

**IDENTIFICATION OF EMERGENT OFF-NOMINAL
OPERATIONAL REQUIREMENTS DURING
CONCEPTUAL ARCHITECTING OF THE MORE
ELECTRIC AIRCRAFT**

A Thesis
Presented to
The Academic Faculty

by

Michael James Armstrong

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

Georgia Institute of Technology
December 2011

**IDENTIFICATION OF EMERGENT OFF-NOMINAL
OPERATIONAL REQUIREMENTS DURING
CONCEPTUAL ARCHITECTING OF THE MORE
ELECTRIC AIRCRAFT**

Approved by:

Professor Dimitri Mavris,
Committee Chair
School of Aerospace Engineering
Georgia Institute of Technology

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

Professor Vitali Volovoi
School of Aerospace Engineering
Georgia Institute of Technology

Mr. Mat French
Rolls-Royce/LibertyWorks®:
Integrated Power Systems
Rolls-Royce North America

Professor Brian German
School of Aerospace Engineering
Georgia Institute of Technology

Date Approved: November 3, 2011

*To my family and my faith:
Invaluable sources of support and motivation.*

PREFACE

The earliest conception of this work came from a discussion I had in April of 2007. I had just spent that last six months with a group of students grappling with the design challenges associated with the slow transition towards a new paradigm in aircraft subsystems design. The ‘More Electric’ aircraft wasn’t a new concept. However, recent traction towards the integration of electrical technologies led the Energy Optimized Aircraft and Equipment Systems Program Committee (EOASYS) from the AIAA to sponsor a “Grand Challenge.” A handful of students from our lab were tasked to explore design oriented solutions towards the development and evaluation of novel aircraft vehicle systems.

What proceeded was one of the most formative experiences of my academic career. Our team was deluged by the magnitude of this integrative ‘nightmare.’ The physical complexity associated with electrifying aircraft subsystems was dizzying enough. While the implementation of ‘more electric’ concepts are attractive in some respects, the jury was still out considering improvements at the system level. Any promised benefits seemed to lose their distinction when considering all of the unannotated side effects. This challenge was compounded by the organizational complexity of industry players, a fundamental need to avoid programmatic risk, large certification question marks, and unknown impacts on aircraft maintenance operations.

Elusive as this challenge was, our team did come to see some clarity. The status quo of traditional aircraft vehicle systems decomposition was under fire. A dramatically different architecture concept demanded a dramatically new method for development and design. A physical and disciplinary decomposition based on the ATA Chapter decomposition began to be supplanted by a focus on the functional

interdependencies of aircraft technologies.

Needless to say, six months was insufficient time to solve all of the problems associated with revolutionary subsystem architecture design and evaluation. However, we made a meager start. And as with all good research, the more questions we felt we answered, the more questions arose. And this leads me back to spring of 2007.

Our team had just presented to the External Advisory Board at the Aerospace Systems Design Laboratory. The questions were pointed and the feedback was encouraging. However, one comment stood out in my mind regarding architecture sizing. While at the reception following the presentation, an experienced and particularly interested engineer asked rhetorically, “What actually sizes an aircraft component?” Before waiting for a response he proceeded to the effect, “***It’s not what you want the component to do, it’s what the component has to do when the system is doing what you don’t want it to do.***”

This anecdote became the essence of my research for the next few years. What followed were forays into systems engineering: optimization, robust design, scenario based design, reliability theory, system safety analysis... What is a component actually tasked to do and how does one systematically identify this for non-conventional architecture concepts? How can one avoid biasing the selection of an architecture concept by defining or applying requirements in an architecture specific manner? What emerged was a new perspective.

This thesis represents my humble endeavor to provide insights towards these lofty and imposing interrogatories. I have benefited much from the experience and insights of others. And there is still much to be accomplished towards managing the impacts of complexity during architecture definition. However, I hope this work incites appropriate deference to off-nominal requirements early in the exploratory design process.

ACKNOWLEDGEMENTS

I would first like to acknowledge the support of my advisor, Prof. Dimitri Mavris. I am indebted to him for the doors which have been opened to me through his support and guidance. The opportunities he has afforded me have helped me to grow as a student, a scholar, a member of industry and academia, and as an individual. I am grateful for the freedom he gave me to learn to excel on my own, and the experience, example, and counsel he provided to ensure that I did.

Thanks also goes to my committee for their thoughtful direction and correction. This work has greatly benefited from proponents who I trust to give honest feedback and constructive criticism. Special thanks to Dr. Elena Garcia for her continual oversight and patient mentoring.

I would also like to thank the Rolls-Royce and the Integrated Power Systems Team. The relationships I formed here afforded indispensable practical perspectives towards this work and great opportunities for the future. Mr. Mat French deserves specific recognition. I appreciate his consistent confidence and attentive collaboration.

Additional thanks goes to members of the EOASYS Program Committee in the AIAA under whose auspices this work was conceived. The interactions I had with this committee, from our “Grand Challenge” to the TEOS Forum, have changed the way I look at the aerospace industry and aircraft design.

Finally, I would like to thank all those who contributed to my education, both in and out of the classroom. I would like to recognize the faculty at the Georgia Institute of Technology and my fellow students from the Aerospace Systems Design Laboratory. I have benefited greatly from the educational experiences I was provided and extend my deepest appreciation for those who made these possible.

TABLE OF CONTENTS

DEDICATION	iii
PREFACE	iv
ACKNOWLEDGEMENTS	vi
LIST OF TABLES	xi
LIST OF FIGURES	xiv
LIST OF SYMBOLS	xx
LIST OF ACRONYMS	xxiv
SUMMARY	xxviii
I THESIS OVERVIEW	1
II MOTIVATION	4
2.1 Aircraft Systems	4
2.2 Future Electrical Power Demands	10
2.3 More Electric Aircraft (MEA)	12
2.3.1 Current MEA Research	18
2.4 Design Outsourcing	20
2.5 The New Aircraft Systems Integration Paradigm	24
2.5.1 Aircraft Subcontractor ‘Electrification’	25
2.6 Motivation Overview	29
III REQUIREMENTS DEFINITION FOR VEHICLE SYSTEMS	31
3.1 Aircraft Conceptual Design	32
3.2 Conceptual Architecting	36
3.2.1 Architecture	37
3.2.2 Combinametric Complexity	42
3.3 Requirements Definition	46
3.4 Emergent Requirements	48

3.5	Thesis Objectives	50
IV	SIZING CRITICAL EMERGENT REQUIREMENTS	52
4.1	Time Dependence	54
4.1.1	Unit Level Time Dependence	55
4.2	Operating Mode Dependence	65
4.2.1	Scenario Based Design	66
4.2.2	Traditional Aircraft Operating Mode Identification	78
4.2.3	Load Shedding and Performance Degradation	85
4.3	Reliability/Safety/Criticality Dependence	88
4.3.1	Safety and Reliability	89
4.3.2	Aircraft Level Criticality Requirements	94
4.3.3	Allocation of Safety and Reliability Requirements	97
4.3.4	System Safety Assessments	114
4.4	Emergent Requirements Overview	123
V	METHOD	127
5.1	Continuous Functional Hazard Assessment	129
5.1.1	Functional Hazard Relationships Definition	138
5.2	PSSA Continuous Expansion	143
5.2.1	Proportional Function Loss	143
5.2.2	System Level Implementation	150
5.3	Architecture Definition	152
5.3.1	System Level Example	158
5.4	Method Overview	168
VI	HYPOTHESIS TESTING	172
6.1	Hypothesis Testing	173
6.2	Hypothesis 1 Testing	174
6.3	Hypothesis 2 Testing	176
6.4	System of Interest	177

6.4.1	Electric Technologies	179
6.4.2	Proof of Concept Architectures	184
6.5	Function/Hazard Relationships	187
6.5.1	Thrust Loss Hazards	192
6.6	System Models	207
6.6.1	Electrical	208
6.6.2	Hydraulic	211
6.6.3	Pneumatic	213
6.6.4	Powerplants	221
6.6.5	System Reliabilities	228
6.7	Optimization Formulation	237
6.8	Hypothesis Testing Overview	242
VII	ANALYSIS RESULTS	244
7.1	Hazard Probability and Performance Risk	246
7.1.1	Function Specific Hazard Probability	252
7.2	Hazard Correlation	257
7.3	Unit Level Importance	263
7.3.1	Reliability Based Unit Importance	263
7.3.2	Capability Based Unit Importance	270
VIII	RESULTS SUMMARY	278
8.1	Hypothesis 1 Validation	279
8.2	Hypothesis 2 Validation	280
IX	CONCLUDING REMARKS	283
9.1	Significant Contributions	286
9.2	Ancillary Research Opportunities	289
APPENDIX A	SCENARIO BASED STRATEGIC PLANNING AND HUMAN- COMPUTER INTERACTION	292

APPENDIX B	SCENARIO BASED REQUIREMENTS ENGINEERING TOOLS	295
APPENDIX C	SCENARIO BASED OBJECT-ORIENTED ANALYSIS/DESIGN TOOLS	305
APPENDIX D	ALGORITHM FOR DETERMINING STATISTICAL SIGNIFICANCE OF UNIT FAILURES	313
APPENDIX E	ANALYTICAL HAZARD FUNCTION PROPAGATION	320
APPENDIX F	ADJACENCY MATRICES FOR VEHICLE SYSTEMS ARCHITECTURES	340
APPENDIX G	OPTIMIZATION ROUTINE FOR CONVENTIONAL ARCHITECTURE	344
APPENDIX H	FUNCTION CALL FOR OPTIMIZATION OF 'ALL-ELECTRIC' ARCHITECTURE	354
APPENDIX I	HAZARD PROBABILITY FOR ALL APPLIED FUNCTIONAL HAZARDS FOR THE CONVENTIONAL ARCHITECTURE	359
APPENDIX J	HAZARD PROBABILITY FOR ALL APPLIED FUNCTIONAL HAZARDS FOR THE 'ALL-ELECTRIC' ARCHITECTURE	364
APPENDIX K	FUNCTIONAL HAZARD CORRELATION FOR THE CONVENTIONAL ARCHITECTURE	369
APPENDIX L	FUNCTIONAL HAZARD CORRELATION FOR THE 'ALL-ELECTRIC' ARCHITECTURE	371
APPENDIX M	CUMULATIVE COMPONENT CRITICALITY IMPORTANCE FOR THE CONVENTIONAL AND 'ALL-ELECTRIC' ARCHITECTURES	372
APPENDIX N	CUMULATIVE COMPONENT CAPABILITY IMPORTANCE FOR THE CONVENTIONAL AND 'ALL-ELECTRIC' ARCHITECTURES	375
REFERENCES		382

