-DEP is capable of attaining a load factor of over 1.5, and a bank angle of over 50° in both takeoff and cruise nominal conditions. Additionally, the maxima for takeoff occur at around 70 knots, which is roughly $1.2 \times V_{stall}$ for the T-DEP – a velocity that shows up in multiple regulatory requirements. The takeoff capability drops beyond 90 knots due to the fact that the thrust provided by the high lift propulsors peaks at around 70 knots and drops off to zero above 90 knots. In the cruise configuration (flaps retracted, HLP off), the T-DEP's capability reduces below about 82 knots, which is close to the stall speed without HLPs and flaps (73 knots with flaps [45]).

The first obvious case to consider is when the thrust degradation results in a maximum load factor of less than 1. In the takeoff configuration seen in figure 42(a), this is found to occur at a 50% thrust degradation at 70 knots ($1.2 \times V_{stall}$). Since this occurs right after takeoff, it is rated catastrophic in terms of the hazard severity. For the cruise configuration seen in figure 42(b) computed at an altitude of 1500 feet,

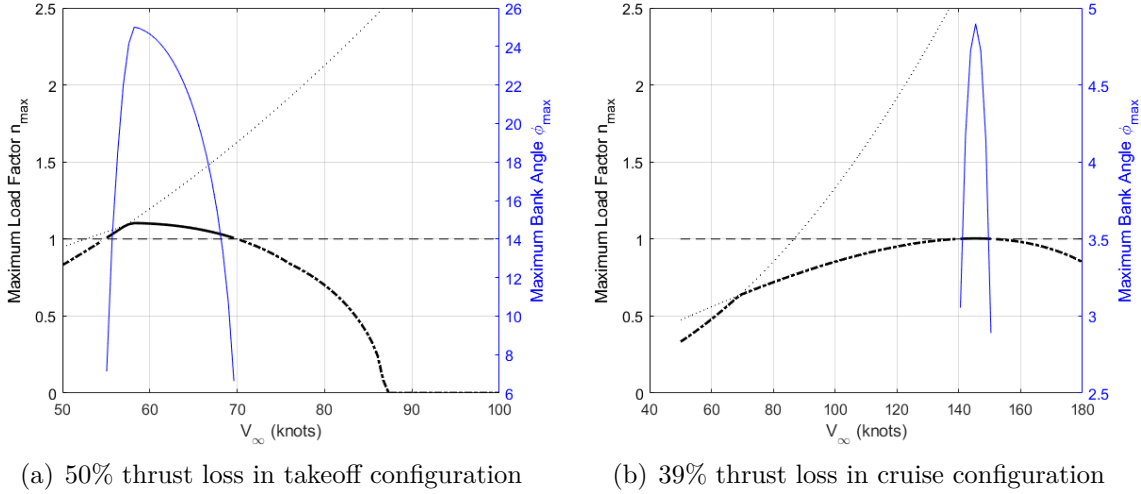


Figure 42: Thrust loss resulting in $n_{max} = 1$ for the T-DEP

the aircraft can barely maintain a steady level flight with a thrust degradation of 39% at 140 knots. However, such a thrust loss does not make this off-nominal condition catastrophic automatically, since the aircraft is likely to have enough time to descend and activate the high lift propulsors to make an emergency landing. Therefore, the condition of losing 39% thrust is characterized as ‘Hazardous’ for the cruise configuration.

The next off-nominal consideration comes from certification considerations. The X-57 can be classified as a low-speed ($V_{NO} < 250$ kn, certification level 1 ($\leq 1pax$)) multi-engine aircraft according to 14 CFR 23.2005 [72]. Interestingly, the aircraft it is based on, the Tecnam P2006T is a certification level 2 aircraft ($3pax$). However, there is little change to the regulatory framework between the two as a result of this change. One particular standard requirement of interest here comes from the accepted means

of compliance (MoC) standard ASTM F3173 sections 4.9.1 and 4.9.2 [9, 73]. Section 4.9.1 states,

“4.9.1 *Takeoff* – It shall be possible, using a favourable combination of controls, to roll the aeroplane from a steady 30° banked turn through an angle of 60°, so as to reverse the direction of turn within:

4.9.1.1 For an aeroplane of 2722 kg [6000 lbs] or less maximum weight, 5 s from the initiation of roll”

ASTM F3173 section 4.9.2 requires that 4.9.1 be met for the T-DEP at a critical loss of thrust, with the flaps in takeoff position at 70 knots ($1.2 \times V_{stall}$) [9]. While it would be ideal to simulate this condition using a 6-DoF dynamic model to evaluate the aircraft’s response, thrust degradation scenarios can be explored at the conceptual stage using Eq. 64 to determine the % thrust loss beyond which the aircraft cannot maintain a 30° bank angle. Figure 43(a) gives the result of a 39% degradation in thrust

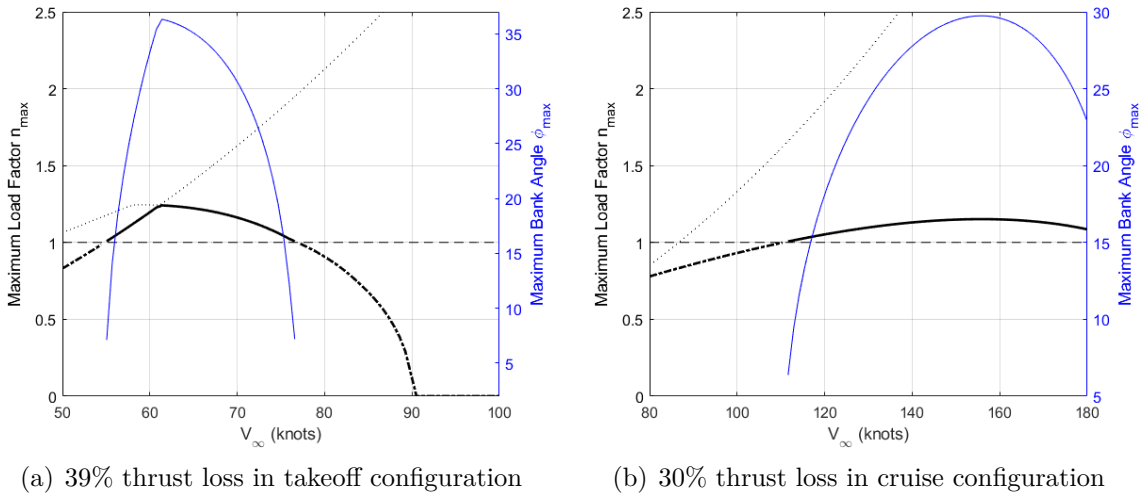


Figure 43: Thrust loss resulting in $\phi_{max} \leq 30^\circ$ for the T-DEP

for the T-DEP. In this off-nominal scenario, the aircraft is barely able to manage a 30° bank angle at 70 knots as is required by the regulations. Therefore, this scenario is rated as hazardous in terms of severity. Since the T-DEP aircraft does not have an

obvious definition of a critical loss of thrust in terms of a traditional one-engine out scenario, such certification considerations can be reverse-engineered to define what a critical loss of thrust is. In this case, using a safety metric of ϕ_{max} within C-FHA, a critical loss of thrust can be defined at a 39% loss of thrust during takeoff – as that which does not meet ASTM F3173 section 4.9.2. The cruise condition does not have any regulatory requirement for bank angle attainable to the best of the author’s knowledge. Therefore, engineering judgement is used to utilize the capability of 30° bank angle as a scenario to define a ‘Major’ hazard severity condition. Figure 43(b) shows that above a 30% loss of thrust in cruise configuration, the T-DEP cannot attain a 30° bank angle. Thus this condition is rated as ‘Major’.

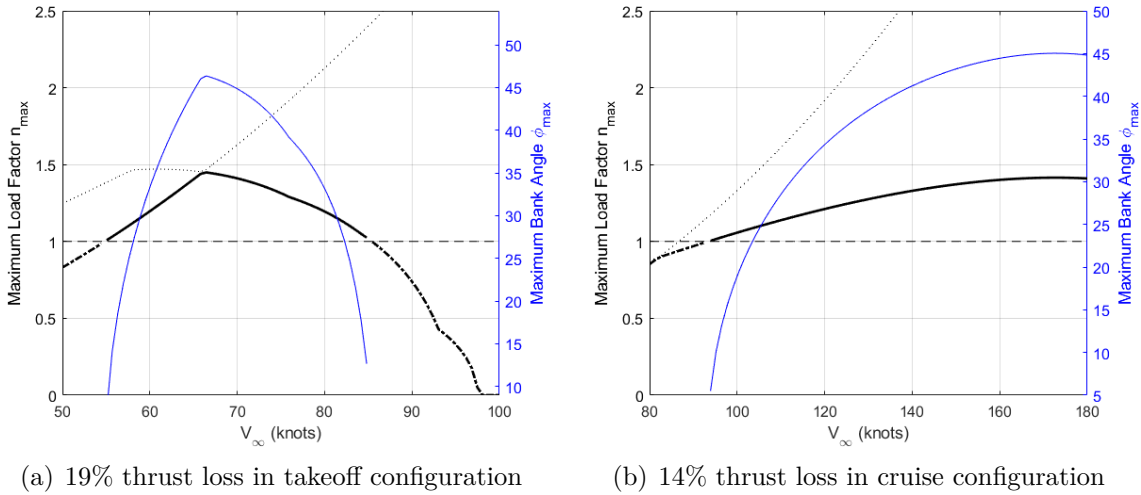
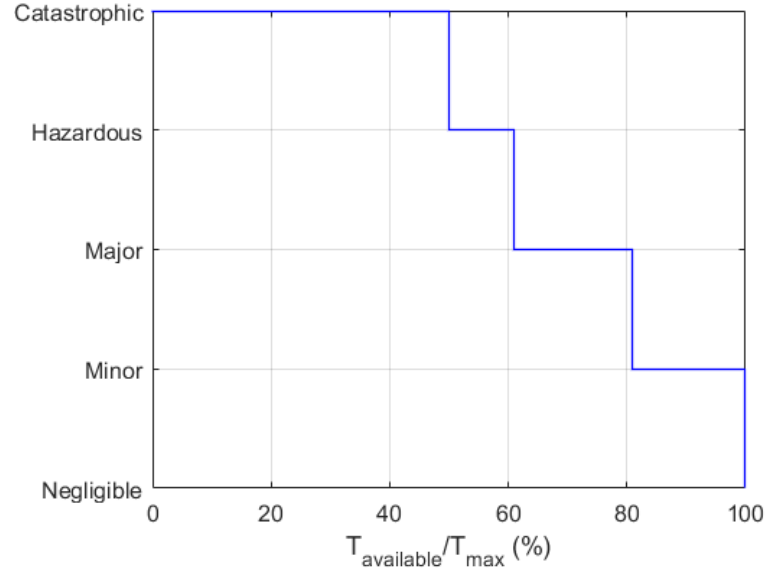


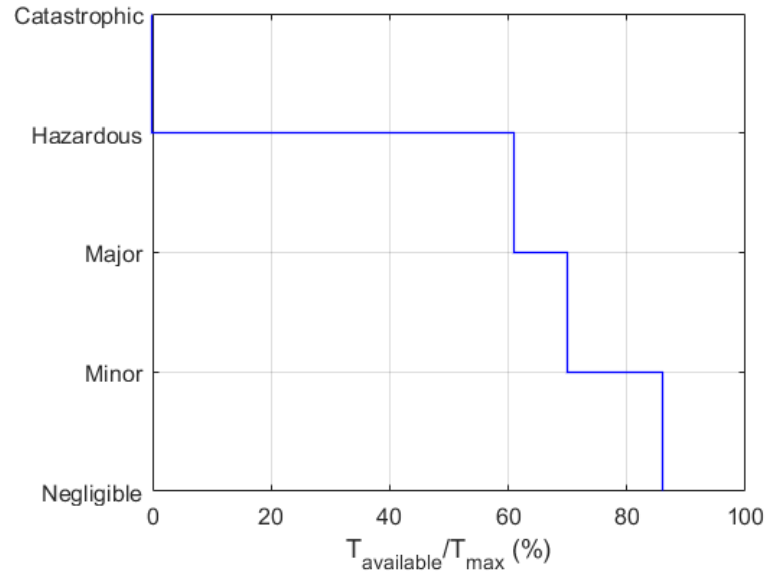
Figure 44: Thrust loss resulting in $\phi_{max} \leq 45^\circ$ for the T-DEP

The final case in the present analysis pertains to utilizing engineering judgement to call a situation when the T-DEP in takeoff configuration cannot attain a 45° bank angle as a major hazard. Ideally, subject matter experts may assign a severity based on their judgement of appropriate off-nominal scenarios. Figure 44 provides the thrust degradation scenarios designated as having a ‘Major’ severity during takeoff and ‘Minor’ in cruise configuration. Thus, a thrust loss of 19% during takeoff, or 14% during cruise are assigned their severity.

The results stated above can be utilized to define a function-loss hazard severity curve for the takeoff and cruise conditions using the n_{max} , ϕ_{max} safety metrics (see fig. 45).



(a) Takeoff



(b) Cruise

Figure 45: C-FHA hazard severity for the T-DEP aircraft due to thrust degradation using n_{max} , ϕ_{max} metrics

4.3.4.3 Maximum Potential Climb Gradient (MPCG)

The maximum potential climb gradient metric was first introduced as energy based metric under chapter 4.2. It is defined using equations 18 and 19. The derivation and equations are repeated here for ease of reading.

$$P_{S_{degraded}} = \frac{(T_{degraded} - D)V_{\infty}}{W} \quad (66)$$

$$\begin{aligned} \gamma_{max} &= \sin^{-1} \left(\frac{dh/dt}{V_{\infty}} \right) \\ &= \sin^{-1}(P_{S_{degraded}}/V_{\infty}) \end{aligned} \quad (67)$$

Under a thrust degradation scenario, the MPCG metric is a direct indicator of the specific excess power available to the aircraft. Additionally, some certification requirements posed by 14 CFR 23 Subpart B specify a minimum climb gradient that the aircraft should be able to demonstrate under a critical loss of thrust. The only information needed to compute this metric includes the degraded values of thrust, the drag computed using Eq. 42, the maximum takeoff gross weight, and an assumed velocity. Since specific excess power contours are usually plotted against axes of altitude and velocity, MPCG contours are examined in a similar way in the results in this section.

Figure 46 examines the MPCG (in %) contours against altitude and velocity for four different thrust degradation scenarios in the takeoff configuration. The lowest plot gives the MPCG at nominal conditions of 0% thrust loss ($T_A = T_{degr}/T_{max}$ is the thrust available ratio under degradation). Regulatory requirements given in 14 CFR 23.2120(a)(1) necessitate the T-DEP to have an 8.3% climb gradient capability at 50 feet above the runway with all engines operating [72]. As can be seen in the lowest plot, the T-DEP is capable of meeting this requirement for runway altitudes of ≤ 5000 feet.

Next, the topmost subplot is discussed, with a thrust loss of 50%. As is visible, at 50% or more degradation in thrust, the T-DEP is no longer able to maintain even

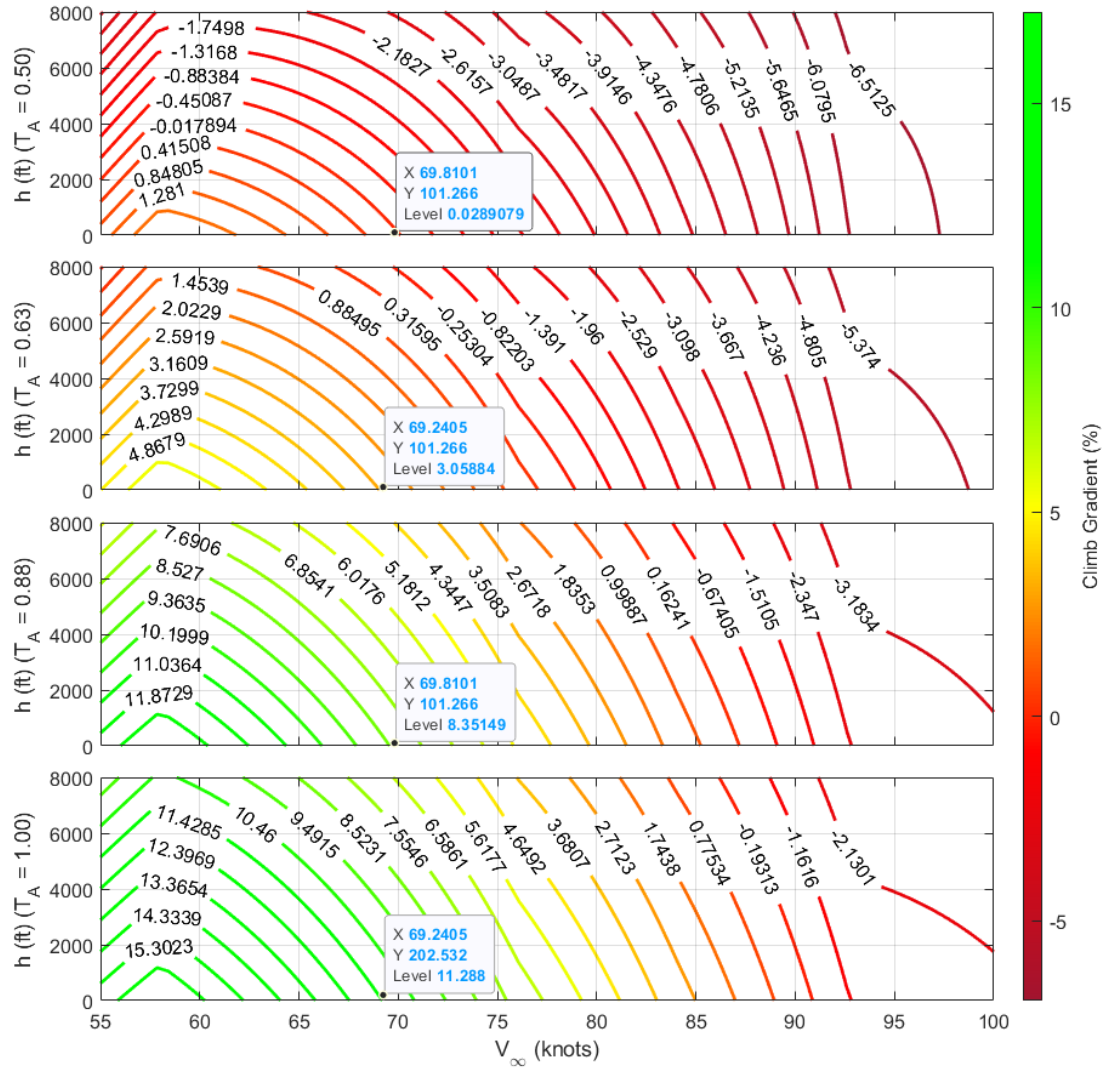


Figure 46: MPCG under thrust degradation scenarios at takeoff for the T-DEP

a steady level flight at sea level (let alone a climb!) at 70 knots ($1.2 \times V_{stall}$). This result complements a similar result from the n_{max} , ϕ_{max} metrics given in figure 42. This hazard is therefore characterized as ‘Catastrophic’.

The second subplot from the top in figure 46 displays the results for MPCG under a 37% degradation in thrust. 14 CFR 23.2120(c) requires the aircraft to be able to manage a 3% climb gradient during balked landing [72]. While there is no stipulation

for this to be met during a critical loss of thrust, a scenario under which an aircraft might have to go abort landing and go-around under a loss of thrust scenario can be imagined. In such an off-nominal scenario, any more than 37% loss of thrust means that the T-DEP cannot maintain a 3% climb gradient at sea level. This is rated ‘Hazardous’.

The third subplot in figure 46 shows the performance of the T-DEP in terms of its MPCG under a 12% loss of thrust ($T_A = 0.88$). Beyond this value, the T-DEP is unable to maintain an 8.3% climb gradient at sea level at 70 knots. While this is not a regulatory requirement, engineering judgement can be used to categorize any worse a thrust loss as at least a ‘Minor’ hazard.

Figure 47 examines the MPCG (in %) contours against altitude and velocity for four different thrust degradation scenarios in the cruise configuration. The lowest plot gives the MPCG at nominal conditions of 0% thrust loss. As can be seen in the lowest plot, the T-DEP is capable of maintaining a positive climb gradient at all velocities and altitudes in the cruise phase.

The second subplot from the bottom gives MPCG under an off-nominal scenario of 14% thrust loss. 14 CFR 23.2120(b)(1) requires the T-DEP to be able to provide a climb gradient of 1.5% at an altitude of 5000 feet in cruise conditions under a critical loss of thrust. Any more than 14% thrust loss means that the T-DEP will be unable of meeting this requirement. This condition is therefore rate ‘Major’. Conversely, since a traditional definition of a critical loss of thrust (one engine inoperative) does not apply to the T-DEP, regulations such as these could be used to reverse engineer what a critical loss of thrust means. Therefore, a 14% thrust loss could be classified as a critical loss of thrust.

The third subplot from the bottom considers a scenario where thrust has been degraded by 39%. In this case, the aircraft is unable to maintain a steady level flight at any combination of velocity and altitude and must prepare for an emergency

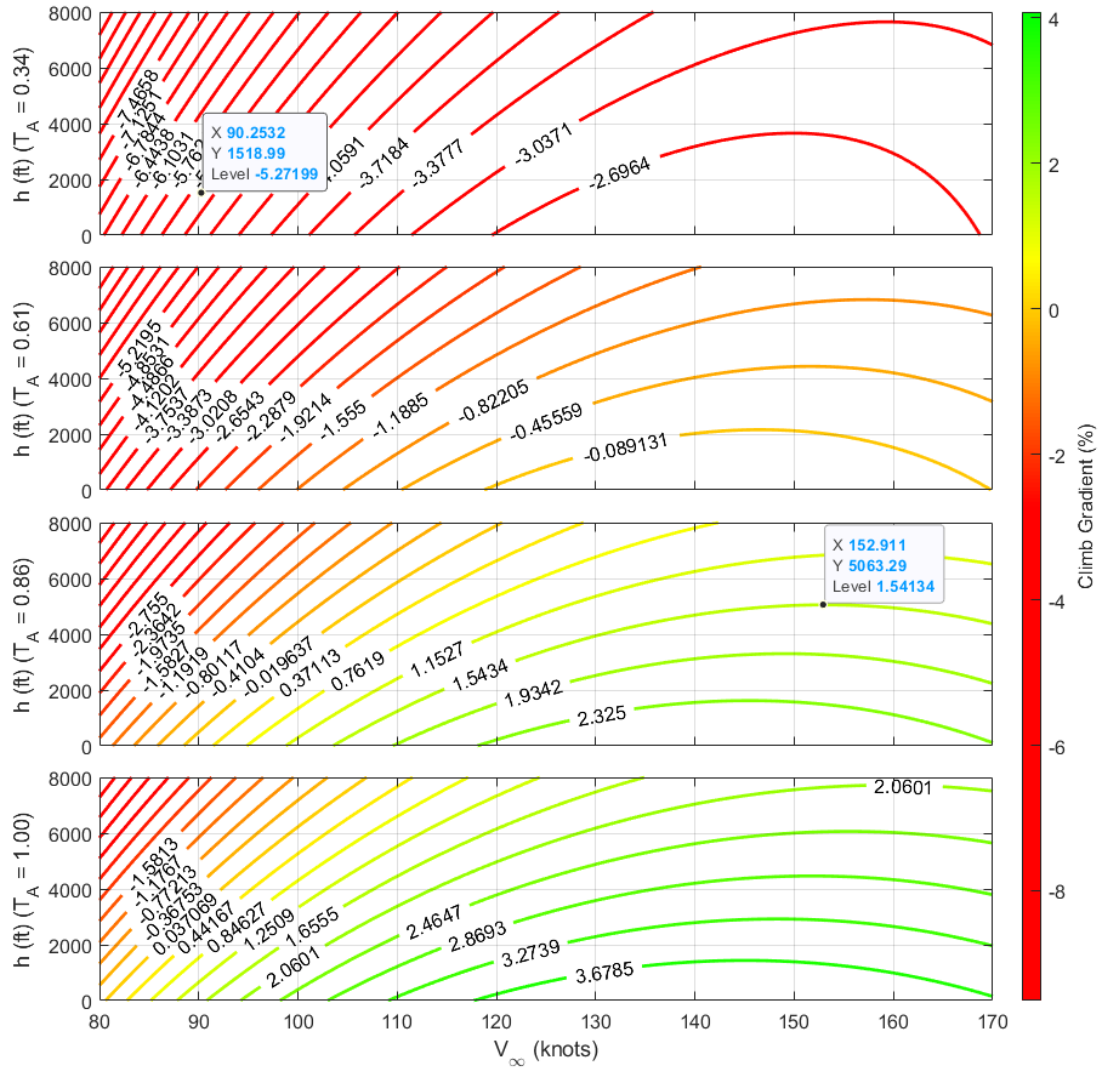


Figure 47: MPCG under thrust degradation scenarios at cruise for the T-DEP

landing. This is therefore rated as ‘Hazardous’.

Finally, in the topmost subplot, a thrust loss of 66% or more results in the T-DEP being unable to maintain a 3° or 5.2% glideslope at the point of transitioning from the cruise configuration to landing configuration (1500 feet, 90 knots). If the failure state is such that switching on the functioning number of high lift propulsors (HLPs) does not result in the takeoff power availability to cross 50% (see Fig. 46),

this can lead to a crash. Therefore, this cruise condition is conservatively categorized as ‘Catastrophic’.

The results stated above are utilized to define a function-loss hazard severity curve for the takeoff and cruise conditions using the MPCG (γ_{max}) safety metric (see Fig. 48).

4.3.4.4 C-FHA Results Summary

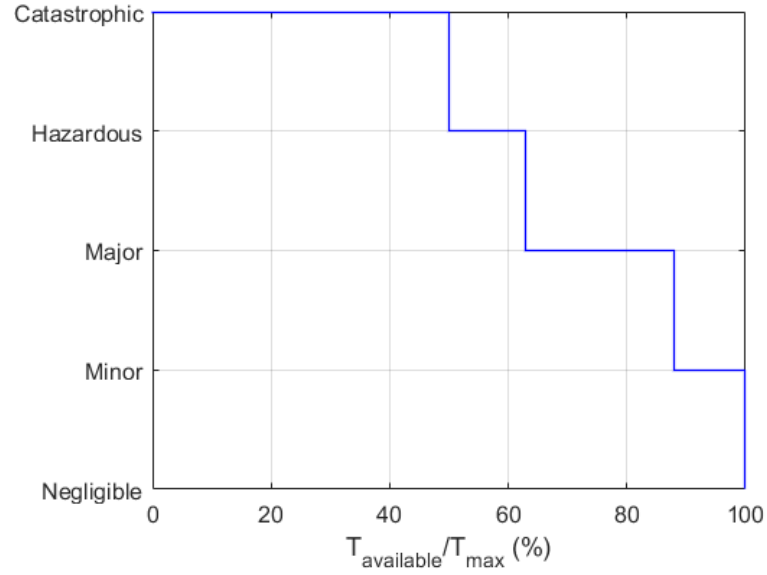
In this final step of C-FHA, the results generated using various safety metrics are combined to get one hazard severity to functional degradation mapping for every aircraft configuration of interest.

Figure 49 shows the hazard severity computed at takeoff and cruise configurations of the T-DEP. It is evident that the MPCG (γ_{max}) metric ends up being the more stringent in terms of allocating hazard severity to loss of thrust for both configurations. With this, the process of allocating hazard severity to continuous functional degradation (C-FHA) is complete. The results of this exercise are summarized in table 17.

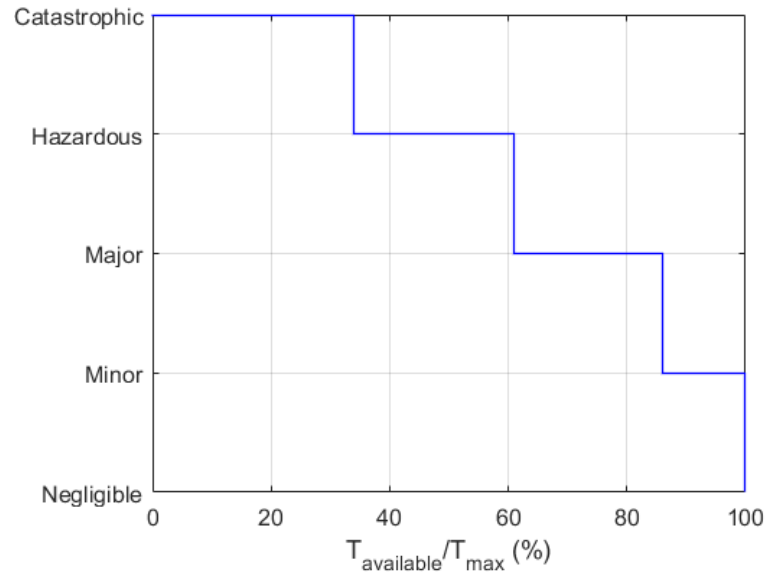
Table 17: Summary of hazard severity for continuous thrust loss for the T-DEP

Severity Configuration	Minor	Major	Hazardous	Catastrophic
Takeoff	$0.88 \leq T_A < 1$	$0.63 \leq T_A < 0.88$	$0.50 \leq T_A < 0.63$	$T_A < 0.50$
Cruise	$0.86 \leq T_A < 1$	$0.61 \leq T_A < 0.86$	$0.34 \leq T_A < 0.61$	$T_A < 0.34$

Table 2 provides the allowable failure rates for different hazard severity for aircraft certified under different assessment levels. Combining those with the functional hazard severity allocation for an assessment level II (≤ 1 pax, multiengine) T-DEP airplane provides us with allowable failure rate requirements allocated to the ‘Provide Thrust’ function under different continuous thrust degradation scenarios. Minor, Major, Hazardous, and Catastrophic failures must have a failure rates $\leq 10^{-3}$, $\leq 10^{-5}$, $\leq 10^{-6}$ and $\leq 10^{-7}$ per flight hour respectively. This results in figure 49 being recast



(a) Takeoff

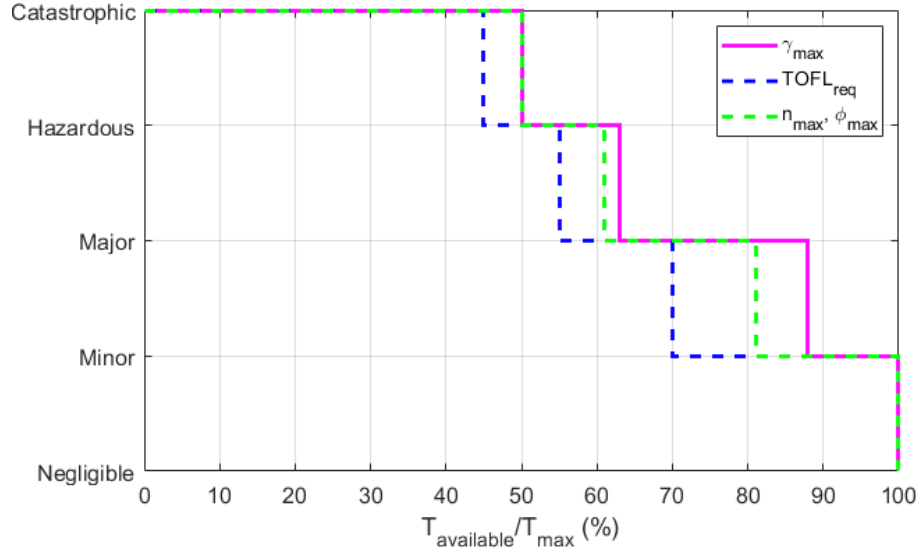


(b) Cruise

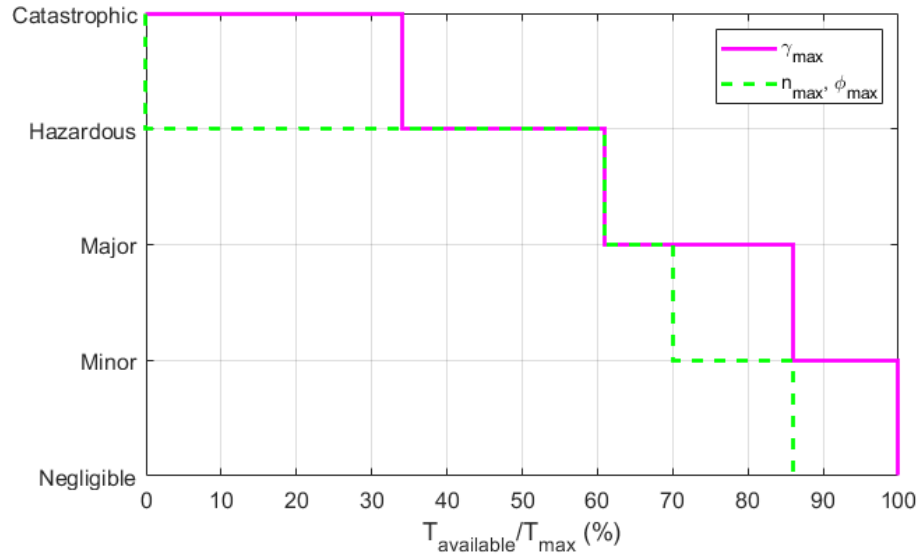
Figure 48: C-FHA hazard severity due to thrust degradation using MPCG (γ_{max}) metrics

into allowable failure rate requirements versus function loss curves which are shown in figure 50

When compared to figures 34 the results obtained by treating function loss as continuous and utilizing aircraft conceptual models are evidently better. Figure 49,



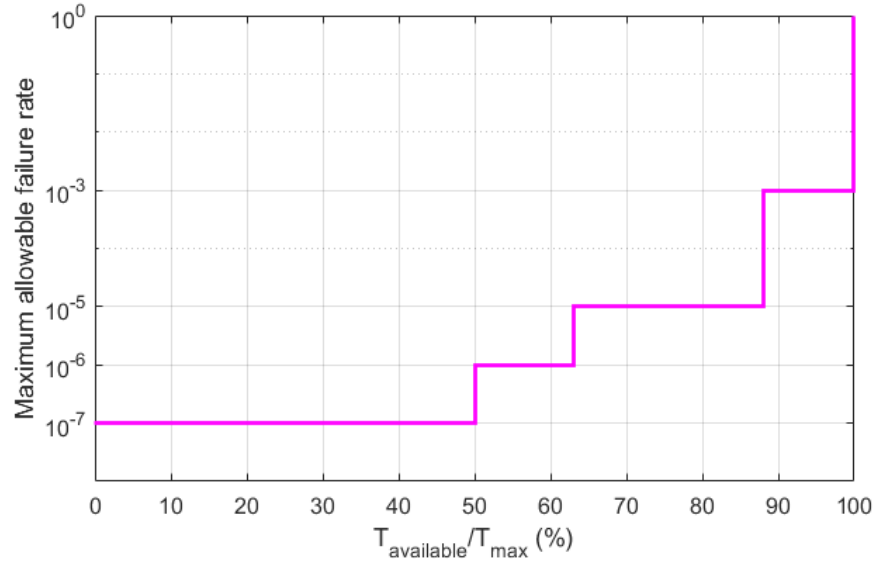
(a) Takeoff



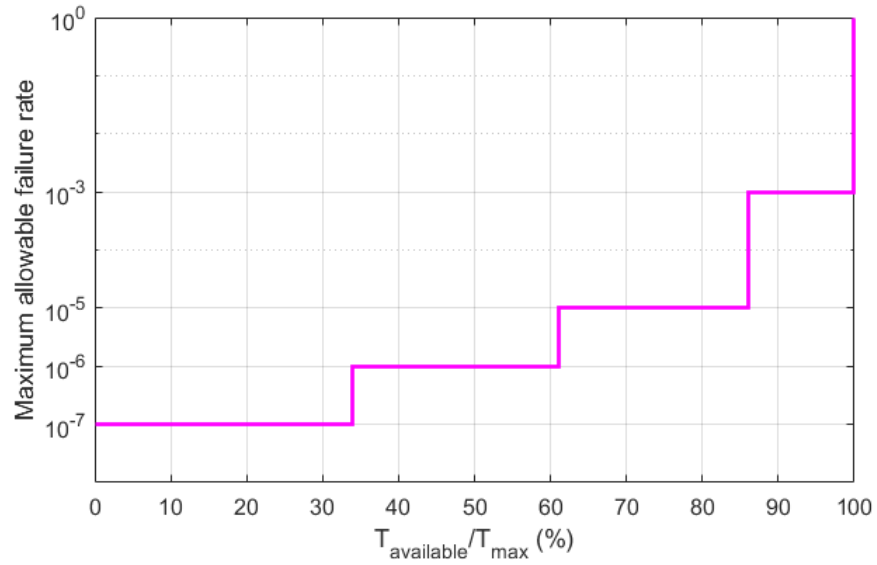
(b) Cruise

Figure 49: Summary of C-FHA hazard severity due to thrust degradation for the T-DEP aircraft using the different safety metrics discussed

50, and table 17 provide a much better resolution of the hazard severity allocated to the function ‘Provide Thrust’, thus avoiding any biases in architecture design. The results from C-FHA being backed by physics based models, are also more accurate to heuristically defined hazards using traditional FHA. When higher fidelity models are



(a) Takeoff



(b) Cruise

Figure 50: Summary of C-FHA allowable failure rate allocation to thrust degradation for the T-DEP

available, the analyses in the present section can be augmented to provide a better characterization of the safety related off-nominal requirements.

4.3.5 Performance-based Multi-state Analysis Results

Revisiting the T-DEP power system architecture from figure 33 shows that the T-DEP aircraft has 2 cruise motors providing thrust on the cruise configuration, while the 12 high lift propulsors (HLP) augment thrust and high lift characteristics during the takeoff phase. Additionally, each battery provides half the power to each cruise motor through redundant traction power buses, pre-chargers, and inverters. Thus, a cruise motor may fail completely, or it may operate at half power – that is, cruise motors have three operational states individually (one nominal, two failed). Similarly, the HLPs may fail individually due to different faults that get introduced into the system. Asymmetric thrust loss is not considered in the C-FHA analysis due to the conceptual level of detail of the models. Even then, this leaves the T-DEP power system under consideration with 51 unique failure states as are shown in figure 51.

No. HLP failed	0	1	2	3	4	5	6	7	8	9	10	11	12
No. CM failed													
0	1.00	0.95	0.91	0.86	0.82	0.77	0.72	0.68	0.63	0.59	0.54	0.49	0.45
0.5	0.89	0.84	0.80	0.75	0.70	0.66	0.61	0.57	0.52	0.47	0.43	0.38	0.34
1	0.78	0.73	0.68	0.64	0.59	0.55	0.50	0.45	0.41	0.36	0.32	0.27	0.22
2	0.55	0.51	0.46	0.41	0.37	0.32	0.28	0.23	0.18	0.14	0.09	0.05	0.00

Figure 51: T-DEP multistate T_a/T_{max} in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)

No. HLP failed	0	1	2	3	4	5	6	7	8	9	10	11	12
No. CM failed													
0	1	1	1	1	1	1	1	1	1	1	1	1	1
0.5	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75
1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
2	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 52: T-DEP multistate T_a/T_{max} in cruise configuration. Colored by C-FHA hazard severity from Fig. 49(b)

The unique (assumed) symmetric failure states for thrust involve failures of 0-12 HLPs, and 4 states of the two cruise motors combined. The resultant thrust of these states is computed using the propulsion model given in chapter 4.3.3.3. The ratio of this computed thrust to the nominal takeoff thrust is given in figures 51, 52. The different cells are colored from red to green to characterize hazard severity of ‘Catastrophic’ to ‘Negligible’

While conceptual analysis under C-FHA considered symmetric loss of thrust as off-nominal scenarios, asymmetric thrust loss is likely to result in more constraining requirements for an architecture like the X-57, with its cruise motors located at the wingtips. For asymmetric thrust loss in this case, only motors on one side (left) of

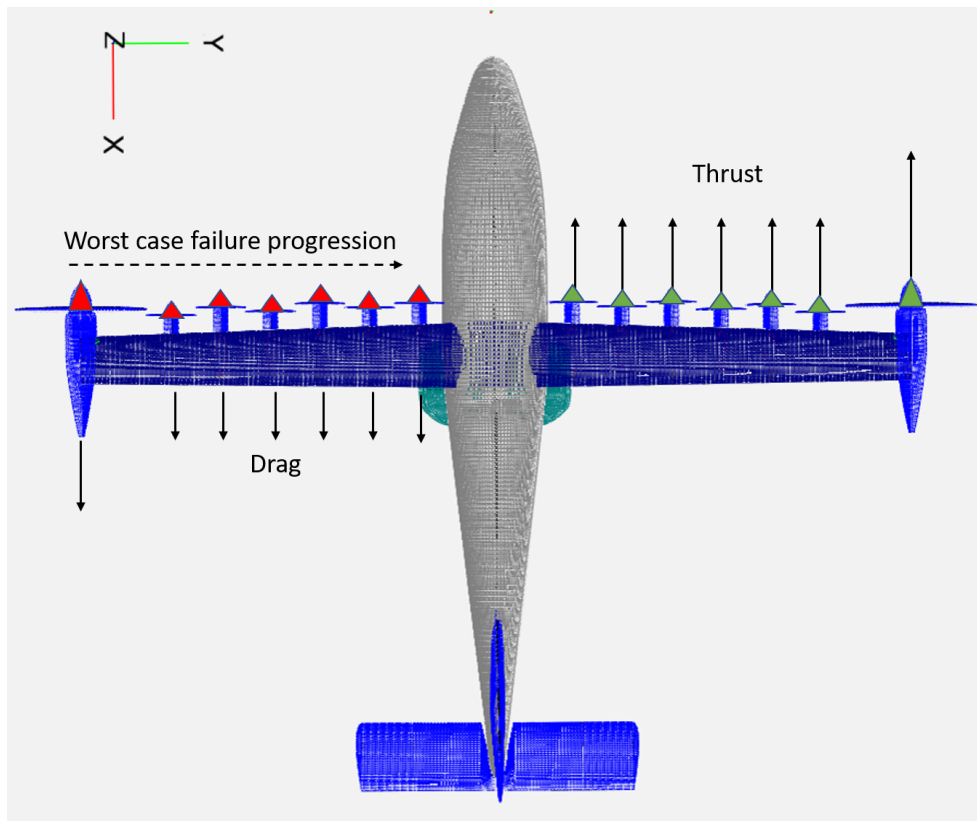


Figure 53: T-DEP asymmetric loss of thrust multi-state failures

the wing are assumed to fail. The left cruise motor can once again take 3 states - nominal, or fail at 50% or 0% thrust. The number of states with n high lift propulsors

(HLPs) failing is given by 6C_n . However, the most critical of these states is when the most outboard n HLPs fail generating a greater yawing moment. Thus, instead of investigating all $3 \times 2^6 = 192$ asymmetric thrust loss failure states, only 21 (3 cruise motor states \times 7 HLP states (0 to 6 HLP fails)) represent the most critical and need to be investigated. This is qualitatively shown in figure 53.