LIST OF TABLES

1	Aircraft Systems Decomposition [210]	8
2	Comparison of Aircraft Secondary Power Distribution Systems [15]	16
3	Distribution of Externalized Design Activity (1995 to 2005): Sample Means Budget Percentage [196]	23
4	Notional Morphological Analysis for Platform Level Functional Fulfillment	42
5	Number of Potential Combinations of Solution Considering Redundancy	43
6	Notional Morphological Analysis for Derived Functional Fulfillment as Required by Functions from Table 4	45
7	Uses for Scenarios in Various Fields [113]	68
8	CREWS Scenario Classification Categories [251]	73
9	Evaluation of Scenario Based Design Tools for the Identification of Emergent Operational Requirements w.r.t CREWS Scenario Classification Views [251]	75
10	Alternative Missions for the AV-8B Harrier II [1]	79
11	Liscouët-Hanke Operating Mode Degradations [190]	84
12	Probability Relationships for Failure and Reliability [243]	91
13	AC 25:1309-1A Failure Classifications [95]	95
14	SAE ARP4754 Failure Classifications [272]	95
15	MIL-STD-882D Mishap Categories [72]	96
16	Overview of Non-Discipline Specific Tools, Methods, and Techniques List Supplied by Kritzingner [177]	101
17	Means for Reliability Allocation and Analysis	102
18	Descriptions of Deviation Guide Words for HAZOP [168]	103
19	Root Cause Identification Methods as Reviewed by the DOE [71]	106
20	Fault Tree Logic from Andrews and Moss [10]	118
21	Fault Event Objects from Andrews and Moss [10]	119
22	Node Failure Probabilities for the Notional System in Figure 46	165
23	Architecture Sizing Shedding Heuristics	175

24	Conventional Architecture Allocation Variables	188
25	‘All-Electric’ Architecture Allocation Variables	189
26	Hazards for Conventional and ‘All-Electric’ Architecture Concepts . .	191
27	Unit Models (Capability Transfer Functions)	207
28	Electrical Distribution Capability Transfer Functions	209
29	Electrical Transformation Capability Transfer Functions	211
30	Hydraulic Capability Transfer Functions	212
31	Pneumatic Capability Transfer Functions	214
32	Bootstrap ACM System of Equations	219
33	PowerPlant Capability Transfer Functions	222
34	Brayton Cycle APU System of Equations	227
35	Hazards for Conventional and ‘All-Electric’ Architecture Concepts . .	232
36	Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	249
37	Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture	251
38	Takeoff and Cruise Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	253
39	Take-off and Linear Approx. Functional Hazard Probability Assess- ment for the ‘All-Electric’ Vehicle Systems Architecture	255
40	Functional Hazard Correlations for Takeoff Operation	261
41	Units of Highest Importance for the Conventional Architecture	268
42	Units of Highest Importance for the ‘All-Electric’ Architecture	268
43	Units of Highest Capability Importance for the Conventional Architec- ture	276
44	Units of Highest Capability Importance for the ‘All-Electric’ Architecture	276
45	Continuous Off-Nominal Architecture Performance Metrics	287
46	Convention for Unit Requirements Relationships Relationship Types .	321
47	Information Communicated with Graph Edges from Figure 109	330
48	Propagation of Function/Hazard Relationship for the Edges in Figure 110a.	334

49	Information Communicated with Graph Edges from Figure 112	336
50	Information Communicated with Graph Edges from Figure 113	339
51	Conventional Architecture Adjacency Matrix Indices given by Allocation Variables	340
52	Conventional Architecture Adjacency Matrix Indices Equal to One . .	341
53	‘All-Electric’ Architecture Adjacency Matrix Indices given by Allocation Variables	342
54	‘All-Electric’ Architecture Adjacency Matrix Indices Equal to One . .	343
55	Take-off Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	360
56	Cruise Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	361
57	Linear Approximation Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	362
58	Step Approximation Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture	363
59	Take-off Functional Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture	365
60	Cruise Functional Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture	366
61	Linear Approximation Functional Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture	367
62	Step Approximation Functional Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture	368
63	Conventional Functional Hazard Correlations	370
64	‘All-Electric’ Functional Hazard Correlations	371

LIST OF FIGURES

1	Overview of Thesis Development and Testing	2
2	Trend in Commercial Aircraft Power Demand [15]	10
3	Commercial Aircraft Power per Seat for Conventional, More Electric, and New Aircraft Concepts [205]	11
4	Power and Thermal Management Trends and Challenges [217]	12
5	MOET Architecture Evaluation Process [154]	19
6	Typology of Technological Systems and the Transition from Conventional to More Electric Aircraft Architectures [134]	24
7	Wheelwright-Clark Product Development Process	34
8	Moir and Seabridge Conceptual Design Process	34
9	Harel's Magic Square of System Development	53
10	Comparison of General Dynamics and Torenbeek Equations for Fuel System Weight Estimation for Airplanes with Self-sealing Tank from Roskam [253]	57
11	Tradeoff Between Predictive Capability, Model Flexibility, and Model- ing Difficulty for Vehicle Systems Modeling Methods	64
12	The Compete Preliminary Air-to-Air Fighter Constraint Diagram from Mattingly [201]	81
13	Liscouët-Hanke Bleedless Architecture Electric Power System Genera- tor Contributing Power Requirements from Technical Loads (TL), En- vironment Control System (ECS), Commercial Control System (CCS), and Wing Ice Protection System (WIPS) [190]	83
14	Low, Medium, and High Risk in Terms of Hazard and Probability of Occurrence	89
15	Adapted from EMMA's [European Airport Movement Management by A-SMGCS (Advanced - Surface Movement, Guidance and Control systems)] Hazard Impact Assessed at the Boundary of Scope [231]	92
16	Relationship Between Contributory Hazards & Adverse Effects [96]	93
17	SAE ARP 4754 Safety Assessment Process Model [272]	98
18	System Safety Analysis During the Design Process [61]	99
19	Process for Structure What-If Techniques [197]	105

20	Notional Causal Chart for a Fire from Rooney [252]	108
21	Expanded Risk Bow-Tie [284]	109
22	Operational Safety Assessment Process Overview from Hammer et. al. [117]	110
23	Functional Hazard Analysis Worksheet from Ericson [90]	113
24	Series and Parallel Components in Reliability Block Diagram	120
25	Conversion of Complex Graph to Minimal Path Sets	122
26	Load Sharing Reliability Structuring	122
27	Interacting Dependence Domains	125
28	SONOMA (Systematic Off-NOM inal Requirements Analysis) . . .	129
29	Perspective Change from Traditional to Taguchi Quality Control . . .	131
30	Notional Representation of Functional Hazard Assessment Result . .	132
31	Notional Representation of Functional Hazard Assessment Result . .	133
32	Notional Relationship Between Hazard Level, Function Failure, and Fault Duration	135
33	Hazard Effect Mitigation for Notional Physical System (A) and Control (B) Failure	136
34	Reduction in Rate of Climb Requirements for loss of engine in FAR 25 [69]	139
35	Effect on performance constraint given a loss of thrust	141
36	Thrust loss hazard relationship as informed by analysis results seen in Figure 35	142
37	Reposing Load Sharing Reliability Block Diagram	145
38	Notional Reliability Curves for Load Sharing Elements	146
39	Load Sharing Reliability of the Functional Group A,B,C with Reliabil- ities as Illustrated in Figure 38	146
40	Notional Function Loss Criticality Curve	148
41	Comparison of Functional Group Reliability from Figure 38 Compared with Functional Criticality Constraint from Figure 40	148
42	Continuous Reliability Assessment/Optimization	149
43	Formatting Propagation of Capabilities	152

44	Notional Flashlight Functional Induction Example [203]	155
45	Types and Requirements Relationships for Systems Architectures . . .	156
46	Notional System Graph for Load Shedding Optimization	159
47	Variable values in equation 13 for the notional system in Figure 46 . .	159
48	Failure Allocation for Load Shedding Optimization with Failure of Node 4 of the System Graph in Figure 46	161
49	System Level Function Failure Probabilities with Optimal Shedding .	166
50	Hazard Probabilities with Optimal Shedding for Hazard Functions H_1 (Equation 17) and H_2 (Equation 18)	167
51	Process Used for Integrating Emergent Operational Requirements Dur- ing Architecture Design, SONOMA	169
52	Focus of the Two Hypothesis Regarding the Application of Load Shed- ding Optimization	174
53	Comparative Baseline Hazard Relationships	176
54	Boundaries of the Business Jet Vehicle Systems Architecture	178
55	Conventional Architecture Diagram	185
56	“All-Electric” Architecture Diagram	186
57	Takeoff Field Length and Balanced Field Length Compositions	194
58	Take Off Field Length for Business Jet with Variation in Thrust Available	197
59	Hazard Associated with the Required TOFL for a Business Jet During Thrust Loss Conditions	198
60	Business Jet Free Body Diagram for Climbing Flight	201
61	Aircraft Range with Variations in Thrust Loss and Fuel Consumed ($alt = 35kft, alt_{max} = 50kft$)	204
62	Range to Landing Field with Variations in Fuel Spent	204
63	Range limitations due to Functional Failures	206
64	Generator Efficiency Relationship	210
65	Rudimentary Hydraulic System [211]	212
66	Cross Flow Heat Exchanger Diagram	215
67	Heat Exchanger Flow Requirements	216
68	Bootstrap ACM System Diagram	217

69	Bootstrap ACM T-S Diagram	218
70	Typical Centrifugal Ram Compressor Map	219
71	Ram Compressor Operating Envelope	220
72	Centrifugal Ram Compressor Transfer Function	221
73	Thrust Specific Fuel Consumption Variation with Flight Conditions .	223
74	Limits to Engine Auxiliary Load Available with Variation in Available Fuel Flow, Altitude, and Mach Number	224
75	Limits to Engine LP Bleed Available with Variation in Available Fuel Flow, Altitude, and Mach Number	225
76	Ideal and Actual Brayton Cycle T-S Diagram Used for APU Modeling	226
77	Maximum Bleed Air Mass Flow Proportion (k_{bleed}) with Input Airflow of $\dot{m}_{in} = 0.2kg/s$	228
78	Transfer Functions for Auxiliary Power Unit Output Capabilities . . .	228
79	Assumed Relationship Between Reliability and Functional Requirement Magnitude	229
80	Reliability Degradation for a Unit with Uniform Reliability	230
81	Reliability of Combined Unit Capabilities with Complex Unit Reliability Structure	233
82	P_n limits for Conventional and ‘All-Electric’ Failure Cases	236
83	Ensuring Validity of Gradient Based Optimization Small Augmentations of the Objective Function	239
84	Means for Determining Optimum Failure Allocation for Unit Failures	241
85	Hazard Probability Constraint	246
86	Comparisons of Risks Introduced by Functional Failures for the Conventional Architecture	254
87	Comparison of Risks Introduced by Functional Failures for the ‘All-Electric’ Architecture	256
88	Correlation Between the Magnitude of System Level Functional Hazards	258
89	Comparison of Functional Hazards with Load Shedding Optimization	259
90	Correlation Between System Functions for Both the Conventional and ‘All-Electric’ Architectures	261

91	Bounds on the Integration Towards Cumulative Risk Importance Identification for the Accessory Gear Box in the Conventional Architecture for Takeoff Functional Hazards	266
92	Risk Importance of the Accessory Gear Box in the Conventional Architecture for Takeoff Functional Hazards	267
93	Shift in System Hazard Probability with 10% Reduction in Peak Steady State AGB Capability for Takeoff Requirements	272
94	Cumulative Component Capability Risk Importance with Varying Backward Finite Difference Derivative Differentials	274
95	Process Used for Integrating Emergent Operational Requirements During Architecture Design, SONOMA	288
96	Schoemaker's Process for Scenario Development in Strategic Planning [260]	293
97	Inquiry-Based Cycle Model for Requirements Analysis [234]	296
98	QOC Diagram Showing Different Navigation Properties [195]	297
99	Process for Formal Scenario Analysis [139]	300
100	Tools for Formal Scenario Analysis [139]	301
101	Task Knowledge Structure for "Taking and X-ray" Johnson [153]	303
102	Notional use-case Model of ATM System [146]	307
103	Harel's Watch State Chart Illustrations [119]	309
104	Interaction Diagram for ATM Cash Withdrawal Operation [146]	311
105	Simple Relationship	322
106	Allocation Relationship	324
107	Combination Relationship	326
108	'Combination' Hazard Relationship for Three Notional Downstream Units	328
109	Combination-Allocation Relationship for Notional System Providing Electrical Power	329
110	Requirements Propagation with Complex Allocations and Combinations	332
111	Function/Hazard Relationships for Edges of the Staggered Combination Graph Depicted in Figure 110a.	333
112	Grouped Allocation-Combination Relationship	337

113	Irreducible Allocation-Combination Relationship	338
114	Normalized Cumulative Risk for Conventional Architecture Units . . .	373
115	Normalized Cumulative Risk for 'All-Electric' Architecture Units . . .	374
116	Cumulative Component Capability Importance Values for Conventional Architecture at Takeoff	376
117	Cumulative Component Capability Importance Values for Conventional Architecture at Cruise	377
118	Cumulative Component Capability Importance Values for 'All-Electric' Architecture at Takeoff	378
119	Cumulative Component Capability Importance Values for 'All-Electric' Architecture at Cruise	379
120	Averaged Cumulative Component Capability Importance Values for the Conventional Architecture	380
121	Averaged Cumulative Component Capability Importance Values for the 'All-Electric' Architecture	381

LIST OF SYMBOLS

$[A]$	System Functional Dependency Adjacency Matrix
α	Thrust Lapse $\left(\frac{T}{T_{SL}}\right)$
β	Weight Lapse $\left(\frac{W}{W_{TO}}\right)$
Δs	Field Length Overhead
η, β	Weibull Parameters
$\lambda(t)$	Failure Rate
\mathcal{I}_k^\square	Cumulative Component Importance
ρ	Functional Hazard Correlation Matrix
θ	Flight Path Angle
ζ_{BR}	Braking Rolling Resistance Parameter
ζ_{TO}	Takeoff Rolling Resistance Parameter
$\{\bar{\alpha}\}$	Vector of Capability Allocation Variables
$\{C\}$	Vector of Unit Capabilities at Downstream Indices
$\{K\}$	Vector of Unit Capability Limits
$\{Op(t)\}$	Vector of Operating Conditions at Time t
$\{X\}$	Vector of Unit Capabilities
${}^R\mathcal{I}_k^\square$	Cumulative Component Risk Based Importance
${}^R I_k^\square$	Component Risk Based Importance

a_{ij}	Adjacency Matrix Functional Mapping Value
alt	Altitude
C_{D0}	Parasitic Drag Coefficient
C_{DR}	Resistance Drag Coefficient
Cap	Unit Design Capabilities
D	Drag
$dist$	Distance to Suitable Landing Location
$f(\{X\}, \{Op\})$	Unit Capability Transfer Function
$f(t)$	Probability Density
F_F	Probability of Functional Failure
F_S	Probability of System Failure
F_F	Probability of Function Level Failure
F_S	Probability of System Level Failure
g_0	Gravitational Constant
h	Altitude
H_F	Functional Hazard
H_S	System Level Hazard
h_{obs}	Obstacle Height
I_k^B	Birnbaum's Component Importance of Unit k
I_k^C	Component Criticality Importance of Unit k

I_k^{CC}	Component Capability Importance of Unit k
k_1, k_2	Induced Drag Constants
L	Lift
M	Mach Number
n	Load Factor
P_s	Specific Excess Power, $\left(\frac{d}{dt} \left(h + \frac{V^2}{2g_0}\right)\right)$
q	Dynamic Pressure, $\left(\frac{1}{2}\rho V^2\right)$
R	Range
$R(t)$	Survival Function
R_{FFO}	Cumulative Overall Functional Failure Risk
R_{FFU}	Cumulative Undesirable Functional Failure Risk
R_{FF}	Functional Failure Risk
R_F	Function Level Reliability
R_{req}	Range Required
R_{SFO}	Cumulative Overall System Failure Risk
R_{SFU}	Cumulative Undesirable System Failure Risk
R_{SF}	System Failure Risk
R_{SL}	System Level Reliability
S	Sing Planform Area
s_g	Ground Roll Distance

s_R	Rotation Distance
s_{BR}	Braking Roll Distance
s_{CL}	Obstacle Clearance Distance
s_{Tot}	Maximum Total Takeoff Distance
s_{TR}	Transition Distance
T_{SFC}	Thrust Specific Fuel Consumption
T_{SL}	Installed Thrust at Sea level
V	Velocity
V_{dec}	Decision Speed
V_{fail}	Failure Speed
V_{safety}	Safety Speed
W_{TO}	Takeoff Gross Weight

LIST OF ACRONYMS

- ACM** Air Cycle Machine
- AEA** All Electric Aircraft
- AFRL** Air Force Research Laboratory
- AGB** Accessory Gear Box
- AIAA** American Institute of Aeronautics and Astronautics
- APU** Auxiliary Power Unit
- ARP** Aerospace Recommended Practice
- ATA** Air Transport Association
- BFL** Balanced Field Length
- CCS** Commercial Control System
- CON OPS** Concept of Operations
- CREWS** Cooperative Requirements Engineering With Scenarios
- DLR** Deutsche Zentrum für Luft- und Raumfahrt
- DoD** Department of Defense
- DOE** Department of Energy
- ECS** Environment Control System
- EHA** Electro-Hydraulic Actuator

ELMS Electric Load Management System

EMA Electro-Mechanical Actuation

EMM External Mitigation Means

EMP Electric Motor Pump

EOASYS Energy Optimized Aircraft and Equipment Systems

ESG Engine Starter Generator

ETOPS Extended Operations

FAA Federal Aviation Administration

FAA AC FAA Advisory Circular

FAR Federal Aviation Regulation

FHA Functional Hazard Analysis

FMEA Failure Mode & Effects Analysis

FMECA Failure Mode Effects and Criticality Analysis

FMRI Final Mishap Risk Index

FSA Formal Scenario Analysis

FTA Fault Tree Analysis

HAZAN Hazard Analysis

HAZOP Hazard and Operability Studies

HCI Human Computer Interaction

IBCM Inquiry-Based Cycle Model

IMM Internal Mitigation Means

IMRI Initial Mishap Risk Index

INVENT Integrated Vehicle Energy Technology Demonstration

JAA Joint Aviation Authorities

MBSE Model Based Systems Engineering

MEA More Electric Aircraft

MIL-STD Military Standard

MOET More Open Electric Technologies

MTTR Mean Time to Repair

OEM Overall Equipment Manufacturer

OOA&D Object-Oriented Analysis/Design

PCU Power Converter Unit

POA Power Optimized Aircraft

PSSA Preliminary Systems Safety Analysis

QOC Questions-Options-Criteria

RBD Reliability Block Diagram

SAE Society of Automotive Engineers

SONOMA Systematic Off-Nominal Requirements Analysis

SWIFT Structured What-If Technique

SyRelAn System Reliability Analysis

TA&M Task Analysis and Modeling

TL Technical Loads

TOFL Takeoff Field Length

UML Unified Modeling Language

WIPS Wing Ice Protection System

SUMMARY

Increases in power demands and changes in the design practices of overall equipment manufacturers has led to a new paradigm in vehicle systems definition. The development of unique power systems architectures is of increasing importance to overall platform feasibility and must be pursued early in the aircraft design process. Many vehicle systems architecture trades must be conducted concurrent to platform definition. With an increased complexity introduced during conceptual design, accurate predictions of unit level sizing requirements must be made. Architecture specific emergent requirements must be identified which arise due to the complex integrated effect of unit behaviors.

Off-nominal operating scenarios present sizing critical requirements to the aircraft vehicle systems. These requirements are architecture specific and emergent. Standard heuristically defined failure mitigation is sufficient for sizing traditional and evolutionary architectures. However, architecture concepts which vary significantly in terms of structure and composition require that unique failure mitigation strategies be defined for accurate estimations of unit level requirements.

Identifying of these off-nominal emergent operational requirements require extensions to traditional safety and reliability tools and the systematic identification of optimal performance degradation strategies. Discrete operational constraints posed by traditional Functional Hazard Assessment (FHA) are replaced by continuous relationships between function loss and operational hazard. These relationships pose the objective function for hazard minimization. Load shedding optimization is performed for all statistically significant failures by varying the allocation of functional

capability throughout the vehicle systems architecture.

Expressing hazards, and thereby, reliability requirements as continuous relationships with the magnitude and duration of functional failure requires augmentations to the traditional means for system safety assessment (SSA). The traditional two state and discrete system reliability assessment proves insufficient. Reliability is, therefore, handled in an analog fashion: as a function of magnitude of failure and failure duration. A series of metrics are introduced which characterize system performance in terms of analog hazard probabilities. These include analog and cumulative system and functional risk, hazard correlation, and extensions to the traditional component importance metrics.