The idea of performance-based multistate analysis is inspired by the work of Dominguez-Garcia [60] and Agte [16], who utilized 6-DoF dynamic simulation models to identify off-nominal states and their probabilities. However, they stopped short of allocating severity requirements to the system and component level. In the present work, in order to evaluate the effect of asymmetric loss of thrust, a preliminary 6-DoF model that can perform trim analysis is utilized. The details of the aircraft model are given in chapter 4.3.3. The implemented 6-DoF framework’s structure is given in figure 35. The T-DEP model is created so that each motor is its own object, providing thrust according to its state, in its own axis. Similarly, the aerodynamic forces and moments are computed for every lifting surface individually. These forces and moments are then transferred to the aircraft’s reference point with suitable transformations to be used in the equations of motion. This framework provides an added benefit to the C-FHA analysis. While C-FHA considered only the function ‘Loss of thrust’, the present 6-DoF model considers failures of the different high lift or cruise motors. Since the high-lift motors also augment the lift characteristics in addition to providing thrust, a loss of HLPs results in a loss of not just the thrust, but a reduction in the T-DEP’s aerodynamic performance as well. This is captured in the 6-DoF model that is generated, thus allowing a more integrated and complete assessment of the T-DEP architecture. Finally, a trim algorithm proposed by Marco et al. [120] that utilizes a minimization technique to determine a trim solution for any input combination of aircraft state, control deflections, environmental conditions, and propulsive state is implemented alongside the 6-DoF model. The trim objective is to

match the mission V_∞ , h , while maintaining wings level ($\phi = 0$) and maximizing γ .

Table 18 provides results of the 6-DoF trim analysis for the T-DEP in the cruise configuration at 1500 feet and 105 knots. The column ‘CM-1 Loss %’ gives the ratio of thrust loss on the left cruise motor – 0 denotes nominal operation, 0.5 denotes 50% thrust loss, while 1 denotes complete loss. The angles γ_{max} , θ , ψ , as well as the control deflections δ_a , δ_r are in degrees. τ denotes the throttle setting on the left and right cruise motors. At nominal conditions, the T-DEP can climb at an angle of 1.17° , which is just over a 2% gradient (in agreement with conceptual analysis from Fig 47).

The throttle setting translates to thrust using equation 27, where it can be seen that thrust is proportional to the square of the throttle setting. Maximum continuous power is modeled as 90% throttle setting to represent 90% RPM (2250 RPM) of the cruise motor. Thus, 50% of maximum continuous power occurs at $90\%/\sqrt{2} = 64\%$. The second row of table 18 denotes cruise motor-1 (left) at 50% thrust (64% throttle). As is visible, the T-DEP cannot maintain steady level flight if half the thrust is lost in any one of the wingtip cruise motors. This is assigned a severity of ‘Major’ since the T-DEP is forced to conduct an emergency landing. For a complete loss of thrust from the left wingtip cruise motor, the trim solution provided a maximum climb gradient of -4.84% (-2.77°), which still allows a glideslope of less than 3° . This is also considered a ‘Hazardous’ condition in agreement with the results of figure 52. The energy rate margin (ERM) metric is defined in equation 23, and provides a ratio of the specific excess power being utilized in climb, to the maximum specific excess power available after degradation in thrust. Thus, even after a failure, if this metric is closer to 1, it denotes that most of the excess power is going towards ensuring a maximum climb gradient. The nominal case from table 18 shows this to be close to 1. The other two cases do not depict a value since they are under a negative climb gradient, which reduces the utility of this metric. However, it is important to note

Table 18: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)

CM-1 Loss %	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0	2.04	7.7	0	0	0	0.9	0.9	0.97
0.5	-0.31	6.38	-4.53	0.69	-13.75	0.64	0.9	-1.33
1	-4.84	3.84	-4.97	0.76	-15.09	0	0.66	-1.83

that under the complete loss of the left cruise motor, the right cruise motor cannot operate at maximum continuous power due to trim considerations. The rudder does not have enough authority to negate the yawing moment generated from the right wingtip cruise motor at over 66% throttle setting (54% thrust). Thus, a lot of the capacity of the right cruise motor that could have been used to increase the climb gradient to ensure a steady level flight is wasted.

Table 19: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

CM-1 Loss %	# HLP failed	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0	0	9.95	6.1	0	0	0	0.9	0.9	1
0	1	8.94	6.09	-4.98	0	-11.69	0.9	0.88	0.97
0	2	7.55	5.89	-4.92	0.02	-11.63	0.9	0.82	0.9
0	3	6.26	5.78	-4.73	0.07	-11.27	0.9	0.76	0.82
0	4	5.08	5.77	-4.67	0.1	-11.22	0.9	0.72	0.74
0	5	4.05	5.87	-4.91	0.16	-11.87	0.9	0.69	0.66
0	6	3.11	6.05	-4.91	0.21	-11.96	0.9	0.67	0.58
0.5	0	5.56	3.66	-5	-0.05	-11.63	0.64	0.7	0.74
0.5	1	4.05	3.37	-4.87	-0.02	-11.43	0.64	0.61	0.6
0.5	2	2.67	3.17	-4.84	0.02	-11.44	0.64	0.52	0.45
0.5	3	1.41	3.08	-4.97	0.06	-11.83	0.64	0.43	0.27
0.5	4	0.24	3.06	-4.88	0.1	-11.7	0.64	0.35	0.05
0.5	5	-0.80	3.16	-4.93	0.15	-11.91	0.64	0.28	-0.22
0.5	6	-1.75	3.35	-4.94	0.2	-12	0.64	0.23	-0.61
1	0	0.59	0.85	-4.89	-0.06	-11.36	0	0.29	0.12
1	1-6	No Trim Solutions							

Table 19 provides results for the off-nominal cases resulting from asymmetric loss of thrust during takeoff. The idea is to consider the most critical conditions. When n high lift propulsors have failed, it is assumed the ones near to the wingtip fail first

to generate the most adverse yaw (see fig. 53). The first column provides the loss of capacity of the left wingtip cruise motor. A total of 21 states (1st row nominal, 20 off-nominal) are shown. Under nominal conditions, the T-DEP manages an MPCG of 9.95% (5.68°) at 1.2x stall speed. Conditions showcasing negative γ_{max} are considered catastrophic since the aircraft cannot maintain a steady level flight right after takeoff. The energy rate margin (ERM) metric is also given for the different failure states. An ideal value of 1 for ERM would mean that the aircraft is utilizing all thrust available to reach the γ_{max} value. However, the majority of asymmetric failure states for the T-DEP showcase an ERM that is smaller than 1 but greater than 0. This means that even after failures, the T-DEP has additional thrust capability available that can be utilized to increase the climb gradient. However, the aircraft cannot trim due to a lack of vertical tail's (VT) lateral authority. This is especially true for the cases where ERM lies between -1 and 0. In these cases, the aircraft is descending without utilizing available thrust due to a lack of VT authority. As a result, if HLPs or even the cruise motor on the left side suffer failures, the throttle setting to the right cruise motor needs to be cut back in order to allow the VT to counter the adverse yaw generated. This in turn means that less excess power is available to climb, which reduces γ_{max} . Partial loss of thrust in cruise showcases values of ERM that are less than -1. As discussed while introducing the metric, this means that the aircraft is in descending flight when it should be climbing, and its thrust available post failure is less than the drag generated in the trim solution. Thus, the aircraft is thrust limited when CM-1 loses 50% of its thrust output. When CM-1 fails completely, the aircraft is limited both by its thrust as seen by ERM metric, but also by its rudder authority since CM-2 throttle is set at less than 0.9 (maximum continuous) at trim.

Figure 54(a) provides a summary of γ_{max} for the 20 off-nominal states of the T-DEP aircraft when considering the most critical asymmetric loss of thrust scenarios as discussed previously. The cells are colored according to the hazard severity

No. HLP failed	0	1	2	3	4	5	6
CM-1 Loss %							
0	9.95	8.94	7.55	6.26	5.08	4.05	3.11
0.5	5.56	4.05	2.67	1.41	0.24	-0.80	-1.75
1	0.59	-	-	-	-	-	-

(a) $\tan(\gamma_{max})$ (%)

No. HLP failed	0	1	2	3	4	5	6
CM-1 Loss %							
0	1	0.97	0.9	0.82	0.74	0.66	0.58
0.5	0.74	0.6	0.45	0.27	0.05	-0.22	-0.61
1	0.12	-	-	-	-	-	-

(b) *ERM*

Figure 54: T-DEP multistate asymmetric thrust loss in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)

considerations based on the different requirements for γ_{max} as discussed under C-FHA (see Ch. 4.3.4.3). Thus, while C-FHA assigned hazard severity purely based on loss of thrust as seen in fig. 51, the present results indicate that thrust asymmetry considerations dominate the requirements allocation as compared to simple loss of thrust considerations. Figure 54(b) provides the ERM metric for the different states discussed above in a more intuitive format.

Overall, it can be seen that performance-based multistate analysis provides much greater resolution in terms of aircraft level failure states and the requirements posed by them compared to the benchmark results from tables 6, 7. It also identifies requirements posed due to functional loss considerations (e.g. asymmetric loss of thrust) that would not be apparent through the extended C-FHA approach.

4.3.6 Summary of Experiment 1.2

This experiment demonstrated how safety metrics of interest can be used to identify and characterize hazards during off-nominal operations during conceptual and early

preliminary design. It provided the details of the conceptual models and a preliminary 6-DoF model of the T-DEP that were created to estimate the safety metrics from table 5. Wherever possible, certification considerations were utilized to identify the threshold values of the safety metrics. At other times, engineering judgement was utilized to identify thresholds. These thresholds are then used to characterize the hazard severity of the different functional degradation scenarios, as well as the different off-nominal failure states of the T-DEP. It was noticed that the maximum potential climb gradient (MPCG) metric was the most constraining in allocating safety requirements to the functional degradation scenarios. This metric was utilized along with the energy rate margin (ERM) metric to characterize the T-DEP's multi-state asymmetric loss of thrust conditions. There it was noticed that while the T-DEP has the specific excess power to improve its performance under failure, it is restricted by the lateral control authority of the vertical tail due to the large yawing moments generated from wingtip propellers. Overall, compared to benchmark results from literature, experiment 1.2 demonstrated that the proposed combination of continuous FHA with performance-based multistate analysis provides a more comprehensive treatment of loss of thrust off-nominal conditions at the conceptual and preliminary design stages. The new methods also provide a greater resolution into hazard severity allocation at the aircraft level than the benchmark. These results, therefore, fulfil the purpose of the experiment given in Ch. 4.3.1.1, and verify hypothesis 1.2.

4.4 Unit Level Allocation

The next research subquestion in this dissertation deals with allocating the aircraft level requirements generated in previous sections at the unit level. Research question 1.3 is restated here for convenience:

Research Question 1.3:

How can the identified aircraft level off-nominal requirements be allocated to the unit level?

Allocation of system reliability requirements to the components is completed in the present work by utilizing a network based bottom-up analysis to determine the effect of single component failures on the terminal components of interest. Here an assumption is made with respect to aircraft operations – that the probability of multiple components failing at the same time is low enough to be ignored during the allocation exercise. Losses of terminal components (cruise motors or high lift motors for the T-DEP) result in a loss of a function (thrust). Thus, the effect of single component failures on the aircraft function loss, or on aircraft failure state can be quantified, and the resultant requirements identified from Ch. 4.3. These requirements can then be identified to the unit level, leading to hypothesis 1.3 which is stated as:

Hypothesis 1.3: *If unit level failures are mapped to system level failure states, the allowable failure rate requirements generated at the system level can be allocated to the unit level*

4.4.1 Experiment 1.3

The intent of the present section is to test hypothesis 1.3. A bottom up analysis to quantify effects of component failures in terms of aircraft performance for the T-DEP is carried out automatically using a network algorithm. The results of this analysis are used to complete the unit level allocation of reliability requirements. A brief overview of the steps followed in this experiment is given in figure 55.

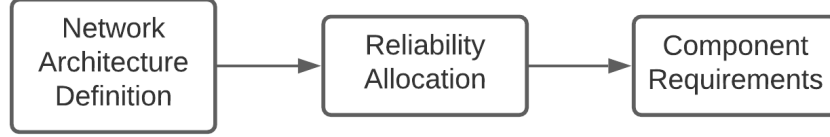


Figure 55: Allocating aircraft level requirements to the unit level

4.4.1.1 Purpose of the Experiment

Research question 1.2 and the solutions proposed generated safety related off-nominal requirements in terms of hazard severity and allowable failure rates at the aircraft level for the T-DEP power system architecture. RQ 1.3 takes this forward by trying to allocate those aircraft level requirements to the component level. This research subquestion deals with requirement 3 that was stated under research question 1 in chapter 3.2. Thus, the following are the main objectives of this experiment:

- Demonstrate the ability to determine the impact of component failures at the aircraft level
- Demonstrate a method to allocate reliability to the unit level by utilizing information generated above

4.4.2 Network-based Bottom-up Analysis

For a bottom analysis to be automatically conducted, the algorithm used in this thesis considers a failure state of every component individually and determines its effect in terms of failures of the terminal components. Consider a simplified system along with its network adjacency matrix given by figure 56. An adjacency matrix (A) is a square matrix with rows and columns denoting the components of the system. If component i connects forward to component j , $A_{ij} = 1$, otherwise $A_{ij} = 0$. This system has dummy components D_1 , D_2 that aid with system reliability computations as will be explained later. The components of interest are the source components S_i , intermediate components I_i , and terminal components T_i . The system level failure

states are characterized by the failures in its terminal, function satisfying components T_i . Thus, this system has $2^3 = 8$ possible states (1 nominal, 7 off-nominal) that were provided earlier in table 4.

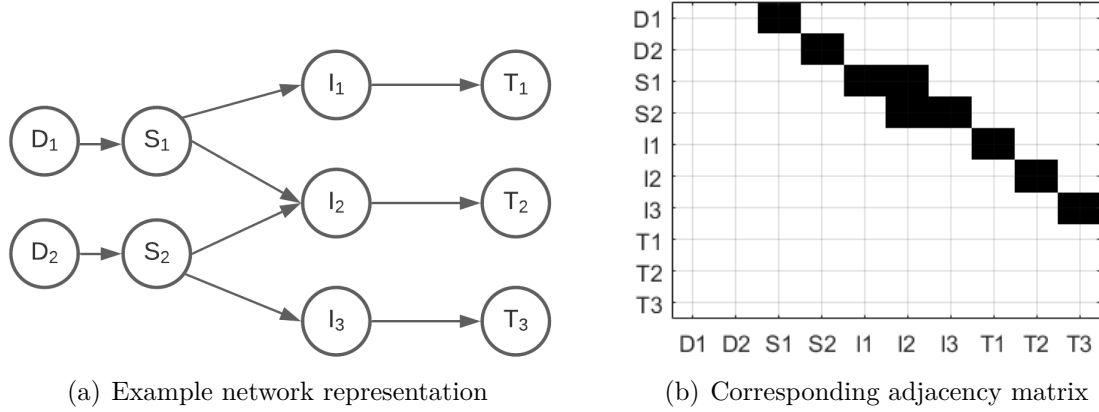


Figure 56: An example system with two sources and three terminal components in network representation

For the given system represented as a network of prime movers (nodes S_i), terminal components that satisfy system function (T_i) and intermediate components, Algorithm 1 is used to determine system failures states if any component (A_i) fails:

Algorithm 1: Generate a set of terminal components that fail if any system component fails

Result: Set of S_i that fail if component A_i fails
Generate system adjacency matrix M ;
Set $F = M$;
Set $F(i, :) = 0$ % set out-going network connections to 0;
Initialize $C = \text{zeros}(\text{size}(M))$;
Initialize $jj = 1$;
while F^{jj} is not zero **do**
 $C = C + F^{jj}$;
 $jj = jj + 1$;
end
truncate C to keep rows corresponding to all S_i and columns corresponding to all T_i and assign to C^* ;
Initialize $kk = 1$;
while $kk \leq \text{numCols in } C^*$ **do**
 if $\max(T(:, kk)) == 0$ **then**
 T_i corresponding to kk^{th} column of C^* has failed;
 Store T_i ;
 $kk = kk + 1$;
 else
 T_i corresponding to kk^{th} column of C^* has NOT failed;
 end
end

4.4.2.1 The Reliability Allocation Problem

Algorithm 1 generates a list of terminal failure states by individually setting each component to a failed state and evaluating the system level impact. If a terminal component loses a path to at least one source, the terminal component is assumed failed. Failing intermediate components is akin to breaking a link in a chain, whose end effects can thus be examined. Table 20 gives the results after applying the algorithm to the notional system from figure 56. Individual component failures are considered causal factors, with multiple components resulting in a common system state. Each failure state (T_i failed) is assigned a hazard severity H_i based on C-FHA or multistate analysis. This in turn results in a reliability requirement that must be satisfied. The total system reliability of not being in any state T_i is given by the ‘state

Table 20: System states resulting from component failures

Causal factors	S_1	I_1	T_1	I_2	T_2	S_2	I_3	T_3
Common system states			T_1		T_2			T_3
Hazard Severity			H_1		H_2			H_3
Reliability Requirement			$R(H_1)$		$R(H_2)$			$R(H_3)$
State Reliability	$R(S_1).R(I_1).R(T_1)$			$R(I_2).R(T_2)$		$R(S_2).R(I_3).R(T_3)$		

reliability' column, which identifies the unique, independent component failures that can result in the failure of T_i . This is not an exact formula of the system reliability from the given state but truncates the results to consider only one failure at once. The reliability of the system from state T_1 must meet the requirements posed by the hazard analysis. This is represented by the following equation,

$$R(S_1).R(I_1).R(T_1) > R(H_1) \quad (68)$$

Put another way, the system state reliability requirement $R(H_1)$ must be allocated to individual components S_1, I_1, T_1 such that Eq. 68 is satisfied. This is considered a classic reliability allocation problem. There is no single answer as to what is the correct way of going about this. Instead, literature treats reliability allocation problem as an optimization problem, where decision makers apply weights to each component depending on different factors, and then minimize a predetermined cost function to allocate reliability to the components [125]. The simplest way to complete such an allocation is to divide the reliability requirement equally between all elements as follows:

$$R(A_i) \geq R(H_1)^{1/3} \quad (69)$$

where A_i can be components S_1, I_1 , or T_1 . Notice that in such a case, Eq. 68 is satisfied. However, not all components are equally reliable, and therefore assigning them equal reliability requirements may not be the best solution. The question then is – how can this system level reliability be portioned to get a fair allocation of

requirements to the unit level?

4.4.2.2 The Critical Flow Method

Silvestri et al. [163] have provided a good review of the different reliability allocation methods, their advantages and disadvantages. They proposed a ‘Critical Flow Method’ that utilizes factors of influence to discriminate against different kinds of units. They recommend allocating system reliability requirement $R(t)$ to components using [163],

$$R_i(t) = R(t)^{W_i} \quad (70)$$

Where W_i is the weight for each component that is computed using,

$$W_i = \frac{IG_i}{\sum_{j=1}^n IG_j} \quad (71)$$

where IG is the global index of the specific component calculated using,

$$IG_i = \frac{C_i \cdot T_i \cdot K_i \cdot O_i}{A_i} \quad (72)$$

where C_i gives the component criticality and is $(1/n)$, n being the number of components in parallel. It allocates a higher reliability to a less critical component.

A_i represents the state of the art index, with 0 denoting old components, and 1 representing state-of-the-art. It assigns higher reliability to state-of-the-art components and lower to old components.

K_i represents component complexity. Suggested values include 0.33 for less complex components, 0.66 for normal, and 1 for highly complex components. It allocates higher reliability to less complex components.

T_i denotes the running time of a component to the time of the mission. Generally, for the test problem (T-DEP power system), this value is taken as 1.

Finally, O_i represents the operating conditions. Components exposed to the environment are allocated lesser reliability requirements, while those that operate in sheltered environments are allocated higher reliability. The suggested values here are 0.33 for

easy conditions, 0.66 for normal, and 1 for difficult conditions. Readers interested in more detail are referred to Ref. [163] for more.

4.4.3 The T-DEP Bottom-up Network Analysis

Algorithm 1 is used on the T-DEP power systems architecture given in figure 33 to obtain unique aircraft level failure states due to single component failures. Table 21 provides details about such unique failure states at the aircraft level and the causal factors. Due to symmetry in the T-DEP architecture, only one set of failures that

Table 21: Bottom-up analysis: T-DEP power architecture unique system level failure states and severity using C-FHA results

Failed Component (causal factor)	System level failure states	Thrust available after failure	Hazard Severity (C-FHA results)
CM-1	CM-1	$T_{ATO} = 0.84,$ $T_{Acruise} = 0.5$	Hazardous
PC-1B or Inv-1B	CM-1 at 50%	$T_{ATO} = 0.92,$ $T_{Acruise} = 0.75$	Major
PC-01 or Inv-01 or Mot-01	Mot-01	$T_{ATO} = 0.94,$ $T_{Acruise} = 1$	Minor
TPB-BL	Mot-1,3,5 ; CM-1 at 50%	$T_{ATO} = 0.75,$ $T_{Acruise} = 0.75$	Major
Battery-B	Mot-1,3,5,8,10,12; CM-1,2 at 50%	$T_{ATO} = 0.5,$ $T_{Acruise} = 0.5$	Hazardous

is identical to other failures is considered. For instance, failure in either left or right cruise motor individually leads to the same result of a hazardous flight condition. Similarly, any of the 12 pre-chargers ,inverters, or motors supplying the individual high lift propulsors failing lead to loss of the said HLP. Therefore, the aircraft level hazard severity is a combination of these 12 identical but independent scenarios. For the cruise pre-chargers or inverters, the result of either left or right failing is a 50% loss of thrust to the corresponding cruise motor. Any one of the four traction power

buses failing results in a Major condition according to C-FHA analysis. Finally, any one of the batteries failing is considered hazardous.

Before allocating reliability requirements to any of these components, the results of these corresponding failures using the preliminary 6-DoF trim analysis are considered. Table 22 shows the trim analysis results of maximizing γ after individual component failures. The lower bounds on the climb gradient discussed in Ch. 4.3.4.3 are used to determine the hazard severity. The results agree quite closely with the C-FHA results of table 21, except for the failure of the traction power buses. A single traction power bus failing results in a 25% thrust loss in takeoff as well as cruise configurations. C-FHA (see table 17) assigns a severity of ‘Major’ to the condition. However, an important distinction is made in the 6-DoF trim analysis results in this case. The loss of a TPB results in the loss of half of a cruise motor and 3 HLPs on the same side. Under this asymmetric thrust condition, the T-DEP cannot utilize all the excess power available to it as is seen by the energy rate margin (ERM) metric being just 0.33 during takeoff – pointing towards a limited rudder authority in this case. Therefore, the aircraft ends up having a much lower climb gradient than if it had been a symmetric thrust failure of the same magnitude. Applying the same logic as in Ch. 4.3.4.3 for the lower bounds, this condition is categorized as ‘Hazardous’ instead of ‘Major’.

Table 22: Bottom-up analysis: T-DEP power architecture unique system level failure states and severity using performance-based multistate 6-DoF analysis

Failed Component	Failure State	Mission Segment		Aircraft States			Flight Controls			ERM	Severity		
		Configuration	V_∞ (knots)	h (ft)	$\tan(\gamma_{max})$ (%)	θ (deg)	ψ (deg)	δ_a (deg)	δ_r (deg)			τ_L	τ_R
CM-1	CM-1	Takeoff	70	50	0.593419	0.85	-4.89	-0.06	-11.36	0	0.29	0.12	Hazardous
		Cruise	105	1500	-4.83833	3.84	-4.97	0.76	-15.09	0	0.66	-1.83	
PC-1B or I-1B	CM-1 at 50%	Takeoff	70	50	5.555853	3.66	-5	-0.05	-11.63	0.64	0.7	0.74	Major
		Cruise	105	1500	-0.31416	6.38	-4.53	0.69	-13.75	0.64	0.9	-1.33	
PC-01 or I-01 or Mot-01	Mot-01	Takeoff	70	50	8.942355	6.09	-4.98	0	-11.69	0.9	0.88	0.97	Minor
		Cruise	105	1500	N/A								
TPB-BL	Mot-1,3,5 ,CM-1 at 50%	Takeoff	70	50	1.762965	3.27	-5	0.06	-11.9	0.64	0.5	0.34	Hazardous
		Cruise	105	1500	-0.31416	6.38	-4.53	0.69	-13.75	0.64	0.9	-1.33	
Battery-B	Mot-1,3,5, 8,10,12, CM-1,2 at 50%	Takeoff	70	50	0.436335	4.57	0	0	0	0.64	0.64	0.89	Hazardous
		Cruise	105	1500	-2.61859	5.09	0	0	0	0.64	0.64	-1.02	

4.4.4 Component Reliability Allocation Results

The hazard severity due to component loss is allocated at the aircraft level. For T-DEP which is an assessment level II aircraft, this means aircraft level catastrophic, hazardous, major, and minor failures must have a probability of $< 10^{-7}$, $< 10^{-6}$, $< 10^{-5}$, and $< 10^{-3}$ per flight hour respectively. The failure rate is related to the reliability at time t by Eq. 5, repeated here for convenience.

$$R(t) = e^{-\lambda t}$$

and the failure probability at time t is given from Eq. 6 as,

$$F(t) = 1 - e^{-\lambda t}$$

The reliability requirements allocated at the component level should ensure that the total reliability at the aircraft level stays acceptable as per table 2. Thus, losing either CM-1 or CM-2 will result in a hazardous state. Similarly, losing either one of four traction power buses will result in a hazardous state. Thus, the aircraft level reliability requirements due to hazard severity given in table 22 can be related to components using the equations that follow. Since both cruise motors are assumed to be identical, the probability of either of them failing is $2\times$ the probability of one failing. This information can be used to simplify the cruise motor failure requirements as,

$$F_{CM-1}(t) + F_{CM-2}(t) \leq 1 - e^{-10^{-6}t} \quad (73)$$

$$1 - e^{-\lambda_{CM}t} \leq (1 - e^{-10^{-6}t})/2 \quad (74)$$

$$\lambda_{CM} \leq \frac{-1}{t} \ln \left(\frac{1 + e^{-10^{-6}t}}{2} \right) \quad (75)$$

The time dependence of eq. 75 is surprising given exponential failure models assume constant failure rates. However, by plotting this dependence, as seen in figure 57, it can be seen that there is a 1% change in λ_{req} when t goes from $10^2 \rightarrow 10^4$ hours.

Thus, the present work assumes $t = 5000$ hours as the age of the components being considered. Then, the (rounded off) required failure rate for the cruise motors is given by eq. 76.

$$\lambda_{CM,req} \leq 5 \times 10^{-07} \text{ (hr}^{-1}\text{)} \quad (76)$$

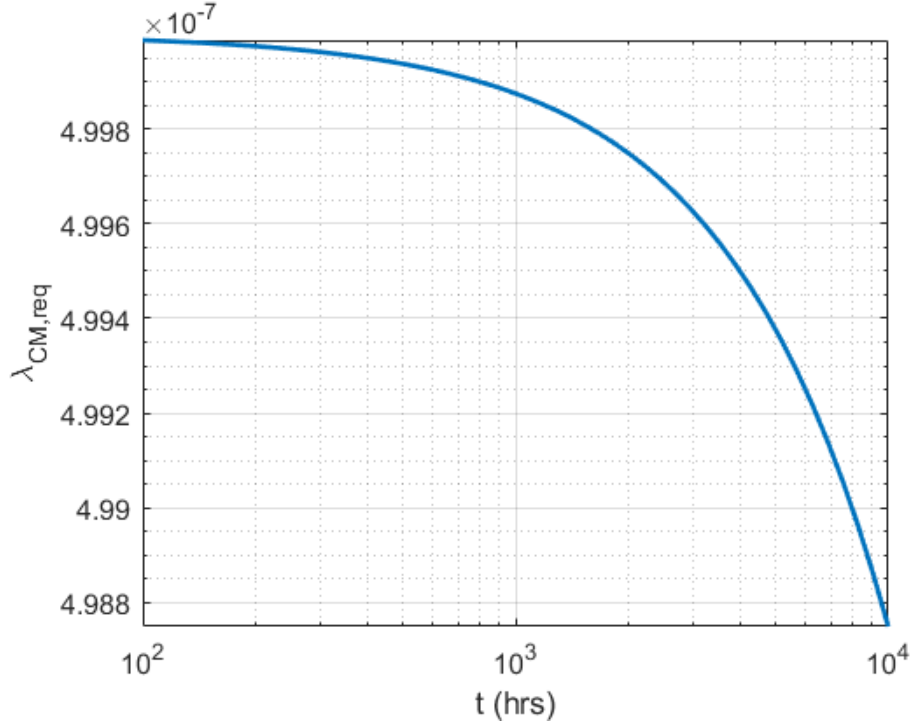


Figure 57: Cruise motor required failure rate with time

Similarly, for the traction power buses,

$$F_{TPB-AL}(t) + F_{TPB-AR}(t) + F_{TPB-BL}(t) + F_{TPB-BR}(t) \leq 1 - e^{-10^{-6}t} \quad (77)$$

$$1 - e^{-\lambda_{TPB}t} \leq (1 - e^{-10^{-6}t})/4 \quad (78)$$

$$e^{-\lambda_{TPB}t} = R_{TPB}(t) \geq \ln\left(\frac{3 + e^{-10^{-6}t}}{4}\right) \quad (79)$$

For $t = 5000$ hours, this translates to a failure rate requirement on the traction power bus given by (rounded) Eq. 80.

$$\lambda_{TPB,req} \leq 2.5 \times 10^{-07} \quad (80)$$

A trend is visible through equations 75, 79 that could be generalized. If a failure in any one of M identical components C results in an equivalent aircraft level failure state (but NOT the same failure state) with a failure rate requirement of λ_r , then the individual failure rate requirement assuming an exponential failure probability model is given by,

$$\lambda_{C,req} \leq \frac{-1}{t} \ln \left(\frac{(M-1) + e^{-\lambda_r t}}{M} \right) \quad (81)$$

A battery failure, similar to a cruise motor failure has a failure rate requirement given by (rounded),

$$\lambda_{Batt,req} \leq 5 \times 10^{-07} \text{ (hr}^{-1}\text{)} \quad (82)$$

Next, the failures resulting in high lift propulsors is considered. An HLP subsystem is considered one where a pre-charger, HLP inverter, and HLP motor are in series. There are 12 such subsystems whose independent failures can result in an equivalent aircraft level hazard – that corresponds to losing Mot-01 in table 22.

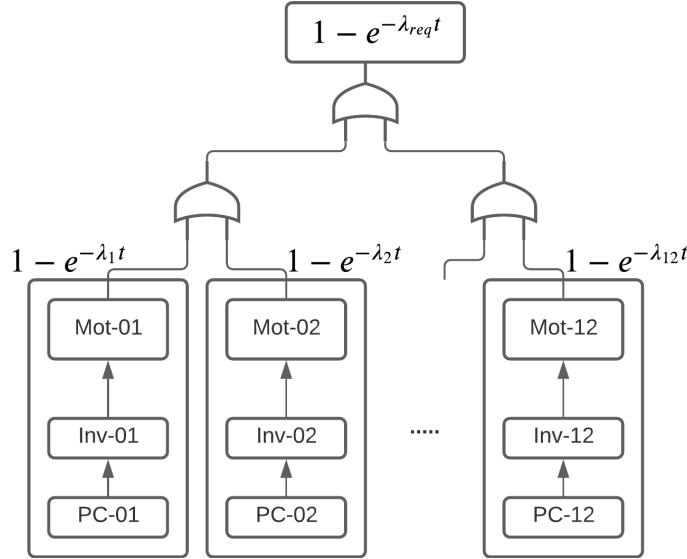


Figure 58: Mot-01 subsystem failure rate determination

Based on the equations 76, 80, the failure rate requirement for any one out of M equivalent subsystems failing is simply the aircraft level requirement divided by M .

Table 23: Mot-01 subsystem critical flow method weights

Parameter	Mot-01	Inv-01	PC-01
C_i	1	1	1
A_i	1	1	1
K_i	1	0.66	0.33
T_i	1	1	1
O_i	1	0.66	0.66
IG_i	1	0.4356	0.2178
W_i	0.605	0.263	0.132

Thus,

$$\lambda_{Mot-01-subsys} \leq \frac{10^{-3}}{12} = 8.33 \times 10^{-5} \text{ hr}^{-1} \quad (83)$$

$$R_{Mot-01} \cdot R_{Inv-01} \cdot R_{PC-01} \geq e^{-\lambda_{Mot-01-subsys} t} \quad (84)$$

Equation 84 provides an equation between the reliabilities of Mot-01, Inv-01, and PC-01, and the failure rate requirement of the subsystem of the three components. An allocation at the unit level in such a case can lead to multiple solutions. The method used here is the Critical Flow Method described in Ch. 4.4.2.2. Table 23 provides the parameter values for the critical flow method to allocate reliability to the components. K_i represents component complexity. The electric motor is assumed to be the most complex component of the three, with the pre-charger being the least, hence allocating values 1, 0.66, 0.33 to the motor, inverter, and pre-charger. Finally, the electric motor operates in conditions most exposed to the environment, with the inverter and pre-charger being relatively well shielded, affording the O_i values of 1, 0.66, 0.66 respectively. Since this series subsystem has no components in parallel, C_i is 1. All components are assumed to be state of the art, making $A_i = 1$ for all. Finally, all components are operational for the same time period, giving equal values for the T_i parameter as well.

The weights generated for the three components are given as the output of table 23,

which are used to allocate component reliability as follows,

$$R_{Mot-01}(t) \geq R_{Mot-01-subsys}^{0.605} \quad (85)$$

$$e^{-\lambda_{Mot-01,req}t} \geq (e^{\lambda_{Mot-01-subsys}t})^{0.605} \quad (86)$$

$$\lambda_{Mot-01,req} \leq 0.605 \lambda_{Mot-01-subsys} \quad (87)$$

$$\leq 5.03965 \times 10^{-5} \text{ hr}^{-1} \quad (88)$$

Similarly, the HLP inverter and pre-charger are allocated failure rate requirements as follows,

$$\lambda_{Inv-01,req} \leq 2.19079 \times 10^{-5} \text{ hr}^{-1} \quad (89)$$

$$\lambda_{PC-01,req} \leq 1.09956 \times 10^{-5} \text{ hr}^{-1} \quad (90)$$

A similar process can be conducted for the subsystems consisting of the cruise motor inverters and their pre-chargers. Here, I-1B, PC-1B (see fig. 33) can be grouped as a subsystem supplying 50% power to the cruise motor. A failure in any component of this subsystem results in a hazard severity of ‘Major’ according to table 22. Since there are four such subsystems, each one must have a failure rate requirements of $\leq 2.5 \times 10^{-6}$. Utilizing the same IG parameter values for the inverter and pre-charger gives a weight of 0.67 and 0.33 to them. Thus, their failure rate requirements are given as,

$$\lambda_{I-1B,req} \leq 1.675 \times 10^{-6} \text{ hr}^{-1} \quad (91)$$

$$\lambda_{PC-1B,req} \leq 8.25 \times 10^{-7} \text{ hr}^{-1} \quad (92)$$

4.4.5 Summary of Experiment 1.3

This experiment demonstrated how reliability requirements that get generated at the aircraft level using C-FHA and performance-based multistate analysis can be allocated to the unit level. With equations 76, 80, 82, 89, 90, 91, and 92, failure rate requirements generated at the aircraft level in chapter 4.3 are allocated to the component

Table 24: Component failure rate requirement allocation

Component	Failure rate requirement (hr^{-1})
Cruise Motor	$\leq 5 \times 10^{-7}$
CM Inverter	$\leq 1.675 \times 10^{-6}$
CM Pre-charger	$\leq 8.25 \times 10^{-7}$
Traction Power Bus	$\leq 2.5 \times 10^{-7}$
Battery	$\leq 5 \times 10^{-7}$
HLP Motor	$\leq 5.03965 \times 10^{-5}$
HLP Inverter	$\leq 5.19079 \times 10^{-5}$
HLP Pre-charger	$\leq 1.09956 \times 10^{-5}$

level for the power system architecture of the T-DEP aircraft. These requirements are summarized in table 24. The purpose of experiment 1.3 was to demonstrate the ability to determine the impact of component failures at the aircraft level. This was accomplished using a network-based bottom up analysis algorithm to identify aircraft level failure states that result from component failures. The hazard severity of these states was quantified using results generated from C-FHA and performance-based multistate 6-DoF trim analysis. Finally, a method to allocate the resultant reliability requirements using the critical flow method [163] was demonstrated resulting in failure rate requirements being allocated to the component level. With this, experiment 1.3 is complete with its purpose satisfied. It verifies hypothesis 1.3 which deals with the allocation of failure rate requirements at the component level and fulfils the broad purpose of research question 1.3.

4.5 Chapter Summary

This chapter was motivated by the first group of observations from Ch. 2.5 that led to the formulation of a set of research questions and hypotheses for the first research area. In particular, this chapter focused on demonstrating a set of methods that allow identification, characterization, and allocation of safety related off-nominal requirements. Towards that goal, literature was found to converge around utilizing

performance-based methods to quantify off-nominal system response to be used as a surrogate for hazard severity. Two methods, in particular, an extension to Continuous Functional Hazard Assessment (C-FHA), and Performance-based Multistate Analysis were down-selected and tailored for use with novel aircraft architectures at the conceptual and preliminary level of design.

The safety metrics necessary for quantifying off-nominal operational states of the aircraft formed the first research sub-question which was answered using a focused literature review. While there is no one size fits all solution for finding appropriate safety metrics to use for every novel architecture, a set of metrics useful for the Test Distributed Electric Propulsion aircraft (T-DEP) inspired by the X-57 were identified in table 3.

The next research sub-question focused on estimating these metrics by developing suitable conceptual and preliminary 6-DoF models that can simulate the aircraft's response to thrust degradation scenarios. Thresholds for these metrics were set based on certification considerations or engineering judgement. Experiment 1.2 compared the hazard severity requirements allocated to the aircraft functional degradation and multistate failures with those obtained from literature sources resorting to traditional analyses. It demonstrated a clear benefit of utilizing the proposed methods in terms of improved resolution of hazards. It also provided results based on physics based models instead of relying on heuristics, while allowing the designers to update their results once higher fidelity models are available. Some additional insights regarding the T-DEP architecture include the fact that certain hazards were not due to insufficient thrust after a failure, but due to insufficient lateral stability provided by the vertical tail.

Finally, the third research sub-question dealt with allocating the requirements generated at the aircraft level to the components. A network-based bottom-up analysis algorithm was developed to identify the impact of component failures on the aircraft

level functional availability and failure states. It was assumed that in an aerospace application, the probability of two components failing at once during a flight is small enough to be neglected, therefore allowing single failure considerations drive the reliability allocation problem. Finally, a Critical Flow Method was demonstrated to allocate reliability to components of a subsystem that cannot be dealt with using simple considerations of redundancy. Experiment 1.3 demonstrated that by using the above mentioned methods, allowable failure rate requirements can be allocated to the unit level from the system level, thus verifying hypothesis 1.3.

Taken together, the three sub-hypothesis and the techniques used to verify them were found to satisfy all the requirements posed by research question 1. This verified the solution proposed by hypothesis 1, and completes the discussion on research area 1.