Continuous FHA, load shedding optimization, and analog SSA constitute the SONOMA process (**S**ystematic **O**ff-**N**ominal **R**equirements **A**nalysis). Analog system safety metrics inform both architecture optimization (changes in unit level capability and reliability) and architecture augmentation (changes in architecture structure and composition). This process was applied for two vehicle systems concepts (conventional and ‘more-electric’) in terms of loss/hazard relationships with varying degrees of fidelity.

Application of this process shows that the traditional assumptions regarding the structure of the function loss vs. hazard relationship apply undue design bias to functions and components during exploratory design. This bias is illustrated in terms of inaccurate estimations of the system and function level risk and unit level importance. It was also shown that off-nominal emergent requirements must be defined specific to each architecture concept. Quantitative comparisons of architecture specific off-nominal performance were obtained which provide evidence to the need for accurate definition of load shedding strategies during architecture exploratory design.

Formally expressing performance degradation strategies in terms of the minimization of a continuous hazard space enhances the system architects ability to accurately

predict sizing critical emergent requirements concurrent to architecture definition. Furthermore, the methods and frameworks generated here provide a structured and flexible means for eliciting these architecture specific requirements during the performance of architecture trades.

CHAPTER I

THESIS OVERVIEW

A complete overview of the work presented in this thesis is outlined in figure 1. This image outlines the structure adopted in the composition of this thesis towards the development and testing of hypotheses.

The second and third chapters of this thesis begin by reviewing the motivation for this work. This includes a historical perspective of advances made with respect to the ‘more-electric’ aircraft and a review of the technological and organizational implications of increasing the technical complexity of the aircraft vehicle systems. The need to introduce innovative power systems concepts during platform level conceptual design requires a systematic means for identifying sizing critical emergent requirements early in the design process.

The fourth chapter begins to explore the sources of emergent requirements in terms of different aspects of architecture complexity. Time, operating mode, and safety and reliability dependence are specifically reviewed. It is observed that off-nominal operating scenarios pose sizing critical requirements for aircraft vehicle systems and require consideration of all of these behavioral aspects of complexity. The objective for the thesis is therefore to provide a risk based means for identifying off-nominal operational requirements which can be rapidly deployed during conceptual design.

Chapter five poses the exploration of off-nominal emergent requirements in terms of a process which expands traditional safety and reliability tools and systematic load shedding optimization. In so doing the hypotheses are generated. The first addresses the benefits for load shedding optimization during exploratory design. The second considers the impact of inaccurate estimations of the function loss vs. hazard

Ch. II & III	<p>Obs: Advances in electrical technology has lead to major increases in the amount of electric power that must be made available on military and commercial platforms.</p> <p>Obs: Vehicle systems architecture trades greatly increase the combinametric complexity of the aircraft platform concept design space.</p> <p>Motivation: The definition and validation of innovative power systems concepts by subsystem integrators is becoming more critical during the earlier phases of the design process.</p> <p>Objective: Develop tools and techniques for systematic identification of emergent requirements during concept architecture validation.</p> <p>RQ: What factors contribute to the operational/behavioral complexity and lead to emergent requirements for aircraft vehicle systems?</p>	<p>Obs: Increased technological risk has changed the way aircraft are designed. More responsibility on the subsystem manufacturers to provide innovative integrated subsystem solutions.</p>
	<p>RQ: With varying vehicle systems architecture, how do sizing critical operating modes vary?</p> <p>Obs: Off-nominal operating modes have the potential to present significant and architecture specific increases to unit level requirements.</p> <p>Obs: Load shedding and performance degradation strategies are traditionally either predefined or tacitly identified during concept definition.</p> <p>Obs: Traditional scenario based methods prove insufficient for specifying the operations impact of off-nominal sizing cases.</p>	<p>RQ: With varying vehicle systems architecture, how do safety/reliability requirements vary?</p> <p>Obs: Safety and reliability requirements are expressed as probability constraints on the behavioral space at the platform level.</p> <p>Obs: Traditional methods for hazard identification and system assessment assign static or discrete hazard value to loss or excess of a function.</p> <p>Obs: The traditional approach to hazard assessment generalizes expected result of failure, avoiding exploration of the scenario tree.</p>
Ch. IV	<p>RQ: How does time dependence effect vehicle systems architecture trades?</p> <p>Obs: Time governs the attributes of all energy storage units.</p> <p>Obs: Power system transient requirements are emergent.</p> <p>Obs: Reliability of system components is time dependent</p>	<p>RQ: How can performance degradation related requirements be identified and explored concurrent to conceptual architecture trades?</p> <p>Objective: Provide systematic risk and reliability based means for the identification of off-nominal operational requirements which can be rapidly implemented during concept architecture trades</p>
Ch. V	<p>Hypothesis1: Optimizing load shedding strategies yields more accurate predictions of unit level requirements than heuristically defined performance degradation during the exploratory design of revolutionary vehicle systems architecture.</p> <p>Method1: The severity of system level failures are expressed continuously in terms of the magnitude of the functional failure.</p> <p>Result: Continuous Hazard Probability Comparison</p>	<p>Hypothesis2: Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements.</p> <p>Method2: Optimal failure allocation is performed for statistically significant failure cases to ensure adequate coverage of off-nominal requirements.</p> <p>Result: Hazard Correlation Comparison</p>
Ch. VI & VII	<p>Method3: Probability of systems failure is expressed in terms of the magnitude of functional loss (% functional failure).</p> <p>Result: Cumulative Component Capability Importance</p>	<p>Method3: Probability of systems failure is expressed in terms of the magnitude of functional loss (% functional failure).</p> <p>Result: Cumulative Component Capability Importance</p>

Figure 1: Overview of Thesis Development and Testing

relationship. Three methods are introduced which constitute the Systematic Off-Nominal Requirements Analysis (SONOMA) process: Continuous Functional Hazard Assessment, Load Shedding Optimization, Analog System Safety Assessment.

Chapter six gives an overview of how the hypotheses were tested. The function/-hazard relationships used for hypothesis validation are introduced for two aircraft vehicle systems concepts: conventional and 'all-electric'. The concept architectures are defined and structured for load shedding optimization. Unit level capability transfer functions are defined for each of the units in both architectures. Finally, the optimization process is formalized. This includes the definition of all statistically significant failure cases and the process for identifying optimal capability allocation.

Chapter seven gives the results of this evaluation in terms of analog system safety assessment metrics. These metrics are intended to inform both architecture augmentation and optimization. Metrics introduced in this chapter inform architecture augmentation and include system and function level hazard probabilities, analog and cumulative risk, and hazard correlation. Analog extensions of Birnbaum's and component criticality importance inform architecture optimization. An additional importance metric is also introduced which assesses unit level importance in terms of variations in unit capability.

The results are summarized in terms of their connections to the overall thesis objective and motivations in chapters eight and nine. Additional comments are also made regarding the significant contributions and potential future research opportunities related to this work.

CHAPTER II

MOTIVATION

With significant advances in aircraft electrical technologies in the last century the demand for electrical power on commercial and military platforms is increasing dramatically. Many international research efforts have addressed the implication of electrical technologies. Conventional systems technologies are perceived to be approaching the limits of their performance potential and electrical technologies retain promise for future growth. While benefits in take off gross weight are uncertain, electrical technologies have the potential to improve maintenance, reliability, and efficiency.

Addressing the architectural complexity of aircraft power systems during conceptual design poses difficult issues in the generation and deployment of requirements. This chapter discusses the motivations for this thesis and the current environment for vehicle systems design. First, it addresses what is meant by classifying the terms platform, system, unit, etc. Second, it introduces the increased power demands seen by the industry and reviews the historical developments in vehicle systems. Third, it explores the trend towards design outsourcing as can be found in the literature. Lastly, it looks at the change in responsibility of the subsystem contractors. This lays the stage to further explore how architectural complexity effects the ability of the aircraft designer to generate and manage unit level requirements during conceptual architecting as discussed in the next chapter.

2.1 Aircraft Systems

There are many definitions of the term “system.” The International Council on Systems Engineering defines a system as:

“a collection of components organized to accomplish a specific function or set of functions [126].”

The Reliability Engineering Design Handbook is more detailed in outlining types of responsibilities and components involved in a system. They describe a system as:

“a composite of equipment and skills and techniques capable of performing or supporting an operational role, or both. A complete system includes all equipment, related facilities, materials, software, services, and personnel required ... to be considered self-sufficient in its intended operational environment [163].”

Although the general definitions of a system denote various elements with inter-relationship fulfilling some need, further qualification is necessary. The first qualification which must be made is the system’s complexity. Complexity is a measure or property which greatly impacts the difficulty of system definition, evaluation, and design [59]. Crutchfield defined complexity as the measure of difficulty in predicting the optimal forecasts of a system [58]. The more information necessary to generate optimal performance of a system, the higher the statistical complexity. Given the intractability of the aircraft systems architecture design space, it can be safely classified as a complex system. Wilkins’ definition of a complex systems applies to aircraft vehicle systems. This definition states:

“a system which has heterogeneous smaller parts, each carrying out some specialized function, not necessarily exclusively, which then interact in such a way as to give integrated responses [59].”

Complex systems, like military and commercial aircraft, are modeled and envisioned with multiple levels of abstraction in order to manage design scope. Traditional

systems engineering involves a process of decomposition. This process, although useful for the sake of complexity, provides difficulty due to the standardization of assumptions and a fixed conception, which may limit innovative possibilities.

The second system qualifier concerns the level of control the engineer has over unit level attributes to drive performance. Different types of systems require different approaches and tools during the design process. Both an airplane and the world wide web fit the definition of a system. However, each has a vastly different form and must be approached in different ways. Thus, a distinction should be made between complex monolithic systems and complex systems of systems.

A monolithic system, is comprised of components which are intended to operate strictly within the context of the system and which are not intended to be used independently of the system as a whole [198]. An example of a monolithic system is a personal computer. Many elements of this complex system can be qualified as systems on their own (hard drive, graphics card, keyboard, mouse, etc.) and they all operate to fulfill some task within the overall system. The system (computer) is comprised of system elements (mouse, hard drive, etc.). However, each of these system elements is intended to be used only within the context of the personal computer system. The monitor, for example, could be described as a complex system independently, but it does not fulfill its intended function unless it is integrated with the other elements of the PC. Therefore, the computer is not a system of systems but a monolithic system consisting of exchangeable complex elements. The operation of the system relies on the performance of the individual system elements and the system elements are intended to perform functions within the framework defined by a system.

A system of systems, on the other hand, consists of a group of autonomous elements which can and do operate to fulfill functions independently from the conglomerate system [198]. The elements within a system of systems operate to fulfill specific functions which are not necessarily directly determined by the system of systems.

Some have gone so far as to described a system of systems as a physically distributed group of elements which interoperate by means of central or distributed management [267, 84]. This indicates that the elements within the system can be and are often geographically distributed. The Internet, the US Missile Defense Network, and the World Wide Air Transportation Network are excellent examples of systems of systems. The elements within these systems fulfill functions (often multiple elements fulfilling the same function) imposed/derived independently from the system as a whole. However, these elements combine to fulfill an overall task.

Difficulties arise when systems are misclassified as monolithic or ‘system-of-systems.’ These stem from the amount of control the designers assume when defining the system and performing system trades [198]. For this thesis, it is assumed that all requirements, functions, and environments driving the sizing of systems technologies originate from the development of the aircraft as a whole. Although aircraft systems architects do not have complete control over all attributes of the outsourced design elements, all requirements are assumed to originate in context of the aircraft platform. The aircraft can thus be considered as a monolithic system. Assuming a monolithic system has allowed the systems designers to decompose the problem hierarchically with relatively fixed physical and functional relationships between the decomposed groupings.

Traditionally the aircraft platform is decomposed into ‘systems’ whose requirements flow down to lower levels of abstraction. Moir and Seabridge describe the aircraft in terms of four primary systems: vehicle systems, avionics systems, cabin systems, and mission systems [210]. Each of these systems represents packages which must be developed in order for the system to be designed. These packets of work receive requirements from functions and specification allocated to this specific system regarding its physical components and disciplinary sub elements. Furthermore, systems are further decomposed into ‘subsystems’ as shown in table 1. Subsystems are

Table 1: Aircraft Systems Decomposition [210]

General Vehicle Systems	Propulsion System Fuel System Electrical Generation and Distribution Hydraulic System Pneumatic System Flight Control Systems Landing Gear Steering/Braking/Antiskid Environment Control System/Pressurization Fire Protection Ice Protection Probe Heating Vehicle Systems Management System
Military Vehicle Systems	Crew Escape Canopy Ejection Biological and Chemical Protection Arrestor Mechanism In-Flight Refueling
Commercial Cabin Systems	Galley Passenger Evacuation Entertainment Systems Telecommunications Toilet Waste Water Gaseous Oxygen Cabin and Emergency Lighting
Avionics Systems	Displays and Controls Communications (including IFF and SFR) Navigation (including DME and ADF) Flight Management System Automated Landing Systems Warning Equipment (TCAS/GPWS/TAWS) Altimeter/Air Data Measurement/Weather Radar Accident Data Recorder/Cockpit Voice Recorder Internal Lighting
Mission Systems	Sensing (Electro-optical, MAD, Acoustic, Radar, Cameras) Armament (Weapons Systems, Defensive Aids) Electronic Warfare Systems Mission Computing Data Link Station Keeping Head Up Display Helmet-mounted Displays

composed of elements referred to as ‘units’ or ‘components’.

Typical systems decompositions has led to the development of specifications which assist aviation manufacturing and maintenance. In 1956, the Air Transport Association of America (ATA) introduced numbering schemes for classifying standard systems in terms of component groupings [5]. The ATA Chapters classify groupings of elements based on physical and disciplinary similarity and are broken down further into segments, or lower level groupings of similar components. Although intended primarily for aircraft maintenance, ATA Spec 100 has acted as the decomposition framework for aircraft systems design [204, 294].

Revolutionary technologies introduce significant changes to conventional vehicle systems decomposition. As will be discussed in the next sections, advances in electrical generation, distribution, and storage, power electronics, ice protection, environmental control/pressurization, flight control actuation, utility actuation, and support systems have the potential to fundamentally change vehicle systems breakdowns. Additionally, advances in in cabin, avionics, and missions systems introduce dramatically increased electrical demands which fundamentally alter the traditional integration considerations for these technologies. Increases in the performance promised by systems requiring increased electrical power has impacted the implementation of every aircraft system function.

In discussing complex systems it is necessary to identify what is mean by the terms system, subsystem, component, and unit. The window of abstraction used for these terms can refer to any level of the systems hierarchy. For this work the total aircraft is termed the ‘platform’. This platform interacts with the environment in performing in its mission and other significant scenarios. The combination of all traditional vehicle systems is termed the system. Finally, units and components represent the lowest level of decomposition in the architecture.

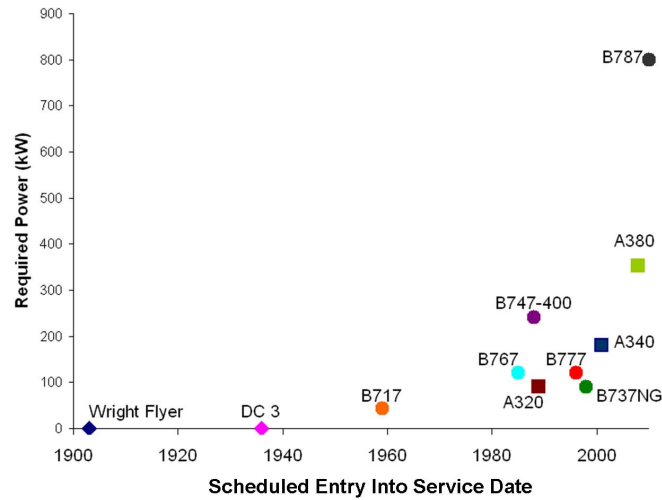


Figure 2: Trend in Commercial Aircraft Power Demand [15]

2.2 Future Electrical Power Demands

With the development of electrical technologies the modern aircraft is facing a marked increase in power demand on aircraft in the last ten years. As illustrated in figure 2, the 787 represents a dramatic increase in the amount of power required on a conventional platform due to electrical ECS and ice protection. The 787 requires over five times the power available on the 777 (Boeing's most recent commercial class aircraft). In order to reliably support critical functions, the 787 is reported to have generation capacity of approximately 1.45 MW using four engine mounted and two APU mounted generators [238].

While the power increase necessitate by A380 systems architecture is much lower, an upward trend remains in required power per seat for conventional architectures (see figure 3). The A380 requires approximately double the power per engine compared to other Airbus commercial platforms in order to provide electrical actuation.

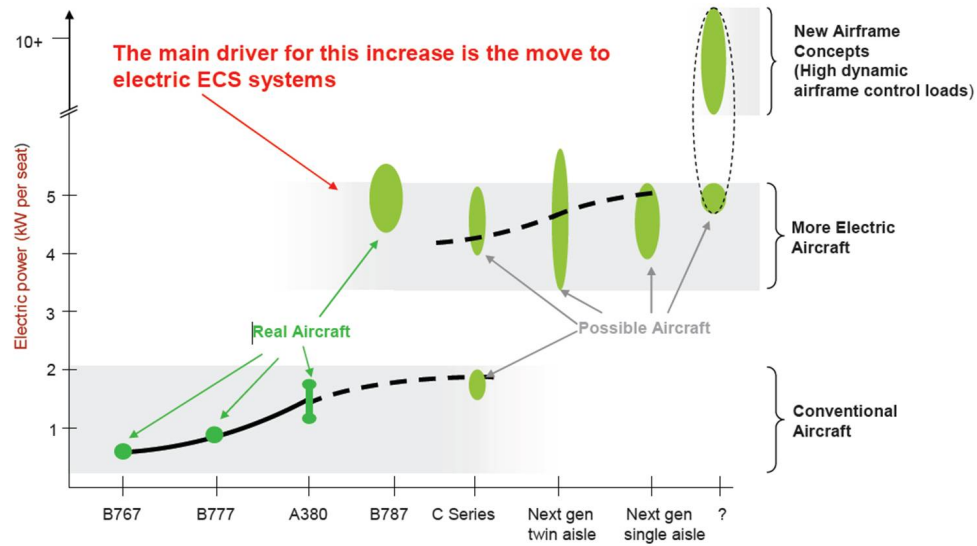


Figure 3: Commercial Aircraft Power per Seat for Conventional, More Electric, and New Aircraft Concepts [205]

Conceptual design decisions regarding systems architecture technology pose dramatically different power demands. An approximate 300kW difference in power demand per engine exists between the two modern ‘more electric’ commercial architectures (Boeing’s 787 and Airbus’ A380). The sensitivity of platform performance to architectural decisions is becoming a critical factor for the optimal design of next generation aircraft.

The electrical power requirements on the military side are more pronounced and are not primarily driven by electrical technology used in vehicle systems. Electrical demands from mission systems are drastically increasing required power generated on a military platform. Directed energy weapons (DEW), such as High Energy Laser Systems (HEL) [37], [128], High Powered Microwaves (HPM) [17, 239], and other Active Denial [115] systems have the potential to greatly expand aircraft capabilities while dramatically increase power required on a platform. Figure 4 displays the power and thermal demands the Air Force platforms will be subject to in the near future.

Similar trends towards increasing power demands are emerging for all future fixed wing platforms: commercial, military, manned, unmanned [205].

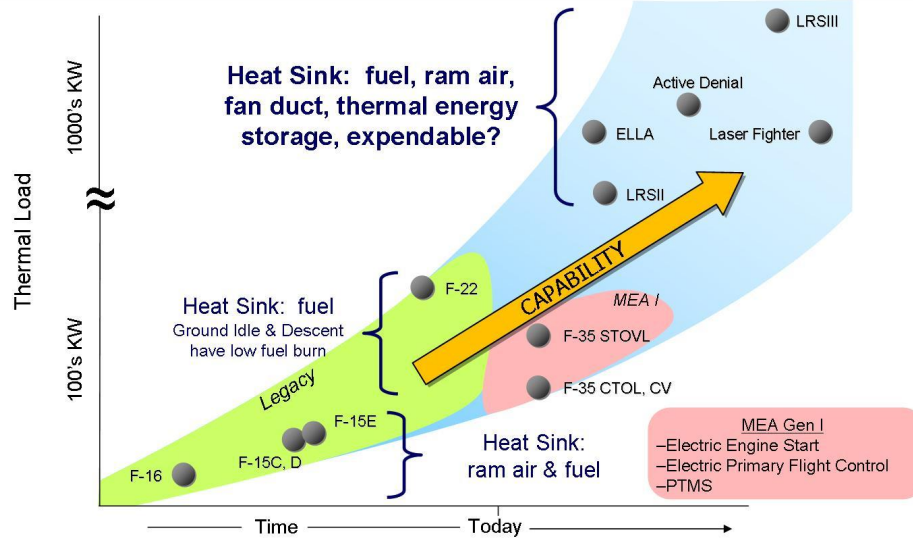


Figure 4: Power and Thermal Management Trends and Challenges [217]

The current challenges arising from the implementation and integration of electrical technologies in the aircraft subsystems architecture has been compared to the revolution necessitated at the advent of the turbojet era [203]. Potential order of magnitude changes in power demand on military and commercial platforms challenges the historically adopted methods for systems design. With large variations in power and thermal requirements necessitated by current and future technological developments, systems architecture becomes a critical consideration for aircraft designer during the conceptual design phase.