CHAPTER V

A BAYESIAN PROBABILITY AND DECISION FRAMEWORK WITH MULTISTATE EXTENSION

The previous chapter dealt with the identification, characterization, and allocation of safety related off nominal requirements at the aircraft and component level for the test problem of interest - the T-DEP aircraft. This chapter presents the work on the second research area which deals with the treatment of uncertainty in quantitative risk assessment of novel architectures primarily due to the lack of data and experience with the components and novel technologies used. Research area two is based on the observation group 2 identified in chapter 2.5. Traditional methods fall short in providing a complete treatment of ‘epistemic’ uncertainty in the frequentist approach. The unavailability of sufficient failure data means that the aleatory uncertainty is large too. This lead to research question 2, which is reproduced here for convenience:

Research Question 2:

What method or group of methods can allow estimation of unit and system reliability - accounting for both epistemic and aleatory uncertainty under scarcity of available data, while also providing a mathematically defensible framework for compliance decision making?

Chapter 3.3 states the requirements that any solution answering RQ 2 must meet. They include (i) the ability to estimate unit level failure probabilities under a scarcity of data; (ii) Explicit treatment of epistemic and aleatory uncertainty; (iii) A mathematically defensible framework for compliance decision making; (iv) Estimation of multistate system reliability. These requirements are further grouped into three broad

categories. The solutions for these three categories are given by the procedure notionally given in figure 59.



Figure 59: Procedure used to answer research question 2

The first of the three deals with estimation of unit level probabilities under uncertainty, and can be posed as a smaller, research subquestion:

Research Question 2.1:

What method or group of methods can allow estimation of unit level reliability while accounting for both epistemic and aleatory uncertainty under scarcity of available data?

An enabler noted in observation group 2 in Ch. 2.5 is a ‘Bayesian’ probability approach to modeling failure rates. There are two broad schools of thought in probability theory - the ‘*frequentist*’ and the ‘*Bayesian*’. Kaplan and Garrick state that the prior deals with frequency type of information and is objective. Whereas when there is a lack of such information, they state what choice is there but to utilize ‘probability’, which is essentially a statement of belief in a certain outcome [100]. This subjective ‘probabilistic’ approach is the bedrock of ‘Bayesian’ probability theory.

Instead of only using data, a Bayesian approach relies on using available information – including data, models, as well as subject matter expertise [58]. Bayesian inference techniques for safety and reliability assessment have been applied to numerous problems in literature [21,28,43,177] and are considered mature and mathematically sound for the purpose. The utility of this approach can be attested to when one considers that numerous industries consider these techniques standard [1,79,80,102].

Furthermore, as technologies mature and more data are available, a Bayesian inference model can be continuously updated and tends towards the ‘frequentist’ models with sufficient data.

5.1 *A Bayesian Probability Framework*

5.1.1 Basic Principles

Bayesian statistics borrows its name from Thomas Bayes (1701-1761), who discovered the first specific case of what would later be called Bayes’ Theorem,

$$P(A_i|B) = \frac{P(B|A_i).P(A_i)}{P(B)} \quad (93)$$

$$= \frac{P(B|A_i).P(A_i)}{\sum_{j=1}^n P(B|A_j).P(A_j)} \quad (94)$$

This equation of Bayes’ theorem is valid in the context of n discrete events A_i and A_j etc. $P(B|A_i)$ is the probability of event B occurring given A_i has already occurred and is known as the conditional probability of B given A_i . In a Bayesian sense, $P(A_i)$ is the prior probability and represents one’s (subjective) hypothesis/belief about the outcome A_i . As Mantis [119] states in his Ph.D. thesis,

“Therein lies the shock value of Bayes’ theorem, as subjectivity appears
for the first time in the previously objective field of statistics”

$P(B|A_i)$ represents the observations made while testing the hypothesis, and $P(A_i|B)$ is the posterior probability or the new hypothesis, or the original hypothesis now corrected by the new observations made [119]. When data is already available in the form of $P(B|A_i)$, a casual observer may ask why not utilize it directly as in a ‘frequentist’ sense. This is because the resulting inference, especially under limited observations, may be misleading when prior opinion is not considered. The posterior is, in some sort, a weighting function. When limited observations are available, the posterior tends to be biased by prior opinion. As observations become exceedingly numerous, the weight of the evidence pushes the posterior towards the likelihood

functions, reducing the importance of the prior opinion and thus tending towards a ‘frequentist’ result. With these basic principles elucidated, the next section explores how the Bayesian statistical theory applies to component reliability.

5.1.2 Failure Rate Distributions - A Bayesian Approach

Instead of only using data, a Bayesian approach relies on using information - which includes data, models, and other available information like subject matter expert (SME) knowledge [58]. Instead of a point estimate as under the *frequentist* paradigm, the failure rate (λ) under the Bayesian framework is given by a distribution that quantifies uncertainty in its estimate. When available failure data (\bar{y}) is provided, the failure rate λ conditioned over \bar{y} is given by the conditional distribution as given by Eq. 95.

$$p(\lambda|\bar{y}) = \frac{p(\bar{y}|\lambda)p(\lambda)}{p(\bar{y})} \quad (95)$$

Equation 95 gives the Bayesian posterior distribution $p(\lambda|\bar{y})$ based on the likelihood of observing the data that was observed $p(\bar{y}|\lambda)$, and the analyst’s prior belief $p(\lambda)$, normalized over all realizations of the data $p(\bar{y})$. Note that Eq. 95 is simply a statement of Bayes’ theorem applied to multiple independent identically distributed observations $\bar{y} = y_1, y_2, \dots y_n$ ¹.

5.1.2.1 The Likelihood

The likelihood $p(\bar{y}|\lambda)$ is a function that seeks to determine the likelihood of observing the data \bar{y} given a hypothesis for λ . It is a statistical model used to represent the aleatory uncertainty associated with the data and the underlying physical phenomenon [172].

In the context of aircraft design, while numerous distributions can be used to

¹Preliminary work of this chapter has been published in Refs. [30,34]

model component failure data, the three most common distributions used are the Binomial, Poisson, and Exponential [58]. Figure 60 provides a guideline for the different types of likelihood distributions that can be utilized to model failure phenomenon in aerospace applications. As seen in Fig. 60, a Binomial model is generally used to model failures on demand, a Poisson model is used when there are failures in time or initiating events, while an exponential distribution is used when the time to failure is being modelled [58].

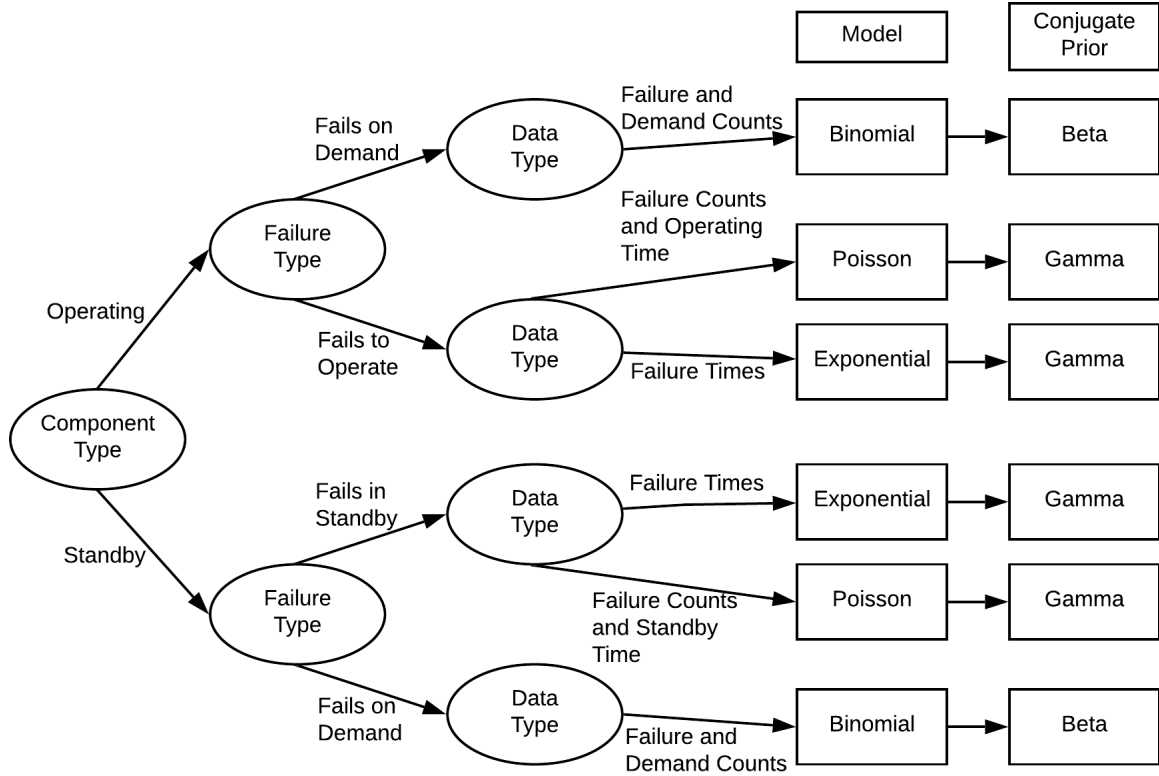


Figure 60: Guidelines for selecting the Likelihood and Prior distributions (adapted from [58])

5.1.2.2 The Prior

For a new design problem, the analyst's initial estimation of disciplinary uncertainty is based on expert opinion [119]. The prior distribution $p(\lambda)$ captures information that is denoted by the analyst's subjective state of belief regarding the failure rate. Since this distribution is based on the analyst's knowledge about the component or

event, it captures the epistemic uncertainty associated with estimating the failure rate (λ) [172].

There are two broad categories of prior distributions – the *informative prior* and the *non-informative prior*. The non-informative priors seek to minimize the information bias within a prior, thus allowing the posterior to be dominated only by the data available. Informative priors, on the other hand, contain information that can influence the posterior and is usually generated based on the analyst’s own knowledge, along with subject matter expert (SME) opinion on the unknown parameter λ . A prior distribution is typically determined before any data are observed.

Priors may also be classified as conjugate or non-conjugate. Conjugate priors can be used with certain likelihood functions to ensure that the posterior follows the same family of distributions. This can allow an analyst to have analytical solutions for the posterior and simplify calculations. Conjugate priors for different choices of likelihood functions are given in Fig. 60. Therefore, if a Gamma prior is used along with an exponential likelihood, the resulting posterior is guaranteed to follow a Gamma distribution with modified parameters. In cases of non-conjugate priors, numerical methods like Markov Chain Monte Carlo (MCMC) can be used to determine the posterior.

Selection of the prior distribution needs to be made carefully by the analyst. For instance, if an event has a probability of zero set by the prior, no amount of data observed otherwise can change the posterior. In the absence of data, the prior distribution becomes the posterior! The reader is directed to the work of Dezfuli et al. [58] which provides comprehensive guidance on selecting the appropriate distributions to model the priors by considering opinions of SMEs, and component failures from other domain applications among other cases. This is particularly pertinent because while modeling failure rates for novel aircraft components, data may not be readily available, or may not be from an aerospace background.

5.1.2.3 Posterior Distribution

The likelihood multiplied by the prior distribution gives a joint distribution of the data and parameter λ . The normalizing constant in the denominator $p(\bar{y})$ can be obtained by integrating λ out of this joint distribution to give the posterior distribution as shown in Eq. 96.

$$p(\lambda|\bar{y}) = \frac{p(\bar{y}|\lambda)p(\lambda)}{\int_{\lambda} p(\bar{y}|\lambda)p(\lambda)} \quad (96)$$

This posterior provides an updated state of knowledge of the failure rate taking into account the analyst's subjective state of belief, and available failure rate data. When heritage data is available, it can be used by eliciting its applicability from SMEs and averaging the posterior distributions according to the applicability of the data [58]. When available data are small, the prior has a greater influence on the posterior which reduces as more and more data become available. As a result, in the abundance of available data, the Bayesian posterior starts replicating the *frequentist* estimate – an outcome that is desirable.

Overall, a Bayesian approach has numerous benefits over the traditional *frequentist* approach in addition to the better treatment of both levels of uncertainty which makes it suitable for application to the safety assessments of novel aircraft architectures. First, a Bayesian posterior can be continuously updated as more data become available by treating the existing posterior as a prior and updating it with the likelihood of any newly observed data. Second, a 95% credible interval for λ has a 95% probability of the true value of λ lying within in [112], unlike the more complicated interpretation of *frequentist* confidence intervals.² Third, a Bayesian predictive posterior can be generated which provides the probability of a future observation being a

²A 95% *frequentist* confidence interval states that if multiple samples of failure data were collected a large number of times, 95% of the generated confidence intervals will contain the true λ ; an interpretation that is less useful in the current application.

certain value. Such a predictive posterior can be useful in the paradigm where repairs and health monitoring of systems is considered.

With this background, hypothesis 2.1 is restated here:

Hypothesis 2.1: *Utilizing a Bayesian probability framework to model unit level failure rates results in a more comprehensive treatment of both epistemic and aleatory uncertainty under scarcity of available data.*

5.1.3 Experiment 2.1

The intent of this section is to test hypothesis 2.1 stated above. However, before testing whether the Bayesian framework postulated provides a ‘better’ treatment of uncertainty, the term ‘better’ must be defined in this context. Paté-Cornell describes six levels of treatment of uncertainty in risk analysis in Ref. [146], with each level providing a more comprehensive or ‘better’ treatment of uncertainty than the previous. These definitions are used in the present work to demonstrate how the proposed approach is better than traditional. These six levels can be summarily explained as follows [146]:

1. **Level 0** involves the simple detection of potential hazards or different states of system failure without attempting to assess risk quantitatively
2. **Level 1** is the accumulation of worst-case scenarios without involving any notion of probability. It simply yields the maximum loss level and can be considered a ‘worst case’ approach.
3. **Level 2** can be called a ‘quasi-worst case’ approach. It attempts to evaluate the worst possible conditions that can be ‘reasonable’ expected when i) there is uncertainty regarding what the worst-case will be, or ii) the worst-case is highly unlikely.

4. **Level 3** focuses on obtaining a ‘best-estimate’ or a measure of central tendency (mean, median, etc.) of the risk/loss distribution
5. **Level 4** Most probabilistic risk analysis (PRA), quantitative risk assessment (QRA), or probabilistic safety assessment (PSA) processes lie here. It involves obtaining a distribution of probabilities of different system states and captures mainly aleatory uncertainty. Risk is represented not as a point estimate, but by a curve. However, all uncertainties are aggregated into one curve, making it difficult to extract epistemic uncertainty regarding expert disagreements or competing models.
6. **Level 5** is the highest treatment of uncertainty and involves a set of risk curves (one for each expert) that is provided to decision makers without attempting to aggregate the results. This means representing the information exactly as encoded, and translating it as far into models and analyses as is possible before inevitably aggregating the results or obtaining central tendency. Epistemic uncertainty is generally estimated using a statistical treatment or using Bayesian probabilities to encode expert opinion. This helps address the issue of ‘secondary’ probabilities or uncertainty about probabilities.

5.1.3.1 Purpose of the Experiment

Hypothesis 2.1 states that a Bayesian probability framework will provide a more comprehensive treatment of uncertainty for novel architectures. To that extent, the following are the main objectives of this experiment:

1. Demonstrate that failure rate information can be synthesized using subject matter expert opinion and available data in a Bayesian framework
2. Demonstrate that the results generated in such a framework provide a more comprehensive treatment of uncertainty than a benchmark traditional approach

5.1.3.2 Experiment Setup

In order to meet the objectives of this experiment, multiple steps need to be carried out. First, results must be generated using a traditional ‘*frequentist*’ paradigm to be used as a benchmark for comparison. Second, appropriate failure rate priors must be determined to correspond to expert opinion. Third, available data must be encoded and used to update the priors through appropriate likelihood distributions to generate the posterior distribution. Fourth, steps two and three can be repeated with different initial assumptions to generate a ‘*family of curves*’ as Paté-Cornell calls it [146] to demonstrate a comprehensive treatment of uncertainty. The components of the T-DEP power systems architecture from figure 33 will be the ones on which these results will be demonstrated.

5.1.4 Benchmark Component Failure Rates

Traditional safety analyses at the conceptual or preliminary level consider central tendency, usually the mean or median of the failure rates to represent component failure rates. Therefore, for the benchmark results in the present study, mean failure rates of the different components are compiled from various sources. The detailed failure rates from different sources are compiled in Appendix C.

Battery: Generic battery failure rate data is available from historical databases given in Ref. [2, 5]. Additional data available for lithium ion batteries include a recent NASA report [53] that suggests using a failure rate of $9.3 \times 10^{-6} \text{ hr}^{-1}$. Boeing 787 reported two battery safety events in about 104000 combined flight hours of battery operation [134], while NPRD-2016 [117] provides a failure rate of $2.99 \times 10^{-5} \text{ hr}^{-1}$. These values are aggregated to give a point estimate of the failure rate as

$$\lambda_{Batt,mean} = 7.6159 \times 10^{-6} \text{ hr}^{-1} \quad (97)$$

Electric Motor: Failure rates from historical databases [2, 5, 7] are averaged with data from newer sources in Ref. [49, 53, 117] to give a mean failure rate of

$$\lambda_{EM,mean} = 9.7761 \times 10^{-6} \text{ hr}^{-1} \quad (98)$$

Motor Inverter: Similar to above components, historical data from Ref. [2] is averaged with latest data in Ref. [49, 53] to get

$$\lambda_{Inv,mean} = 3.51 \times 10^{-5} \text{ hr}^{-1} \quad (99)$$

Traction Power Bus: Data from Refs. [2, 5, 117] is averaged to get a mean failure rate give by,

$$\lambda_{TPB,mean} = 4.2177 \times 10^{-6} \text{ hr}^{-1} \quad (100)$$

Pre-Charger: Data for resistors and contactor switches is obtained from Refs. [3, 5, 7, 117] and added up to get the pre-charger failure rate.

$$\lambda_{PC,mean} = 5.2594 \times 10^{-5} \text{ hr}^{-1} \quad (101)$$

Utilizing mean values is probably the most common approach to modeling component failure rates in literature. Therefore, using this approach as a benchmark is not only convenient, it is also a realistic depiction of the studies performed in conceptual or preliminary design stages. This approach falls under the 3rd level in the six levels of treatment of uncertainty discussed previously. While useful, utilizing measures of central tendency from available data does not provide a complete treatment of uncertainty, especially for novel architectures where data might be insufficient. The next section will explore how data from the exact same sources can be utilized to efficiently capture and propagate uncertainty in the component failure rates.

5.1.5 Bayesian Component Posteriors

For all components in Fig. 33, a Poisson likelihood model is assumed since failures generally occur during operation with the number of failures and corresponding operating time being the information documented (see fig. 60) [58]. A prior is selected based on an analyst's subjective bias about the component failure rate.

In order to demonstrate a comprehensive (level 5) treatment of uncertainty with the intent of providing alternate failure rate models to decision makers, two different (imaginary) analysts are invented that perform the Bayesian exercise separately. They are called Analyst A and Analyst B. Both these analysts provide their characterization of domain specific (epistemic) uncertainty through their subjective opinions on the failure rates of different components. This information is encoded using the prior distributions, which are assumed to be gamma distributed (conjugate prior for Poisson likelihood) to make the posterior calculations easier. For Poisson likelihood models, a Jeffry's non-informative conjugate prior is a Gamma distribution with shape $\alpha = 0.5$, and rate $\beta = 0$. Although this is not a proper distribution (integral over all λ is not finite), it results in a proper posterior distribution. Since a Gamma prior is conjugate to the Poisson likelihood, the posterior also takes the form of a Gamma distribution [58].

$$\text{Prior} : \lambda_{prior} \sim \text{Gamma}(\text{shape} = \alpha_{prior}, \text{rate} = \beta_{prior}) \quad (102)$$

$$\text{Likelihood} : y_i | \lambda \sim \text{Poisson}(\lambda t_i, y_i) \propto \frac{(\lambda t_i)^{y_i} e^{-\lambda t_i}}{y_i!} \quad (103)$$

$$\text{Posterior} : \lambda_{posterior} | \bar{y} \sim \text{Gamma}(\alpha = \alpha_{prior} + \sum y_i, \beta = \beta_{prior} + \sum t_i) \quad (104)$$

In a gamma distribution used for failure analysis, the shape parameter α can be interpreted as the number of failures, while the rate parameter β can be interpreted as the number of hours of operational experience with a component. Thus, a high value of β can be interpreted as having a lot of operating hours experience, while a

lower value indicates a lack of experience and is likely to result in a much wider spread in the posterior distribution. Similarly, higher α values for a given rate parameter means a component is likely to have higher failure rates. Recent data sources are used next to update the analyst's prior to get a component's failure rate posterior. In sources where point values are provided for failure rates, Dezfuli et al. [58] provide a method to convert these to likelihood estimates, which are then used here to reach a posterior distribution. When a mean value for the failure rate λ is available in a Poisson distribution, it can be treated as being an equivalent of a number of failures $= 0.5$, and time $= 1/(2 \times \text{mean})$. The raw failure rate data used in the following analysis are provided in Appendix C.

5.1.5.1 Analyst A

Since the T-DEP power system architecture utilizes numerous electrical components that have little precedence in aircraft applications, Analyst A chooses to take the path of accepting ignorance by utilizing non-informative priors for all the components. For a Poisson likelihood, conjugate non-informative priors are Gamma distributed with shape $\alpha = 0.5$ and rate $\beta = 0$. Additionally, Analyst A only utilizes the latest data that is available for the components of interest in aircraft applications since it provides a more accurate representation of the aleatory uncertainty associated with the T-DEP components. This data is then used to update the non-informative priors to get the posteriors of interest.

Battery Posterior: A non informative prior is assumed for the battery. Data available for lithium ion batteries include a recent NASA report [53] that suggested using 9.3 failures per million hours. Additionally, Boeing 787 reported two battery safety events in about 104000 combined flight hours of battery operation (2 batteries per aircraft, 52000 flight hours) [134], while NPRD-2016 [117] provides 8 failures in 2.6735E5 hours of operation for battery packs. This results in the following battery

failure rate posterior:

$$\textit{Analyst Prior} : \lambda_{prior_A} \sim \textit{Gamma}(\alpha = 0.5, \beta = 0) \quad (105)$$

$$\textit{Likelihood} : y_i | \lambda \sim \textit{Poisson}(\lambda t_i, y_i) \quad (106)$$

$$\textit{Posterior} : \lambda_{posterior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 19.8, \beta = 1371350) \quad (107)$$

Electric Motor Posterior: Similar to a battery, a non-informative prior is assumed.

$$\textit{Analyst Prior} : \lambda_{prior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 0.5, \beta = 0) \quad (108)$$

Ref. [53] suggests using 9.24 failures per one million hours. Ref. [49] provides a failure rate of 6.6E-5 per flight hour for three-phase electric drives(applied with a weight of 10x), while NPRD [117] provides additional failure rates of 7.23887E-7 and 3.9586E-7 per hour. The posterior is given by:

$$\textit{Posterior} : \lambda_{posterior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 15.74, \beta = 3029546) \quad (109)$$

Motor Inverter Posterior: A non-informative prior is considered as before.

$$\textit{Analyst Prior} : \lambda_{prior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 0.5, \beta = 0) \quad (110)$$

Ref. [53] suggests using 4.75 failures in one million hours. Ref. [49] provides a failure rate of 8.5E-5 per flight hour (applied with a weight of 10x) for electronics related to three-phase electric drives. The final posterior is:

$$\textit{Posterior} : \lambda_{posterior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 10.25, \beta = 1058800) \quad (111)$$

Traction Power Bus Posterior: A non-informative prior is considered by Analyst A.

$$\textit{Analyst Prior} : \lambda_{prior_A} | \bar{y} \sim \textit{Gamma}(\alpha = 0.5, \beta = 0) \quad (112)$$

NPRD [117] data includes zero failures for 1,363,267 hours of operating experience for electric buses. Together, the posterior is:

$$Posterior : \lambda_{posterior_A} | \bar{y} \sim Gamma(\alpha = 0.5, \beta = 1363267) \quad (113)$$

Pre-Charger Posterior: Failure data for pre-chargers was not found readily available in literature. However, upon closer inspection (as a Bayesian analyst may have to do to determine the prior), analyst A notices that a pre-charger typically incorporates a resistor and a contactor switch to manage a sudden rush of current from damaging the inverter circuit. A non-informative prior is used the same as above in this case too.

$$Analyst Prior : \lambda_{prior_A} | \bar{y} \sim Gamma(\alpha = 0.5, \beta = 0) \quad (114)$$

Data for resistor and switch failures from NPRD [117] is scaled and used to update the precharger prior to give Analyst A's posterior:

$$Posterior : \lambda_{posterior_A} | \bar{y} \sim Gamma(\alpha = 0.5, \beta = 58688) \quad (115)$$

5.1.5.2 Analyst B

Analyst B takes a different approach. Knowing that the components under consideration have been in use in ground and other applications for a longer time, Analyst B decides to let historical data from these similar components from dissimilar applications guide the prior distribution by weighting such data. This is to incorporate some influence from historical data from dissimilar applications guide the characterization of epistemic uncertainty, while not letting it overwhelm the limited data available for state of the art components being developed for aircraft applications. Thus, Analyst B updates an initial Jeffry's non-informative conjugate prior using weighted historical data to generate an analyst's prior. This is then updated using the latest relevant component data to obtain the posterior.

Battery Posterior: An analyst's prior is constructed by updating a non-informative prior with historical data [2, 5] weighted at just 10% applicability since a lot of the historical data is not for Li-ion batteries.

$$\text{Non-informative Prior} : \lambda_{prior} \sim \text{Gamma}(\alpha = 0.5, \beta = 0) \quad (116)$$

$$\text{Likelihood} : y_i | \lambda \sim \text{Poisson}(\lambda t_i, y_i) \propto \frac{(\lambda t_i)^{y_i} e^{-\lambda t_i}}{y_i!} \quad (117)$$

$$\begin{aligned} \text{Analyst Prior} : \lambda_{prior_B} | \bar{y} &\sim \text{Gamma}(\alpha = 0.5 + \Sigma y_i, \beta = 0 + \Sigma t_i) \\ &: \lambda_{prior_B} | \bar{y} \sim \text{Gamma}(\alpha = 11.45, \beta = 3966800) \end{aligned} \quad (118)$$

Eq. 118 can now be used as an analyst's prior. Data available for lithium ion batteries include a recent NASA report [53] that suggested using 9.3 failures per million hours. Additionally, Boeing 787 reported two battery safety events in about 104000 combined flight hours of battery operation (2 batteries per aircraft, 52000 flight hours) [134], while NPRD-2016 [117] provides 8 failures in 2.6735E5 hours of operation for battery packs. This results in the following battery failure rate posterior:

$$\text{Analyst Prior} : \lambda_{prior_B} \sim \text{Gamma}(\alpha = 11.45, \beta = 3966800) \quad (119)$$

$$\text{Likelihood} : y_i | \lambda \sim \text{Poisson}(\lambda t_i, y_i) \quad (120)$$

$$\text{Posterior} : \lambda_{posterior_B} | \bar{y} \sim \text{Gamma}(\alpha = 30.75, \beta = 5338150) \quad (121)$$

Electric Motor Posterior: Similar to a battery, an analyst's prior is constructed by updating a non-informative prior with historical data [2, 5, 7] with a 10% weighting since it includes data for old electric motors.

$$\text{Analyst Prior} : \lambda_{prior_B} | \bar{y} \sim \text{Gamma}(\alpha = 26.15, \beta = 1.2417E7) \quad (122)$$

Ref. [53] suggests using 9.24 failures per one million hours. Ref. [49] provides a failure rate of 6.6E-5 per flight hour for three-phase electric drives(applied with a weight of 10x), while NPRD [117] provides additional failure rates of 7.23887E-7 and 3.9586E-7

per hour. The posterior is given by:

$$Posterior : \lambda_{posterior_B} | \bar{y} \sim Gamma(\alpha = 41.39, \beta = 15446550) \quad (123)$$

Motor Inverter Posterior: An analyst's prior is constructed by updating a non-informative prior with historical data [2] weighted 10% as before.

$$Analyst Prior : \lambda_{prior_B} | \bar{y} \sim Gamma(\alpha = 4.5, \beta = 286940.5) \quad (124)$$

Ref. [53] suggests using 4.75 failures in one million hours. Ref. [49] provides a failure rate of 8.5E-5 per flight hour (applied with a weight of 10x) for electronics related to three-phase electric drives. The final posterior is:

$$Posterior : \lambda_{posterior_B} | \bar{y} \sim Gamma(\alpha = 14.25, \beta = 1345800) \quad (125)$$

Traction Power Bus Posterior: An analyst's prior is constructed by updating a non-informative prior with historical data [2, 5] weighted 10% as before.

$$Analyst Prior : \lambda_{prior_B} | \bar{y} \sim Gamma(\alpha = 0.85, \beta = 8,467,600) \quad (126)$$

Note that this prior suggests that the analyst believes an electric bus is likely to fail less than once in over 8 million hours! NPRD [117] data includes zero failures for 1363267 hours of operating experience for electric buses. Together, the posterior is:

$$Posterior : \lambda_{posterior_B} | \bar{y} \sim Gamma(\alpha = 0.85, \beta = 9830867) \quad (127)$$

Pre-Charger Posterior: Failure data for a pre-charger was not found readily available in literature by the authors. However, upon closer inspection (as a Bayesian analyst may have to do to determine the prior), analyst B notices that a pre-charger typically incorporates a resistor and a contactor switch to manage a sudden rush of current from damaging the inverter circuit. An analyst's prior is therefore constructed by updating a non-informative prior with historical data for the two components taken

in series [5, 7] weighted 20% for the connector switches, and 100% for the resistor. These are then scaled to assume a similar operating time and the number of failures added to give (see Appendix C),

$$\textit{Analyst Prior} : \lambda_{\textit{prior}_B} | \bar{y} \sim \textit{Gamma}(\alpha = 6.1145, \beta = 1476012) \quad (128)$$

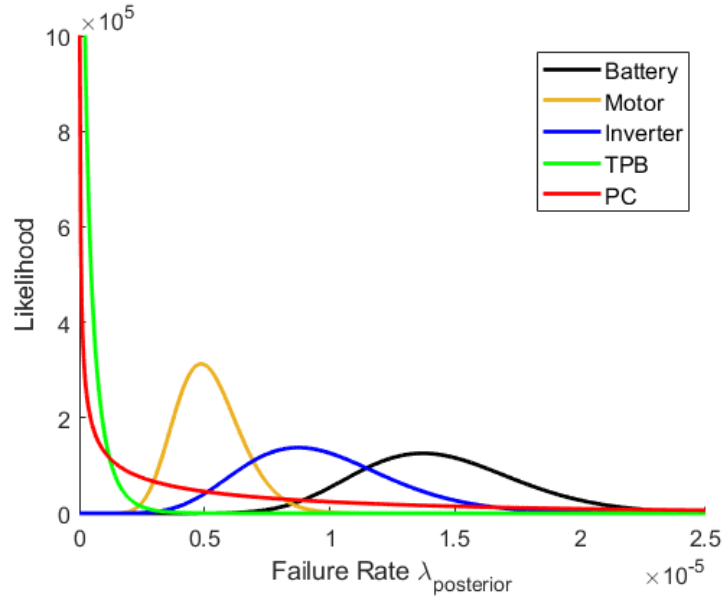
Data for resistor and switch failures from NPRD [117] is scaled and used to update the precharger prior to give Analyst B's posterior:

$$\textit{Posterior} : \lambda_{\textit{posterior}_B} | \bar{y} \sim \textit{Gamma}(\alpha = 6.1145, \beta = 1534700) \quad (129)$$

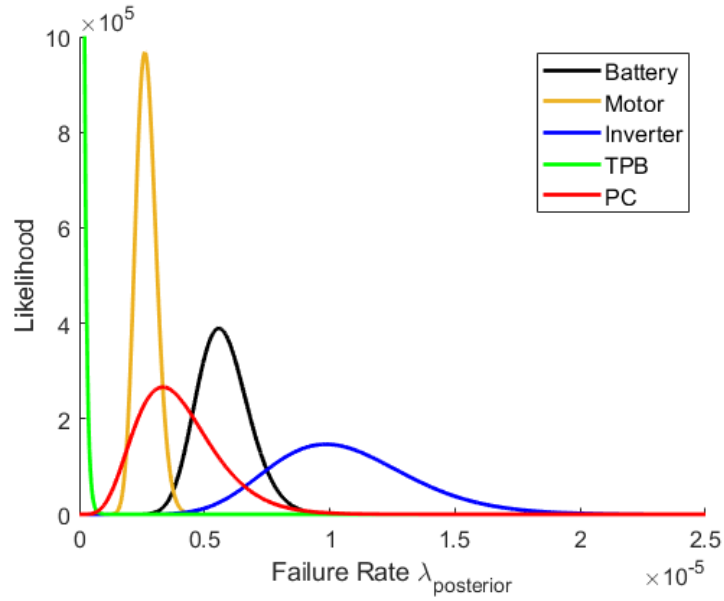
5.1.6 Bayesian Posterior Results - A family of curves

The failure rate posteriors generated by Analysts A and B are provided in figure 61. In the present experiment, Analyst A represents someone with little disciplinary knowledge, who treats uncertainty by looking at available data. Analyst B is someone who provides disciplinary information to bias available observations. This is incorporated in the present experiment by assuming that weighted historical data from other applications (e.g. ground, naval, etc.) will provide some perspective into every component's expected behavior in novel aircraft applications. This is also visible in part in the posteriors shown in figure 61. Since analyst A accepts ignorance regarding epistemic uncertainty and uses non-informative conjugate priors, the spread in failure rate posteriors is visibly larger than those of Analyst B who uses weighted historical data to inform prior beliefs. Overall, the failure rates for analyst B are also found to be lower, although this need not be the case every time and can depend on the expert opinion utilized. The reduced variability in Analyst B's posteriors is an indication of the reduced state of epistemic uncertainty in the estimation of failure rates.

In practice, multiple such Bayesian posteriors can be generated by subject matter experts by encoding their own understanding of the disciplinary uncertainty (epistemic) through different priors. In the present instance, a family of two curves per



(a) Analyst A



(b) Analyst B

Figure 61: Bayesian failure rate posteriors for the two analysts

component is provided as a proof-of-concept to demonstrate a level-5 treatment of uncertainty discussed earlier. As more data becomes available, the effect of these priors reduces and the posteriors tend to approach ‘frequentist’ estimates in failure rates obtained using data only. This is because as more and more data is generated,

the epistemic uncertainty related to lack of knowledge and experience reduces as well, and the overall uncertainty ends up being dominated by fundamental stochastic behavior of the manufacturing and operational processes (aleatory). When compared to the benchmark results that utilize central tendency, it is quite clear that a Bayesian approach provides a better treatment of uncertainty in the failure rate data. Thus the purpose of experiment 2.1 is complete.

5.1.7 Summary of Experiment 2.1

Experiment 2.1 was set up to test if a Bayesian probability framework provides a more comprehensive treatment of epistemic and aleatory uncertainty under a scarcity of available data. In designing the experiment, the six levels of treatment of uncertainty in risk analysis defined by Paté-Cornell [146] were explained. These served as a metric against which benchmark mean failure rates were compared to generated Bayesian posteriors utilizing the same available datasets. It was demonstrated that while central measures of tendency like mean failure rates are used during conceptual and preliminary design to conduct safety analysis, these correspond to the 3rd level in the six levels of treatment of uncertainty. Bayesian posteriors generated for two imaginary analysts making different discipline specific assumptions to encode epistemic uncertainty demonstrated the Bayesian framework's capability to provide decision makers with alternate models, thus providing the highest treatment of uncertainty according to Paté-Cornell [146]. While two analysts were considered for a proof of concept, the Bayesian framework is not restricted to the number of different posteriors that can be generated and translated through the analyses. Different subject matter experts may encode different disciplinary assumptions into the prior distributions, which when updated with the available datasets will generate different posteriors. Overall, the results from experiment 2.1 satisfied the purpose of the experiment and therefore verify hypothesis 2.1.

5.2 *A Bayesian Decision Framework*

So far, safety related off-nominal requirements in terms of allowable failure rates have been allocated to the components in chapter 4.4. Chapter 5.1 generated failure rate posteriors for the different components while providing a comprehensive treatment of uncertainty. The next obvious task is then to make a compliance finding. However, it would be ideal to not lose the gains made in quantifying uncertainty while making compliance findings. This leads to the second sub-question of the current chapter which is restated here for convenience:

Research Question 2.2:

How can mathematically defensible compliance decisions be made without losing the gains made in quantifying uncertainty?

Compliance finding is fundamentally an exercise in decision making under uncertainty. The Bayesian probability framework introduced previously can be considered as a probability of frequency framework [100]. That is, if the failure rate is a measure of the frequency of failures, the Bayesian posteriors from Ch. 5.1.6 provide a probability distribution that represents the level of confidence in this frequency. This enabling feature of a Bayesian probability framework can be leveraged in a decision theoretic setup.

Consider A as an action space which includes $a \in A$ as actions pertaining to compliance finding; typically $A = \{\text{accept}, \text{reject}\}$. For instance, a decision maker takes an action a pertaining to whether a component is compliant or not with the safety requirements. This action is a function of the observations made regarding the number of failures (y_i), and the operating times (t_i). Such a function is called a decision rule $\delta(\bar{y})$. Under a Bayesian framework, a loss is used to denote the opposite of utility. Every action has a potential utility, and therefore a potential loss. A loss

function $L(X, a)$ represents the loss incurred when a decision maker takes an action a when the true (unknown) state of the component is X .

Definition 5.2.1 (Bayesian Expected Loss). *Bayesian expected loss is the expectation of the loss function with respect to the posterior distribution*

$$\rho(a, \pi) = E^{\lambda|\bar{y}} L(a, \lambda) = \int_{\lambda} L(\lambda, a) \pi(\lambda|\bar{y}) d\lambda \quad (130)$$

where π gives the posterior distribution of λ .

Definition 5.2.2 (The Expected Loss Principle). *After data \bar{y} has been observed, the preferred action between two actions $a_1 = \delta_1(\bar{y})$ and $a_2 = \delta_2(\bar{y})$ is the one for which the posterior expected loss is smaller. Such an action a^* minimizing the posterior expected loss is called Bayes action.*

Thus, to fully leverage the uncertainty quantification afforded by a Bayesian probability framework, determining the *Bayes* action provides a mathematically defensible way of making a compliance finding at the component level.

As an example, assume two hypothetical components A and B have been allocated failure rate requirements, and their failure probability posteriors have been computed using the Bayesian approach explained earlier. Placing the probability requirements on the CDFs of the Bayesian failure posteriors, analysts can compute the probability with which reliability requirements can be met (probability of frequency). This is shown notionally in Fig. 62. For example, the probability with which component B in the notional example can meet the reliability requirement is given by the dashed line showing $p(\lambda_{posterior} < \lambda_{allowable})$ on the CDF in Fig. 62.

Decision makers now need to make a decision on whether the corresponding probability of meeting the requirement is good enough to consider component B compliant with the safety requirements. In a Bayesian decision theoretic setup, such a compliance decision regarding component B is considered an action a

$$a \in A, \quad A = \{compliant, non - compliant\}$$

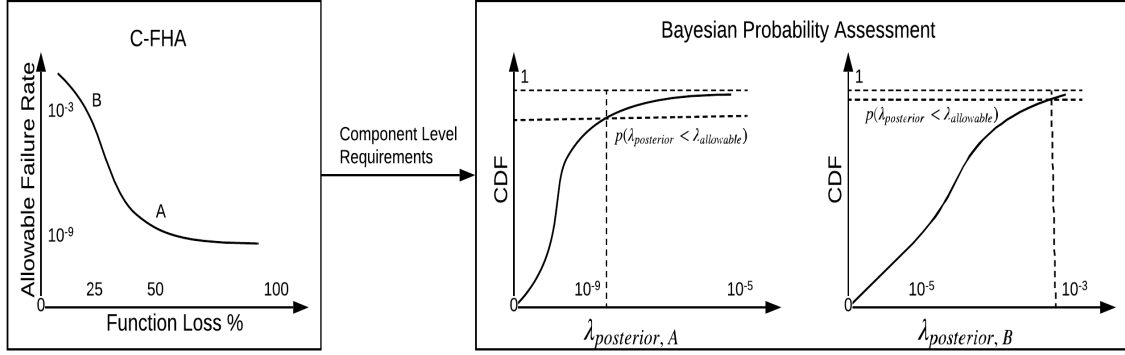


Figure 62: Notional Integrated Risk Assessment - Probability of meeting component failure rate requirements

If the true value of the compliance finding (in reality - unknown) is given by x

$$x \in X, X = \{compliant, non - compliant\}$$

then a loss function (x, a) can be defined to represent the penalty to be paid if the analyst chooses action a when the true compliance value is x , under available information $p(\lambda_{posterior} < \lambda_{allowable})$. That is to say, imagine an analyst takes an action $a_1 = \{complaint\}$, when the true value of compliance finding (theoretical and unknown in reality) was $x_2 = \{non - compliant\}$, the loss incurred would be $L(x_2, a_1)$ and so on.