Observation: *Advances in electrical technology have led to major increases in the amount of electric power that must be made available on military and commercial platforms.*

2.3 More Electric Aircraft (MEA)

During the late 1930's and early 1940's major developments were emerging which revolutionized Aerospace Engineering. Gas turbine technology was drastically changing conceivable aircraft capability. The Heinkel He-178, the Gloster Meteor, and the

Bell Aircomet (XP-59A) became the first jet aircraft developed in Germany, England, and the United States respectively [202]. Airplane designers began to explore new challenges that came with this enabling technology. Airplanes began to operate with greater speed and maneuverability, higher altitude, and greater efficiency. Aerodynamics, structures, controls, and all other aircraft disciplines were adapting to enhance and enable the performance promised by jet engine improvements [8, 211].

Hickie comments on this period in aircraft design history,

“By the early 1940s it was clear that the major technological challenge facing the industry in the post-war years would be the advent of the jet engine... Although the American aircraft industry had no involvement in the invention of the jet engine ... companies like Boeing had well managed, well resourced and well educated design teams, a large body of useful complementary technical knowledge, and an innovatory culture. As a result they were more quickly and successfully able to exploit the new scientific and technological knowledge associated with the invention of jet aircraft in the 1940s [131].”

Concurrent to advances in jet propulsion other design decisions were being made which set the stage for conventional aircraft systems design. In the late 30's and early 40's US engineers at Patterson Field (now Wright-Patterson Air Force Base) began looking into the increased need for power-assisted flight control. Studies showed that hydraulics were superior to electrical power for on board functions. Electrical generation devices were found inferior due to overall capability and power conditioning devices proved to be inferior in terms of volumetric concerns [200, 44]. Lockheed's Kelly Johnson looked into both electrical and hydraulic sources for powered flight control with the development of the Constellation. Hydraulics emerged as the design of choice [150].

Comparatively few aircraft used electricity for major on board power solutions. The 1941 Focke-Wulf 190-A utilized electrical devices for on board functions. The flight control system was not powered, but electrically supported functions did include actuation and locking of the landing gear, servo-motor actuation for flaps and tailplane, propeller pitching, and cannon firing. The British Aerospace community pursued the use of electrical power for flight functions during the 1950's. The V bombers (Avro Vulcan, Handley Page Victor, and Vickers-Armstrong Valiant) utilized electricity for many of the actuation functions [155]. The Avro Vulcan went the furthest in electrical actuation by employing 10 electro-hydrostatic actuators for flight control with no hydraulic backup. Commercially, British aerospace engineers also pushed the envelope of electrical usage with the VC-10. Vickers-Armstrong engineers used a 2 hydraulic, 2 electric flight control actuation architecture. This control concept has been considered the precursor to the Airbus A380 control architecture strategy [92]. However, these aircraft developments can be viewed as more of the exception than the rule. Hydraulic systems outpaced electrical developments and provided an efficient and less complex approach for powered actuation [155].

Based on a half century of systems engineering and design in the jet age, the modern aircraft industry almost universally adopted a hybrid of mechanical, hydraulic, electric, and pneumatic nonpropulsive power systems [15, 210]. However, driven by maintenance, complexity, flexibility, controllability, and cost issues, and following significant technological advances beginning in the 70's, research efforts began to emerge which explored a more extensive use of electrical systems for nonpropulsive power [155, 44].

As early as 1972 aerospace engineers could see the benefits of the expanded use of electrical systems in the aircraft design. Potentially motivated by the impending oil crisis in 1973 [155], NASA researchers proposed benefits of the removal of the accessory gear box through the integration of a shaft mounted starter generator [264]. As

early as the late 70's NASA began to take a holistic look at the aircraft nonpropulsive power production and usage leading to the concept of the "All Electric Aircraft" (AEA) [129, 56].

Cronin wrote regarding a 1979 study,

"Recent NASA/Lockheed studies have identified the all-electric airplane as an energy efficient transport and one that offers the benefits of eliminating such labor-intensive systems as high-pressure hydraulics, engine bleed air, pneumatics and the nonelectric engine-start systems. Also, there is a significant reduction in the ground maintenance/logistic support, when the ground equipment associated with the multiple power sources is replaced with electric power [56]."

The following two decades saw a marked increase in government and privately sponsored research initiatives towards the development of electrical aircraft systems. The initial 'All-Electric' Boeing and Lockheed studies promised marked improvement over the conventional architecture. In 1984 Lockheed released results from the Integrated digital/electric aircraft (IDEA) concept study. This all electric concept study applied electrical generation, distribution, actuation, environment control (ECS), and flight control system (FCS) technologies to the L-1011/500 (Tristar) as a baseline configuration. These study results showed a 11.3% reduction in block fuel and a 7.9% reduction in DOC for in the baseline configuration. Then a unique 'all-electric' IDEA configuration was introduced. This configuration showed an additional 3.4% reduction in block fuel and 3.1% reduction in DOC [56]. Boeing all electric studies applied to a 767 type aircraft promised up to 3% reduction in fuel consumption resulting primarily to the elimination of the bleed system for the environmental control [283].

These studies spurred further investigation by more 'impartial' academic institutions. The college of Aeronautics in the UK launched a study in 1985. This effort

identified and corrected invalid assumptions in the previous studies. It was found that the reduction in fuel burn achieved through electric ECS was not on the level of 3% as predicted by Boeing, but more realistically less than 1%. The performance improvements suggested by Lockheed were also refuted. Weight savings for electrical flight controls were found to be greatly reduced, if not eliminated altogether. The state of technological development and questionable performance improvements would not provide sufficient incentive to adopt the risk of pursuing the all electric aircraft [155].

However, the industry began to feel that a change in the status quo for aircraft systems design was soon to occur. In 2000, Emadi and Ehsani wrote:

“There is little doubt that the aircraft power system architecture is heading for major changes. Increasing use of electric power to drive aircraft subsystems that, in the conventional aircraft, have been driven by a combination of mechanical, electrical, hydraulic, and pneumatic systems, is seen as a dominant trend in advanced aircraft power systems [87].”

Avery summarized this sentiment by generalizing the benefits of electrical technologies in table 2.

Table 2: Comparison of Aircraft Secondary Power Distribution Systems [15]

System	Complexity	Maintenance	Technological Maturity
Electrical	Complex	Simple	System - Mature New Technologies - Immature
Hydraulic	Simple	Complex & Hazardous	Mature
Mechanical	Very Complex	Frequent & Slow	Very Mature
Pneumatic	Simple	Complex	Very Mature

Limited performance improvements available through advances in conventional technologies and advances in high power density, solid state electronics, electric drives, and microprocessors began to impact electrical aircraft equipment development [87,

137]. The 80's and 90's saw many additional research efforts funded by the US Air Force, the French and UK governments, and the European Union [92]. These studies addressed efficient power conversion, generation, and management in addition to the development of electric actuation technologies. In 1992, the US military's Joint Aeronautical Commanders Group formed the More Electric Aircraft Joint Planning Team, tasked to plan R&D efforts for electrical non-propulsive power for military aircraft. NASA also became involved in pursuit of US commercial electrical aircraft concepts [44].

US efforts in the 90's to pursue the "More Electric Aircraft" (MEA) represented a fiscal investment of over \$290 M [155] with MEA initiatives beginning in 1995. Shortly thereafter, in 1996, the European Union's Fifth Framework Program on R&D proposed their own power systems studies towards the Power Optimized Aircraft (POA) [91]. The MEA and POA objectives were focused on the assessment of specific electric technologies. Specifically, POA's motives were to "identify, optimize, and validate innovative aircraft equipment which contribute to the reduction in consumption of non-propulsive power [92]." While the intent of the MEA studies were to eliminate or reduce the need for a centralized hydraulic system, the focus was primarily technological development and assessment [44].

The results of these research efforts were well summarized during the Technologies for Energy Optimized Aircraft Equipment Systems (TEOS) Forum in 2006. This forum observed that electrical technologies are at the demonstration level and were found to possess the potential for superior performance over conventional technologies. However, maximum performance improvements cannot be achieved through integration within a conventional architecture. It was additionally observed that many challenges still exist and must be addressed in the integration of electrical technologies and functional thinking is requisite for the integration of these technologies [94].

Both the MEA and POA research efforts continued into the 2000's and have triggered additional, ongoing efforts in the United States and Europe. Building on the knowledge generated over the last few decades, the aerospace community then faced the challenge of integration.

2.3.1 Current MEA Research

While many electric aircraft studies remain primarily interested in validating technologies, the focus of a few new efforts has moved to the challenges of integration. Two recent integration focused research efforts are the EU's More Open Electrical Technologies (MOET) and the Air Force Research Laboratory's (AFRL) Integrated Vehicle Energy Technology Demonstration (INVENT). These programs developed new architectures intended to be more favorable for the integration of electric technologies. While these two efforts focus on different issues for electrical systems integration, detailed platform level modeling of the vehicle systems was pursued.

The European Commission 6th Framework Programme MOET followed a three year plan starting in July of 2006. Coordinated by Airbus France, 46 companies and 15 research centers, in 14 European countries worked to address three main themes. The three objectives were to explore architecture, power electronics, and platform validation [154] for the more electric commercial aircraft concept. Three of the five MOET objectives address electrical networks, integration, and platform level design. These studies include hardware validation testing, modeling and simulation, and platform level impact assessment.

The platform level impacts of electrical systems integration were assessed following the results of the technology and systems studies of a conceptual conventional baseline platform and a conceptual more electric aircraft. The process for these architecture assessments is shown in figure 5.