In such a framework, the Bayesian expected loss $\rho(a, p)$ is the expectation of this loss function $L(x, a)$ with respect to the posterior failure rate, and is given by Eq. 131.

$$\rho(a, p) = \int_{\lambda} L(x, a) p(\lambda | \bar{y}) d\lambda \quad (131)$$

An action a^* that minimizes the expected loss given by Eq. 131 should be the action taken by the analyst and is also called *Bayes action*. As is visible from the above mathematical framework, the analyst needs only to compute the Bayesian posterior and supply a loss function $L(x, a)$, and the framework provides a recommendation for compliance finding based on minimization of the expected loss. It is a mathematically defensible method for compliance decision making while accounting for epistemic

and aleatory uncertainty. With this background, hypothesis 2.2 is restated here to reiterate the claim made in the above discussion.

Hypothesis 2.2: *If the posterior expected loss using suitable loss functions can be determined for system components, then the action that minimizes such an expected loss would inform the compliance action to be taken under uncertainty*

5.2.1 Experiment 2.2

The intent of this section is to test hypothesis 2.2 stated above. The previous experiment (see Ch. 5.1.3) compared the level of treatment of uncertainty between traditionally used mean failure rates as a benchmark against Bayesian posterior distributions created by two imaginary analysts. In the present case, compliance decisions can be similarly compared. A benchmark method to determine compliance is compared to the results obtained using an expected loss framework explained above.

5.2.1.1 Purpose of the Experiment

Hypothesis 2.2 states that minimizing a posterior expected loss would be the solution to research sub-question 2.2. RQ 2.2 focuses on obtaining a mathematically defensible way to make compliance finding without losing the higher treatment of uncertainty afforded by a Bayesian probability framework. This informs the main objective of the present experiment:

1. Demonstrate that computing the posterior expected loss captures and translates the uncertainty information encoded by the Bayesian posteriors while enabling compliance decision making

5.2.2 Benchmark Results

For the T-DEP architecture, table 24 provides the failure rate requirements allocated to the different components. Similarly, a simple failure rate analysis using central tendency to provide mean component failure rates is given in chapter 5.1.4. For the present experiment, a simple operation of comparing these two, as is done in traditional preliminary system safety assessment yields component compliance finding as given in table 25. As can be seen, the vast majority of the components in the T-DEP

Table 25: Benchmark compliance results

Component	Failure rate requirement (hr^{-1})	Benchmark failure rates λ_{mean} (hr^{-1})	Compliance Decision ($\lambda_{mean} \leq \lambda_{req}$?)
Cruise Motor	$\leq 5 \times 10^{-7}$	9.7761×10^{-6}	Non-compliant
CM Inverter	$\leq 1.675 \times 10^{-6}$	3.51×10^{-5}	Non-compliant
CM Pre-charger	$\leq 8.25 \times 10^{-7}$	5.2594×10^{-5}	Non-compliant
Traction Power Bus	$\leq 2.5 \times 10^{-7}$	4.2177×10^{-6}	Non-compliant
Battery	$\leq 5 \times 10^{-7}$	7.6159×10^{-6}	Non-compliant
HLP Motor	$\leq 5.03965 \times 10^{-5}$	9.7761×10^{-6}	Compliant
HLP Inverter	$\leq 5.19079 \times 10^{-5}$	3.51×10^{-5}	Compliant
HLP Pre-charger	$\leq 1.09956 \times 10^{-5}$	5.2594×10^{-5}	Non-compliant

architecture seem to be non-compliant with the reliability requirements generated from Ch. 4.4.4. This approach simply compares the failure rate requirement to the mean failure rates obtained from (limited) data to make a compliance assessment. Any uncertainty information encoded in the failure rates is thus lost. The results of this exercise serve as a benchmark to compare the output of the Bayesian decision theoretic approach discussed next.

5.2.3 Loss Functions

With the component level reliability (allowable failure rate) requirements now available from Ch. 4.4.4, and failure rate posteriors available from Ch. 5.1.6, the Bayesian decision framework described in Ch. 5.2 is now utilized to determine compliance finding. To proceed, decision makers must come up with loss functions that capture the potential loss (opposite of utility or benefit) of any action. For the present case, a loss

function can be allocated based on a decision matrix (also called confusion matrix). Table 26 provides a simple loss function that allocates four different losses based on the true (unknown) state of the component, and the decision action taken. The fol-

Table 26: Generic loss function $L(X, a)$

True State X	Decision Action a	
	$a_1 = \{Compliant\}$	$a_2 = \{Non - Compliant\}$
$X_1 = \{Compliant\}$	L_{11}	L_{12}
$X_2 = \{Non - Compliant\}$	L_{21}	L_{22}

lowing discussion provides some insights into the choice of this generic loss function and the typical values in it [172]:

1. L_{11} is the loss incurred when a component is deemed compliant when it is truly compliant. Since this is a desirable outcome, and the minimization of loss is desired, L_{11} is typically negative.
2. L_{12} is the loss incurred when a component is deemed compliant when it is not in truth. This is the worst possible outcome from a safety standpoint, and therefore is accorded the largest positive loss. That is $L_{12} = \max(L_{ij})$.
3. L_{21} is the loss incurred when a component is deemed non-compliant when in reality it is compliant. While this is undesirable, it is better than the previous case and is typically provided a small positive loss.
4. L_{22} is the loss incurred when a component is rightfully declared non-compliant. Since this is desirable, L_{22} is typically provided the largest magnitude of negative loss. That is $L_{22} = \min(L_{ij})$.

The Bayesian expected loss given by Eq. 131 gets simplified because of the loss function provided by Table 26 to give,

$$\rho(a_1, p) = L_{11} \cdot p + L_{21} \cdot (1 - p) \quad (132)$$

$$\rho(a_2, p) = L_{12} \cdot p + L_{22} \cdot (1 - p) \quad (133)$$

Where $p = p(\lambda_{posterior} \leq \lambda_{req})$ is the probability of the component meeting its requirements. Each term in equations 132, 133 above provides information. For instance, the first term $L_{11}p$ in Eq. 132 gives the (negative) loss value of choosing to call a component compliant under posterior probability of it meeting the requirements. The second term computes the loss of calling the component compliant weighted by $1 - p$, which is used to measure the true state X_2 . The losses due to both these estimations of X_1, X_2 and their probabilities are added up to provide the net loss due to taking the decision action $a_1 = \textit{compliant}$. Eq. 133 provides a similar consideration for the action a_2 .

The test problem of interest is the T-DEP power system architecture from Fig. 33. In the discussion that follows, a decision maker D utilizes the posteriors generated by analysts A and B from chapter 5.1.6 to compute the expected losses. The assumed loss function is given by table 27.

Table 27: Loss function $L(X, a)$ for decision maker D

True State X	Decision Action a	
	$a_1 = \{\textit{Compliant}\}$	$a_2 = \{\textit{Non - Compliant}\}$
$X_1 = \{\textit{Compliant}\}$	\$-1,000,000	\$500,000
$X_2 = \{\textit{Non - Compliant}\}$	\$3,000,000	\$-2,000,000

Decision maker D looks at the compliance problem in terms of costs it would impose on the company developing the T-DEP architecture. A correct compliance finding is assumed to result in a loss of \$-1 million (profit), whereas a correct finding of the lack of compliance prevents the company from having to face potential future costs of \$2 million. A decision of non-compliant when true state is compliant levies a cost of \$500,000 to go through the certification process again and to generate additional data, whereas a wrongful ‘compliant’ decision is assumed to result in future (litigation and others) costs of \$3 million. These values in the present analysis are notional. The idea is to provide a working example of how decision makers might utilize the described Bayesian decision framework in making a compliance finding.

5.2.4 Bayesian Expected Loss Results

The Bayesian expected loss for the different components of the T-DEP power systems architecture from Fig. 33 is computed using equations 132, 133. These equations require a value for p – the probabilities of meeting requirements. These are obtained by computing the cumulative distributions of the component posteriors and finding $p(\lambda_{posterior} \leq \lambda_{req})$. Table 28 shows these probabilities for meeting failure rate requirements for the different components for the two Bayesian analysts A, B from Ch. 5.1.6.

Table 28: Probability of meeting failure rate requirements for Bayesian analysts

Component	Failure rate requirement (hr^{-1})	Analyst A	Analyst B
		$p(\lambda_{posterior,A} \leq \lambda_{req})$	$p(\lambda_{posterior,B} \leq \lambda_{req})$
Cruise Motor	$\leq 5 \times 10^{-7}$	0	0
CM Inverter	$\leq 1.675 \times 10^{-6}$	0.00001	0
CM Pre-charger	$\leq 8.25 \times 10^{-7}$	0.24463	0.00162
Traction Power Bus	$\leq 2.5 \times 10^{-7}$	0.59098	0.93573
Battery	$\leq 5 \times 10^{-7}$	0	0
HLP Motor	$\leq 5.03965 \times 10^{-5}$	1	1
HLP Inverter	$\leq 5.19079 \times 10^{-5}$	1	1
HLP Pre-charger	$\leq 1.09956 \times 10^{-5}$	0.74407	0.99915

Using these posterior probabilities of meeting the requirements, decision maker D utilizes the loss function from table 27 to compute the expected loss of taking actions $a_1 = \{compliant\}$ or $a_2 = \{non - compliant\}$. The results of this analysis for Analyst A's posteriors are provided in table 29. It is worth noting that Analyst A had assumed non-informative priors and only the latest data to compute the posteriors. Under these circumstances, the compliance results using the expected loss for Analyst A's posteriors end up matching the benchmark results from table 25. That is, the high lift motors and their inverters are the only components found compliant with the requirements generated. However, that does not mean the two approaches are equivalent. Results in table 29 translate the posterior probabilities of component failure rates to determine the loss incurred in taking either action a_1 or a_2 . In doing

so, the uncertainty information encoded during the Bayesian probability analysis is not lost and instead is translated through the loss functions to decision makers. This, therefore, is a higher treatment of uncertainty than the benchmark where point estimates strip away uncertainty in failure rates to give only binary results a_1 or a_2 , as against providing a probability informed penalty of making either decision.

Table 29: Expected loss and compliance finding using Analyst A’s posteriors

Component	$\rho(a_1, p)$	$\rho(a_2, p)$	Decision Action
Cruise Motor	\$ 3,000,000	\$ -2,000,000	$a_2 =$ Non-compliant
CM Inverter	\$ 2,999,960	\$ -1,999,975	$a_2 =$ Non-compliant
CM Pre-charger	\$ 2,021,480	\$ -1,388,425	$a_2 =$ Non-compliant
Traction Power Bus	\$ 636,080	\$ -522,550	$a_2 =$ Non-compliant
Battery	\$ 3,000,000	\$ -2,000,000	$a_2 =$ Non-compliant
HLP Motor	\$ -1,000,000	\$ 500,000	$a_1 =$ Compliant
HLP Inverter	\$ -1,000,000	\$ 500,000	$a_1 =$ Compliant
HLP Pre-charger	\$ 23,720	\$ -139,825	$a_2 =$ Non-compliant

Table 30 provides the expected loss incurred by decision maker D in taking either compliance action using Analyst B’s posterior failure rates. Analyst B had utilized weighted historical data to simulate expert opinion to allocate prior distributions to the components. These priors were then updated using the same data as Analyst A to determine the likelihoods. The resulting posteriors were different from Analyst A, and were found to have a reduced variance, indicative of reduced epistemic uncertainty in the posteriors. The compliance finding is again found by minimizing the expected loss for different components. In this case, in addition to the high lift motors and their inverters, the traction power buses and high lift pre-chargers are also found to be compliant. This is an interesting development that warrants further discussion. The HLP prechargers have a probability of meeting the requirement of 74% for analyst A, which is improved to over 99% for analyst B when historical data is used to inform the prior. Similarly, the traction power bus with a probability of meeting requirements of 59% for analyst A has a higher value of over 93% for analyst B. These changes suggest that analyst B’s expert opinion encoded through the priors biases the posterior enough

Table 30: Expected loss and compliance finding using Analyst B’s posteriors

Component	$\rho(a_1, p)$	$\rho(a_2, p)$	Decision Action
Cruise Motor	\$ 3,000,000	\$ -2,000,000	$a_2 =$ Non-compliant
CM Inverter	\$ 3,000,000	\$ -2,000,000	$a_2 =$ Non-compliant
CM Pre-charger	\$ 2,993,520	\$ -1,995,950	$a_2 =$ Non-compliant
Traction Power Bus	\$ -742,920	\$ 339,325	$a_1 =$ Compliant
Battery	\$ 3,000,000	\$ -2,000,000	$a_2 =$ Non-compliant
HLP Motor	\$ -1,000,000	\$ 500,000	$a_1 =$ Compliant
HLP Inverter	\$ -1,000,000	\$ 500,000	$a_1 =$ Compliant
HLP Pre-charger	\$ -996,600	\$ 497,875	$a_1 =$ Compliant

to make these two components compliant. Another effect of incorporating subject matter opinion by analyst B is visible in the compliance finding of the cruise motor pre-charger unit. The probability of meeting its requirements reduces from analyst A to B, denoting that reducing the variance may not always result in better compliance outcomes. If anything, the decision maker can be more sure of declaring the CM pre-chargers as non-compliant.

5.2.5 Summary of Experiment 2.2

Experiment 2.2 was set up to test the proposed Bayesian decision framework against a more conventional benchmark approach typically used in PSSA compliance finding. The intent of this experiment was to demonstrate that minimizing the posterior expected loss informs the compliance action to be taken while making full use of the improved uncertainty quantification afforded by the Bayesian probability framework.

Towards that goal, a benchmark compliance finding was completed using the mean failure rates using historical and latest data available for the components of interest. The point estimates were compared to the requirements generated in Ch. 4.4.4. This method, while standard in traditional PSSA, does not translate the gain in uncertainty made during the Bayesian probability analysis thus preventing the decision makers from getting the full picture. A Bayesian decision framework was introduced to utilize the expected loss principle to allow decision makers to choose the cost of

making a decision under different truth values. These costs were then weighted using the probability of meeting failure rate requirements (probability of frequency framework) to get a posterior expected loss for each decision action being considered by the decision maker. While minimizing such a loss informed the compliance decision to be taken, the loss values of every alternative preserved the uncertainty information encoded by Bayesian probability analysts and provided the decision makers with a more holistic perspective of the compliance actions. The results generated using analyst A's posteriors (non-informative priors) showed agreement with the benchmark results. Results generated using Analyst B's posteriors, which utilized weighted historical data to simulate SME opinion as a prior, demonstrated an improved compliance finding due to the reduced epistemic uncertainty. Overall, this experiment successfully demonstrated the objective for which it was designed, thus verifying hypothesis 2.2.

5.3 Multi-state Reliability

A multi-state system is one where the system and its components may assume more than two levels of performance. Reliability analysis that considers these multiple possible states is known as multi-state (MS) reliability analysis [176]. Novel aircraft architectures, by definition (see def. 2.1.1.1), are likely to have novel means of satisfying an aircraft level function. These terminal components satisfying the aircraft level functions may fail in multiple different states, or in multiple combinations due to the complexity of such architectures. Therefore, novel architectures are likely to have multi-state failures. In the present work, the T-DEP architecture can be considered a multi-state architecture due to the different unique failure states that can result from combinations of the cruise motor or high lift propulsor failures. Chapter 4.3.5 focused on determining the safety related off-nominal scenarios and their severity in a multi-state fashion. These resulted in the allocation of failure rate requirements to

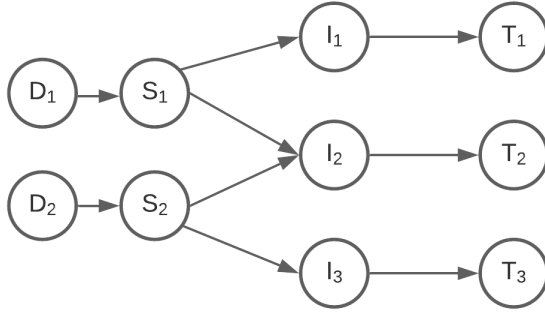
the unit level in chapter 4.4.4. In chapter 5.2.4, a Bayesian decision framework was introduced that provided component level compliance finding. The next logical step is to consider the reliability of the multi-state system failures to meet the requirements generated (see fig. 59). These considerations, as well as the final requirement posed under research question 2 in chapter 3.3 leads to the following research sub-question:

Research Question 2.3:

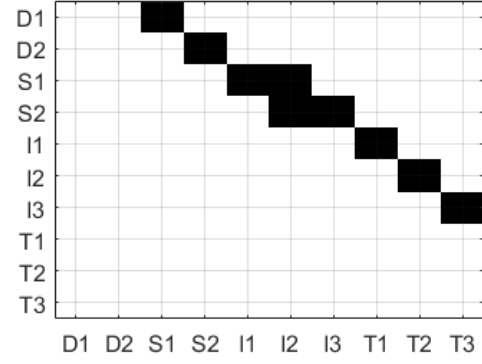
What method can allow the estimation of multistate system reliability while accounting for both epistemic and aleatory uncertainty under scarcity of available data?

5.3.1 A Multi-state Network Reliability Approach

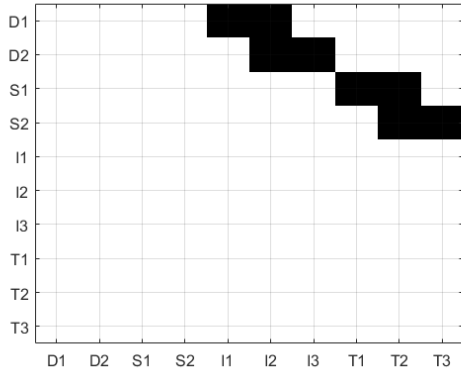
Computation of multi-state system reliability is a well established problem with numerous potential solutions provided in literature. Of these, a Monte-Carlo simulation approach can be utilized for computing the reliability of almost every complex, real-world multi-state system [176]. In this method, a system is typically represented as a network with nodes or edges representing different components. An adjacency matrix that denotes the connections between such notes is created to depict the connections within the system of interest. Consider a simplified system that was introduced earlier along with its network adjacency matrix given by figure 63. An adjacency matrix (A) is a square matrix with rows and columns denoting the components of the system. If component i connects forward to component j , $A_{ij} = 1$, otherwise $A_{ij} = 0$. This system has dummy components D_1 , D_2 that aid with system reliability computations. The components of interest are the source components S_i , intermediate components I_i , and terminal components T_i . The system level failure states are characterized by the failures in its terminal, function satisfying components T_i . Thus, this system has $2^3 = 8$ possible states(1 nominal, 7 off-nominal) that were provided earlier in table 4. A terminal component can be considered to have failed in a network approach if there



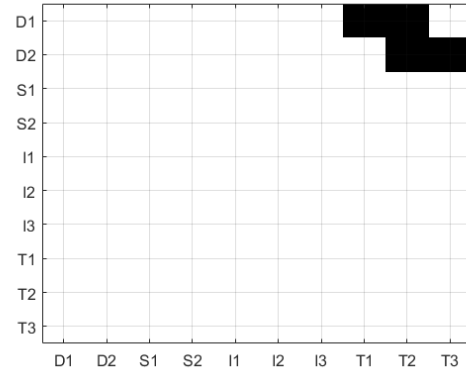
(a) Example network representation



(b) Corresponding adjacency matrix A



(c) Corresponding A^2



(d) Corresponding A^3

Figure 63: An example system with two sources and three terminal components in network representation

exists no paths between the source and the terminal component of interest.

An adjacency matrix allows the determination of the existence of a path between a source and a terminal component of interest due to some interesting properties. The non-zero elements of A^1 provide the components that are connected by a path with an edge-length of 1. For instance, if $A^1(i, j) = 1$, then component i is connected to component j with a path of length 1. This is by definition of the adjacency matrix and is trivial. However, this property extends to higher orders as well. For instance, if $A^2(i, j) = k$, then components i and j are connected by k different paths of edge-length 2. Generalizing, if $A^n(i, j) = k$, then components i, j are connected by k paths of length n . Finally, $A^{N+1} = 0$ when $N = n\text{rows}(A) = n\text{cols}(A)$. This is visible

in figure 63(c), where the matrix elements in rows S_1, S_2 with columns T_1, T_2, T_3 are non-zero, meaning these components are connected with a path of length 2. Similarly, components D_1, D_2 are connected with T_1, T_2, T_3 with paths of length 3 as shown in figure 63(d). Thus, $(A + A^2 + A^3 + \dots A^N)(i, j)$ provides the total number of paths of varying lengths between components i, j .

In the present work, components are modeled as nodes, with the columns of the adjacency matrix giving incoming connections from components upstream, while rows give outgoing network connections to downstream components. This is visible in the example case in Fig. 63(b) for the system provided. To simulate the failure of any component, all its incoming connections are set to 0. For instance, if component j were to fail, all elements in column j of the corresponding adjacency matrix A would be set to zero. The sources only have outgoing connections (rows) but no incoming connections (columns). Thus source failures can only be simulated by having an upstream dummy component D , so that incoming (columns) edges of a source can be set to zero. Once failures have been introduced into the adjacency matrix, the resultant paths between the sources and terminal components can be re-calculated to see if there are any places where those paths are disconnected (failed path from source to terminal component). This knowledge can be used in a Monte-Carlo simulation.

Lam and Szeto [106] provide two algorithms to evaluate the network reliability and path-connectedness of a network given by an adjacency matrix A . These have been modified and combined in the present work to evaluate the multi-state reliability of novel aircraft architectures with multiple sources and sinks (terminal components), and with Bayesian posterior probabilities. While the original algorithms assume constant reliability p for every component, the modified algorithm utilizes failure probability ($p=1 - e^{-\lambda t}$). The failure rate λ is sampled from the Bayesian posterior distribution for every Monte-Carlo experiment/iteration, thus translating the uncertainty in failure rates through the system reliability evaluation. When a

component fails, it may result in the terminal component T_i getting disconnected from the source components S_i , identifiable with having zero paths between the two. In such a case, the terminal component is considered failed, with its state $x_T = 0$. A state vector $X = \{x_{T_1}, x_{T_2}, \dots, x_{T_k}\}$ is introduced to capture the state of the terminal components of the system. X , therefore, defines the state of the system, with different combinations of terminal component failures representing multi-state system failures. The modified algorithm for multi-state reliability assessment is provided below.

Algorithm 2: Evaluate MS network failure probability (F_{X_k}) for a given matrix A with given component unreliability p_i

Result: MS failure probability F_{X_k} of system network with adjacency A
 n_exp = number of experiment;
for $n \leftarrow 1$ **to** n_exp **do**
 Let A_{rand} be a random $N \times N$ matrix whose column j is $p = (1 - e^{-\lambda t})$,
 where λ is sampled from the posterior failure probability of component j ;
 if the ij^{th} entry of A_{rand} is greater than p and the corresponding ij^{th} of A
 is 1 **then**
 | let the ij^{th} entries of A_{rand} be 1 ;
 else
 | let the ij^{th} entries of A_{rand} be 0 ;
 end
 Compute $A_{path} = \sum_1^N A_{rand}^i$;
 Compute A_{trim} by trimming A_{path} to keep rows corresponding to source
 elements S and columns corresponding to terminal elements T ;
 Compute and store the system state vector X by summing up the
 columns of A_{trim} ;
end
If X_k is a unique system state, $F_{X_k}(t) = n_{X_k}/n_exp$, where n_{X_k} is the
number of iterations that result in X_k

This algorithm provides the probability of every unique system failure state, computed within one single Monte-Carlo simulation. The modification made in algorithm 2 from Ref. [106] are given in blue. With this multi-state reliability algorithm expounded, hypothesis 2.3 is restated as follows:

Hypothesis 2.3: *A multistate network reliability approach utilizing Monte Carlo simulations, suitably adjusted to work with Bayesian failure rate posteriors will provide accurate estimation of the system level reliability under uncertainty.*

5.3.2 Experiment 2.3

Since hypothesis 2.3 is a feasibility hypothesis, the intent of this experiment is to demonstrate that algorithm 2 can compute the multi-state failure rates of a complex system.

5.3.2.1 Purpose of the Experiment

The test problem for this thesis is the T-DEP architecture given in Fig. 33, whose multi-state failures and their hazard severity was documented in chapter 4.3.5. Table 2 requires that each of the failure states from Fig. 51, 52, 54 have a failure rate of less than those mentioned for assessment level II aircraft depending on the hazard severity of those states. Component failure rate requirements (Ch. 4.4.5), component failure rate posteriors (Ch. 5.1.6), as well as component compliance (Ch. 5.2.4) have been obtained in the previous chapters. While component compliance results give an insight into the reliability of the components, their impact on the aircraft/system level in a multi-state fashion is not obvious for complex systems. Thus, the purpose of this experiment can be stated as,

1. Demonstrate network based multi-state reliability analysis approach to compute T-DEP power system multi-state failure rates using the proposed Monte-Carlo algorithm

5.3.3 Multi-state Reliability Results

For the T-DEP architecture, the multi-state failure rate requirements stem from results provided in Figs. 51, 52, and 54. The corresponding failure rate requirements

are given by figures 64, 65, and 66.

No. HLP failed	0	1	2	3	4	5	6	7	8	9	10	11	12
No. CM failed													
0		<10 ⁻³	<10 ⁻³	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷
0.5	<10 ⁻³	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷
1	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	0.27	<10 ⁻⁷
2	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷

Figure 64: T-DEP multi-state λ_{req} in takeoff configuration. Colored by C-FHA hazard severity from Fig. 49(a)

No. HLP failed	0	1	2	3	4	5	6	7	8	9	10	11	12
No. CM failed													
0													
0.5	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵
1	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶
2	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷

Figure 65: T-DEP multi-state λ_{req} in cruise configuration. Colored by C-FHA hazard severity from Fig. 49(b)

No. HLP failed	0	1	2	3	4	5	6
CM-1 Loss %							
0		<10 ⁻³	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵
0.5	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷
1	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷

Figure 66: T-DEP asymmetric multi-state λ_{req} in takeoff configuration. Colored by asymmetric thrust loss hazard severity from Fig. 54

A potential shortcoming of Monte-Carlo analysis to evaluate reliability is that events that are unlikely with a low probability of occurrence tend to be disproportionately missed. To solve this issue, the present analysis assumes a operating time of $t = 5000hr$ to compute component failure probabilities ($F(t)$) using Eq. 6. A Monte-Carlo simulation of 1 million experiments is carried out as detailed in algorithm 2 following which the probability of the system in different failure states ($F_{X_k}(t)$) is

computed. The failure states (X_k) are represented by the terminal components (high lift propulsors or cruise motors) losing full or partial power supply. The failure rates of the different system states are then back-calculated using Eq. 134.

$$\lambda_{X_k} = \frac{1}{t} \ln \left(\frac{1}{1 - F_{X_k}(t)} \right) \quad (134)$$

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6	7	8	9	10	11	12
0		4.71E-05	3.05E-05	1.19E-05	3.17E-06	6.11E-07	8.72E-08	7.60E-09	1.40E-09	<1E-10	<1E-10	<1E-10	<1E-10
0.5	1.10E-05	1.63E-05	1.07E-05	4.59E-06	1.52E-06	4.11E-07	8.40E-08	1.32E-08	1.40E-09	<1E-10	<1E-10	<1E-10	<1E-10
1	3.31E-06	4.88E-06	3.27E-06	1.41E-06	4.72E-07	1.31E-07	1.06E-05	7.72E-06	2.29E-06	3.93E-07	3.28E-08	1.60E-09	<1E-10
2	5.20E-08	6.78E-08	4.74E-08	2.20E-08	7.60E-09	1.40E-09	1.55E-07	1.14E-07	3.56E-08	1.26E-08	5.40E-09	6.00E-10	9.84E-07

(a) Analyst A

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6	7	8	9	10	11	12
0		6.10E-05	2.80E-05	7.94E-06	1.60E-06	2.22E-07	2.66E-08	1.80E-09	4.00E-10	<1E-10	<1E-10	<1E-10	<1E-10
0.5	1.53E-05	1.66E-05	7.98E-06	2.51E-06	5.84E-07	1.03E-07	1.38E-08	1.60E-09	2.00E-10	<1E-10	<1E-10	<1E-10	<1E-10
1	3.18E-06	3.48E-06	1.71E-06	5.44E-07	1.24E-07	2.12E-08	5.62E-06	3.02E-06	6.75E-07	8.40E-08	6.80E-09	2.00E-10	<1E-10
2	1.88E-08	2.40E-08	1.12E-08	2.00E-09	1.00E-09	0.00E+00	4.56E-08	2.24E-08	5.40E-09	1.40E-09	2.00E-10	0.00E+00	1.65E-07

(b) Analyst B

Figure 67: Multi-state failure rates for the two Bayesian analysts for takeoff C-FHA hazards colored by compliance finding

Figure 67 provides results of the multi-state failure rate of the different failure conditions of the T-DEP power system from figure 33. During the component-specific compliance finding from Ch. 5.2.4, it was discussed how Analyst A's posteriors encode a larger epistemic uncertainty and result in more components being declared non-compliant compared to Analyst B. Similar trends are visible at the aircraft level multi-state compliance analysis. When compared to the failure rate requirements allocated from C-FHA analysis at the system level (Fig. 67), Analyst A's posteriors result in a larger number of aircraft level failure states being non-compliant compared to Analyst B's posteriors.

Also of note is that component allocation assumed multiple component failures

were unlikely, thus allowing reliability requirement allocation based on single component failures. The results in the present experiment suggest that multiple component failures may be a cause for concern when it pertains to certain failure states in the T-DEP power system. Consider the non-compliant (in red) failure states using Analyst B's posteriors. A state where a cruise motor has lost half power, along with a single (any one out of 12) high lift motor failing is deemed non-compliant of the reliability requirements generated. This failure state has no single component failure and must involve two different components (CM inverter/PC and HL motor/inverter/PC) failing. Similarly, a state with total thrust loss (2 CM lost, 12 HLP lost) is possible only through a complete loss of both batteries, or through multiple combinations of traction power bus failures, or individual component failures. However, this state is found to have a higher failure rate than the 10^{-7} per flight hour required for a catastrophic event.

In a way, such a Monte-Carlo reliability analysis by modeling the system as a multi-state network allows the analysts to consider all possible combinations of failures, irrespective of whether it involves multiple components failing at once. While such states may be perceived as being highly unlikely in preliminary safety analysis, analyses such as these do not require any assumptions and can capture the compliance of off-nominal states of a system better.

No. HLP failed -> No. CM failed	0
0	
0.5	1.10E-05
1	3.31E-06
2	5.20E-08

(a) Analyst A

No. HLP failed -> No. CM failed	0
0	
0.5	1.53E-05
1	3.18E-06
2	1.88E-08

(b) Analyst B

Figure 68: Multi-state failure rates for the two Bayesian analysts for cruise C-FHA hazards colored by compliance finding

Figure 68 provides the failure rate results for the two analysts for the three different off-nominal states the T-DEP power system architecture can take in its cruise configuration. The results using the posteriors of both Bayesian analysts reach the same conclusions at the system level – that partial loss of thrust from a cruise motor, and a complete loss of one cruise motor are scenarios that are non-compliant with the reliability requirements. This result was hinted at when the cruise motors and their inverters were found to be non-compliant with the safety requirements generated in Ch. 5.2.4 by the decision maker D using both Analysts’ posteriors. While a total loss of thrust in cruise might be catastrophic, it sufficiently meets the failure rate requirements of $< 10^{-7}$ per flight hour.

The next set of results examined are the failure rates of the asymmetric loss of thrust states of the T-DEP architecture. The output of the Monte-Carlo runs is processed to determine the number of system failure states with the left HLP and cruise motor failed asymmetrically and doubled to consider the mirror case when the right side fails. The resultant failure rates are given in figure 69.

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6
0		7.41E-05	1.66E-05	2.43E-06	2.34E-07	1.12E-08	4.00E-10
0.5	1.77E-05	9.91E-06	2.90E-06	8.33E-07	1.55E-07	1.36E-08	1.20E-09
1	3.68E-06	2.12E-06	6.09E-07	1.46E-07	2.40E-08	2.00E-09	4.00E-10

(a) Analyst A

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6
0		7.66E-05	1.38E-05	1.50E-06	1.08E-07	2.40E-09	4.00E-10
0.5	2.01E-05	9.22E-06	2.04E-06	3.56E-07	4.84E-08	2.80E-09	<1E-10
1	2.73E-06	1.25E-06	2.60E-07	4.48E-08	4.40E-09	4.00E-10	<1E-10

(b) Analyst B

Figure 69: Asymmetric loss of thrust – multi-state failure rates for the two Bayesian analysts for takeoff. Colored by compliance finding

An important distinction between the results of figure 67 and 69 must be qualified. The number of HLP failed term at the top represents the difference between the HLP failures on the left and right side of the fuselage for Fig. 69. Thus, even a case with 6 left HLP failures and 5 right HLP failures would fall under 1 asymmetric HLP failure in figure 69. The failure rate requirements, in this case, are based on figure 66. These requirements were in turn computed by assuming a worst-case scenario of the most outboard propulsors failing first during multi-state analysis conducted in Ch. 4.3.5. Under these conservative assumptions, the results indicate that the T-DEP failure states consisting of half a cruise motor failing (CM at half power), along with up to 2 HLP failing on the same side are non-compliant with the safety requirements. It is interesting to note that a majority of these failure states are categorized as ‘Major’ or ‘Hazardous’ severity, and not ‘Catastrophic’. This means failures that would typically go under the radar in conceptual or preliminary design have the potential to drive safety related off-nominal requirements. Such an insight would not have been possible in a traditional safety analysis framework during conceptual or preliminary design, since the focus during these is to minimize the risk posed by catastrophic failures.

5.3.4 Summary of Experiment 2.3

The intent of this experiment was to demonstrate that a Monte-Carlo algorithm suitably modified to work with Bayesian failure rate posteriors and network-based multi-state reliability approach provides accurate estimation of the multi-state reliability of the T-DEP power system architecture. The need stemmed from evaluating the system level impacts of the combined performance based off-nominal requirements identification, and a Bayesian unit level failure rates determination framework. The performance based off-nominal conditions were characterized by Fig. 51, 52, and 54. The corresponding failure rate requirements were provided in Fig. 64, 65, and 66.

A modified Monte-Carlo algorithm (see alg. 2) was introduced to compute the

probability of the different T-DEP power system failure states. Operating time was set to $t = 5000hr$ to overcome the tendency of a Monte-Carlo analysis to under-sample the remote probability states. One million Monte-Carlo samples were generated and analyzed to generate the failure rates of the different states using Eq. 134. The results have been provided in Fig. 67, 68, and 69.

Results pertaining to symmetric failure states analyzed by C-FHA indicated that multi-component failures are not as unlikely as were previously assumed, and in fact result in failure states that are non-compliant with the requirements from table 2. Certain multi-state C-FHA analyzed failures were non-compliant across both Bayesian analyst's posteriors. These include (i) losing half a cruise motor and one high lift propulsor (HLP), (ii) Losing one cruise motor equivalent (two half CMs or one full) + 6 to 8 HLPs. Finally, a complete loss of thrust scenario was also found to be non-compliant with failure rate requirements. Some of these results may be explained by considering the component level compliance from Ch. 5.2.4. For instance, the cruise motors, their inverters, and the batteries were found to be non-compliant for both the Bayesian analyst's posteriors. These components drive a majority of the non-compliant failure states observed in the results in the present experiment. However, they alone cannot explain results where one cruise motor and 8 HLPs have failed – pointing towards multiple component failures as a cause. The importance of different components in terms of system reliability is considered later in chapter 6.1.

The next multi-state reliability considered involved the asymmetric thrust loss failures from Ch. 4.3.5 and table 19. The failure rates computed from the Monte-Carlo simulations indicate that failures of half/full cruise motor with up to two HLPs on one side tend to be non-compliant with the reliability requirements. These failures correspond to a severity category of 'Major' to 'Hazardous'. This indicates that reliability requirements for the T-DEP architecture are driven by some of the less critical failure states. This goes counter to the assumption typically made during

traditional safety analysis during preliminary design where ‘Catastrophic’ failures drive reliability requirements.

These results satisfy the intent of the present experiment by demonstrating results and insights from multi-state reliability analysis of the T-DEP architecture. They, therefore, verify hypothesis 2.3.

5.4 Chapter Summary

The second research question (RQ 2) was motivated by observations group 2 from Ch. 2.5. With the characterization and unit level allocation of safety related off-nominal requirements completed in Ch. 1.5, the next logical step was to evaluate the system level and unit level reliability. To that end goal, the overall intent of RQ 2 was to provide a better treatment of uncertainty in the reliability estimations of novel aircraft architectures at the system and component level. RQ 2 was further divided into three research sub-questions – (i) RQ 2.1 that dealt with component level reliability assessment; (ii) RQ 2.2 that dealt with component compliance decision making; and (iii) Multi-state system level reliability assessment.

One hypothesis was stated for each research sub-question above. Hypothesis 2.1 (H-2.1) recommended a Bayesian probability framework for failure rate estimation of the novel components while providing better treatment of uncertainty. The metrics used to define ‘better’ in this instance were the 6-levels of treatment of uncertainty by Paté-Cornell [146]. For experiment 2.1 (E-2.1), a benchmark approach considered point estimates (mean) for component failure rates. Two Bayesian analysts A, B were imagined providing two different prior distributions to encode disciplinary knowledge as epistemic uncertainty. The resulting distributions were found to represent a level 5 treatment of uncertainty, better than the level 3 afforded by the benchmark, thus verifying H-2.1.

Hypothesis 2.2 (H-2.2) suggested that minimizing the posterior expected loss

would provide an uncertainty-informed compliance decision for the novel aircraft architecture components. In verifying H-2.2, experiment 2.2 considered a benchmark method of compliance of testing where the point failure rate estimates generated in E-2.1 are compared to failure rate requirements generated in Ch. 4.4.4. A Bayesian decision framework was developed that computes the posterior expected loss for each component using a loss function that is defined by a decision maker. Minimizing the expected loss for the two analysts' posteriors resulted in slightly different compliance findings. However, the results not only indicated whether a component was compliant or not but also included the probability weighted cost of taking either decision. This provides the decision makers with additional information and alternate models, leading to better uncertainty-informed decision making.

By now, component failure rates and compliance decisions were made for the T-DEP architectures. RQ 2.3, therefore, looked at compliance finding at the system level in a multi-state context where the system may fail in multiple states. Hypothesis 2.3 (H-2.3) suggested a Monte-Carlo network reliability algorithm suitably modified to work with Bayesian posteriors and for multi-state failures as a solution. For experiment 2.3 (E-2.3), a Monte-Carlo simulation was run to generate one million working and failed system states using Bayesian component failure probabilities from E-2.1. The output was then post-processed to identify the failure rates of different failure states postulated in the C-FHA and asymmetric thrust loss analysis from Ch. 4.3.5. These results suggested that multiple failures are not as unlikely as first assumed, resulting in certain failure states not meeting reliability requirements. The asymmetric thrust loss states' reliability analysis showed that more failure states that were categorized as 'Major' or 'Hazardous' do not meet requirements as compared to 'Catastrophic'. This means that the less safety critical failures have a tendency to drive reliability requirements for the T-DEP power systems architecture.

With these results, the proposed hypotheses for the three parts of RQ 2 were

successfully verified, completing the intent of research area 2 from Ch. 3.3

CHAPTER VI

THE INTEGRATED FRAMEWORK - SENSITIVITIES AND TRADE STUDIES

The intent of the present chapter is to integrate the tools and methods discussed so far into a framework that allows better incorporation of safety related off-nominal considerations into early design stages for novel aircraft architectures. The need for such an integrated solution is also felt through the last requirement posed by the overall research objective in Ch. 3.1. The requirement to integrate this framework into early design trade studies stems from observation group 3 in Ch. 2.5 which can be summarized to say that traditional methods fall short when it comes to enabling design trade-off analysis under safety related off-nominal considerations. This motivates research question 3, which is restated here:

Research Question 3:

How can design trade studies for novel aircraft architectures and technologies be conducted in early design while incorporating safety related off-nominal scenarios?

An overview of the developed framework was first provided in Ch. 3.5 and is provided here again in figure 70. The framework assumes that the configuration has been sized – this includes the weight breakdown including mass properties, geometric definitions including wing and other areas including locations of control surfaces if any, architecture definition that includes any redundancy considerations for the internal energy flows of the systems, any available aerodynamics and propulsion models, and finally any available subsystem sizing details. The first task then is to identify a set of appropriate safety metrics of interest for the given architecture. This part was

completed and demonstrated in Ch. 4.2.

Next, adequate models are developed for the functions of interest to characterize the effect of functional degradation on safety metrics. In the present work, since the test problem is the T-DEP aircraft with novel architecture to provide thrust and high lift, models that evaluate the safety metrics given in table 5 at the conceptual and preliminary stage were created in Ch. 4.3.3, 4.3.4. The outputs of these models included the safety metrics of interest under functional or component loss scenarios. Certification requirements and engineering judgement were used to set thresholds on these metrics that helped characterize the severity of the hazards postulated. A bottom-up network algorithm in Ch. 4.4 was used to allocate the requirements to the components.

With the safety related off-nominal requirements now characterized and allocated, a Bayesian probability and decision framework with a multi-state extension were introduced in Ch. 5. Here, component Bayesian failure rate posteriors with compliance finding were completed, along with a system level multi-state reliability and system level multi-state compliance findings.