At the aircraft level, weight and drag deltas were determined between the baseline

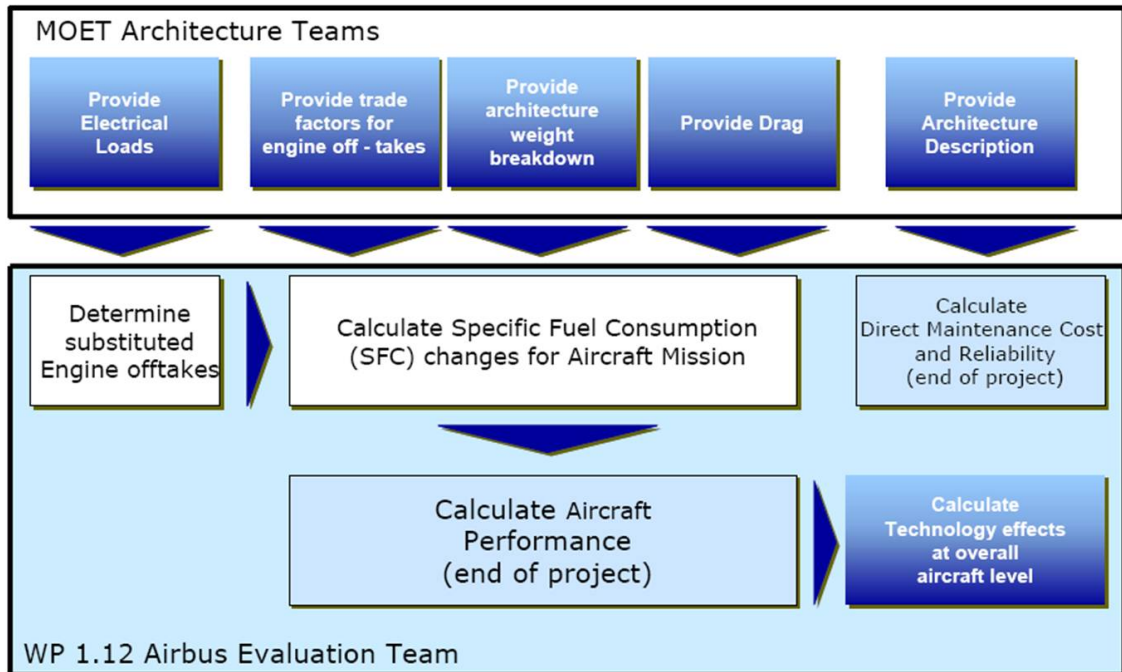


Figure 5: MOET Architecture Evaluation Process [154]

and more electric concept systems. Changes in maintenance costs were determined by expected deltas in % direct maintenance cost (DMC) due to technology insertion. The expected impacts only took changes in the APU, Electric, Bleed, ECS, and Cooling Systems into account. Results showed that the more electric concept “deliver(s) airplane benefits in terms of maintenance, operational flexibility, and technology growth potential without fuel-burn performance penalty.” Weight was not determined to be a determining factor between the ‘more-electric’ and baseline concepts.

Concurrent with the EU’s MOET program, the AFRL was assessing the benefits and challenges of more electric power/thermal systems architecture on military platforms. The Integrated Vehicle Energy Technology (INVENT) program was intended to maximize platform efficiency while minimizing thermal management issues. The INVENT architecture consisted of four subsystems: the Robust Electrical Power System (REPS), Adaptive Power and thermal Management System (APTMS), the High

Performance Electric Actuation Systems (HPEAS), and Advanced Engine Technology Integration. 12 major contractors and 3 service teams were brought together in these studies in a effort to push towards the dynamic total systems modeling, vehicle level system optimization, and hardware in the loop validation. The INVENT program introduced significant technical and organizational integration challenges in the optimization of vehicle subsystems.

2.4 Design Outsourcing

The aerospace industry is characterized by high an increasing technological risk, radical fluctuations in demand, sensitivity to political choices, and major organizational restructuring [131]. Early in the twentieth century, the aerospace industry included a large number of aircraft design competitors. These companies operated in an environment of relatively low risk due to the growing commercial airline markets. World War II caused the growth and consolidation of some aircraft manufactures but at the close of the war 35 aircraft manufacturers were still operating worldwide (16 in the US, 14 in the UK, and 5 in France [114]).

Increased technological complexity, lengthening development times [114], and increasingly price-conscious consumers [121] have not only changed the way airplanes are manufactured, but, as current trends indicate [196], changed in the way airplanes are designed. These factors, combined with fierce competition between Boeing, Lockheed, McDonnell-Douglas, and Airbus led John Newhouse described the business of aircraft design a “Sporty Game” in 1982 [223]. Further competition and consolidation created an industry in the early 90’s dominated by 5 prime commercial manufacturers, approximately 50 prime suppliers, 225 engine and large system manufacturers, and 2,000 equipment, parts, and material suppliers [114].

The last 20 years have seen additional major changes the aircraft industry structure. As the breadth of knowledge necessary for aircraft design increases, aircraft

manufacturers must decide if they can adopt the risk associated with cultivating a new technical knowledge base in-house [196]. With a lack of in-house skills and a desire to maintain ‘core competence’, this risk is often offset through outsourcing of systems and unit level design activities [121]. In 2006, Hickie addressed changes in the market due to the mitigation of risk referring to literature from Lawrence and Thornton [183]:

“It has been argued that, in recent decades, Boeing’s leadership has demonstrated a risk aversion (following the financial crisis associated with the development of the 747), and a commitment to short-term shareholder value, that has led the company to be less technologically innovatory, and has allowed Airbus to take market leadership with superior products [131].”

In order to maintain a competitive technical edge and while still sidestepping undesirable risk, strategic access to development funds became the challenge of the late 20th century for Boeing. This led Boeing to seek out foreign risk sharing partnerships. Key components and sub-assemblies have become the responsibility of external and often foreign suppliers. This outsourcing gains access to external government investment and opened new markets, while avoiding limitations on US government funding. Pritchard and MacPherson write:

“During this era [1970 - 1992], Airbus could rely on government repayable investment up to 100% for a new aircraft program. Although the 1992 EU-US Large Aircraft Agreement limited such launch aid to 33%, the US abandoned the 1992 agreement in 2004 – cutting repayable launch investment to 0%. So, in a nutshell, Boeing learned to find government financial support mechanisms for its foreign suppliers to replace its own self-funding of aircraft launches ... The goal was to give Boeing a ‘level

playing field' by denying Airbus EU repayable launch investment. In effect, this forced Airbus to become a system integrator along the lines pioneered by Boeing on the 787 program [237]."

It is estimated that Japan covered approximately half the cost of the development of parts built by Japanese companies for the 767 [236]. Although the aircraft industry outsourcing has increased total costs, the systems integrator sees a reduction of costs for units and subsystems through their risk sharing partners [196]. It has been estimated that up to 90% of the parts for the 787 have been outsourced [237]. While Airbus and other OEM's retain more design in-house, general trends indicate a greater reliance on the design expertise of external entities.

Technological risk is not the sole factor driving the trend towards an increase in design outsourcing. Alliances are formed for "offensive purposes [121]." Additional to risk and cost related motivations, these purposes may also include access to new markets, resources, technology, capabilities, or knowledge [121].

Motivated by technology integration [290], accessing and securing of markets, reductions development costs, risk sharing, large commercial manufacturers are moving away from the traditional vertically integrated business and supply chain model [131]. An emerging trend for aircraft manufacturing is a combination of increased horizontal integration through globalization, and increased vertical integration by a lengthening of the supply chain [121].

A trend towards outsourcing does not just include an increase in manufacturing from external entities. The traditional decision of "make-or-buy" has been changed to the decision "make-or-cooperate [171]". The last two decades has seen a marked increase in design outsourcing in contrast to manufacturing outsourcing. Pritchard and MacPherson again observed:

“Build-to-print subcontracting relationships are being replaced by internationally devolved design and engineering tasks for airframe development, signaling a profound change in the structure and geography of commercial aircraft production ... Today’s commercial aircraft industry is far different from the early days of jet production, when each aircraft company invented on its own [237].”

Table 3: Distribution of Externalized Design Activity (1995 to 2005): Sample Means Budget Percentage [196]

Function	1995 %	2005 %	% Change	Difference
Product Design	13.1 (2.15)	26.2 (2.05)	100	+13.1
Component Design	28.2 (3.12)	43.1 (3.14)	52.8	+22.8
Tooling Design	20.3 (3.73)	36.7 (2.28)	80.7	+16.4
Design Research	11.2 (2.78)	39.4 (2.71)	251.7	+28.2
Contract R&D	10.3 (4.83)	21.3 (3.76)	109.7	+11.3
All Design Activity	21.8 (3.63)	36.6 (3.19)	67.8	+31.2

Note: Sample Number N=51 (Standard Error in Parenthesis)

These design trends are not exclusive to the aerospace industry. In 2009, MacPherson and Vanchan [196] surveyed 51 US outsourcing companies regarding their design outsourcing activities between 1995 and 2005. For their study, corporate managers of internal R&D or design departments from 68 durable goods manufacturers were surveyed regarding their design budgets. The manufactures surveyed represented the aerospace, machinery, electronics, construction equipment, automotive, military, and household goods industries. Of the 68 companies, 17 indicated that R&D was 100% performed internally. 9 of which were prohibited from outsourcing. The results of these surveys are summarized in table 3.