All of these tools and methods can be put together into one integrated framework that enables evaluation of off-nominal safety related requirements and reliability of novel aircraft architectures in early design. At this stage, the framework can be used to inform design decisions, as well as close the loop to perform trade-studies. It can also be used to optimize the conceptual sizing using reliability information in a reliability based design optimization (RBDO) loop (beyond the scope of the present work). The outputs of this framework can be used to inform the late stage preliminary design and onward. This framework given in figure 70 is the final hypothesis of this dissertation as stated below:

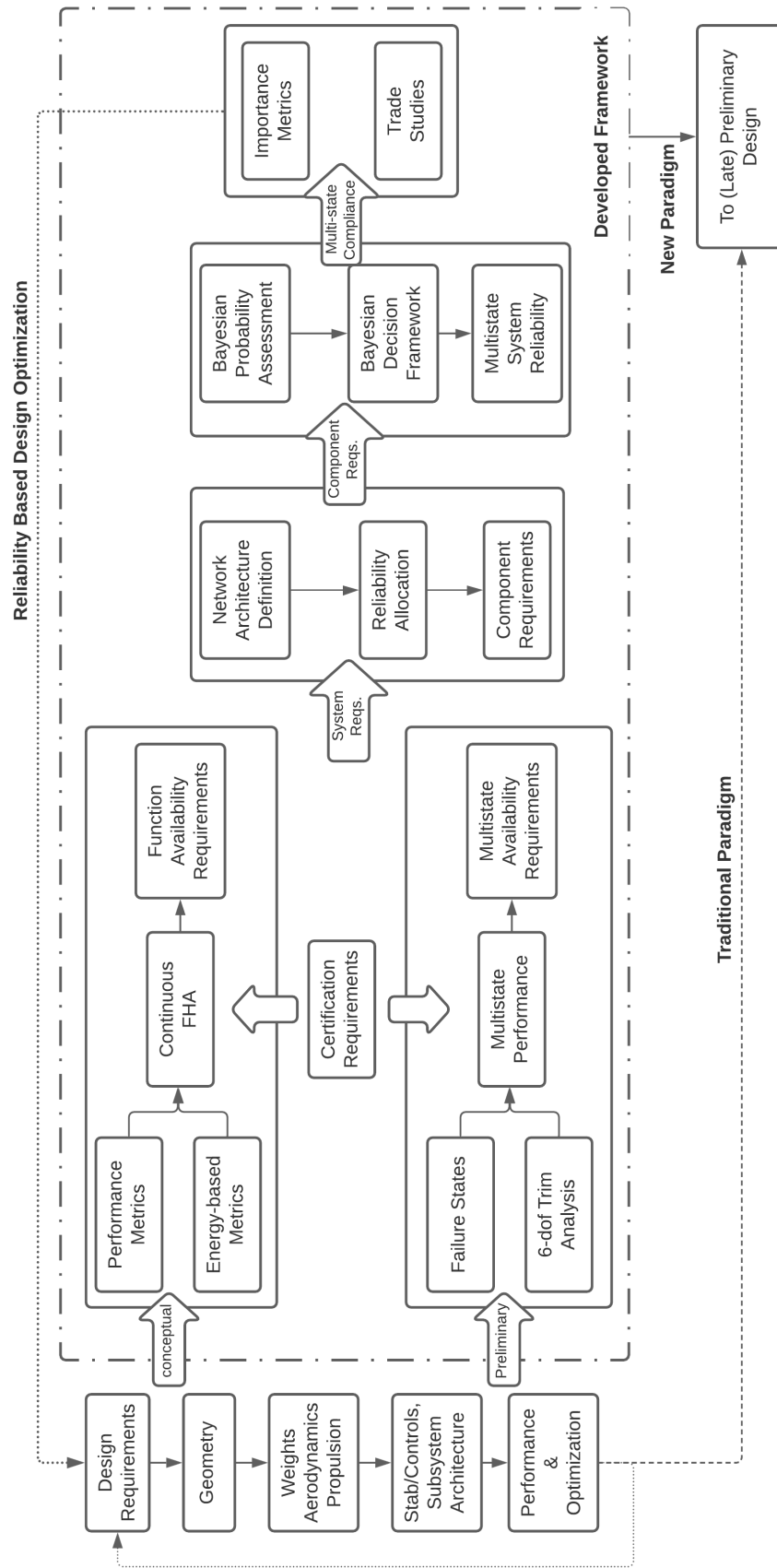


Figure 70: Integrated Framework to Evaluate Off-Nominal Requirements & Reliability of Novel Architectures in Early Design

Hypothesis 3: *The integrated framework given in figures 24 or 70 enables design trade studies while incorporating safety related off-nominal requirements and reliability of novel aircraft architectures in early design*

In order to verify hypothesis 3, the present chapter takes a two-pronged approach. First, component level multi-state importance metrics are established and evaluated to determine the sensitivity of multi-state system reliability to the component failure rate posteriors. Second, design trade-studies in terms of resizing the vertical tail and oversizing cruise inverters are demonstrated with any benefits in off-nominal operations quantified.

6.1 Unit Level Importance

Component importance measures are used in reliability theory to quantify the criticality of components within a system. They may be used (i) to provide a ranking of components with respect to their influence on system level reliability, (ii) to determine the top contributors to unreliability, (iii) to focus on making improvements that will have the greatest reliability effect, and (iv) to perform sensitivity studies [153].

6.1.1 Experiment 3.1

The multi-state reliability results provided in Ch. 5.3.3 depend on numerous assumptions made throughout the analysis. Since the focus of the present chapter is on enabling trade-studies, quantifying the sensitivity of system multi-state reliability results with respect to the reliability of individual components forms experiment 3.1. This sensitivity analysis will help identify components that drive the reliability of the different failure states of the T-DEP aircraft power system architecture. Once these components and the failure states they most affect are determined, this information can be used to focus the development efforts with the goal of improving their individual reliability.

6.1.2 Reliability of Complex Systems

Complex systems typically involve multiple components to enable the satisfaction of a top level function with a level of fault-tolerance through adequate reliability. Even when the component failures of such systems are assumed to be binary (working/failed), these can result in different off-nominal states for the system of interest.

6.1.2.1 The Structure Function

The present state of such a system can be denoted through a structure function, that relates the state of the components to that of the system [123]. Assume x_i denotes the binary state (working/failed) of component i . That is, $x_i = 0$ when a component has failed and $x_i = 1$ when it is working. A state vector $\bar{x} = (x_1, x_2, \dots, x_n) \in \{0, 1\}^n$ can be used to denote the state of the n components in the system. The structure function $\phi(\bar{x})$ can then be defined to determine the present state of the system. When the system itself has binary failure states, $\phi(\bar{x}) : \{0, 1\}^n \rightarrow \{0, 1\}$. For two component state vectors \bar{l} and \bar{m} , the following properties hold true [123].

$$\begin{aligned}\bar{l} + \bar{m} &= (l_1 + m_1, l_2 + m_2, \dots, l_n + m_n) \\ \bar{l} \cdot \bar{m} &= (l_1 \cdot m_1, l_2 \cdot m_2, \dots, l_n \cdot m_n)\end{aligned}$$

The set of \bar{x} is assumed partially ordered with a property of ' \leq '. For instance, if $m_i \leq l_i$ for $i = 1, 2, \dots, n$, with $m_i < l_i$ for some i , then $\bar{m} \leq \bar{l}$. Finally, a structure function $\phi(\bar{x})$ is said to be monotone, if (i) $\phi(0) = 0$, $\phi(1) = 1$, and (ii) $\phi(\bar{m}) \leq \phi(\bar{l})$ if $\bar{m} \leq \bar{l}$. Thus, since the structure function is monotone, it represents that the system level reliability can be improved if the component level is improved [123].

A couple of examples of the structure function are provided next. Assume a system made of n components in series. It will be in a working state only if all components

are in a working state as given by,

$$\begin{aligned}
\phi_{series}(\bar{x}) &= \prod_{i=1}^n x_i \\
&= x_1 \cdot x_2 \dots \cdot x_n \\
&= \min(x_1, x_2, \dots, x_n)
\end{aligned}$$

Similarly, a parallel structure can be given by,

$$\begin{aligned}
\phi_{parallel}(\bar{x}) &= 1 - \prod_{i=1}^n (1 - x_i) \\
&= x_1 + x_2 \dots + x_n \\
&= \max(x_1, x_2, \dots, x_n)
\end{aligned}$$

The structure functions for complex systems (combinations of series and parallel) get complicated and are not always the best means to represent the system of interest. The intent in introducing the structure function is to enable a discussion on multi-state reliability that will then tie into multi-state component importance.

The above discussion assumes the system failure is binary. In a system such as the T-DEP architecture in the present thesis where component failures are assumed to be binary, while the system level may have multi-state failures, the structure function can be modified to $\phi(\bar{x}) : \{0, 1\} \rightarrow [0, 1]$, where $[0, 1]$ is a continuous set that denotes the proportion of maximum capability available in a given system failure state.

6.1.2.2 Multi-state System Reliability

While the term reliability and its definition have been discussed earlier, the present section seeks to introduce the formalism used when quantifying multi-state reliability using state vectors and structure functions. The failure probability of a system failing in a time interval $[0, t]$ is given by,

$$F(t) = \Pr(T \leq t) = \int_0^t f(\tau) d\tau$$

The reliability is simply the complement of the failure probability,

$$R(t) = 1 - F(t) = Pr(T > t)$$

where $Pr(T > t)$ denotes the probability of the system to remain functioning after time t . If the component state vector $\bar{x}(t)$ is generated based on component i operational reliability $x_i(t) = Pr_i(T > t)$, the system multi-state reliability can be given as,

$$R_{MS}(t) = Pr(\phi(\bar{x}(t)) > d) \quad (135)$$

where $d \in [0, 1]$ denotes the proportion of system capability left. For instance, d may represent the thrust available after a failure in an aircraft power systems architecture. In some cases, $d = \{d_1, d_2, \dots, d_k\}$ is a set of k discrete performance levels a system may take under failure.

6.1.3 Multi-state Component Importance Measures

With the background of how multi-state reliability may be characterized using a structure function provided, the present section introduces traditionally utilized measures of component importance along with their multi-state extensions used in this thesis. There are typically two kinds of multi-state importance measures – (i) Type 1 which measure how specific components affect multi-state system reliability, and (ii) Type 2 which measure how a particular component failure state affects multi-state system reliability [152]. Since the T-DEP architecture assumes the component failures are binary, Type 1 multi-state importance measures are of interest in the present work and are discussed next.

6.1.3.1 Birnbaum Importance

Birnbaum [37] introduced the concept of component importance in 1968, with a measure that is defined by,

$$\begin{aligned}
I_i^{BB} &= \frac{\delta R_S(t)}{\delta R_i(t)} \\
&= R_S(t|R_i(t) = 1) - R_S(t|R_i(t) = 0) \\
&= Pr(\phi(\bar{x}) = 1 \mid x_i = 1) - Pr(\phi(\bar{x}) = 1 \mid x_i = 0)
\end{aligned} \tag{136}$$

The Birnbaum importance measure is the partial derivative of the system reliability R_S with respect to the component reliability R_i [153] and denotes the maximum loss in system reliability when a component i switches from working to failed [123].

For the T-DEP architecture and multi-state reliability considerations, hazard severity is used to denote system capability d defined above. Therefore, $d = \{1, 2, 3, 4, 5\}$ correspond to ‘Negligible’, ‘Minor’, ‘Major’, ‘Hazardous’, ‘Catastrophic’ respectively. Then, the multi-state reliability definition from Eq. 135 is used. Multi-state Birnbaum importance measure from Ref. [152] is modified to provide a custom defined measure in this thesis, and is given by,

$$\begin{aligned}
MI_i^{BB} &= Pr(\phi(\bar{x}) < d \mid x_i = 1) - Pr(\phi(\bar{x}) < d \mid x_i = 0) \\
&= \frac{Pr(\phi(\bar{x}) < d \cap x_i = 1)}{Pr(x_i = 1)} - \frac{Pr(\phi(\bar{x}) < d \cap x_i = 0)}{Pr(x_i = 0)}
\end{aligned} \tag{137}$$

The proposed multi-state Birnbaum measure given in Eq. 137 considers the hazard severity as a classifier of system state. For the T-DEP aircraft power system, this is a departure from the failure states that were defined so far as different combinations of cruise motors or high lift propulsors failing. Considering the severity of different failure states in the importance measures enables decision makers to determine which components are driving the off-nominal severity of interest. Consider the ‘Catastrophic’ severity conditions ($d = 5$). For a component i under consideration, the first term in Eq. 137 calculates the probability of the aircraft to stay in a severity

that is less critical than ‘Catastrophic’ ($\phi(\bar{x}) < d = 5$) given component i is working ($x_i = 1$). The second term subtracts from the first, the probability of the system failing in a severity that is less critical than ‘Catastrophic’, given component i has failed ($x_i = 0$). Similarly, for a ‘Major’ hazard severity, the multi-state Birnbaum importance measure developed above will consider all nominal and off-nominal conditions that are less critical than ‘Major’ (so ‘Negligible’ and ‘Minor’ are included, others are excluded) in the probability computation.

The statement of Eq. 137 is a simplification of the equation described above using Bayes’ theorem of conditional probability. Writing it in this format makes it easier to compute the proposed importance measure from the same set of Monte-Carlo simulations that were completed for experiment 2.3 (see alg. 2 and Ch. 5.3.3).

6.1.3.2 Criticality Importance

One shortcoming of the Birnbaum importance measure is that it does not consider the magnitude of reliability change with respect to the system’s baseline reliability. This is remedied by the Criticality Importance measure, which corrects Birnbaum’s measure with the ratio of component unreliability $F_i(t)$ to system unreliability $F_S(t)$ [25,123]. It is also defined as the probability that component i is critical for the system and failed at time t , when it is known that the system has failed at time t [153]. Mathematically these statements are represented as,

$$\begin{aligned} I_i^{CI} &= I_i^{BB} \frac{F_i(t)}{F_S(t)} \\ &= I_i^{BB} \frac{1 - R_i(t)}{1 - R_S(t)} \end{aligned} \quad (138)$$

For the multiple states characterized by hazard severity defined for the Birnbaum importance (see Ch. 6.1.3.1), $d = \{1, 2, 3, 4, 5\}$ corresponding to ‘Negligible’, ‘Minor’, ‘Major’, ‘Hazardous’, ‘Catastrophic’ respectively are utilized to define the multi-state

extension of Criticality Importance in this thesis.

$$\begin{aligned}
MI_i^{CI} &= MI_i^{BB} \frac{1 - R_i(t)}{1 - R_{MS,sys}(t)} \\
&= MI_i^{BB} \frac{1 - Pr(x_i = 1)}{1 - Pr(\phi(\bar{x}) < d)}
\end{aligned} \tag{139}$$

where $Pr(\phi(\bar{x}) < d)$ is the probability of the system being in a state that is less critical than d , and is considered the system reliability (from) severity d . Eq. 139 can be computed from the same Monte-Carlo runs conducted for experiment 2.3 and thus requires no additional failure simulations to be conducted.

6.1.3.3 Reliability Achievement Worth (RAW)

Reliability achievement worth measures the maximum relative increase in system reliability that can be generated by component i [152]¹. It is given by,

$$\begin{aligned}
I_i^{RAW} &= \frac{R_S(t \mid R_i(t) = 1)}{R_S(t)} \\
&= \frac{Pr(\phi(\bar{x}) = 1 \mid x_i = 1)}{Pr(\phi(\bar{x}) = 1)}
\end{aligned} \tag{140}$$

For a multi-state case similar to measures above where d denotes the hazard severity, a modified RAW measure is provided as,

$$\begin{aligned}
MI_i^{RAW} &= \frac{Pr(\phi(\bar{x}) < d \mid x_i = 1)}{Pr(\phi(\bar{x}) < d)} \\
&= \frac{Pr(\phi(\bar{x}) < d \cap x_i = 1)}{Pr(\phi(\bar{x}) < d)Pr(x_i = 1)}
\end{aligned} \tag{141}$$

The RAW is typically greater than 1, with a value of 1 suggesting that component i has no potential to improve on system reliability. The multi-state RAW measure from Eq. 141 is computed from the same set of Monte-Carlo results from E-2.3 just like the measures discussed before.

¹An analogous but not equal measure is the risk achievement worth which measures the relative increase in system unreliability when it is known that component i has failed [153]

6.1.3.4 Fussell-Vesely (FV)

The Fussell-Vesely measure captures the maximum relative decrement in system reliability that can be caused by component i [152]. It is given by,

$$\begin{aligned} I_i^{FV} &= \frac{R_S(t) - R_S(t|R_i(t) = 0)}{R_S(t)} \\ &= \frac{Pr(\phi(\bar{x}) = 1) - Pr(\phi(\bar{x}) = 1 \mid x_i = 0)}{Pr(\phi(\bar{x}) = 1)} \end{aligned} \quad (142)$$

For the multi-state failures grouped according to hazard severity as in the above cases, the modified multi-state FV measure is given as,

$$\begin{aligned} MI_i^{FV} &= \frac{Pr(\phi(\bar{x}) < d) - Pr(\phi(\bar{x}) < d \mid x_i = 0)}{Pr(\phi(\bar{x}) < d)} \\ &= \frac{Pr(\phi(\bar{x}) < d)Pr(x_i = 0) - Pr(\phi(\bar{x}) < d \cap x_i = 0)}{Pr(\phi(\bar{x}) < d)Pr(x_i = 0)} \end{aligned} \quad (143)$$

Eq. 143 puts it into a form where the values can be computed for each component of the T-DEP power system architecture by utilizing the results of the Monte-Carlo simulation carried out for experiment 2.3, just as all the newly defined measures above.

6.1.3.5 Reliability Reduction Worth (RRW)

The last importance measure considered in this thesis is the RRW. It is defined by Levitin et al. [113] as an index measuring the potential damage caused to the system by a particular component. The binary expression for RRW is given as [152],

$$\begin{aligned} I_i^{RRW} &= \frac{R_S(t)}{R_S(t \mid R_i(t) = 0)} \\ &= \frac{Pr(\phi(\bar{x}) = 1)}{Pr(\phi(\bar{x}) = 1 \mid x_i = 0)} \end{aligned} \quad (144)$$

$$= \frac{1}{1 - I_i^{FV}} \quad (145)$$

Since the RRW measure is directly related to the FV measure, its multi-state extension is given as,

$$MI_i^{RRW} = \frac{1}{1 - MI_i^{FV}} \quad (146)$$

6.1.4 Multi-state Component Importance Results

The dataset of one million Monte-Carlo experiments simulated for experiment 2.3 (see Ch. 5.3.3) is analyzed in the present experiment to evaluate the measures defined above. The Criticality Importance (CI) measure normalizes Birnbaum importance (BB) with system and component unreliability values. Therefore, of the two, only CI is reported here. All the results in this section are for the Monte-Carlo simulations generated using the posteriors of Analyst B from Ch. 5.3.3. The results based on Analyst A's posteriors show a similar pattern and are provided in Appendix D. For

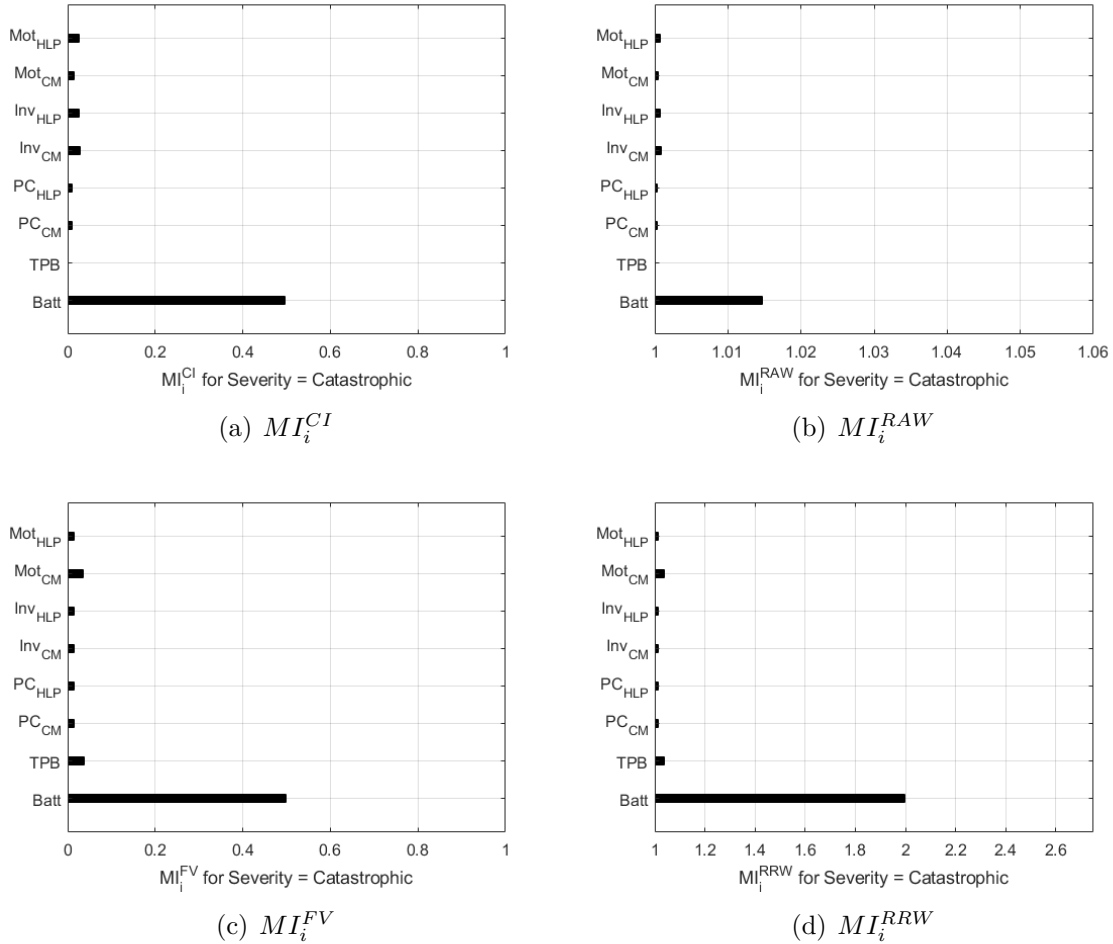


Figure 71: Multi-state importance metrics for Catastrophic failure conditions (Analyst B)

the T-DEP power system architecture (from fig. 33), figure 71 provides results for

multi-state importance measures discussed above for failure states that are classified as catastrophic. It is apparent that the batteries have the highest contribution in terms of all four measures in failure states that are categorized as ‘Catastrophic’. A higher CI measure means that the T-DEP aircraft has a higher chance of entering a catastrophic failure when whenever a battery fails compared to any other component. Similarly, if designers were looking for ways to improve the system reliability when it pertains to catastrophic failures, the RAW measure hints that focusing on the batteries is likely to have the largest impact. Similarly, the FV and RRW measures signify that any decrease in the battery’s reliability is likely to hit the reliability of the T-DEP architecture against Catastrophic failures the hardest compared to any other component.

Figure 72 provides the importance measures for the T-DEP aircraft’s reliability against ‘Hazardous’ failures. Once again, the CI measure indicates that system reliability against a hazardous state is most sensitive to battery reliability. This is verified by the RAW measure which indicates that if the system reliability is to be improved against hazardous failures, designers should focus efforts on improving the battery reliability. The FV – which measures the maximum decrement in system reliability due to a component, when equal to 1, indicates that every single battery failure results in a hazard severity of ‘Hazardous’. This is a confirmation of the results from Ch. 4.4.3. A value of $MI_{batt}^{FV} = 1$ results in an undefined (infinite) value for the RRW measure for the battery. In addition to the battery, it is interesting to note that while the improvement in traction power bus (TPB) or the cruise motor (CM) reliability may not drive the system level reliability from ‘Hazardous’ failures, any reduction these two components’ reliability can lead to a big reduction at the system level.

Figure 73 provides the results of multi-state importance measures for the different failure states from fig. 51 that fall under severity ‘Major’. The CI measure points out

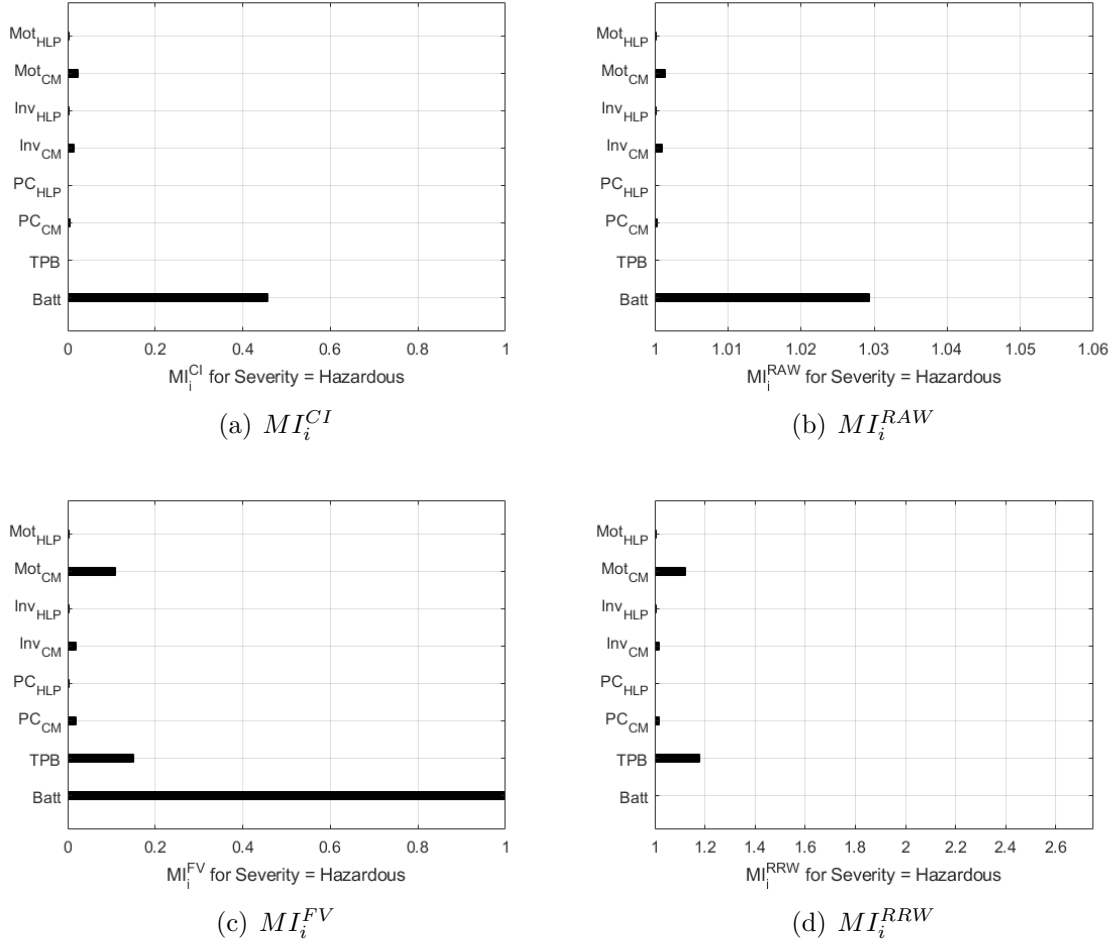


Figure 72: Multi-state importance metrics for Hazardous failure conditions (Analyst B)

that most components except the TPB influence the system level reliability to a similar extent. The RAW measure singles out the cruise motor inverter as the component which can have the greatest impact in improving the aircraft level reliability of the T-DEP architecture against failure states characterized as ‘Major’. While looking at the maximum decrement in aircraft reliability that a component could cause using the FV measure, the CM, TPB, and batteries stand out. That is because a failure in either of these directly leads to a hazard with severity ‘Major’ or worse. Apart from these components, the cruise motor inverter and pre-chargers are identified by the RRW measure as the components that can have the highest negative impact on

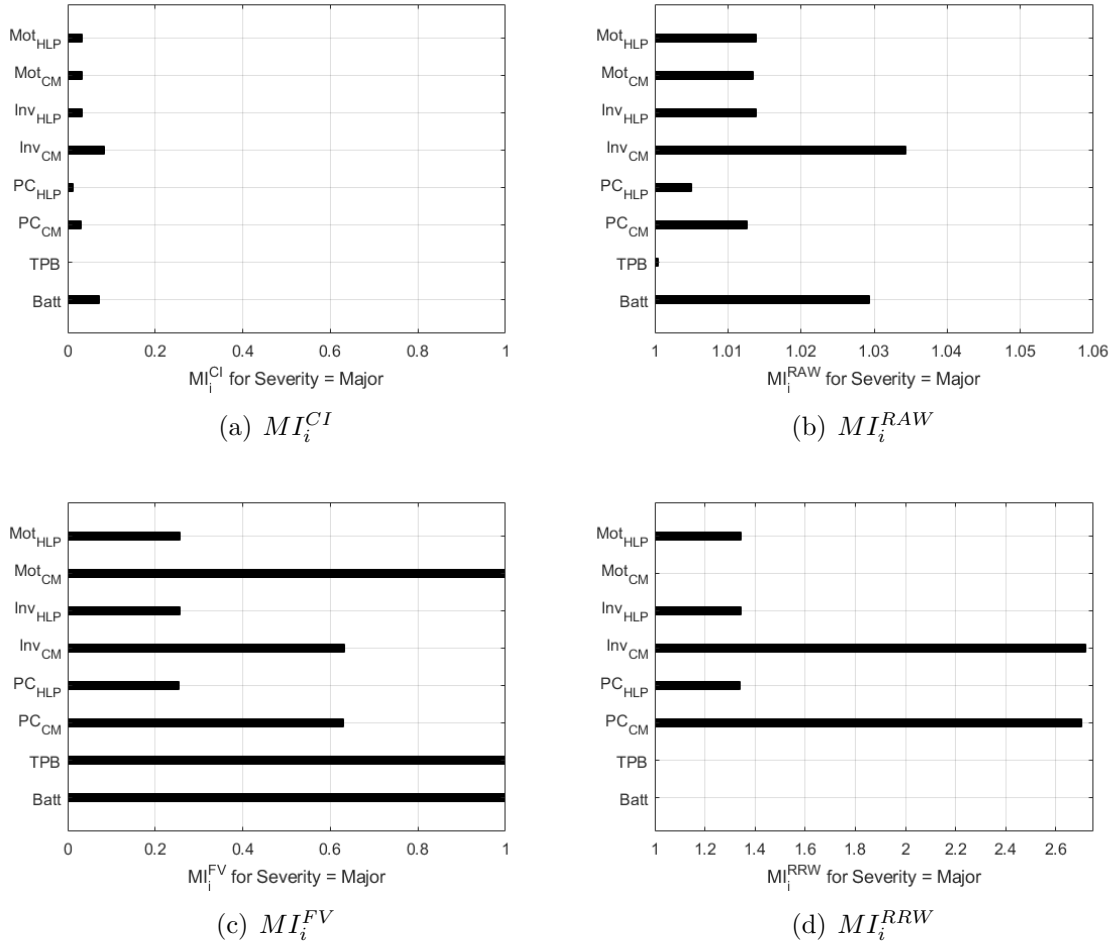


Figure 73: Multi-state importance metrics for Major failure conditions (Analyst B)

T-DEP reliability against ‘Major’ conditions if their component reliability were to drop.

The final set of results in figure 74 provide the T-DEP component importance measures against a failure severity of ‘Minor’. Since most component failures result in a hazard severity of at least ‘Minor’, the T-DEP reliability from this state is not sensitive to the components’ reliability. This is visible in the FV measure as well, where all components have a value of 1 - reaffirming that their failure results in a severity of at least ‘Minor’. The RAW measure however shows that in case this reliability of the T-DEP was to be improved, the focus should be on the high lift motors, their inverters, as well as the cruise motor inverters.

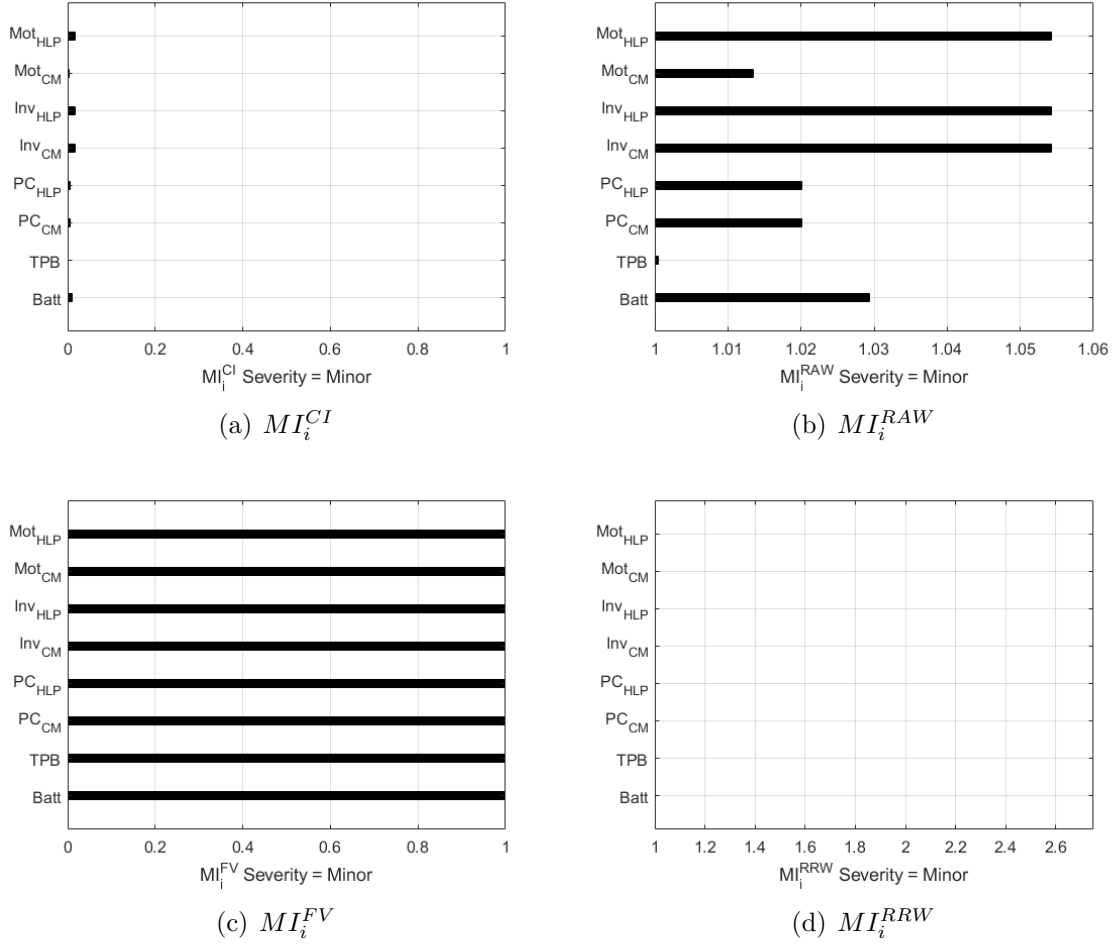


Figure 74: Multi-state importance metrics for Minor failure conditions (Analyst B)

6.1.5 Summary of Experiment 3.1

The intent of this experiment was to evaluate the sensitivity of T-DEP failure states with respect to the reliability of individual components. This can provide a ranking of components with respect to their influence on system reliability, determine top contributors to unreliability, determine the components to focus on to improve system reliability and to perform sensitivity studies. For these end goals, component importance measures were introduced. Since novel architectures are expected to have multiple failure states, extensions to traditional importance measures were developed in the present work to determine the effect of different components on different off-nominal conditions.

Results generated for the T-DEP architecture indicate that the batteries are the most critical component when it pertains to ‘Catastrophic’ or ‘Hazardous’ failures. An improvement or degradation in battery reliability is likely to have a bigger impact on the reliability of the T-DEP aircraft against these hazard severity conditions as compared to any other component. The traction power bus (TPB) and the cruise motors(CM) are the other components that show some influence on the T-DEP reliability from ‘Hazardous’ severity.

For ‘Major’ conditions, the cruise inverters and batteries were shown to have the highest impact in terms of improving the system reliability. Therefore, any decision makers wanted to improve reliability for the ‘major’ hazards must consider these two components first. The RRW metric gives the maximum damage that can be caused by a component failure. Since the loss of a Battery, TPB, or a CM leads to a ‘hazardous’ state, these components are evidently most important. Apart from these, the cruise inverter and pre-charger were found to affect the system unreliability the most for the ‘Major’ failure severity.

Finally, since any single component failure causes a ‘Minor’ severity, the FV measure for these are all 1, and the RRW measures are undefined. In order to improve the reliability of the system from ‘Minor’ failures, the high lift cruise motors, their inverters, and the cruise motor inverters were found to yield the most improvement. That is these components may be focused upon to improve system reliability in a ‘Minor’ failure state.

Overall, this experiment successfully identified the component driving the reliability of the T-DEP architecture in different failure severity states. It provided the sensitivity of the system reliability with respect to that of components while also providing evidence of how such information can be used to improve aircraft components and system reliability. This completed the purpose of experiment 3.1.

6.2 Trade-studies

Two trade studies conducted in this thesis are motivated by results from asymmetrical loss of thrust scenarios from experiment 1.2 (see ch. 4.3.5). In particular, recall discussion related to tables 18 and 19. For the case when there is a complete loss of one cruise motor in table 18, the remaining cruise motor is set at 64% throttle while descending at a gradient of -4.84%. The reason the remaining cruise motor cannot be operated at its maximum continuous power (90% throttle) is due to a lack of lateral stabilizing force from the vertical tail (VT) to trim the T-DEP architecture. The ERM metric for this case is -1.83, indicating that not only is this off-nominal condition limited by lateral control authority (determined from the throttle), but also by the maximum thrust available even if the remaining cruise motor were to be operated at maximum continuous power. Now consider the takeoff asymmetric loss of thrust results from table 19. Most states evaluated show some degree of limitation due to a lack of VT's lateral control authority. This is evident by looking at the ERM metric (defined in Ch. 4.2), which considers the specific power utilized in the trim solution with maximum γ , to the specific excess power available in the failed state. The values of the ERM metric are all less than 1, with the right engine throttle not set to 90% maximum continuous power setting. This indicates a limitation due to a lack of VT authority. This is particularly important in cases of losing half a cruise motor and 5 or 6 high lift propulsors on the same side. Such failed states can only be trimmed at a negative climb gradient with a negative ERM metric, indicating that there is sufficient excess power available to climb, but it cannot be used since the aircraft cannot be trimmed at those.

The above discussion inspires the two trade studies performed in this thesis. For the first, designers might ask the question, “*But what if we were to resize the VT?*”. That trade study is the focus of the next experiment. The second trade study considers a larger resized VT along with boosted cruise inverters that can supply additional

power in case the other cruise inverter fails, thus maintaining additional thrust on the partially failed cruise motor.

6.2.1 Experiment 3.2 - Resized Vertical Tail (VT)

Experiment 3.2 is intended to test whether resizing the vertical tail (VT) is likely to result in better safety outcomes for asymmetric loss of thrust scenarios measured by the maximum climb gradient attainable under trim, and an improved ERM metric. In particular, the VT is resized to consider a 10% larger chord as well as span dimensions resulting in a 21% increase in VT area as seen in table 31. In this trade-study, the rest of the aircraft parameters are assumed constant. The result of the VT resizing is considered in terms of updated mass properties and lateral aerodynamic coefficients. The updated aerodynamic coefficients are generated using AVL [62] and are provided in table 32.

Table 31: T-DEP aircraft resized VT geometry

Parameter	Value	Unit
Planform area- S_{vt}	2.36	m ²
Span- b_{vt}	1.78	m
Reference chord- c_{vt}	1.58	m
Leading edge sweep	37.45	deg

Table 32: Estimated lateral aerodynamic coefficients of the T-DEP with resized VT

	β	\hat{p}	\hat{r}	δ_a	δ_r
C_Y	-1.2937	-0.0729	1.1459	0.0427	0.3939
C_n	0.3865	0.0688	-0.4976	0.0309	-0.1969
C_l	-0.0275	-0.6628	0.2275	0.1650	0.0163

The asymmetric thrust loss cases of tables 18 and 19 are re-evaluated for the present experiment with the updated parameters. The expected results include improvement to the γ_{max} and ERM metrics for cases where the remaining cruise motor was throttled to less than maximum continuous power.

6.2.2 Results - Resizing the VT

Table 33 provides the 6-DoF trim analysis results for the T-DEP aircraft under asymmetric thrust loss conditions during cruise. This table is read in a similar fashion to table 18. The column ‘CM-1 Loss %’ gives the ratio of thrust loss on the left cruise motor – 0 denotes nominal operation, 0.5 denotes 50% thrust loss, while 1 denotes complete loss. The angles γ_{max} , θ , ψ , as well as the control deflections δ_a , δ_r are in degrees. τ denotes the throttle setting on the left and right cruise motors. At nominal conditions, the T-DEP can climb at an angle of 1.17° , which is just over a 2% gradient (in agreement with conceptual analysis from Fig 47). The second row of table 33 denotes cruise motor-1 (left) at 50% thrust (64% throttle). As is visible, the T-DEP cannot maintain steady level flight if half the thrust is lost in any one of the wingtip cruise motors. For a complete loss of thrust from the left wingtip cruise motor, the trim solution provided a maximum climb gradient of -4.18%.

Table 33: Resized VT: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)

CM-1 Loss %	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0	2.04	7.7	0	0	0	0.9	0.9	0.97
0.5	-0.31	6.38	-3.66	1.09	-11.26	0.64	0.9	-1.32
1	-4.23	4.18	-5	1.49	-15.39	0	0.74	-1.6

While nominally this might indicate no difference due to increasing the VT span and chord by 10% each, table 34 provides the change in the maximum climb gradient and ERM between the two cases. It shows that increasing the VT size results in no change in the nominal performance as well as the performance under 50% thrust loss in the left cruise motor. This is expected since these cases were not constrained by the lateral stability considerations in table 18. The last case pertaining to a complete loss of thrust shows an absolute improvement of 0.61% in the climb gradient and 0.23 in ERM. Thus, increasing the VT size results in the T-DEP aircraft improving its

maximum potential climb gradient under the loss of a cruise motor in cruise, along with an absolute improvement in excess power utilization of over 23%.

Table 34: Resized VT: $\Delta \tan(\gamma_{max})$ (%) and Δ ERM under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)

CM-1 Loss %	$\Delta \tan(\gamma_{max})$ (%)	Δ ERM
0	0	0
0.5	0	0.01
1	0.61	0.23

Next, the results of asymmetric thrust loss right after takeoff for the larger VT are compared to results obtained earlier in table 19. Under nominal conditions, the T-DEP manages an MPCG of 9.95% (5.68°) at 1.2x stall speed, same as before. Once again, a cursory visual inspection may not yield much difference between the results of tables 35 and 19. The hazard severity does not change much for the different states considered.

However, tables 36 and 37 provide the difference between these two in terms of their maximum potential climb gradient (MPCG) and ERM metrics. The larger VT results in an absolute increase in MPCG of approximately 0.23%, with ERM improving by about 4-5% in absolute terms. This means that the T-DEP architecture can now utilize an additional 4-5% of its maximum excess power while trimming the aircraft as compared to earlier. While the gains may not be much or may not change hazard severity, they confirm that some of the asymmetric failure states discussed earlier for the T-DEP aircraft are limited by the VT’s lateral control authority. Increasing the VT span and chord does not change the nominal performance, it improves the aircraft’s response to off-nominal failures. This trade study is provided as an example to demonstrate that the framework presented in this thesis can be utilized to conduct numerous such trade studies in order to improve novel aircraft’s design and performance to deal with off-nominal operational considerations.

Table 35: Resized VT: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

CM-1 Loss %	# HLP Failed	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0	0	9.95	6.1	0	0	0	0.9	0.9	1
0	1	9.15	6.21	-4.8	0.39	-12.2	0.9	0.9	0.99
0	2	7.78	6.02	-4.93	0.46	-12.61	0.9	0.84	0.92
0	3	6.50	5.92	-4.9	0.51	-12.6	0.9	0.79	0.85
0	4	5.35	5.91	-4.96	0.58	-12.83	0.9	0.75	0.78
0	5	4.3	6	-4.98	0.64	-12.96	0.9	0.72	0.7
0	6	3.35	6.19	-4.95	0.71	-12.93	0.9	0.7	0.63
0.5	0	5.77	3.78	-4.92	0.35	-12.42	0.64	0.73	0.77
0.5	1	4.28	3.5	-4.93	0.4	-12.51	0.64	0.64	0.64
0.5	2	2.9	3.3	-4.9	0.44	-12.5	0.64	0.55	0.49
0.5	3	1.64	3.21	-4.96	0.51	-12.75	0.64	0.48	0.31
0.5	4	0.49	3.2	-4.99	0.57	-12.89	0.64	0.4	0.11
0.5	5	-0.56	3.3	-5	0.64	-12.98	0.64	0.34	-0.15
0.5	6	-1.50	3.49	-5	0.71	-13.04	0.64	0.3	-0.52
1	0	0.82	0.98	-4.99	0.34	-12.59	0	0.35	0.16
1	1-6	No Trim Solutions							

Table 36: Resized VT: $\Delta \tan(\gamma_{max})$ (%) under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

CM-1 Loss %	$\Delta \tan(\gamma_{max})$ (%)							
# HLP Failed →	0	1	2	3	4	5	6	
0	0.00	0.21	0.23	0.25	0.26	0.24	0.24	
0.5	0.21	0.23	0.23	0.23	0.24	0.24	0.24	
1	0.23	No Trim Solution						

Table 37: Resized VT: Δ ERM under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

CM-1 Loss %	Δ ERM							
# HLP Failed →	0	1	2	3	4	5	6	
0	0	0.02	0.02	0.03	0.04	0.04	0.05	
0.5	0.03	0.04	0.04	0.04	0.06	0.07	0.09	
1	0.04	No Trim Solution						

6.2.3 Summary of Experiment 3.2

The present experiment was designed as a way to test the capability of the developed framework to incorporate safety related off-nominal requirements and reliability into design trade studies. It was observed from the results of experiment 1.2 (see Ch. 4.3.5) provided in tables 18, 19 that the T-DEP aircraft's performance under certain asymmetric thrust loss scenarios was restricted by the lateral control authority available from the VT. This is visible from the ERM metric being less than 1 indicating not all specific excess power is being utilized in improving the maximum potential climb gradient (MPCG) due to a trim penalty. This is the case for most scenarios considered during takeoff, and for the complete loss of cruise motor scenario considered in cruise.

To test whether this is really the case, the vertical tail was resized in this experiment to increase its span and chord by 10% each (21% increase in area). The impact of this change was assumed in terms of increased VT mass (therefore moments of inertia), and the lateral stability and control derivatives of the T-DEP aircraft obtained from AVL [62], as provided in table 32.

Re-evaluating the asymmetric loss of thrust scenarios from experiment 1.2 provided an absolute improvement of about 0.24 to the MPGC (in %) and 5% increase in ERM in takeoff configuration. In the cruise configuration, increasing VT size does not seem to affect the case where half thrust is lost by one cruise motor. This was expected since the discussion around table 19 mentioned that this failure is limited by the thrust available post failure, and not by the VT's lateral control authority. This is also visible given the right engine throttle is set at maximum continuous (0.9) after failure. However, in the case of a complete loss of one cruise motor, the solution was determined to be limited by VT size due to the remaining motor being throttled at less than maximum continuous power. The resized VT resulted in an improvement of 0.61 MPCG (in %) and 23% in ERM metric, in this case, confirming the earlier

observation.

Overall, this experiment successfully demonstrated that the present framework provides meaningful inputs regarding off-nominal considerations that may be skipped in traditional conceptual or preliminary design stages. It also demonstrated how the framework can be utilized in informing decision makers with safety related off-nominal requirements while conducting design trade studies, a capability not available under the traditional safety assessment paradigm.

6.2.4 Experiment 3.3 - Resized VT + Oversized Cruise Inverters

While resizing the VT in experiment 3.2 provided improvements in the maximum potential climb gradient and ERM metrics for asymmetric thrust loss cases that were limited by VT's lateral control authority, it did not make a significant difference to the hazard severity. Additionally, certain scenarios like losing partial thrust in one cruise motor during cruise were found to have no improvement because they are thrust limited.

To verify these potential insights about the T-DEP architecture, the present experiment evaluates the impact of oversizing the cruise motor-inverters. Previously, it was assumed that post failure of one cruise motor-inverter/pre-charger, the remaining subsystem (see fig. 33) provided enough power to system 50% thrust on the degraded cruise motor. This assumption is modified in the present experiment to oversize the cruise motor-inverters to operate in a boosted mode if the other one fails, enabling the degraded cruise motor to generate 67% thrust instead of the previous 50%. This oversizing is performed on top of the resized VT from experiment 3.2 to obtain the cumulative impacts of the two design changes. The throttle setting translates to thrust using equation 27, where it can be seen that thrust is proportional to the square of the throttle setting. Maximum continuous power is modeled as 90% throttle setting to represent 90% RPM (2250 RPM) of the cruise motor. Thus, 67% of maximum

continuous power occurs at $90\% * \sqrt{2/3} = 73.5\%$ throttle setting.

6.2.5 Results - Resizing the VT + Cruise Inverters

The results of table 38 are contrasted against the results of partial cruise motor thrust loss from table 35 in experiment 3.2, and against table 19 in experiment 1.2. The first observation of note is that none of the seven off-nominal scenarios that result in partial thrust loss in a cruise motor along with zero to six high lift motors on the same side of the wing are now ‘Catastrophic’ in hazard severity because the resized T-DEP architecture is able to ensure a positive climb gradient at sea level for each case. Similarly, the case where the partial loss of a cruise motor and 3 HLPs on the same side was assigned a severity of ‘Hazardous’ earlier (see fig. 54), it is now afforded a severity of ‘Major’ because the resized T-DEP can trim at a climb gradient of above 3%. Revisiting the reliability requirements generated from figure 66, the modified requirements eliminate catastrophic failures from partial loss of a cruise motor, and lower the hazard severity when that occurs in conjunction with 3 HLP failures on the same side.

Table 38: Larger VT + CM-Inv: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

CM-1 Loss %	# HLP Failed	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0.33	0	7.36	4.67	-4.96	0.35	-12.52	0.735	0.814	0.89
0.33	1	5.87	4.39	-4.96	0.4	-12.6	0.735	0.736	0.78
0.33	2	4.49	4.19	-4.94	0.45	-12.61	0.735	0.663	0.66
0.33	3	3.23	4.09	-5	0.51	-12.85	0.735	0.598	0.54
0.33	4	2.06	4.08	-4.94	0.57	-12.77	0.735	0.54	0.39
0.33	5	1.01	4.18	-4.93	0.63	-12.81	0.735	0.497	0.22
0.33	6	0.07	4.37	-4.93	0.71	-12.88	0.735	0.47	0.02

The updated multi-state failure rate requirements are given in figure 75, and show the changes to a partial loss of thrust (33% thrust loss as against 50%). Catastrophic hazards have been eliminated from this row, while the case with partial cruise motor

No. HLP failed	0	1	2	3	4	5	6
CM-1 Loss %							
0		<10 ⁻³	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵
0.33	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁵	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶	<10 ⁻⁶
1	<10 ⁻⁶	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷	<10 ⁻⁷

Figure 75: Resized VT + Oversized Cruise Inverters: T-DEP asymmetric multi-state λ_{req} in takeoff configuration. Colored by asymmetric thrust loss hazard severity from Fig. 54

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6
0		7.41E-05	1.66E-05	2.43E-06	2.34E-07	1.12E-08	4.00E-10
0.33	1.77E-05	9.91E-06	2.90E-06	8.33E-07	1.55E-07	1.36E-08	1.20E-09
1	3.68E-06	2.12E-06	6.09E-07	1.46E-07	2.40E-08	2.00E-09	4.00E-10

(a) Analyst A

No. HLP failed -> No. CM failed	0	1	2	3	4	5	6
0		7.66E-05	1.38E-05	1.50E-06	1.08E-07	2.40E-09	4.00E-10
0.33	2.01E-05	9.22E-06	2.04E-06	3.56E-07	4.84E-08	2.80E-09	<1E-10
1	2.73E-06	1.25E-06	2.60E-07	4.48E-08	4.40E-09	4.00E-10	<1E-10

(b) Analyst B

Figure 76: Resized VT + Oversized Cruise Inverters: Asymmetric loss of thrust – multi-state failure rates for the two Bayesian analysts for takeoff. Colored by compliance finding

thrust loss and two HLP failed is now rated ‘Major’ instead of ‘Hazardous’. As a result, the multi-state compliance finding results change from figure 69 to figure 76. In particular, the failure state with partial loss of cruise motor along with two HLP on the same side is now compliant with reliability requirements given by Fig. 75. Table 39 shows the improvement of the suggested cruise inverter oversizing + VT resizing over just the VT resizing results from experiment 3.2 in table 35. The oversizing of the inverter results in an improvement of trim MPCG metric of about 1.6% in absolute terms for the partial loss of cruise motor case. The ERM metric improves by 12

to 54% over just the VT resizing case. This indicates that any cruise motor failure induces a large yawing moment that cannot be neutralized by simply oversizing the vertical tail, but requires improving the cruise motors' functional (thrust) availability to improve the safety outcomes.

Table 39: Larger VT + CM-Inv: Δ ERM and $\Delta \tan(\gamma_{max})$ (%) under asymmetric loss of thrust scenarios at takeoff ($\phi = 0$, $h = 50ft$, $V_\infty = 70$ knots, flaps – takeoff)

# HLP Failed \rightarrow	CM-1 33 % Loss						
	0	1	2	3	4	5	6
Δ ERM	0.12	0.14	0.17	0.23	0.28	0.37	0.54
$\Delta \tan(\gamma_{max})$ (%)	1.60	1.59	1.59	1.59	1.57	1.57	1.57

Table 40: Larger VT + CM-Inv: Trim solutions maximizing γ under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)

CM-1 Loss %	$\tan(\gamma_{max})$ (%)	θ	ψ	δ_a	δ_r	τ_L	τ_R	ERM
0.33	0.45	6.81	-2.46	0.73	-7.58	0.735	0.9	0.87

Table 41: Larger VT + CM-Inv: $\Delta \tan(\gamma_{max})$ (%) and Δ ERM under asymmetric loss of thrust scenarios at cruise ($\phi = 0$, $h = 1500ft$, $V_\infty = 105$ knots, flaps – retracted)

CM-1 Loss %	$\Delta \tan(\gamma_{max})$ (%)	Δ ERM
0.33	0.77	2.19

Table 40 provides the results for partial loss of thrust in one cruise motor in the low speed limits of cruise configuration. Oversizing the cruise inverter along with VT resizing results in a positive maximum potential climb gradient (MPCG) metric as against previous results of just resizing the VT in table 33, or the baseline T-DEP in table 18. However, this does not result in a reduction of hazard severity for this case (previously categorized ‘Major’). Therefore, the compliance finding, that found a partial loss of thrust in cruise ‘non-compliant’ (see fig. 68) remains

unchanged. This indicates that the only way to improve the compliance of this failure state is to improve the reliability of components that contribute to it, or by re-architecting the power systems architecture from fig. 33. However, that is not to say that oversized cruise inverter does not have an effect – to the contrary, it results in a large absolute increase of MPCG of 0.77%, with a jump in ERM from a negative value of less than -1 (indicates thrust limited failure condition) to a positive value of 0.87, a jump of 2.19! This indicates that this one change will enable the T-DEP architecture to utilize as much as 87% of its specific excess power towards maximizing its climb gradient while trimmed. Once again, this experiment demonstrates that the developed framework enables trade studies to evaluate a novel aircraft architecture’s off-nominal performance and safety compliance under different design decisions.

6.2.6 Summary of Experiment 3.3

The present experiment was designed to follow up the results of experiment 3.2 in testing the capability of the developed framework to incorporate safety related off-nominal requirements and reliability into design trade studies for novel aircraft architectures. Results of experiment 3.2 demonstrated benefits in cases where the T-DEP aircraft’s performance under asymmetric thrust loss conditions was limited by the vertical tail’s (VT) lateral control authority. However, certain failure conditions – notably those with $ERM < -1$ from table 18, were postulated to be thrust limited under failure.

To test these, the cruise motor (CM) inverters were oversized in the present experiment to provide 67% thrust (instead of 50%) when a CM faces a partial loss of thrust, in addition to the benefits of increasing the VT size from experiment 3.2. Re-evaluating the asymmetric loss of thrust cases from with one CM providing partial thrust in takeoff configuration from tables 35 provided an improvement in the ERM metric of 12 to 54% in magnitude, while the MPCG metric showed improvements of

about 1.57% or more in magnitude. This changed the hazard severity assigned to these failure states to eliminate catastrophic hazards altogether. The failure state with one cruise motor under partial failure, with two high lift propulsors (HLPs) lost on the same side was found to be compliant with the failure rate requirements as a result.

In the cruise configuration, improvements over table 33 showed that the T-DEP aircraft can manage a positive 0.45% climb gradient under a partial loss of a cruise motor, as against a negative 0.31 earlier. This is an improvement of 0.77% magnitude of MPCG, while the ERM metric improved to 0.87 from a value of -1.32 earlier. This confirmed that the partial loss of thrust in cruise condition is thrust-limited and not limited by the VT's lateral control authority for the T-DEP aircraft.

Overall, experiment 3.3 followed up the results of 3.2 to once again successfully demonstrate the capability of the developed framework in generating meaningful inputs regarding off-nominal requirements that may be skipped in traditional conceptual or preliminary design stages. It enables decision makers to incorporate safety related off-nominal considerations while conducting trade studies in early design phases, a capability not afforded by the traditional safety assessment paradigm.

6.3 Chapter Summary

The third research question (RQ 3) was motivated by observations group 3 from chapter 2.5. This group primarily noted that traditional methods used to conduct safety assessments of novel aircraft concepts limit the scope for exploration and trade studies in preliminary design stages. It also noted that optimizing for nominal considerations could worsen performance under off-nominal conditions. Therefore, the goal of RQ 3 was to enable design trade studies for novel aircraft architectures while incorporating safety related off-nominal considerations. To that end, hypothesis 3 proposed that the integrated framework (see fig. 70) developed in this thesis serves as an enabler

for conducting trade studies informed by safety related off-nominal requirements and reliability of novel aircraft architectures in early design.

The chapter then took a two-pronged approach to verify hypothesis 3. For the first experiment, sensitivities of system multi-state reliability to component failure rate posteriors was established through unit level importance metrics. In a multi-state failure scenario, the component importance metrics were re-defined to incorporate the reliability of the system from a given hazard state. For instance, reliability from ‘Hazardous’ failures was defined as the likelihood of the system ending up in a state that is less severe than ‘Hazardous’, and so on. These multi-state importance metrics were evaluated for the ‘Minor’, ‘Major’, ‘Hazardous’, and ‘Catastrophic’ off-nominal hazard severity scenarios. The batteries were found to have the highest contribution in terms of criticality index (CI), reliability achievement worth (RAW), and reliability reduction worth (RRW) for ‘Catastrophic’ and ‘Hazardous’ failure states. The traction power buses (TPBs), and cruise motors (CMs) were found to have the next highest risk reduction worth for ‘Hazardous’ failures, meaning any decrease in their reliability would affect the system’s reliability from that severity to the greatest extent. For multi-state failures from experiment 1.2 classified as ‘Major’, the cruise motor inverters are the ones that can provide the highest improvement in the system reliability if they are improved. For the risk reduction worth, the cruise inverters and pre-chargers were found to be the most important, hinting at great loss of system level reliability from ‘Major’ hazards if their component reliability was to decrease. In the present dissertation, most single component failures result in at least a ‘Minor’ severity. As a result, the Fussell Vesely (FV) measure gives a value of 1 for all components for this severity class, while the RRW measure is undefined. The RAW measure provides important insights nevertheless. The high lift motors, their inverters, and the cruise inverters were found to promise the maximum system reliability improvement if the component reliability of these components were improved.

The second part of this chapter focused on revisiting some aircraft design and architecting assumptions to improve the system response to off-nominal failure states. In particular, the asymmetric loss of thrust from experiment 1.2 had demonstrated that the T-DEP architecture was limited by the lateral control authority of the vertical tail (VT) in some off-nominal cases, as well as by the thrust available in some cases. To verify these results and demonstrate the capability of the developed framework to conduct design trade-studies, two experiments were proposed. Experiment 3.2 resized the T-DEP aircraft's VT to increase the chord and span by 10% each. The impact of this resizing was considered by modifying the aircraft's mass properties and lateral aerodynamic derivatives. Upon evaluating the asymmetric loss of thrust cases, it was seen that a larger VT results in improvements in the maximum potential climb gradient metric (MPCG) of about 0.24% during takeoff and 0.64% during cruise with one CM lost. The improvement in energy rate margin (ERM) that denotes the percentage of specific excess power after failure that can be utilized for maximizing the climb gradient was found to be around 5% for takeoff, and 23% for cruise. The cases which were thrust limited (partial loss of a CM) showed no improvement as expected.

The last experiment of this thesis considered the resized VT along with oversized CM inverters. The new CM inverters allow the CMs to generate 67% thrust under partial failures which may result from loss of one CM inverter or pre-charger for instance. Such a modified T-DEP architecture now afforded a larger VT as well as greater thrust capability under partial CM failures. The results of experiment 3.3 showed significant improvements in takeoff and cruise MPCG under partial loss of CMs. The takeoff MPCG improved by about 1.6% absolute value, while ERM improved by about 12-54%. In the cruise condition, MPCG improved by 0.77%, while ERM went from -1.32 to 0.87! As a result, the T-DEP aircraft could now maintain a positive climb gradient under any combination of partial loss of a cruise motor and

HLP failures on the same side during takeoff, removing any ‘Catastrophic’ conditions from these failure states. The resultant change in reliability requirements meant that a failure state with partial loss of thrust in one CM, with 2 HLPs on the same side lost was deemed compliant, as compared to non-compliant earlier.

Overall, experiments 3.2 and 3.3 demonstrated two design and architecting trade-studies using the T-DEP aircraft that were enabled by the framework developed in this thesis. The framework enables trade-studies like these to be conducted for novel aircraft architectures while incorporating safety related off-nominal requirements in early design phases. Along with the importance metrics of experiment 3.1, these three experiments help verify hypothesis 3.

CHAPTER VII

CONCLUDING REMARKS

The world of aviation is moving towards revolutionary novel aircraft architectures and technologies as a result of a push towards higher efficiencies, lower operating costs, and lower emissions. This paradigm shift towards novel aircraft architectures and technologies is necessitated as the current concepts reach technological saturation. Efforts to develop such concepts are ongoing in the transport category (14 CFR Part 25) aircraft in terms of hybrid-electric or all-electric architectures. In the normal category (14 CFR Part 23) which form the bulk of General Aviation (GA) operations, these efforts are more pronounced with novel concepts of operation like Urban/Advanced Air Mobility (UAM/AAM), architectures such as electric vertical take-off and landing (e-VTOL), and technologies such as distributed electric propulsion (DEP) being developed by various entities.

While these novel concepts and architectures are required to achieve aggressive targets in fuel efficiency and emissions, their development and implementation face obstacles in terms of uncertainty regarding the reliability and safety risk they pose. The limitations and off-nominal operational considerations generally postulated during traditional safety analysis may not be complete or correct for new concepts. Even when Original Equipment Manufacturers (OEMs) have preferred to take a cautious approach by introducing new technologies in a step-wise manner in aircraft, recent incidents have reiterated the need to do so in a safe manner. This need is felt even more strongly in the case of revolutionary designs that are likely to be introduced in GA. In order to speed up the process of introduction of novel aircraft architectures and technologies, it is paramount for aircraft designers to have the capability

to quantify off-nominal requirements earlier in the design phases in a manner that (i) provides a better treatment of uncertainty in light of limited knowledge and experience with these concepts, and (ii) informs trade studies before degrees of freedom are locked down by design decisions. These observations provided a high-level rationale to motivate the overall research objective of this thesis:

Research Objective:

Develop a framework that will enhance safety assessments of novel aircraft physical architectures and technologies in early design by

1. identifying off-nominal requirements,
2. allocating them to the system and component level,
3. enabling compliance decision-making while addressing both epistemic and aleatory uncertainties, and
4. informing design trade-studies.

A novel aircraft architecture was defined loosely in this dissertation (see def. 2.1.1.1) as one which differs significantly from the traditional paradigm in its physical implementation to fulfil at least one aircraft level function. A thorough literature survey of the current paradigm and the state-of-the-art (SotA) resulted in three groups of observations. The first group focused on characterizing the safety related off-nominal requirements for novel aircraft architectures. The second group focused on the (incomplete) treatment of uncertainty in available data and models when they pertain to failure rates and reliability of novel aircraft architectures and technologies. Finally, observation group 3 focused on how incorporating safety requirements into early design for novel aircraft architectures is a challenge that does not have a solution in

traditional methods.

The three observation groups informed the three broad research areas of this thesis. The overall research formulation of this thesis is provided in figure 77. It provides a top level summary of each research question, the hypotheses stated, sub-research questions and their hypotheses where they have been stated, and the experiments conducted to verify them. A detailed summary of each research area is reproduced here from the respective chapter summaries for convenience.

7.1 Detailed Summary of Findings

7.1.1 Research Area 1: Identification, characterization, and allocation of safety related off-nominal requirements

Chapter 4 was motivated by the first group of observations from Ch. 2.5 that led to the formulation of a set of research questions and hypotheses for the first research area. In particular, it focused on identifying a set of methods that allow identification, characterization, and allocation of safety related off-nominal requirements. Towards that goal, literature was found to converge around utilizing performance-based methods to quantify off-nominal system response to be used as a surrogate for hazard severity. Two methods, in particular, an extension to Continuous Functional Hazard Assessment (C-FHA), and Performance-based Multi-state Analysis were down-selected and tailored for use with novel aircraft architectures at the conceptual and preliminary level of design.

The safety metrics necessary for quantifying off-nominal operational states of the aircraft formed the first research sub-question (RQ 1.1) which was answered using a focused literature review. While there is no one-size-fits-all solution for finding appropriate safety metrics to use for every novel architecture, a set of metrics useful for the Test Distributed Electric Propulsion aircraft (T-DEP) inspired by the X-57 were identified in table 3.

The next research sub-question (RQ 1.2) focused on estimating these metrics

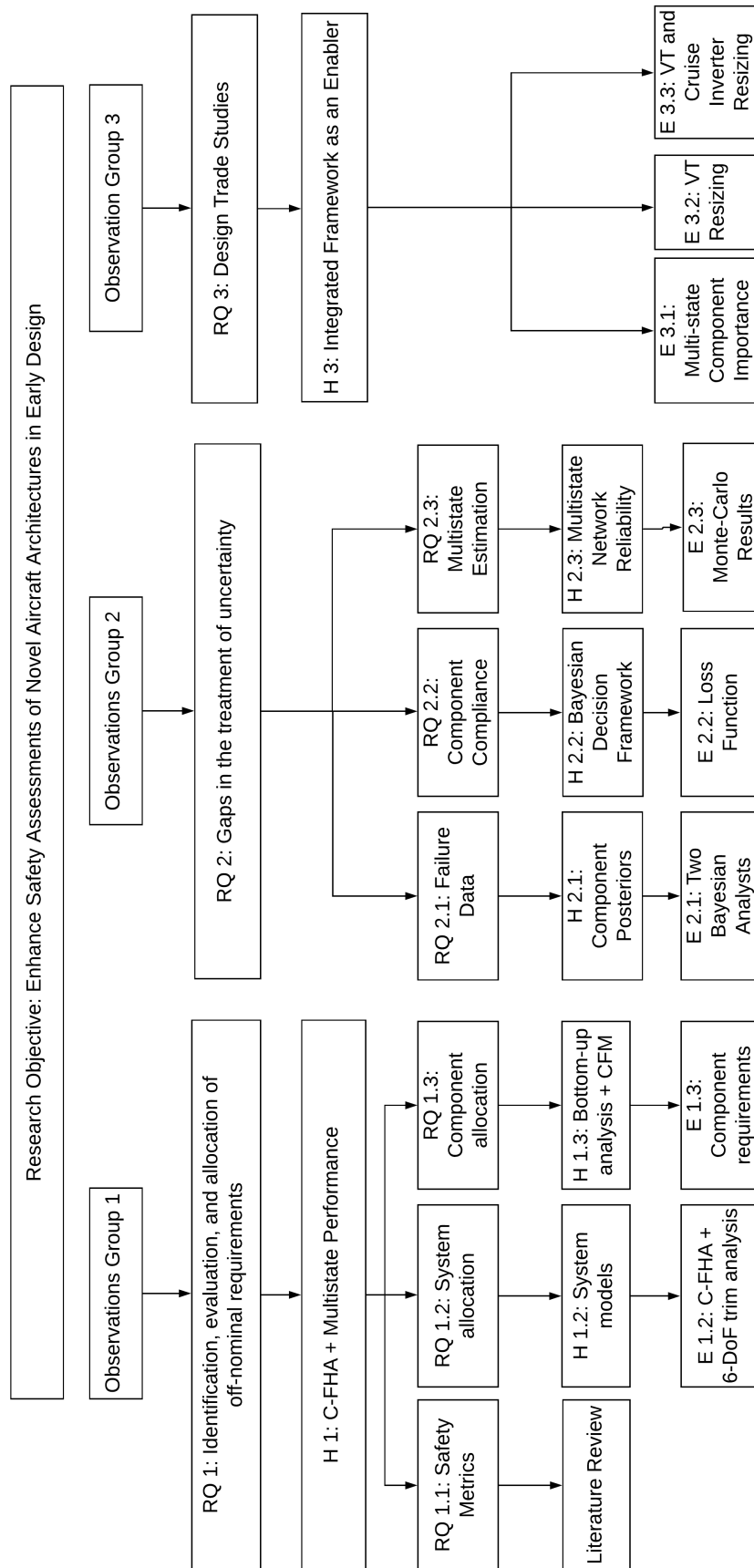


Figure 77: Overview of the Research Formulation

by developing suitable conceptual and preliminary 6-DoF models that can simulate the aircraft's response to thrust degradation scenarios. Thresholds for these metrics were set based on certification considerations or engineering judgement. Experiment 1.2 compared the hazard severity requirements obtained using Continuous-FHA (C-FHA) and performance based multi-state analysis with those obtained from literature sources resorting to traditional analyses. It demonstrated a clear benefit of utilizing the proposed methods in terms of improved resolution of hazards. It also provided results based on physics based models instead of relying on heuristics, while allowing the designers to update their results once higher fidelity models are available. Some additional insights regarding the T-DEP architecture include the fact that certain thrust loss hazards were not due to insufficient thrust after a failure, but due to insufficient lateral stability provided by the vertical tail.

Finally, the third research sub-question dealt with allocating the requirements generated at the aircraft level to the components. A network-based bottom-up analysis algorithm was developed to identify the impact of component failures on the aircraft level functional availability and failure states. It was assumed that in an aerospace application, the probability of two components failing at once during a flight is small enough to be neglected, therefore allowing single failure considerations to drive the reliability allocation problem. Finally, the Critical Flow Method was demonstrated to allocate reliability to components of a subsystem that cannot be dealt with using simple considerations of redundancy. Experiment 1.3 demonstrated that by using the above mentioned methods, allowable failure rate requirements can be allocated to the unit level from the system level, thus verifying hypothesis 1.3.

Taken together, the three sub-hypothesis and the techniques used to verify them were found to satisfy all the requirements posed by research question 1. This verified the solution proposed by hypothesis 1, and completed the discussion on research area 1.

7.1.2 Research Area 2: Gaps in the treatment of uncertainty in failure rates

Chapter 5 dealt with the second research area from research formulation. The second research question (RQ 2) was motivated by observations group 2 from Ch. 2.5. With the characterization and unit level allocation of safety related off-nominal requirements completed in Ch. 3.2, the next logical step was to evaluate the system level and unit level reliability. To that end goal, the overall intent of RQ 2 was to provide a better treatment of uncertainty in the reliability estimations of novel aircraft architectures at the system and component level. RQ 2 was further divided into three research sub-questions – (i) RQ 2.1 that dealt with component level reliability assessment; (ii) RQ 2.2 that dealt with component compliance decision making; and (iii) Multi-state system level reliability assessment.

One hypothesis was stated for each research sub-question above. Hypothesis 2.1 (H-2.1) recommended a Bayesian probability framework for failure rate estimation of the novel components while providing better treatment of uncertainty. The metrics used to define ‘better’ in this instance were the 6-levels of treatment of uncertainty by Paté-Cornell [146]. For experiment 2.1 (E-2.1), a benchmark approach considers point estimates (mean) for component failure rates. Two Bayesian analysts A, B were imagined providing two different prior distributions to encode disciplinary knowledge as epistemic uncertainty. The resulting distributions were found to represent a level 5 treatment of uncertainty, better than the level 3 afforded by the benchmark, thus verifying H-2.1.

Hypothesis 2.2 (H-2.2) suggested that minimizing the posterior expected loss would provide an uncertainty-informed compliance decision for the novel aircraft architecture components. In verifying H-2.2, experiment 2.2 considered a benchmark method of compliance testing where the point failure rate estimates generated in E-2.1 are compared to failure rate requirements generated in Ch. 4.4.4. A Bayesian

decision framework was developed that computes the posterior expected loss for each component using a loss function that is defined by a decision maker. Minimizing the expected loss for the two analysts' posteriors resulted in slightly different compliance findings. However, the results not only indicated whether a component was compliant or not but also included the probability weighted cost of taking either decision. This provides the decision makers with additional information and alternate models, leading to better uncertainty informed decision making.

By now, component failure rates were computed and compliance decisions were made for the T-DEP architecture. RQ 2.3, therefore, looked at compliance finding at the system level in a multi-state context where the system may fail in multiple states. Hypothesis 2.3 (H-2.3) suggested a Monte-Carlo network reliability algorithm suitably modified to work with Bayesian posteriors and for multi-state failures as a solution. For experiment 2.3 (E-2.3), a Monte-Carlo simulation was run to generate one million working and failed system states using Bayesian component failure probabilities from E-2.1. The output was then post-processed to identify the failure rates of different failure states postulated in the C-FHA and asymmetric thrust loss analysis from Ch. 4.3.5. These results suggested that multiple failures are not as unlikely as first assumed, resulting in certain failure states not meeting reliability requirements. The asymmetric thrust loss states' reliability analysis showed that more failure states that were categorized as 'Major' or 'Hazardous' do not meet requirements as compared to 'Catastrophic'. This means that the less safety critical failures have a tendency to drive reliability requirements for the T-DEP power systems architecture.

With these results, the proposed hypotheses for the three parts of RQ 2 were successfully verified, completing the intent of research area 2 from Ch. 3.3

7.1.3 Research Area 3: Sensitivities and Trade-studies

Chapter 6 dealt with the third research area from the research formulation. The third research question (RQ 3) was motivated by observations group 3 from chapter 2.5. This group primarily noted that traditional methods used to conduct safety assessments of novel aircraft concepts limit the scope for exploration and trade studies in preliminary design stages. It also noted that optimizing for nominal considerations could worsen performance under off-nominal conditions. Therefore, the goal of RQ 3 was to enable design trade studies for novel aircraft architectures while incorporating safety related off-nominal considerations. To that end, hypothesis 3 proposed that the integrated framework (see fig. 78) developed in this thesis serves as an enabler for conducting trade studies informed by safety related off-nominal requirements and reliability of novel aircraft architectures in early design.

Chapter 6 then took a two-pronged approach to verify hypothesis 3. For the first experiment, sensitivities of system multi-state reliability to component failure rate posteriors was established through unit level importance metrics. In a multi-state failure scenario, the component importance metrics were re-defined to incorporate the reliability of the system from a given hazard state. For instance, reliability from ‘Hazardous’ failures was defined as the likelihood of the system ending up in a state that is less severe than ‘Hazardous’, and so on. These multi-state importance metrics were evaluated for the ‘Minor’, ‘Major’, ‘Hazardous’, and ‘Catastrophic’ off-nominal hazard severity scenarios. The batteries were found to have the highest contribution in terms of criticality index (CI), reliability achievement worth (RAW), and reliability reduction worth (RRW) for ‘Catastrophic’ and ‘Hazardous’ failure states. The traction power buses (TPBs), and cruise motors (CMs) were found to have the next highest risk reduction worth for ‘Hazardous’ failures, meaning any decrease in their reliability would affect the system’s reliability from that severity to the greatest extent. For multi-state failures from experiment 1.2 classified as ‘Major’, the cruise

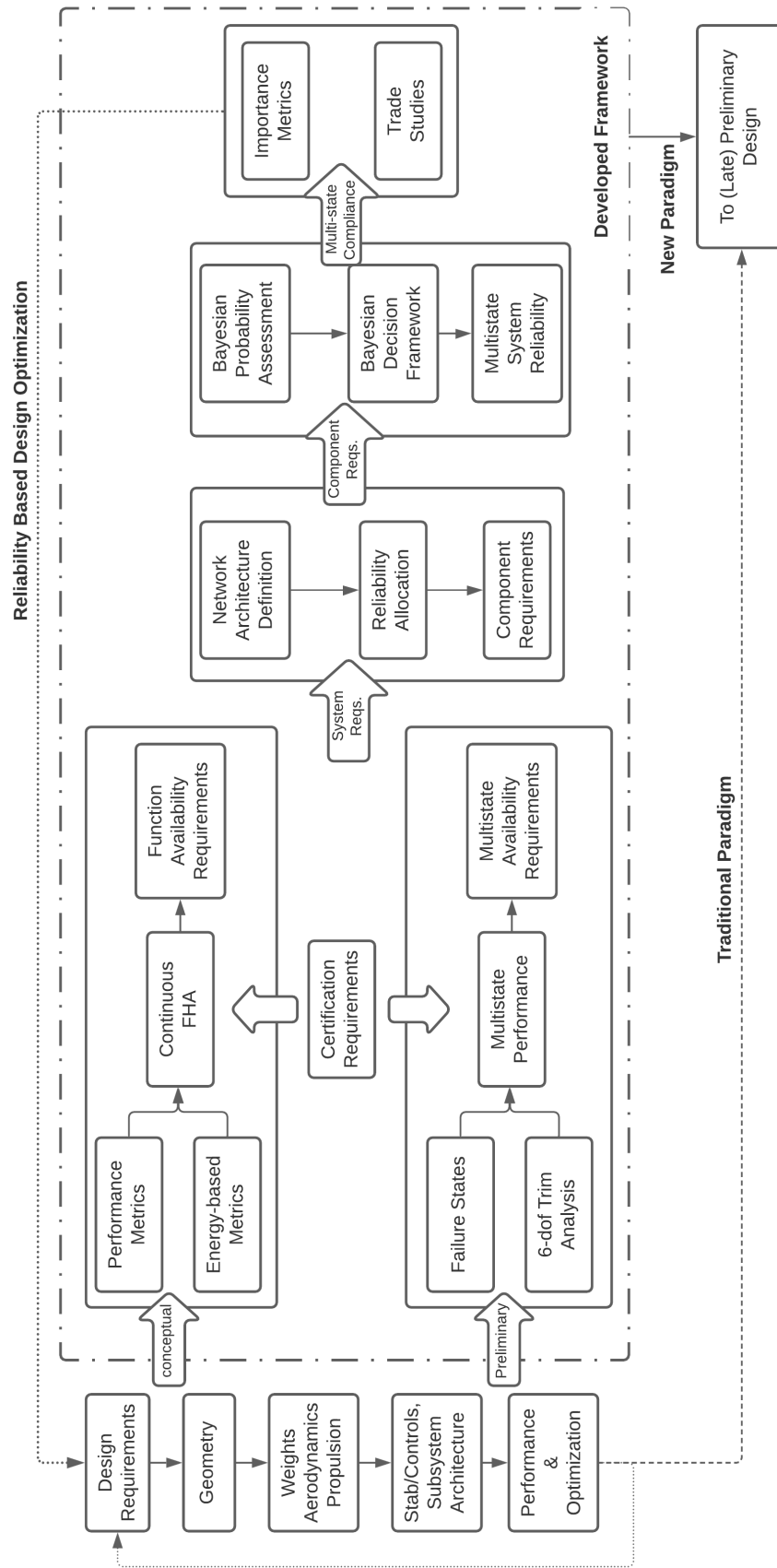


Figure 78: Integrated Framework to Evaluate Off-Nominal Requirements & Reliability of Novel Architectures in Early Design

motor inverters were the ones that can provide the highest improvement in the system reliability if they are improved. For the risk reduction worth, the cruise inverters and pre-chargers were found to be the most important, hinting at great loss of system level reliability from ‘Major’ hazards if their component reliability was to decrease. In the present dissertation, most single component failures result in at least a ‘Minor’ severity. As a result, the Fussell Vesely (FV) measure gave a value of 1 for all components for this severity class, while the RRW measure was undefined. The RAW measure provided important insights nevertheless. The high lift motors, their inverters, and the cruise inverters were found to promise the maximum system reliability improvement if the reliability of these components were improved.

The second part of this chapter focused on revisiting some aircraft design and architecting assumptions in order to improve the system response to off-nominal failure states. In particular, the asymmetric loss of thrust from experiment 1.2 had demonstrated that the T-DEP architecture was limited by the lateral control authority of the vertical tail (VT) in some off-nominal cases, as well as by the thrust available in some cases. To verify these results and demonstrate the capability of the developed framework to conduct design trade studies, two experiments were proposed. Experiment 3.2 resized the T-DEP aircraft’s VT to increase the chord and span by 10% each. The impact of this resizing was considered by modifying the aircraft’s mass properties and lateral aerodynamic derivatives. Upon evaluating the asymmetric loss of thrust cases, it was seen that a larger VT results in improvements in the maximum potential climb gradient metric (MPCG) of about 0.24% during takeoff and 0.64% during cruise with one CM lost. The improvement in energy rate margin (ERM) that denotes the percentage of specific excess power after failure that can be utilized for maximizing the climb gradient was found to be around 5% for takeoff, and 23% for cruise. The cases which were thrust limited (partial loss of a CM) showed no improvement in experiment 3.2 as expected.

The last experiment of this thesis considered the resized VT along with oversized CM inverters. The new CM inverters allow the CMs to generate 67% thrust under partial failures which may result from loss of one CM inverter or pre-charger for instance. Such a modified T-DEP architecture now afforded a larger VT as well as greater thrust capability under partial CM failures. The results of experiment 3.3 showed significant improvements in takeoff and cruise MPCG under partial loss of CMs. The takeoff MPCG improved by about 1.6% absolute value, while ERM improved by about 12-54%. In the cruise condition, MPCG improved by 0.77%, while ERM went from -1.32 to 0.87! As a result, the T-DEP aircraft could now maintain a positive climb gradient under any combination of partial loss of a cruise motor and HLP failures on the same side during takeoff, removing any ‘Catastrophic’ conditions from these failure states. The resultant change in reliability requirements meant that a failure state with partial loss of thrust in one CM, with 2 HLPs on the same side lost was deemed compliant, as compared to non-compliant earlier.

Overall, experiments 3.2 and 3.3 demonstrated two design and architecting trade studies using the T-DEP aircraft that were enabled by the framework developed in this thesis. The framework clearly enables trade studies like these to be conducted for novel aircraft architectures while incorporating safety related off-nominal requirements in early design phases. Along with the importance measures of experiment 3.1, these three experiments help verify hypothesis 3.

7.2 Contributions

The first significant contribution of this thesis is a performance-based framework to identify, characterize, and allocate safety related off-nominal requirements for novel aircraft architectures at the system and component level during conceptual and preliminary design. Towards that end, Continuous-FHA (that considers the magnitude

of functional degradation) is extended to consider the number of terminal, function-satisfying components lost in a failure mode. This extended C-FHA is developed for conceptual level analysis and demonstrated on a test distributed electric propulsion (T-DEP) aircraft inspired from the X-57. When additional design information is available, a preliminary 6 degrees of freedom (6-DoF) model is utilized in a performance-based multi-state analysis framework to evaluate the aircraft's response in different failure states. Combining the results of these conceptual and 6-DoF analyses with certification requirements or engineering judgement allows the characterization of hazard severity at the aircraft system level. Additionally, a network-based bottom up algorithm was demonstrated along with the Critical Flow Method to allocate reliability requirements at the component level. Publications in this research area focus on the identification of certification and off-nominal requirements. The prior includes a model-based framework to automatically extract relevant certification requirements for novel aircraft as well as any potential gaps in their applicability due to technology mismatch. The latter includes initial aspects of C-FHA and multi-state performance-based analysis framework to identify safety-related off-nominal requirements.

Publication: A Model-Based Aircraft Certification Framework for Normal Category Airplanes, AIAA Aviation 2020 (Published) [35]

Publication: Evaluation of Off-Nominal Performance and Reliability of a Distributed Electric Propulsion Aircraft during Early Design, AIAA SciTech 2021 (Published) [34] → AIAA Journal of Aircraft (Under Review)

The second significant contribution of this thesis is in providing a more comprehensive treatment of both epistemic and aleatory uncertainty in reliability and compliance finding. This is achieved using the meager reliability data available for novel concepts in a Bayesian probability and decision framework. The Bayesian framework allows subject matter expert opinion to be encoded in the failure rate models through

prior distributions that capture epistemic uncertainty. This framework also enables the evaluation and propagation of alternative models generated by different subject matter experts to decision makers, leading to a more comprehensive treatment of uncertainty as compared to utilizing traditional measures of central tendency (point estimates). A Bayesian decision framework utilizes the expected loss principle to minimize the posterior expected loss for any component while making a compliance decision. Such a method makes full use of the uncertainty encoded in Bayesian failure rate posteriors to provide a loss value for different compliance actions to decision makers, who can then make an informed choice. Finally, this thesis contributes a modified Monte-Carlo algorithm to estimate multi-state reliability of complex systems while utilizing the Bayesian failure rate posteriors previously generated. Initial aspects of this framework were presented at AIAA Aviation 2019 Forum.

Publication: A Bayesian Safety Assessment Methodology for Novel Aircraft Architectures and Technologies Using Continuous FHA, AIAA Aviation 2019 (Published) [30]

The third significant contribution of this thesis is to demonstrate the integrated framework’s capability in informing sensitivity and trade studies in early design phases for novel aircraft architectures and technologies. This contribution can be divided into two parts.

The first part is the development and implementation of multi-state component importance metrics pertaining to different hazard severity categories. The aircraft system reliability in this instance was re-defined as reliability from a particular severity. So reliability from ‘Hazardous’ severity includes the probability that the aircraft is in a nominal or failed state that is less severe than ‘Hazardous’. This may include ‘Minor’ or ‘Major’ failures, but not ‘Catastrophic’. In such a scenario, table 42 gives the list of multi-state component importance measures developed and implemented

in this thesis. These measures help identify which components have the highest impact on improving or decreasing the aircraft system reliability, as well as the general sensitivity of the system reliability to the component reliability.

Table 42: Multi-state Component Importance Measures

Symbol	Measure Name
MI_i^{BB}	Multi-state Birnbaum Importance
MI_i^{CI}	Multi-state Criticality Importance
MI_i^{RAW}	Multi-state Reliability Achievement Worth
MI_i^{FV}	Multi-state Fussell-Vesely
MI_i^{RRW}	Multi-state Reliability Reduction Worth

The second part is the demonstration of how conceptual and preliminary design trade studies can be informed with safety related off-nominal requirements for novel aircraft architectures using the developed framework. To this end, the two final experiments looked at resizing the vertical tail and oversizing the cruise motor-inverters of the T-DEP aircraft to improve its performance in asymmetric loss of thrust scenarios. Plans for converting this contribution of the present thesis into archival papers are in the works at the time of writing this dissertation. While not directly related to the present work, the author’s Ph.D. journey has resulted in numerous other published works that have contributed to his growth as a researcher and are acknowledged here ¹ [31–33, 38].

Providing a systematic, performance-based framework that enhances the safety

¹Other Publications:

1. Rapid Assessment of Power Requirements and Optimization of Thermal Ice Protection Systems, AIAA Aviation 2018 (Published)
2. A Model-Based System Engineering Approach to Normal Category Airplane Airworthiness Certification, AIAA Aviation 2019 (Published)
3. Evaluating Optimal Paths for Aircraft Subsystem Electrification in Early Design, AIAA Aviation 2019 (Published)
4. Optimal Paths for Progressive Aircraft Subsystem Electrification in Early Design, AIAA Journal of Aircraft (Under Review)

assessment of novel aircraft architectures, and informs the conceptual and preliminary stage design trade studies with safety-related off-nominal requirements is the defining contribution of this thesis. It supports the main research objective of the present work with an example demonstration on a test distributed electric propulsion (T-DEP) aircraft inspired by NASA's X-57. The developed framework is expected to support the ability to more quickly explore the architectural and design space for novel aircraft architectures and technologies while bringing safety-related off-nominal considerations into early design.

7.3 Recommendations for Future Work

The work presented in this thesis has multiple avenues for future research opportunities. These fall into two main categories. The first pertains to addressing the limitations and extending the tools and methods proposed in this thesis. The second pertains to extending the present work to tackle different problems and provide additional capabilities.

In the first category, the present work is limited by the assumptions made and models utilized to demonstrate the developed framework on a test distributed electric propulsion (T-DEP) architecture. The C-FHA analysis can consider numerous other off-nominal scenarios with different safety metrics, apart from the ones considered presently. For instance, an available range or glide distance under a loss of thrust during cruise, or landing performance during the final approach are some other scenarios that could be considered for a more thorough analysis. For the performance-based multi-state analysis, the 6-DoF model developed for the T-DEP aircraft considered trim analysis to evaluate the performance of a failure state for this thesis. A model that can simulate the aircraft's dynamic response under failures will provide a more complete perspective into the aircraft's capabilities under off-nominal conditions. Additionally, such a model can be combined with the provided framework to evaluate

certain certification requirements, leading to a *certification driven design* capability. Such a capability will enable the incorporation of certification requirements into early design, providing a level of confidence that a designed airplane will meet its regulatory requirements before a first prototype is even built. This could be lucrative for original equipment manufacturers due to the large potential cost savings. Many novel aircraft concepts are likely to incorporate some level of autonomy in their design and operations. Therefore, having a capability that can simulate the aircraft’s dynamic response to off-nominal conditions while considering aspects of reconfigurability and adaptive control will enable a more thorough examination of run-time assurance as against design time assurance. Data like flight paths and states generated from such simulation exercises can open avenues of incorporating machine learning techniques into identification and classification of off-nominal scenarios. Another avenue of model extension can look at defining the expected loss function used in the Bayesian compliance finding stage using cost models found in literature. These cost models can then enable trade-offs regarding the cost of improving the reliability of a given component versus the cost of selecting another component versus the cost of adding redundancy to inform architecting considerations earlier in the design phases. This forms the first category of future work that could be explored by interested researchers.

The second category has numerous possibilities of extending the present work, a few of which are discussed here. One of the most obvious avenues for future work could entail applying the developed safety framework on different categories of novel architectures. For instance, the present work utilized the T-DEP architecture as a test case to demonstrate the different techniques and methods for the different research questions. However, numerous novel concepts are being developed concurrently, which include diverse architectures that enable vertical take-off and landing – composite rotorcraft, tiltrotors, turbo-electric, blended wing concepts, etc. to name a

few. These span different airworthiness categories as well as different operational certification categories. The largest diversity in novel architectures is likely to be found in the unmanned aerial systems (UAS) concepts for delivering cargo, or for other applications. While the developed framework is intended to be generalizable to such novel architectures, its implementation is likely to face challenges. Demonstrating this framework on a variety of such concepts would entail defining suitable safety metrics for them (as was noted under RQ 1.1, there is no one-size-fits-all solution), and generating appropriate conceptual and dynamic models to evaluate their performance under functional degradation scenarios as well as in multi-state failure scenarios. While this dissertation provides certain guidelines, down-selecting these metrics for different architectures of interest, creating models to estimate them, and extracting safety criticality of different off-nominal scenarios will need more work. Depending on the components utilized in these diverse concepts, their Bayesian posteriors will have to be determined by gathering SME opinion and relevant data. Another potential challenge in implementing this framework on diverse novel architectures that is left for the future includes identifying suitable certification basis to inform thresholds of safety-metrics as well as postulating multi-state failures for them. A detailed analysis for different such concepts while considering off-nominal requirements could be the second avenue of future research for the presented work.

Finally, while this thesis demonstrated how the developed framework can be used to inform trade studies in the early preliminary design stage, tying back the loop to utilize that information in order to resize or re-architect the aircraft concept was considered beyond the scope of the present work. Future work can focus on tying back the requirements generated from this framework to iteratively constrain the design and architectural space, with a goal of enabling reliability-based design optimization (RBDO) for novel aircraft architectures. This area can form the third avenue for future work.

APPENDIX A

PHYSICAL ARCHITECTURE MATRIX OF ALTERNATIVES

Matrix of alternatives for commercial aircraft architecting solutions from literature [101].

Table 43: Commercial aircraft architecting alternatives (Adapted from Ref. [101])

	Option 1	Option 2	Option 3	Option 4
<i>Function 1: Lifting Payload</i>				
Configuration	Monoplane	Biplane	Box Wing	Tandem
Wing shape	Rectangular	Tapered	Delta	Swept
LE devices	LE flap	Slat	Kruger flap	Leading-edge slot
TE devices	None	Plain Flap	Kruger flap	Slotted flap
<i>Function 2: Storing Payload</i>				
Number of fuselages	BWB	1	2	3
Shape	Cylindrical	Airfoil Shaped	Box shaped	
<i>Function 3: Accelerating Payload</i>				
Engine Type	Piston-prop	Electric	Turbo-prop	Turbo-fan
Number of engines	1	2	3	4
Engine location	Inside VT	Fuselage-mounted	Under wing	Above wing
<i>Function 4: Maintaining pitch stability, control, and trim</i>				
Configuration	HT	V-shaped tail	Tailless	
Horizontal location	Aft of wing	Canard	Three surface	
<i>Function 5: Maintaining yaw stability, control, and trim</i>				
Configuration	VT	V-tail	2 surfaces	
Location	On fuselage	On HT	triple tail	

APPENDIX B

T-DEP DELPHI MODEL

The Dynamic Environment for Loads Prediction and Handling Investigation (DELPHI) [63, 78, 160, 161] framework developed at the Aerospace Systems Design Lab is the 6-DoF flight dynamics environment used in this thesis. DELPHI is developed as an object-oriented python code that can accept any aircraft model, any desired maneuver, and simulate the flight dynamics. In this thesis, it is combined along with a trim analysis algorithm by Marco et al. [120] that utilizes a minimization technique to determine a trim solution for any input combination of aircraft state, control deflections, environmental conditions, and propulsive state. A high-level view of DELPHI is shown in Fig. 79.

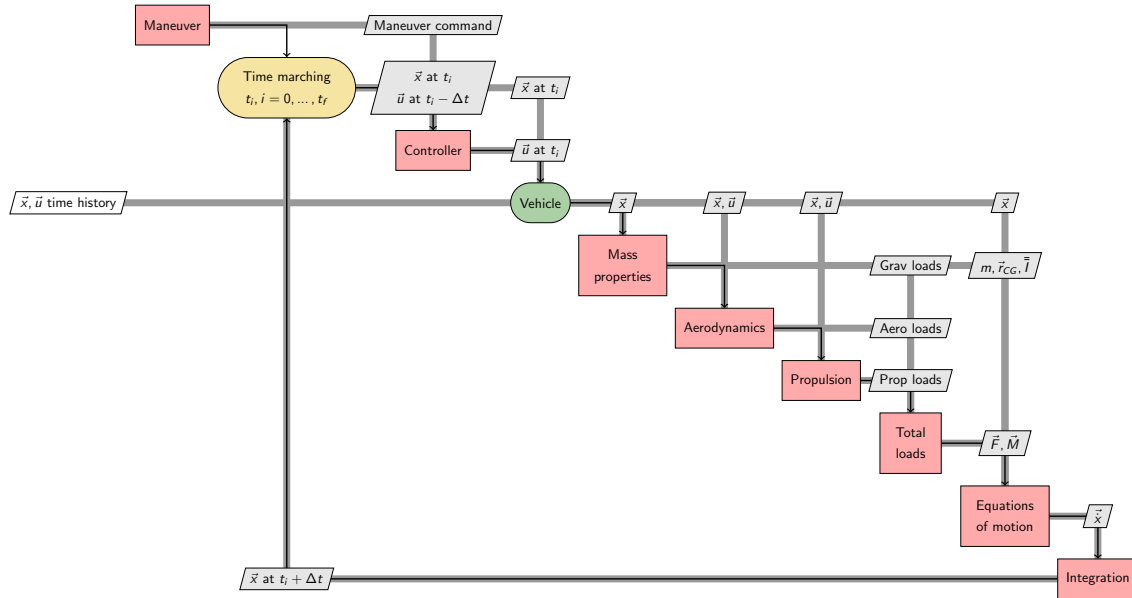


Figure 79: DELPHI framework (Credit: Refs. [34, 161])

Within DELPHI, a desired maneuver can be specified in the *Maneuver block*. The

Controller block compares the desired maneuver to the current state of the aircraft and produces a control vector \vec{u} which specifies all control surface deflection and throttle settings on the vehicle. The *Vehicle block* contains within it the mass properties, aerodynamics, and propulsion. This is where the test distributed electric propulsion architecture (T-DEP) inspired by the X-57 is implemented. Given the current state vector, \vec{x} , and control vector \vec{u} , the vehicle block computes the loads due to gravity, aerodynamics, and propulsion. The net loads, \vec{F} & \vec{M} , are sent to the *Equations of Motion block* which computes the time derivative of the state vector, $\dot{\vec{x}}$. \vec{x} is integrated forward in time using an appropriate time-integration scheme to obtain the state vector at the next time step, \vec{x} at $t_i + \Delta t$. The entire loop is time-marched till the final time t_f is reached.

The *Vehicle block* is implemented such as to allow the user to provide an arbitrary number of aircraft control surfaces and propulsion devices. Flexibility is offered to allow the data for propulsion and aerodynamics to come on any source- be it simple look-up tables, or function calls to an analysis code. This makes the job of implementing the T-DEP architecture easier. Every high lift propulsor and wingtip cruise motor is treated as an independent object generating thrust along its own axis at its own position, all of which are later translated into vehicle level forces and moments.

The equations of motion are cast about a fixed reference point O rather than the CG. This enables, for instance, the dynamics of a moving CG (e.g., due to decreasing fuel mass or fuel transfer) to be modeled. The force and moment equations in vector form are given below:

$$\vec{F}_{total} = m \left(\dot{\vec{V}}_0 + \vec{\omega} \times \vec{V}_0 + \ddot{\vec{r}}_g + \dot{\vec{\omega}} \times \vec{r}_g + 2 \vec{\omega} \times \dot{\vec{r}}_g + \vec{\omega} \times (\vec{\omega} \times \vec{r}_g) \right), \quad (147)$$

$$\vec{M}_{total} = \bar{I} \dot{\vec{\omega}} + \vec{\omega} \times \bar{I} \vec{\omega} + m \vec{r}_g \times \left(\dot{\vec{V}}_0 + \vec{\omega} \times \vec{V}_0 \right), \quad (148)$$

where \vec{r}_g is the position vector from ‘O’ to the center of gravity (CG) of the aircraft, $\vec{V}_0 = \{u, v, w\}^T$ the velocity of the reference point ‘O’, $\vec{\omega} = \{p, q, r\}^T$ the angular

velocity of the aircraft, and \bar{I} the mass moment of inertia matrix of the aircraft about ‘O’. The more specific case where the reference point ‘O’ coincides with the CG can be obtained by setting $\vec{r}_g = 0$ in the above. Kinematic relationships are used to obtain the derivatives of the Euler angles ϕ , θ , and ψ from the angular rates p , q , and r , and also derivatives of the position x_0 , y_0 , and z_0 of the reference point ‘O’ from the velocities u , v , and w . The resulting system of 12 nonlinear ordinary differential equations (in $u, v, w, p, q, r, \phi, \theta, \psi, x_0, y_0, z_0$) for six degrees-of-freedom rigid body motion is numerically integrated to obtain the motion history of the aircraft during the maneuver.

The DELPHI environment has been validated by simulating 14 CFR Part 25- Subpart C specified maneuvers: the checked-pitch maneuver, the rudder-kick maneuver, and the rolling maneuver for a representative business jet aircraft in Refs. [78, 160].

B.1 Mass Properties

Components such as the motors, battery, landing gear from table 11 are treated as point masses distributed at their respective locations with respect to the center of gravity of the aircraft. A simple parallel axis theorem is then used to compute their contributions to the aircraft moments of inertia as,

$$I_{xx} = m((y - y_{CG})^2 + (z - z_{CG})^2) \quad (149)$$

$$I_{yy} = m((x - x_{CG})^2 + (z - z_{CG})^2) \quad (150)$$

$$I_{zz} = m((y - y_{CG})^2 + (x - x_{CG})^2) \quad (151)$$

$$I_{xy} = m((x - x_{CG})(y - y_{CG})) \quad (152)$$

$$I_{xz} = m((x - x_{CG})(z - z_{CG})) \quad (153)$$

$$I_{zy} = m((z - z_{CG})(y - y_{CG})) \quad (154)$$

For lifting surfaces and the fuselage, the moments of inertia calculations given by Ref. [110] are used. For a lifting surface with weight W , semi-span b (or span for

conventional vertical tail), root and tip thicknesses t_r, t_t , root chord c , leading and trailing edge sweep angles λ_L, λ_T ,

$$V = b \left(t_r \left(c + \frac{b}{2} (\tan \lambda_T - \tan \lambda_L) \right) - (t_r - t_t) \left(\frac{c}{2} + \frac{b}{3} (\tan \lambda_T - \tan \lambda_L) \right) \right) \quad (155)$$

$$I_{xx} = \frac{Wb^3}{V} \left((t_r - t_t) \left(\frac{c}{4} + \frac{b}{5} \tan \lambda_T - \frac{b}{5} \tan \lambda_L \right) + t_r \left(\frac{c}{3} + \frac{b}{4} \tan \lambda_T - \frac{b}{4} \tan \lambda_L \right) \right) \quad (156)$$

$$I_{yy} = \frac{Wb}{V} \left(t_r \left(\frac{c^3}{3} + bc \tan \lambda_T \left(\frac{c}{2} + \frac{b \tan \lambda_T}{3} \right) + \frac{b^3}{12} (\tan^3 \lambda_T - \tan^3 \lambda_L) \right) - (t_r - t_t) \left(\frac{c^3}{6} + bc \tan \lambda_T \left(\frac{c}{3} + \frac{b \tan \lambda_T}{4} \right) + \frac{b^3}{15} (\tan^3 \lambda_T - \tan^3 \lambda_L) \right) \right) \quad (157)$$

$$I_{zz} = I_{xx} + I_{yy} \quad (158)$$

The T-DEP fuselage is assumed to be a simple cylinder with radius R_f and length l_f and mass m_f for the purpose of computing the moments of inertial. The formulae from Ref. [110] simplify to yield,

$$I_{xx} = m_f R_f^2 \quad (159)$$

$$I_{yy} = m_f \left(\frac{R_f^2}{2} + \frac{l_f^2}{3} \right) \quad (160)$$

$$I_{zz} = m_f \left(\frac{R_f^2}{2} + \frac{l_f^2}{3} \right) \quad (161)$$

$$I_{xz} = m_f R_f l_f \quad (162)$$

These are then translated to the CG using parallel axis theorem. The component contributions to the aircraft moments of inertia are then added to get the results given in table 12.

B.2 Aerodynamics

The longitudinal aerodynamic model for the T-DEP aircraft is based on regressions that provide aerodynamic coefficients in the wind frame. These regressions are obtained by fitting linear polynomial equations through the digitized data for the X-57 available in Deere et al. [55]. A component build-up approach is used where the aerodynamic coefficients of the entire aircraft are found by adding contributions of each component - wings, nacelles, pylons, stabilator, fuselage, and vertical tail. The aerodynamic coefficients are given as a function of the following:

- States
 - Angle of attack: α
 - Sideslip angle: β
 - Angular rates: p, q, r
- Controls
 - Stabilator incidence angle: δ_s
 - Trim-tab deflection angle: δ_{tt}
 - Flap deflection angle: δ_f
 - Aileron deflection angle: δ_a
 - Rudder deflection angle: δ_r
 - High lift propeller blowing (boolean)

The lift coefficient is found as:

$$C_L(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{L_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{L_{\text{wing} + \text{tip-nacelle}}} + C_{L_{\text{flap}}} + C_{L_{\text{HLN}}} + C_{L_{\text{fuse} + \text{Vtail}}} + C_{L_{\text{stab}}} \frac{S_{\text{stab}}}{S_{\text{wing}}} \quad (163)$$

Note that the lift coefficient is assumed to not be affected by the sideslip angle. The drag coefficient is similarly found as:

$$C_D(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{D_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{D_{\text{wing} + \text{tip-nacelle}}} + C_{D_{\text{flap}}} + C_{D_{\text{HLN}}} + C_{D_{\text{fuse+Vtail}}} + C_{D_{\text{stab}}} \frac{S_{\text{stab}}}{S_{\text{wing}}} \quad (164)$$

The moment coefficient is found as:

$$C_m(\alpha, \delta_s, \delta_{tt}, \delta_f) = C_{m_{\text{blower}}} \frac{\# \text{ of HLP } ON}{12} + C_{m_{\text{wing} + \text{tip-nacelle}}} + C_{m_{\text{flap}}} + C_{m_{\text{HLN}}} + C_{m_{\text{fuse+Vtail}}} + C_{m_{\text{stab}}} \frac{S_{\text{stab}} C_{\text{stab}}}{S_{\text{wing}} C_{\text{wing}}} \quad (165)$$

Deere et al. [55] provide the longitudinal aerodynamic data for the X-57 in terms of different configurations. Of these, a subset are useful in determining the component buildup of longitudinal aerodynamic coefficients. This subset is given in table 44.

Table 44: Configuration component buildup for the X-57 [55]

Config	Fuselage and VT	Wing and Tip Nacelle	30° Flaps	HLN	Aileron	Stabilator (°) Trim Tab (°)
1		x			0	
2		x		x	0	
8		x		x	0	-1,0
11		x	x	x	0	-1,0
12	x	x		x	0	-1,0

The high lift propulsor contributions can be obtained by subtracting C11 without high lift blowing from C11 with high lift blowing and are given by Eq. 166 suitably applied to the parameter of interest.

$$C_{blower} = C_{11\text{-blow}} - C_{11\text{-noblow}} \quad (166)$$

$$C_{L_{11\text{-blow}}} = 0.1153 \alpha + 2.6807 \quad (167)$$

$$C_{L_{11\text{-noblow}}} = 0.075 \alpha + 1.7047 \quad (168)$$

$$C_{D_{11\text{-blow}}} = 0.0461 C_{L_{11\text{-blow}}}^2 - 0.1294 C_{L_{11\text{-blow}}} + 0.2942 \quad (169)$$

$$C_{D_{11\text{-noblow}}} = 0.0579 C_{L_{11\text{-noblow}}}^2 - 0.1283 C_{L_{11\text{-noblow}}} + 0.1661 \quad (170)$$

$$C_{D_{11\text{-noblow}}} = 0.075 \alpha + 1.7047 \quad (171)$$

$$C_{m_{11\text{-blow}}} = 0.0064 \alpha - 0.7585 \quad (172)$$

$$C_{m_{11\text{-noblow}}} = 0.0062 \alpha - 0.407 \quad (173)$$

$$(174)$$

The wing + tip nacelle contributions can be obtained directly from configuration 1 (C1) and are given by Eq. 175 suitably applied to the parameter of interest.

$$C_{wing+tip-nacelle} = C_1 \quad (175)$$

$$C_{L_1} = 0.0633 \alpha + 0.8055 \quad (176)$$

$$C_{D_1} = 0.1033 C_{L_1}^2 - 0.1302 C_{L_1} + 0.0584 \quad (177)$$

$$C_{m_1} = 0.053 C_{L_1}^2 - 0.0604 C_{L_1} - 0.1675 \quad (178)$$

The flap contributions can be obtained by subtracting C8 from C11 without high lift blowing and are given by Eq. 179 suitably applied to the parameter of interest.

$$C_{flap} = C_{11\text{-noblow}} - C_8 \quad (179)$$

$$C_{L_8} = 0.0674 \alpha + 0.6946 \quad (180)$$

$$C_{D_8} = 0.0754 C_{L_8}^2 - 0.0687 C_{L_8} + 0.0419 \quad (181)$$

$$C_{m_8} = 0.0467 C_{L_8}^2 - 0.0452 C_{L_8} - 0.1754 \quad (182)$$

The high lift nozzle (HLN) contributions can be obtained by subtracting C1 from

C2 and are given by Eq. 183 suitably applied to the parameter of interest.

$$C_{flap} = C_2 - C_1 \quad (183)$$

$$C_{L_2} = 0.0721 \alpha + 0.6633 \quad (184)$$

$$C_{D_2} = 0.1059 C_{L_2}^2 - 0.1049 C_{L_2} + 0.0491 \quad (185)$$

$$C_{m_2} = 0.0665 C_{L_2}^2 - 0.085 C_{L_2} - 0.1411 \quad (186)$$

The fuselage + vertical tail (VT) contributions can be obtained by subtracting C8 from C12 and are given by Eq. 187 suitably applied to the parameter of interest.

$$C_{fuse-Vtail} = C_{12} - C_8 \quad (187)$$

$$C_{L_{12}} = 0.082 \alpha + 0.7155 \quad (188)$$

$$C_{D_{12}} = 0.0514 C_{L_{12}}^2 - 0.029 C_{L_{12}} + 0.04 \quad (189)$$

$$C_{m_{12}} = 0.0811 C_{L_{12}}^2 + 0.4284 C_{L_{12}} - 0.5138 \quad (190)$$

Finally, the stabilator contributions are obtained by computing the effective angle of attack on the stabilator. The coefficients are given by,

$$C_{L_{stab}} = 0.065558 \alpha_{stab} + 0.02 \delta_{trimtab} \quad (191)$$

$$C_{D_{stab}} = 0.0871 C_{L_{stab}}^2 + 0.0005 C_{L_{stab}} + 0.0086 \quad (192)$$

$$C_{m_{stab}} = 0.028 C_{L_{stab}} - 0.0056 \delta_{trimtab} \quad (193)$$

where the stabilator angle of attack depends on the aircraft angle of attack, wing incidence ($i_{wing} = 2^\circ$), stabilator incidence (δ_s), and the downwash induced (ϵ_{stab}).

$$\alpha_{stab} = \alpha + i_{wing} + \delta_s - \epsilon_{stab} \quad (194)$$

The downwash angle is computed using regressions provided by Deere et al. [55], reproduced here for completeness.

$$\epsilon_{stab}^\circ = \frac{180}{\pi} \left(\frac{2(m C_{L_{12}} + b)}{\pi AR} + offset \right) \quad (195)$$

Table 45: Coefficients for computing downwash angle [55]

Config	m	b	offset
8	0.65	0.33	0.0
11-noblow	1.0	0.0	-1.6
11-blow	1.0	0.0	-2.7
12	1.5	-0.76	0.0

where, parameters $m, b, offset$ are given in table 45.

These component contributions are combined using equations 163, 164, 165 to get the aircraft level longitudinal aerodynamic coefficients. These are used to evaluate longitudinal loads and moments for the T-DEP aircraft.

APPENDIX C

COMPONENT FAILURE DATA

C.1 Battery

Table 46: Battery failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
111	10.981×10^6		[5]	
		2×10^{-6}	[2]	
		3×10^{-6}	[2]	
		1×10^{-6}	[2]	
		1×10^{-6}	[2]	Prior
1	1,564,315		[2]	(weighted:
		2×10^{-8}	[2]	10%)
0	4.1×10^5		[2]	
0	96,426		[2]	
0	2.0×10^5		[2]	
9.3	1.0×10^6		[53]	
2	104,000		[134]	Likelihood
8	2.6735×10^5		[117]	

C.2 Electric Motor

Table 47: Electric Motor failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
		1.0×10^{-5}	[2]	
		5×10^{-6}	[2]	
		3.2×10^{-6}	[2]	
		2×10^{-6}	[2]	Prior
		1.2×10^{-6}	[2]	(weighted:
6	1.332×10^6		[5]	10%)
89	9,463,428		[7]	
62	1.0465×10^7		[7]	
97	10,194,888		[7]	
9.24	1.0×10^6		[53]	Likelihood
		6.6×10^{-5}	[49]	Likelihood (weighted 10x)
		0.723887×10^{-6}	[117]	Likelihood
		0.39586×10^{-6}	[117]	Likelihood

C.3 *Electric Motor Inverter*

Table 48: Motor Inverter failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
		1.0×10^{-4}	[2]	
		1.0×10^{-4}	[2]	
		6×10^{-5}	[2]	
21	985,505		[2]	
		1.0×10^{-5}	[2]	Prior
2	3.85×10^4		[2]	(weighted:
		3.0×10^{-6}	[2]	10%)
		1.0×10^{-6}	[2]	
9	3.37×10^5		[2]	
2	1.729×10^5		[2]	
3	3.04×10^5		[2]	
4.75	1.0×10^6		[53]	Likelihood
		8.5×10^{-5}	[49]	Likelihood (weighted 10x)

C.4 Traction Power Bus

Table 49: Traction Power Bus failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
0	0.27×10^6		[5]	
		5.0×10^{-7}	[2]	
		2.3×10^{-7}	[2]	
		1.9×10^{-7}	[2]	
		9.0×10^{-5}	[2]	
		8.0×10^{-8}	[2]	
		3.0×10^{-8}	[2]	Prior
		1.0×10^{-8}	[2]	(weighted:
0	3.4×10^4		[2]	10%)
0	4.1×10^5		[2]	
0	2.89×10^5		[2]	
0	5.4×10^5		[2]	
0	9.5×10^5		[2]	
0	1.4×10^6		[2]	
0	2.17×10^6		[2]	
0	26,467		[117]	Likelihood
0	1.3368×10^6		[117]	Likelihood

C.5 Pre-Charger

Table 50: Switch failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
36	6.11×10^6		[5]	Prior
94	135,692,400		[7]	(weighted: 20%)
0	52,934		[117]	Likelihood
0	5754		[117]	Likelihood

Table 51: Resistor failure data

# of failures	Operating time (hrs)	Mean (hr^{-1})	Source	Pooling
				Prior
3.6835	1×10^6		[3]	(weighted: 100%)
0	5.347×10^5		[117]	Likelihood

APPENDIX D

COMPONENT IMPORTANCE

Component importance metrics results for Analyst A are included here.

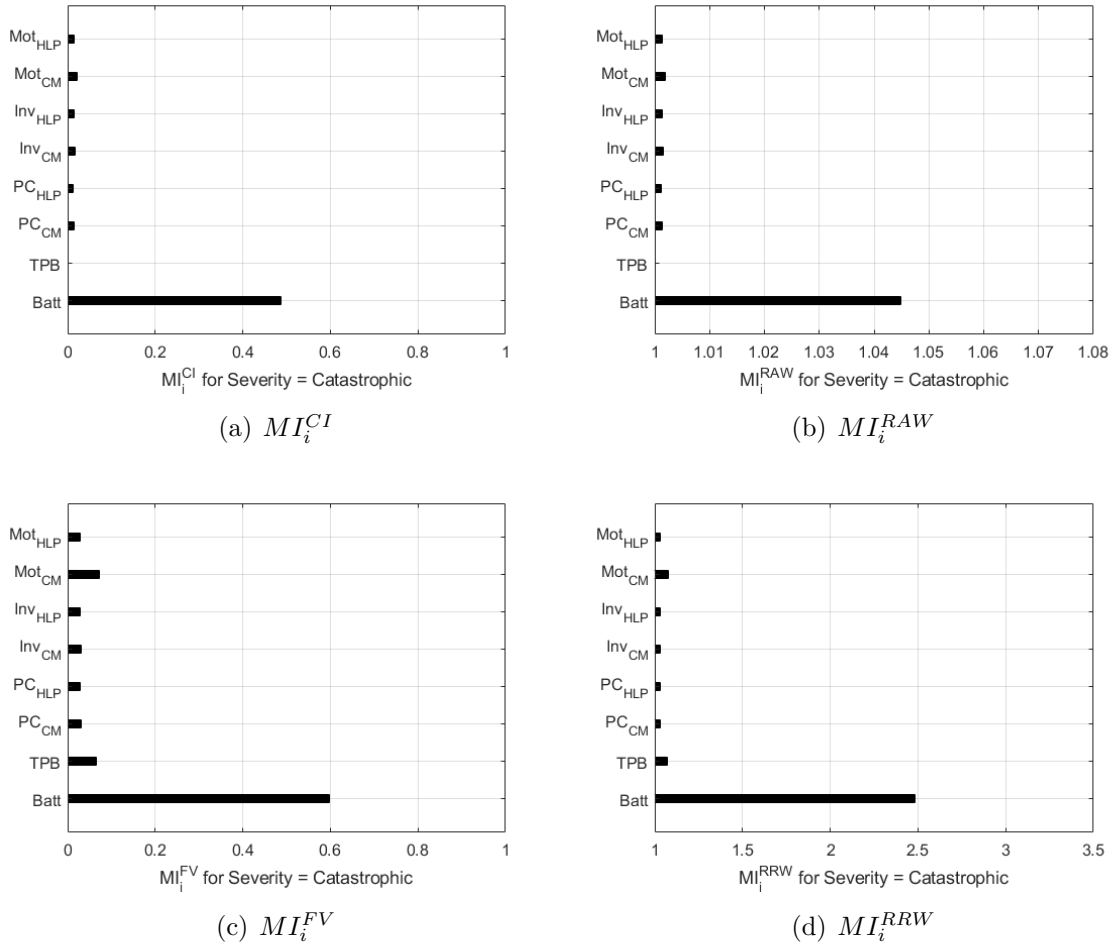
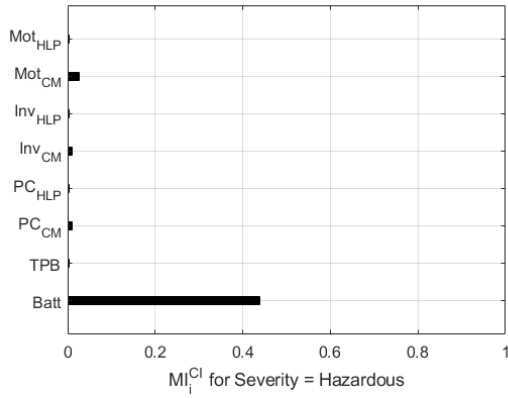
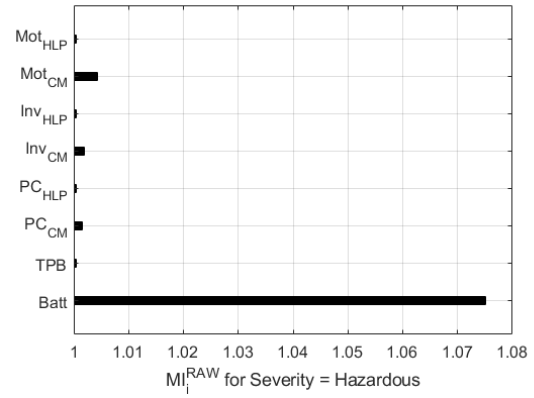


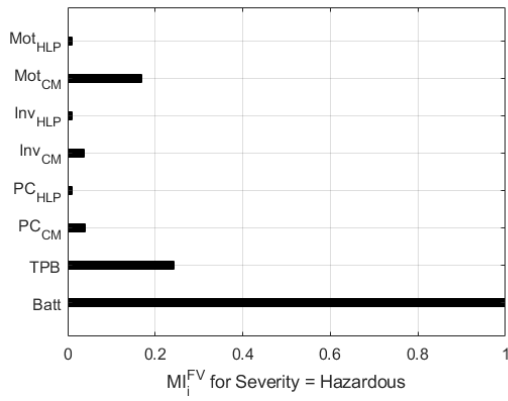
Figure 80: Multi-state importance metrics for Catastrophic failure conditions (Analyst A)



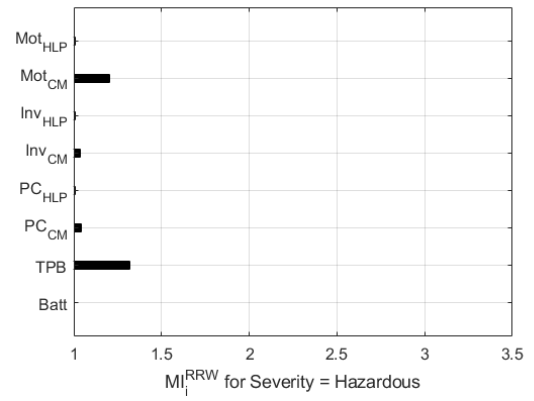
(a) MI_i^{CI}



(b) MI_i^{RAW}

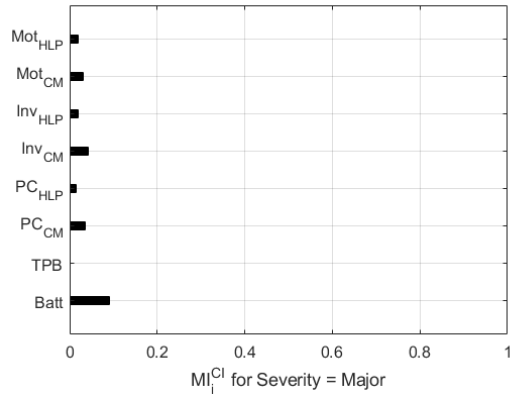


(c) MI_i^{FV}

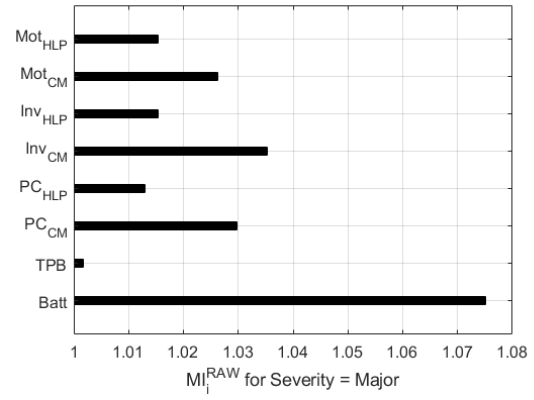


(d) MI_i^{RRW}

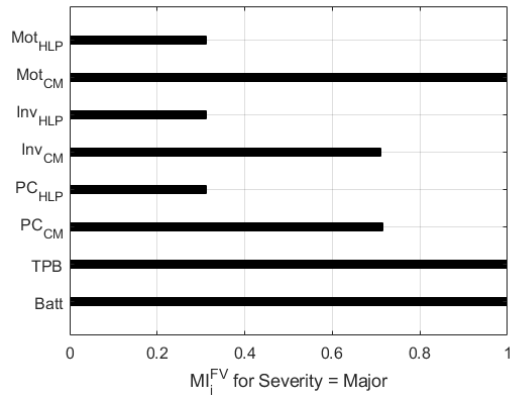
Figure 81: Multi-state importance metrics for Hazardous failure conditions (Analyst A)



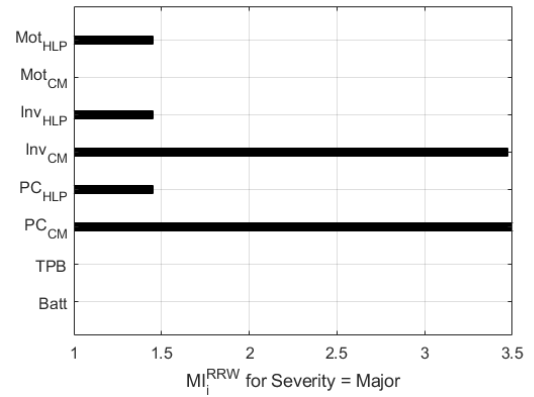
(a) MI_i^{CI}



(b) MI_i^{RAW}

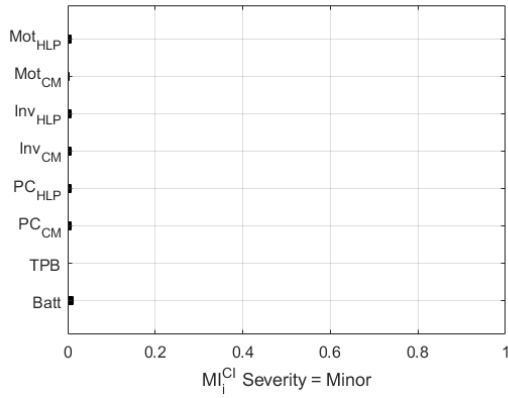


(c) MI_i^{FV}

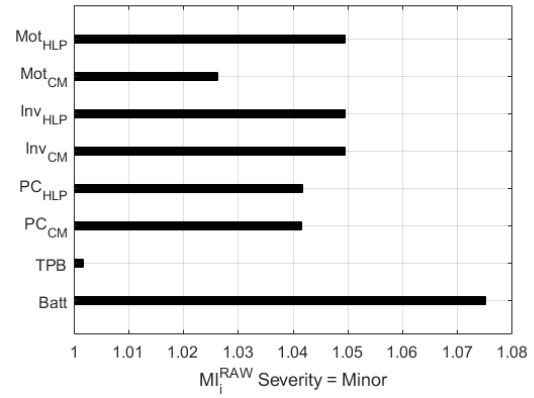


(d) MI_i^{RRW}

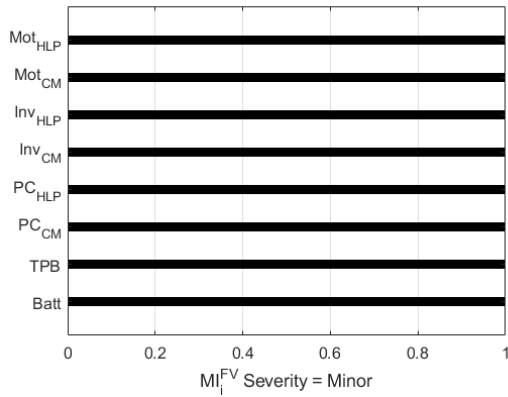
Figure 82: Multi-state importance metrics for Major failure conditions (Analyst A)



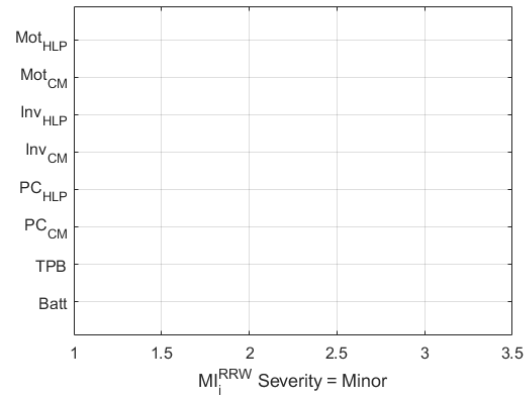
(a) MI_i^{CI}



(b) MI_i^{RAW}



(c) MI_i^{FV}



(d) MI_i^{RRW}

Figure 83: Multi-state importance metrics for Minor failure conditions (Analyst A)

REFERENCES

- [1] “Reactor safety study. An assessment of accident risks in US commercial nuclear power plants. Executive summary,” tech. rep., United States Nuclear Regulatory Commission, 1975.
- [2] *Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment*. No. 508 in TECDOC Series, Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 1989.
- [3] “Military handbook mil-hdbk-217f: Reliability prediction of electronic equipment,” tech. rep., U.S. Department of Defense, 1991.
- [4] “SAE ARP4761: Guidelines and Methods for conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” 1996.
- [5] *Generic Component Reliability Data for Research Reactor PSA*. No. 930 in TECDOC Series, Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 1997.
- [6] “SAE ARP4754: Guidelines for Development of Civil Aircraft and Systems,” 2010.
- [7] “Historical Reliability Data for IEEE 3006 Standards: Power Systems Reliability,” *3006HistoricalData-2012 Historical Reliability Data for IEEE 3006 Standards*, pp. 1–303, 2012.
- [8] “ASTM F3230-17: Standard Practice for Safety Assessment of Systems and Equipment in Small Aircraft,” 2017.
- [9] “ASTM F3173/F3173-18: Standard Specification for Aircraft Handling Characteristics,” 2018.
- [10] “Developmental pillars of increased autonomy for aircraft systems,” Tech. Rep. TR2-EB, ASTM International, 2020.
- [11] “IEEE 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems.” retrieved February 10, 2021, online: <https://standards.ieee.org/standard/1471-2000.html>, 2020.
- [12] “Jaunt air mobility.” retrieved April 15, 2021, online: <https://jauntairmobility.com/aircraft.html>, 2021.
- [13] “Joby aviation.” retrieved February 10, 2021, online: <https://www.jobyaviation.com/news/>, 2021.

- [14] “Volocopter.” retrieved February 10, 2021, online: https://press.volocopter.com/images/2021/2020-12-21_volocopter0974-01.jpg, 2021.
- [15] AGTE, J. S., BORER, N. K., and WECK, O. D., “Multistate design approach to analysis of twin-engine aircraft performance robustness,” *Journal of Aircraft*, vol. 49, no. 3, pp. 781–793, 2012.
- [16] AGTE, J. S., *Multistate analysis and design: case studies in aerospace design and long endurance systems*. PhD thesis, Massachusetts Institute of Technology, 2011.
- [17] ALDEMIR, T., “Computer-assisted markov failure modeling of process control systems,” *IEEE Transactions on Reliability*, vol. R-36, no. 1, pp. 133–144, 1987.
- [18] ALLENBY, K. and KELLY, T., “Deriving safety requirements using scenarios,” in *Proceedings Fifth IEEE International Symposium on Requirements Engineering*, pp. 228–235, IEEE.
- [19] AMELINK, M. H. J., MULDER, M., VAN PAASSEN, M. M. R., and FLACH, J., “Theoretical foundations for a total energy-based perspective flight-path display,” *The International Journal of Aviation Psychology*, vol. 15, no. 3, pp. 205–231, 2005.
- [20] AMENDOLA, A. and REINA, G., “Event sequences and consequence spectrum: A methodology for probabilistic transient analysis,” *Nuclear Science and Engineering*, vol. 77, no. 3, pp. 297–315, 1981.
- [21] AN, D., CHOI, J., and WON, J., “Integrated bayesian reliability analysis under input variable and metamodel uncertainties,” in *51st AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 18th AIAA/ASME/AHS Adaptive Structures Conference 12th*, p. 2594, 2010.
- [22] ANDERSON, J. D., *Aircraft performance and design*. McGraw Hill Education (India), 2010.
- [23] ANDERSON, M., LOPEZ, J., and EVERS, J., “A comparison of trajectory determination approaches for small uav’s,” in *AIAA Atmospheric Flight Mechanics Conference and Exhibit*.
- [24] AOPA, “Aircraft owners and pilots association - what is general aviation?,” retrieved February 11, 2021, Online: https://www.aopa.org/-/media/files/aopa/home/advocacy/what_ga.pdf, 2019.
- [25] ARMSTRONG, M., *Identification Of Emergent Off-nominal Operational Requirements During Conceptual Architecting Of The More Electric Aircraft*. PhD thesis, Georgia Institute of Technology, 2011.

- [26] ARMSTRONG, M., GARCIA, E., and MAVRIS, D., “Aircraft mission and system failure considerations for functional induction based conceptual architecture design,” (Nice, France), 27th International Congress of Aeronautical Sciences, 2010.
- [27] ASTM, “Committee F44 on General Aviation Aircraft.” online: <https://www.astm.org/COMMITTEE/F44.htm>, 2019.
- [28] BANGHART, M., BIAN, L., STRAWDERMAN, L., and BABSKI-REEVES, K., “Risk assessment on the ea-6b aircraft utilizing bayesian networks,” *Quality Engineering*, vol. 29, no. 3, pp. 499–511, 2017.
- [29] BEAUDRY, M., “Performance-related reliability measures for computing systems,” *IEEE Transactions on Computers*, vol. C-27, no. 6, pp. 540–547, 1978.
- [30] BENDARKAR, M. V., BEHERE, A., BRICENO, S. I., and MAVRIS, D. N., “A bayesian safety assessment methodology for novel aircraft architectures and technologies using continuous fha,” in *AIAA Aviation 2019 Forum*, p. 3123, 2019.
- [31] BENDARKAR, M. V., CHAKRABORTY, I., GARCIA, E., and MAVRIS, D. N., “Rapid assessment of power requirements and optimization of thermal ice protection systems,” in *2018 Aviation Technology, Integration, and Operations Conference*, p. 4136, 2018.
- [32] BENDARKAR, M. V., RAJARAM, D., CAI, Y., BRICENO, S. I., and MAVRIS, D. N., “Evaluating Optimal Paths for Aircraft Subsystem Electrification in Early Design,” in *AIAA Aviation 2019 Forum*, p. 2802, 2019.
- [33] BENDARKAR, M. V., RAJARAM, D., CAI, Y., and MAVRIS, D. N., “Optimal Paths for Progressive Aircraft Subsystem Electrification in Early Design (Under Review),” *Journal of Aircraft*, 2021.
- [34] BENDARKAR, M. V., SAROJINI, D., HARRISON, E., and MAVRIS, D. N., “Evaluation of off-nominal performance and reliability of a distributed electric propulsion aircraft during early design,” in *AIAA Scitech 2021 Forum*.
- [35] BENDARKAR, M. V., XIE, J., BRICENO, S., HARRISON, E. D., and MAVRIS, D. N., “A model-based aircraft certification framework for normal category airplanes,” in *AIAA Aviation Forum*, (VIRTUAL EVENT), June 2020.
- [36] BILLS, A., SRIPAD, S., FREDERICKS, W. L., SINGH, M., and VISWANATHAN, V., “Performance metrics required of next-generation batteries to electrify commercial aircraft,” *ACS Energy Letters*, vol. 5, no. 2, pp. 663–668, 2020.
- [37] BIRNBAUM, Z. W., “On the importance of different components in a multicomponent system,” tech. rep., Washington Univ Seattle Lab of Statistical Research, 1968.

- [38] BLEU-LAINE, M.-H., BENDARKAR, M. V., XIE, J., BRICENO, S. I., and MAVRIS, D. N., "A model-based system engineering approach to normal category airplane airworthiness certification," in *AIAA Aviation 2019 Forum*, American Institute of Aeronautics and Astronautics, 2019.
- [39] BOEING, "Boeing 737 Max Software Updates." retrieved July 4, 2019, online: <https://boeing.mediaroom.com/news-releases-statements?item=130336>, 2018.
- [40] BOEING, "Boeing Statement on Lion Air Flight 610 Preliminary Report." retrieved July 4, 2019, online: <https://www.boeing.com/commercial/737max/737-max-software-updates.page>, 2019.
- [41] BOGLIETTI, A., CAVAGNINO, A., TENCONI, A., VASCHETTO, S., and DI TORINO, P., "The safety critical electric machines and drives in the more electric aircraft: A survey," in *2009 35th Annual Conference of IEEE Industrial Electronics*, pp. 2587–2594, IEEE, 2009.
- [42] BOND, A. H. and RICCI, R. J., "Cooperation in aircraft design," *Research in Engineering Design*, vol. 4, no. 2, pp. 115–130, 1992.
- [43] BONIS, A., "Bayesian reliability demonstration plans," in *5th Annual Reliability and Maintainability Conference*, 1966.
- [44] BORER, N., CLAYPOOL, I., CLARK, D., WEST, J., SOMERVILL, K., ODEGARD, R., and SUZUKI, N., "Model-driven development of reliable avionics architectures for lunar surface systems," in *2010 IEEE Aerospace Conference*, pp. 1–21, IEEE, 2010.
- [45] BORER, N. K. and PATTERSON, M. D., "x-57 high-lift propeller control schedule development,"
- [46] BOYD, J. R., CHRISTIE, T. P., and GIBSON, J. E., "Energy maneuverability," *Air Proving Ground Center Report APGC-TR-66-4 Vol*, vol. 1, 1966.
- [47] CAA, "Civil Aviation Authority CAP 739: Flight Data Monitoring." retrieved February 17, 2021, online: <https://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=5613>, 2013.
- [48] CAMPBELL, A., *ARCHITECTING AIRCRAFT POWER DISTRIBUTION SYSTEMS VIA REDUNDANCY ALLOCATION*. PhD thesis, Georgia Institute of Technology, 2014.
- [49] CAO, W., MECROW, B. C., ATKINSON, G. J., BENNETT, J. W., and ATKINSON, D. J., "Overview of Electric Motor Technologies Used for More Electric Aircraft (MEA)," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 9, pp. 3523–3531, 2012.

- [50] CHAKRABORTY, I., *Subsystem architecture sizing and analysis for aircraft conceptual design*. PhD thesis, Georgia Institute of Technology, 2015.
- [51] CHARRIER, J.-J. and KULSHRESHTHA, A., “Electric actuation for flight and engine control; evolution and current trend,” in *45th AIAA Aerospace Sciences Meeting and Exhibit*, p. 1391, 2007.
- [52] CLARKE, S., REDIFER, M., PAPATHAKIS, K., SAMUEL, A., and FOSTER, T., “X-57 power and command system design,” in *2017 IEEE Transportation Electrification Conference and Expo (ITEC)*, pp. 393–400, IEEE, 2017.
- [53] DARMSTADT, P. R., CATANESE, R., BEIDERMAN, A., DONES, F., CHEN, E., MISTRY, M. P., BABIE, B., BECKMAN, M., and PREATOR, R., “Hazards analysis and failure modes and effects criticality analysis (fmeca) of four concept vehicle propulsion systems,” Tech. Rep. NASA/CR-2019-220217, National Aeronautics and Space Administration, 2019.
- [54] DAWKINS, S. K., KELLY, T. P., McDERMID, J. A., MURDOCH, J., and PUMFREY, D. J., “Issues in the Conduct of PSSA,” in *Proceedings of the 17th International System Safety Conference*, vol. 122, 1999.
- [55] DEERE, K. A., VIKEN, S., CARTER, M. B., VIKEN, J. K., COX, D. E., WIESE, M. R., and FARR, N. L., “Computational component build-up for the x-57 maxwell distributed electric propulsion aircraft,” in *2018 AIAA Aerospace Sciences Meeting*, p. 1275, 2018.
- [56] DEODATH, R., JHINGOORIE, J., and RIVEROL, C., “Direct methanol fuel cell system reliability analysis,” *International Journal of Hydrogen Energy*, vol. 42, no. 16, pp. 12032–12045, 2017.
- [57] DEVOOGHT, J. and SMIDTS, C., “Probabilistic reactor dynamics—i: The theory of continuous event trees,” *Nuclear Science and Engineering*, vol. 111, no. 3, pp. 229–240, 1992.
- [58] DEZFULI, H., KELLY, D., SMITH, C., VEDROS, K., and GALYEAN, W., “Bayesian inference for nasa probabilistic risk and reliability analysis,” Tech. Rep. NASA/SP-2009-569, National Aeronautics and Space Administration, 2009.
- [59] DoD, “MIL-STD-882E: Standard Practice for System Safety,” tech. rep., DoD US.
- [60] DOMÍNGUEZ-GARCÍA, A. D., *An integrated methodology for the performance and reliability evaluation of fault-tolerant systems*. PhD thesis, Massachusetts Institute of Technology, 2007.
- [61] DOMINGUEZ-GARCIA, A. D., KASSAKIAN, J. G., SCHINDALL, J. E., and ZINCHUK, J. J., “An integrated methodology for the dynamic performance

- and reliability evaluation of fault-tolerant systems,” *Reliability Engineering & System Safety*, vol. 93, no. 11, pp. 1628–1649, 2008.
- [62] DRELA, M. and YOUNGREN, H., *AVL 3.36 User Primer*. MIT, Feb. 2017.
- [63] DUCA, R., SAROJINI, D., BLOEMER, S., CHAKRABORTY, I., BRICENO, S. I., and MAVRIS, D. N., “Effects of epistemic uncertainty on empennage loads during dynamic maneuvers,” in *2018 AIAA Aerospace Sciences Meeting*, p. 0767, 2018.
- [64] ERICSON, C. A., *Hazard Analysis Techniques for System Safety*. Hoboken, N.J.: Wiley-Interscience, 2005.
- [65] EWING, F. J., WALDRON, B., and THIES, P. R., “A bayesian updating framework for simulating marine energy converter drive train reliability,” *Marine Energy Technology Symposium (METS)*, 2017.
- [66] FAA, “Federal Aviation Administration AC 25.1309-1A - System Design and Analysis.” retrieved February 11, 2021, online: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/22680, 1988.
- [67] FAA, “Federal Aviation Administration AC 120-82 - Flight Operational Quality Assurance.” retrieved February 17, 2021, online: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/23227, 2004.
- [68] FAA, “Federal Aviation Administration AC 120-42B - Extended Operations (ETOPS and Polar Operations).” retrieved February 11, 2021, online: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/73587, 2008.
- [69] FAA, “Federal Aviation Administration AC 135-42 - Extended Operations (ETOPS) and Operations in the North Polar Area.” retrieved February 11, 2021, online: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/74318, 2008.
- [70] FAA, “System Safety Handbook.” retrieved July 7, 2019, online: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/, 2013.
- [71] FAA, “Federal Aviation Administration AC 91-79A - Mitigating the Risks of a Runway Overrun Upon Landing.” retrieved February 17, 2021, online: https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1025626, 2014.

- [72] FAA, “Revision of airworthiness standards for normal, utility, acrobatic, and commuter category airplanes.” retrieved February 11, 2021, Federal Register, online: <https://www.govinfo.gov/content/pkg/FR-2016-12-30/pdf/2016-30246.pdf>, 2017.
- [73] FAA, “83 FR 21850 - Accepted Means of Compliance; Airworthiness Standards: Normal Category Airplanes.” retrieved February 11, 2021, Federal Register, online: <https://www.govinfo.gov/app/details/FR-2018-05-11/2018-09990>, 2018.
- [74] FAA, “FAA Aerospace Forecast Highlights.” retrieved February 10, 2021, online: https://www.faa.gov/data_research/aviation/aerospace_forecasts/, 2020.
- [75] FINGER, D. F., BRAUN, C., and BIL, C., “Comparative assessment of parallel-hybrid-electric propulsion systems for four different aircraft,” *Journal of Aircraft*, vol. 0, no. 0, pp. 1–11, 2020.
- [76] FOOT, P., “The problem of abortion and the doctrine of the double effect,” *Oxford Review*, vol. 5, pp. 5–15, 1967.
- [77] GANDHI, N., RICHARDS, N., BATEMAN, A., BOLSTAD, C., and COSTELLO, A., “Pilot-in-the-loop demonstration of an energy monitor and crew alerting system,” in *AIAA Guidance, Navigation, and Control Conference*.
- [78] GORON, G., DUCA, R., SAROJINI, D., SHAH, S., CHAKRABORTY, I., BRICENO, S. I., and MAVRIS, D. N., “A simulation-based framework for structural loads assessment during dynamic maneuvers,” in *17th AIAA Aviation Technology, Integration, and Operations Conference*, p. 3767, 2017.
- [79] GUARRO, S., “Risk assessment of new space launch and supply vehicles,” in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, pp. 5157–5164, 2012.
- [80] GUIKEMA, S. D. and PATÉ-CORNELL, M. E., “Bayesian analysis of launch vehicle success rates,” *Journal of spacecraft and rockets*, vol. 41, no. 1, pp. 93–102, 2004.
- [81] HALL, D., CHIN, J., ANDERSON, A., SMITH, A., EDWARDS, R., and DUFFY, K. P., “Development of a maxwell x-57 high lift motor reference design,” in *AIAA Propulsion and Energy 2019 Forum*, 2019.
- [82] HASAN, S., HEMM, R., HOUSER, S., and REVELEY, M., “Integrated safety benefits analysis of nasa aviation safety program technologies,” in *AIAA’s Aircraft Technology, Integration, and Operations (ATIO) 2002 Technical Forum*, p. 5893, 2002.

- [83] HASSON, J. and CROTTY, D., “Boeing’s safety assessment processes for commercial airplane designs,” in *16th DASC. AIAA/IEEE Digital Avionics Systems Conference. Reflections to the Future. Proceedings*, vol. 1, pp. 4.4–1 – 4.4–7, IEEE, 1997.
- [84] HAY, D. C., *Requirements Analysis: From Business Views to Architecture*. Pearson, 1 ed., 2002.
- [85] HEMM, R., HORIO, B., and DECICCO, A., “Assessment of system safety risks for nextgen concepts and technologies,” in *12th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference and 14th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, p. 5547, 2012.
- [86] HOWE, D., *Aircraft Conceptual Design Synthesis*. John Wiley & Sons, Ltd, 2000.
- [87] HYUN, K.-C., MIN, S., CHOI, H., PARK, J., and LEE, I.-M., “Risk analysis using fault-tree analysis (fta) and analytic hierarchy process (ahp) applicable to shield tbn tunnels,” *Tunnelling and Underground Space Technology*, vol. 49, pp. 121–129, 2015.
- [88] IATA, “International Air Transport Association Technology Roadmap 2013.” retrieved July 4, 2019, online: <https://www.iata.org/whatwedo/environment/Documents/technology-roadmap-2013.pdf>, 2018.
- [89] ICAO, “Airport Services Manual - Part II - Pavement Surface Conditions (Doc 9137P2),” 2002.
- [90] ICAO, “International Civil Aviation Organization Safety Report 2018.” retrieved July 4, 2019, online: https://www.icao.int/safety/Documents/ICAO_SR_2018_30082018.pdf, 2018.
- [91] ISIKVEREN, A. T., PORNET, C., VRATNY, P. C., and SCHMIDT, M., “Optimization of commercial aircraft using battery-based voltaic-joule/brayton propulsion,” *Journal of Aircraft*, vol. 54, no. 1, pp. 246–261, 2017.
- [92] ISO/IEC 15288, “Systems engineering-system life cycle processes,” *ISO, Geneva, Switzerland*, 2002.
- [93] JAAKKOLA, H. and THALHEIM, B., “Architecture-driven modelling methodologies,” in *Proceedings of the 2011 Conference on Information Modelling and Knowledge Bases XXII*, (NLD), p. 97–116, IOS Press, 2011.
- [94] JARVIS THOMSON, J., “The trolley problem,” *Yale Law Journal*, vol. 94, no. 6, p. 5, 1985.
- [95] JOHANSSON, C., *On System Safety and Reliability in Early Design Phases*. PhD thesis, Linköping University, Sweden, 2013.

- [96] JOHANSSON, C., DERELÖV, M., and ÖLVANDER, J., “How to use an optimization-based method capable of balancing safety, reliability, and weight in an aircraft design process,” *Nuclear Engineering and Technology*, vol. 49, no. 2, pp. 404–410, 2017.
- [97] JUNIAC, A. D., “IATA Annual Review 2018.” retrieved July 4, 2019, online: <https://www.iata.org/publications/Documents/iata-annual-review-2018.pdf>, 2018.
- [98] KABIR, S., “An overview of fault tree analysis and its application in model based dependability analysis,” *Expert Systems with Applications*, vol. 77, pp. 114–135, 2017.
- [99] KABIR, S., WALKER, M., and PAPADOPOULOS, Y., “Dynamic system safety analysis in hip-hops with petri nets and bayesian networks,” *Safety science*, vol. 105, pp. 55–70, 2018.
- [100] KAPLAN, S. and GARRICK, B. J., “On the quantitative definition of risk,” *Risk analysis*, vol. 1, no. 1, pp. 11–27, 1981.
- [101] KELLARI, D., CRAWLEY, E. F., and CAMERON, B. G., “Architectural decisions in commercial aircraft from the dc-3 to the 787,” *Journal of Aircraft*, vol. 55, no. 2, pp. 792–804, 2018.
- [102] KELLY, D. L., “Risk analysis of the space shuttle: Pre-challenger bayesian prediction of failure,” tech. rep., Idaho National Laboratory (INL), 2008.
- [103] KIM, J., KWON, K., ROY, S., GARCIA, E., and MAVRIS, D. N., “Megawatt-class turboelectric distributed propulsion, power, and thermal systems for aircraft,” in *2018 AIAA Aerospace Sciences Meeting*, 2018.
- [104] KOMAL, “Fuzzy fault tree analysis for patient safety risk modeling in healthcare under uncertainty,” *Applied Soft Computing*, vol. 37, pp. 942 – 951, 2015.
- [105] KURDJUKOV, A., NATCHINKINA, G., and SHEVTCHENKO, A., “Energy approach to flight control,” in *Guidance, Navigation, and Control Conference and Exhibit*.
- [106] LAM, H. T. and SZETO, K. Y., “Optimization of reliability of network of given connectivity using genetic algorithm,” 2014.
- [107] LAMBREGTS, A., “Integrated system design for flight and propulsion control using total energy principles,” in *Aircraft Design, Systems and Technology Meeting*.
- [108] LAMBREGTS, A., “Vertical flight path and speed control autopilot design using total energy principles,” in *Guidance and Control Conference*.

- [109] LAMMERING, T., *Integration of Aircraft Systems into Conceptual Design Synthesis*. PhD thesis, Institute of Aeronautics and Astronautics (ILR), RWTH Aachen University, 2014.
- [110] LANHAM, C., “Inertia calculation procedure for preliminary design,” tech. rep., AERONAUTICAL SYSTEMS DIV WRIGHT-PATTERSON AFB OH, 1979.
- [111] LEE, H.-J. and LEE, H.-W., “Method for assessing the electric power system reliability of multiple-engined aircraft,” *Journal of Aircraft*, vol. 30, no. 3, pp. 413–414, 1993.
- [112] LEE, P. M., *Bayesian statistics an introduction*. 4th ed.. ed., 2012.
- [113] LEVITIN, G., PODOFILLINI, L., and ZIO, E., “Generalised importance measures for multi-state elements based on performance level restrictions,” *Reliability Engineering & System Safety*, vol. 82, no. 3, pp. 287–298, 2003.
- [114] LIGHTSEY, B., “Systems engineering fundamentals,” tech. rep., DEFENSE ACQUISITION UNIV FT BELVOIR VA, 2001.
- [115] LISCOUET-HANKE, S., *A Model-Based Methodology for Integrated Preliminary Sizing and Analysis of Aircraft Power System Architectures*. PhD thesis, Université de Toulouse, 2008.
- [116] LUXHØJ, J. T., “Probabilistic causal analysis for system safety risk assessments in commercial air transport,” 2003.
- [117] MAHAR, D., FIELDS, W., and READE, J., “Nonelectronic parts reliability data (nprd-2016),” tech. rep., Quanterion Solutions Incorporated, 2015.
- [118] MAIER, M. W., “Architecting principles for systems-of-systems,” *Systems Engineering*, vol. 1, no. 4, pp. 267–284, 1998.
- [119] MANTIS, G. C., *Quantification and Propagation of Disciplinary Uncertainty via Bayesian Statistics*. PhD thesis, Georgia Institute of Technology, 2002.
- [120] MARCO, A. D., DUKE, E., and BERNDT, J., “A general solution to the aircraft trim problem,” in *AIAA Modeling and Simulation Technologies Conference and Exhibit*, 2007.
- [121] MATTINGLY, J. D., HEISER, W. H., and PRATT, D. T., *Aircraft engine design*. American Institute of Aeronautics and Astronautics, 2002.
- [122] MAVRIS, D., DELAURENTIS, D., BANDTE, O., and HALE, M., “A stochastic approach to multi-disciplinary aircraft analysis and design,” in *36th AIAA Aerospace Sciences Meeting and Exhibit*.
- [123] MCKELVIN JR, M. L., *A methodology and tool support for the design and evaluation of fault tolerant, distributed embedded systems*. PhD thesis, UC Berkeley, 2011.

- [124] MENIS, R., DA RIN, A., VICENZUTTI, A., and SULLIGOI, G., “Dependable design of all electric ships integrated power system: Guidelines for system decomposition and analysis,” in *2012 Electrical Systems for Aircraft, Railway and Ship Propulsion*, pp. 1–6, IEEE, 2012.
- [125] METTAS, A., “Reliability allocation and optimization for complex systems,” in *Annual Reliability and Maintainability Symposium. 2000 Proceedings. International Symposium on Product Quality and Integrity (Cat. No.00CH37055)*, pp. 216–221, 2000.
- [126] MEYER, J. F., “Computation-based reliability analysis,” *IEEE Transactions on Computers*, vol. C-25, no. 6, pp. 578–584, 1976.
- [127] MEYER, J. F., “On evaluating the performability of degradable computing systems,” *IEEE Transactions on Computers*, vol. C-29, no. 8, pp. 720–731, 1980.
- [128] MOIR, I., SEABRIDGE, A., and JUKES, M., *System Safety*, book section 4, pp. 119–158. New York: John Wiley & Sons, Incorporated, 2013.
- [129] MORIARTY, D. and JARVIS, S., “A systems perspective on the unstable approach in commercial aviation,” *Reliability Engineering & System Safety*, vol. 131, pp. 197–202, 2014.
- [130] MOSS, T. R., *The reliability data handbook*. New York: ASME Press, 2005.
- [131] NASA, “X-57 Mini-Poster.” retrieved November 16, 2020, online: <https://www.nasa.gov/sites/default/files/atoms/files/x-57-litho-print-v4.pdf>, 2020.
- [132] NASA, “X-57 Technical Papers.” retrieved February 17, 2021, online: <https://www.nasa.gov/aeroresearch/X-57/technical/index.html>, 2021.
- [133] NASA-LARC, “X-57 Maxwell Simplified CRM v.4.4.1.” retrieved June 8, 2020, online: <http://hangar.openvsp.org/vspfiles/408>, 2013.
- [134] NTSB, “Auxiliary power unit battery fire japan airlines boeing 787-8, ja829j,” Incident Report NTSB/AIR-14/01, National Transportation Safety Board, Jan 7, 2013 2013.
- [135] NTSB, “National Transportation Safety Board - Aviation: Data & Stats.” retrieved February 10, 2021, online: https://www.nts.gov/investigations/data/Pages/Data_Stats.aspx, 2017.
- [136] NTSB, “National Transportation Safety Board: 2017 US Civil Aviation Accident Statistics.” retrieved February 10, 2021, online: <https://www.nts.gov/investigations/data/Pages/AviationDataStats2017.aspx>, 2017.

- [137] OZTEKIN, A. and LUXHØJ, J. T., “Hazard, safety risk, and uncertainty modeling of the integration of unmanned aircraft systems into the national airspace,” in *26th Congress of International Council of the Aeronautical Sciences, Anchorage, Alaska*, vol. 1419, 2008.
- [138] PAPADOPOULOS, Y., *Safety-directed system monitoring using safety cases*. Phd thesis, University of York, 2000.
- [139] PAPADOPOULOS, Y., “Model-based system monitoring and diagnosis of failures using statecharts and fault trees,” *Reliability Engineering & System Safety*, vol. 81, no. 3, pp. 325–341, 2003.
- [140] PAPADOPOULOS, Y. and GRANTE, C., “Evolving car designs using model-based automated safety analysis and optimisation techniques,” *Journal of Systems and Software*, vol. 76, no. 1, pp. 77–89, 2005.
- [141] PAPADOPOULOS, Y. and MARUHN, M., “Model-based synthesis of fault trees from matlab-simulink models,” in *2001 International Conference on Dependable Systems and Networks*, pp. 77–82, IEEE.
- [142] PAPADOPOULOS, Y., PARKER, D., and GRANTE, C., “Automating the failure modes and effects analysis of safety critical systems,” in *Eighth IEEE International Symposium on High Assurance Systems Engineering, 2004. Proceedings.*, pp. 310–311, IEEE.
- [143] PAPADOPOULOS, Y., WALKER, M., PARKER, D., RÜDE, E., HAMANN, R., UHLIG, A., GRÄTZ, U., and LIEN, R., “Engineering failure analysis and design optimisation with hip-hops,” *Engineering Failure Analysis*, vol. 18, no. 2, pp. 590–608, 2011.
- [144] PAPATHAKIS, K. V., “Nasa armstrong flight research center distributed electric propulsion portfolio, and safety and certification considerations,” Presentation 20170009874, NASA, Oct 2017.
- [145] PAPATHAKIS, K. V., BURKHARDT, P. A., EHMANN, D. W., and SESSIONS, A. M., “Safety considerations for electric, hybrid-electric, and turbo-electric distributed propulsion aircraft testbeds,” in *53rd AIAA/SAE/ASEE Joint Propulsion Conference*, 2017.
- [146] PATÉ-CORNELL, M., “Uncertainties in risk analysis: Six levels of treatment,” *Reliability Engineering & System Safety*, vol. 54, no. 2, pp. 95 – 111, 1996. Treatment of Aleatory and Epistemic Uncertainty.
- [147] PATTERSON, M. D. and BORER, N. K., “Approach considerations in aircraft with high-lift propeller systems,” in *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017.

- [148] PORNET, C., GOLOGAN, C., VRATNY, P. C., SEITZ, A., SCHMITZ, O., ISIKVEREN, A. T., and HORNUNG, M., “Methodology for sizing and performance assessment of hybrid energy aircraft,” *Journal of Aircraft*, vol. 52, no. 1, pp. 341–352, 2015.
- [149] PURANIK, T., JIMENEZ, H., and MAVRIS, D., “Energy-based metrics for safety analysis of general aviation operations,” *Journal of Aircraft*, vol. 54, no. 6, pp. 2285–2297, 2017.
- [150] PURANIK, T. G., *A Methodology for Quantitative Data-driven Safety Assessment for General Aviation*. PhD thesis, Georgia Institute of Technology, 2018.
- [151] RAJARAM, D., CAI, Y., CHAKRABORTY, I., and MAVRIS, D. N., “Integrated sizing and optimization of aircraft and subsystem architectures in early design,” *Journal of Aircraft*, vol. 55, no. 5, pp. 1942–1954, 2018.
- [152] RAMIREZ-MARQUEZ, J. E. and COIT, D. W., “Composite importance measures for multi-state systems with multi-state components,” *IEEE Transactions on Reliability*, vol. 54, no. 3, pp. 517–529, 2005.
- [153] RAUSAND, M. and HOYLAND, A., *System reliability theory: models, statistical methods, and applications*, vol. 396. John Wiley & Sons, 2003.
- [154] RAYMER, D., *Aircraft Design: A Conceptual Approach*. AIAA Education Series, 4th ed., 2006.
- [155] RUIJTERS, E. and STOELINGA, M., “Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools,” *Computer Science Review*, vol. 15-16, pp. 29–62, 2015.
- [156] RUTOWSKI, E. S., “Energy approach to the general aircraft performance problem,” *Journal of the Aeronautical Sciences*, vol. 21, no. 3, pp. 187–195, 1954.
- [157] SADRAEY, M. H., *Aircraft Design: A Systems Engineering Approach*. John Wiley & Sons, Ltd, 2012.
- [158] SAGE, A. P. and LYNCH, C. L., “Systems integration and architecting: An overview of principles, practices, and perspectives,” *Systems Engineering*, vol. 1, no. 3, pp. 176–227, 1998.
- [159] SAGLIMBENE, M. S., “Reliability analysis techniques: How they relate to aircraft certification,” in *Annual Reliability and Maintainability Symposium*, pp. 218–222, IEEE, 2009.
- [160] SAROJINI, D., DUCA, R., SOLANO, H. D., CHAKRABORTY, I., BRICENO, S. I., and MAVRIS, D. N., “Framework to assess effects of structural flexibility on dynamic loads developed in maneuvering aircraft,” in *2018 Aviation Technology, Integration, and Operations Conference*, p. 4147, 2018.

- [161] SAROJINI, D., HARRISON, E., and MAVRIS, D. N., “Dynamic environment for loads prediction and handling investigation (delphi),” in *AIAA Scitech 2021 Forum*, 2021.
- [162] SHERRY, L., WANG, Z., KOURDALI, H. K., and SHORTLE, J., “Big data analysis of irregular operations: Aborted approaches and their underlying factors,” in *2013 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1–10, 2013.
- [163] SILVESTRI, A., FALCONE, D., DI BONA, G., FORCINA, A., CERBASO, C., and DURACCIO, V., “A New Method for Reliability Allocation: Critical Flow Method,” in *9th WCEAM Research Papers* (AMADI-ECHENDU, J., HOOHLO, C., and MATHEW, J., eds.), (Cham), pp. 249–261, Springer International Publishing, 2015.
- [164] SUDER, K., “Overview of the nasa environmentally responsible aviation project’s propulsion technology portfolio,” in *48th AIAA/ASME/SAE/ASEE Joint Propulsion Conference & Exhibit*, p. 4038, 2012.
- [165] SURESH, P., BABAR, A., and RAJ, V. V., “Uncertainty in fault tree analysis: A fuzzy approach,” *Fuzzy sets and Systems*, vol. 83, no. 2, pp. 135–141, 1996.
- [166] TELFORD, R. D., GALLOWAY, S. J., and BURT, G. M., “Evaluating the reliability & availability of more-electric aircraft power systems,” in *2012 47th International Universities Power Engineering Conference (UPEC)*, pp. 1–6, Sep. 2012.
- [167] THOMSON, J. J., “Killing, letting die, and the trolley problem,” *The Monist*, vol. 59, no. 2, pp. 204–217, 1976.
- [168] ULRICH, K. T., *Product design and development*. Tata McGraw-Hill Education, 2003.
- [169] VAN DEN BOSSCHE, D., “The a380 flight control electrohydrostatic actuators, achievements and lessons learnt,” in *25th international congress of the aeronautical sciences*, pp. 1–8, 2006.
- [170] VAN DEN HOVEN, M., DE JONG, P., BORST, C., MULDER, M., and VAN PAASSEN, M., *Investigation of Energy Management during Approach - Evaluating the Total Energy-Based Perspective Flight-Path Display*.
- [171] WALKER, M., BOTTACI, L., and PAPADOPOULOS, Y., “Compositional temporal fault tree analysis,” in *International Conference on Computer Safety, Reliability, and Security*, pp. 106–119, Springer, 2007.
- [172] WASHINGTON, A., CLOTHIER, R. A., and WILLIAMS, B. P., “A bayesian approach to system safety assessment and compliance assessment for unmanned aircraft systems,” *Journal of Air Transport Management*, vol. 62, pp. 18 – 33, 2017.

- [173] WHITNEY, D., CRAWLEY, E., DE WECK, O., EPPINGER, S., MAGEE, C., MOSES, J., SEERING, W., SCHINDALL, J., and WALLACE, D., “The influence of architecture in engineering systems,” *Engineering Systems Monograph, MIT Engineering Systems Division, March*, 2004.
- [174] WOODHAM, K. P., GRAYDON, P., BORER, N. K., PAPATHAKIS, K. V., STOIA, T., and BALAN, C., “Fueleap model-based system safety analysis,” in *2018 Aviation Technology, Integration, and Operations Conference*, 2018.
- [175] WROBLEWSKI, G. E. and ANSELL, P. J., “Mission analysis and emissions for conventional and hybrid-electric commercial transport aircraft,” *Journal of Aircraft*, vol. 56, no. 3, pp. 1200–1213, 2019.
- [176] YINGKUI, G. and JING, L., “Multi-state system reliability: A new and systematic review,” *Procedia Engineering*, vol. 29, pp. 531–536, 2012.
- [177] YOUN, B. and WANG, P., “Bayesian reliability based design optimization under both aleatory and epistemic uncertainties,” in *11th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference*, 2006.
- [178] ZAGALSKY, N., “Aircraft energy management,” in *11th Aerospace Sciences Meeting*.

VITA

Mayank Bendarkar hails from Pune, Maharashtra, India. He received his Bachelor and Master of Technology (B.Tech + M.Tech) in Aerospace Engineering in an integrated 5-year program from the Indian Institute of Technology, Bombay in 2014. While there, he volunteered as a student mentor to help first year undergraduate students, was a part of the IIT-B placement cell which maintains relations with companies to aid the on-campus hiring process of over 1500 students, and worked for Avanti Fellows - an organization helping underprivileged kids get access to quality education. He joined the Aerospace Systems Design Lab (ASDL) at Georgia Institute of Technology in January 2015, where he obtained his M.S. in Aerospace Engineering in 2017 and Ph.D. in Aerospace Engineering in May 2021. While at ASDL, he worked as a senior graduate researcher on numerous industry (UTRC, Safran, Toyota TRC) as well as government (FAA, NASA) funded research projects. He has also served as the head TA of the lab from 2017-2018. He is the recipient of the AIAA William T. Piper, Sr. General Aviation Systems Graduate Award 2020 and is a member of the American Institute of Aeronautics and Astronautics (AIAA). In his free time, he can be found hiking the nearby woods or playing video games.