Of the 68 companies surveyed, 9 represented the aerospace community including firms participating significantly in military markets (10-45% of their sales). Of these aerospace companies, 2 indicated that they were non-outsourcers and 6 indicated that they operate under risk sharing agreements. In 1995, 30.3% of the of the design

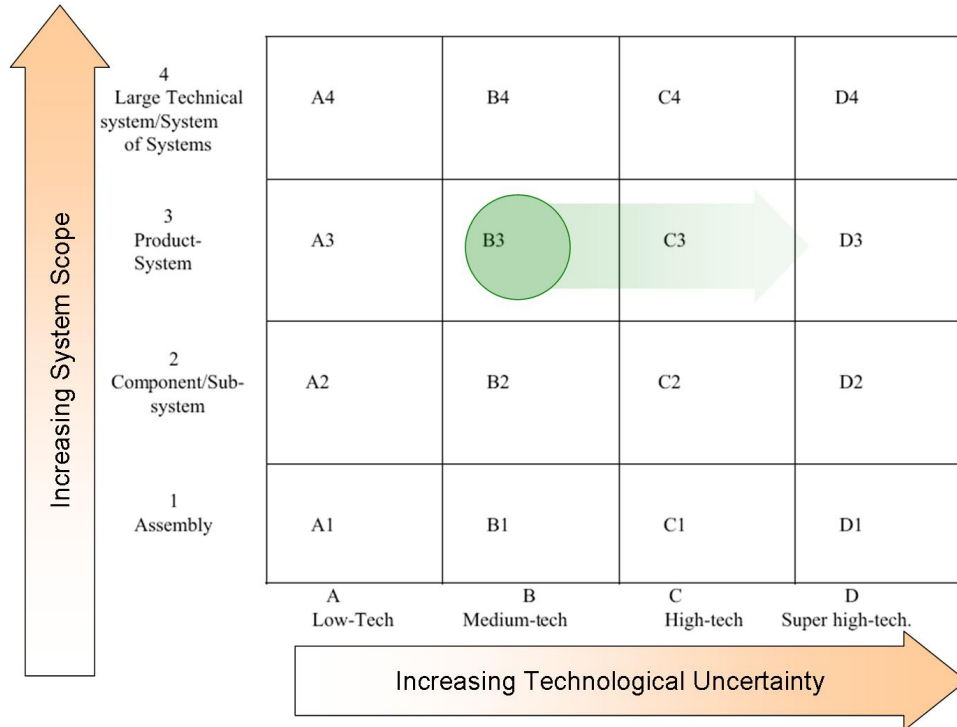


Figure 6: Typology of Technological Systems and the Transition from Conventional to More Electric Aircraft Architectures [134]

budget was allocated to outsourcing compared with 48.7% in 2005. This represents a 60.7% increase in architecture outsourcing in a ten year timeframe.

As design responsibilities are transferred down the supply chain and greater reliance is placed on electrical technologies for mission and flight critical functionality, the aerospace industry is facing a new paradigm in aircraft design. This paradigm is discussed in the following section.

2.5 The New Aircraft Systems Integration Paradigm

Coupled with dramatically increasing electrical power demands introduced by modern technological advances, aircraft OEM's are moving towards increased reliance on external companies for innovative systems solutions.

Hobday et. al. [134] introduce a simple typology for technological systems integration based on literature from Shenhar [268] and Hughes [142]. The intention of

this typology is to express the nature of the systems and the processes required for their integration. This mapping consists of orthogonal characteristics of technological uncertainty and system scope as shown in figure 6. The vertical axis represents systems with increasing scope and the horizontal axis represents the level technological uncertainty associated with the system.

As a “product system” with a least moderate technical uncertainty, commercial and military aircraft can be characterized in row 3 of figure 6. As the level of technological uncertainty increases, systems integration becomes increasingly complex. An aircraft designed with exclusively well-established technologies (column A) or a limited number of new features (column B) poses little difficulty in systems integration. However, as expressed by Hobday, with higher uncertainty technologies, systems integration requires not only innovative technical approaches but adjustments in the relationships between system integrator and component level suppliers. In these cases, capabilities must be developed which enable systems integration and manage integrator/supplier relationships [134].

2.5.1 Aircraft Subcontractor ‘Electrification’

This trend towards large scale power systems outsourcing is made evident by the repositioning and expansion of many of the subsystem manufacturers in order to market themselves as prime electrical systems integrators. Since 1980, electronics, controls, and materials were areas which involved knowledge transfer between companies and spurred the consolidation of aircraft systems manufacturers [108]. While the overall equipment manufacturers (OEM’s) began to contract and outsource, subsystems developers began to expand their capabilities from specific equipment design and manufacturing towards providing a systems integrator role.

One prime example of component suppliers beginning to take a greater role in systems integration is Hamilton Sundstrand. Hamilton Sundstrand has positioned itself

as a major aircraft systems platform level integrator. Joe Adams, Hamilton Sundstrand vice-president, and chief engineer, 787 Programs has expressed their intended role in the aerospace sector:

“Hamilton Sundstrand’s development and integration of such a broad base of systems is a unique role for an aerospace supplier [51].”

In 1999 United Technology Corporation (UTC) created Hamilton Sundstrand through the purchase of Sundstrand Corporation and merging it with Hamilton Standard [108]. With this acquisition and merger, UTC positioned itself as a prime provider of propulsion and power systems and established itself as a key systems supplier on the Boeing 787. Approximately 1300 parts per aircraft are provided by UTC for the 787 [50] which estimate to over \$2 million per shipset [199]. On military platforms, additional to the revenue received through the Pratt & Whitney (P&W) F135 engine, UTC’s Hamilton Sundstrand receives over \$2 million per shipset [36, 199].

Another US company attempting to adopt a systems integrator role is General Electric (GE). Since, 1917 General Electric Aviation has developed propulsive solutions for the aircraft industry. GE has kept in step with a developing market through the technology development and key partnerships. The early 1970’s brought a partnership with Snecma enabling extensive access to the commercial turbofan market, and in 1996, the creation of the GE-P&W Engine Alliance helped push engine technological development. As the most successful engine manufacturer, since 1990 GE has been involved in the production of over 18,000 engines.

While propulsion has been their primary focus for the better part of a century, GE aviation began to pursue a systems integration status around turn of the 21st century. The desire of GE Aviation to move towards prime systems integrator is expressed by their president Vic Bonneau:

“Our integrated electrical power solutions offer superior products and systems involving starting and generation, control, primary and secondary distribution and management, and conversion. Integration processes offer constructors greater installation flexibility and on-time delivery in the initial fit, with higher reliability and reduced maintenance and total ownership costs to end users [25].”

In October 2000, GE announced a \$42 billion merger with Honeywell. Honeywell Aerospace’s capabilities originated in environmental control and heating. Additional vehicle systems design capabilities were developed through a series of mergers and acquisitions including their 1986 purchase of Sperry Aerospace and 1999 merger with Allied Signal. In 2000, before their potential merger, Honeywell’s expertise ranged from primary and secondary power generation, engine start, environmental control, engine controls and accessories, and landing gear equipment [218].

In 2001, this merger was blocked by the European Commission [218], and GE pursued similar systems capabilities with the \$4.8 billion merger with British aerospace equipment company, Smiths Aerospace, in 2007 [301].

GE is not alone in its move towards power systems integrator. Other large engine manufacturers are also positioning themselves in the systems market. Despite challenges in the 70’s and 80’s [184], Rolls-Royce has established itself as the second largest aerospace engine producer. As a primary engine developer for the Boeing 787, Rolls-Royce boasts the Trent 1000 as the first engine to provide power for non-bleed cabin pressurization. Adam McLoughlin, MOET WP2 leader and lead electrical system engineer at Rolls-Royce plc:

“Many of the business sectors within which Rolls-Royce operates are now considering the potential offered by electrically powered systems [205].”

To compete in a more electric era, Rolls-Royce has been involved in developments

towards the more electric engine, low pressure spool generation [209, 211], and has also attempted to take the perspective of electrical system integration. Increasing electrical loads pose problems to the traditional engine design. In order to design an engine to support high steady state and transient loads, Roll-Royce realized the necessity to expand its scope and concurrently address the design considerations of generation and propulsion systems.

Other European companies like Hispano-Suiza are transforming their position from equipment provider to vehicle system integrator. Emerging from the automobile industry, Hispano-Suiza participated in the aerospace industry as an engine developer until the 1970's. Hispano-Suiza, now out of the engine manufacturing business, became a top tier aircraft equipment supplier. A member of Snecma from 1968, Hispano-Suiza became a subsidiary of the SAFRAN Group in 2005 with the merger of Snecma and Sagem and is responsible for Safran's 'more electric' strategy. Focusing on power transmission, management, and conversion and leveraging development from other Safran companies, Hispano-Suiza is working towards "the overall optimization of aircraft electrical architecture (ATA24 equipment), and the integration of electrical systems... [3]" in an attempt to position itself as a provider of platform level power management systems.

It is apparent that the strategic redefining of the large scale systems manufacturers is effecting the development of aircraft systems. The evolving aircraft industry supply chain and increasing technical uncertainty are changing relationships between OEM and equipment supplier. The new strategic positioning of subsystems contractors discussed here is an example of the changing way in which aircraft systems are being designed. Large scale power systems contractors are made responsible for architecting conceptual power systems solutions and manage unit level requirements for component sizing. Companies which were originally responsible for the design and development of specific equipment solutions as dictated by the system integrator are

beginning to assume the role of integrator themselves. In all cases, there is a significant investment towards electrical solutions integrated at the system or platform level.

Observation: *Increased technological risk has changed the way which aircraft are designed. More responsibility is placed on the subsystem manufacturers to provide innovative integrated subsystem solutions.*

2.6 Motivation Overview

Advances in electrical technologies have induced significant challenges to vehicle systems design. The conventional hydraulic and bleed architecture is being rejected in favor of “more electric” architecture concepts. Large increases in the magnitude and variability in power demands supporting flight and mission critical functions has focused much attention on the fundamental aircraft systems architecture. Energy optimization has lead the aerospace industry “to a stage where we are beginning to rationalize and reintegrate things that we have spent many decades separating and ‘optimizing’ [91].” While much of the research in the more electric aircraft has been focused on technological development, validation, and verification within a conventional architecture, current trends look towards the development of new architecture concepts.

The latter half of the twentieth century has seen a dramatic change in the way a large aircraft manufacturer does business. Large aircraft manufacturers and equipment providers are currently adopting new strategies for equipment design and integration. The trend towards increased outsourcing of design activities means that entities external to the OEM are beginning to adopt the role of architect and integrator of vehicle systems technologies.

Coupling the trend towards horizontal integration through design outsourcing for the purpose of risk sharing and market access, with step changes in power required on

military and commercial platforms, the aerospace industry is facing a new paradigm for aircraft systems integration. Generation, distribution, and management of electrical power are becoming a fundamental aspect of the aircraft concepts. Additionally, sources external to the platform developers are becoming more responsible to provide innovative solutions for the platform level design and integration of aircraft power systems. Issues regarding the implementation of vehicle systems architectures must be addressed early in the design process; during the platform concept definition and selection phases.

Observation: *The definition and validation of innovative power systems concepts by subsystem integrators is becoming more critical during the earlier phases of the design process.*

CHAPTER III

REQUIREMENTS DEFINITION FOR VEHICLE SYSTEMS

Addressing electrical vehicle systems trades provides an advantageous perspective during the conceptualization of aircraft platforms. However, it also means that electrical systems requirements must be anticipated earlier in the design process to facilitate concurrent engineering. Revolutionary concept architectures induce new sets of requirements previously not addressed during aircraft conceptual design. These new requirements have the potential to act as show-stoppers for the platform concept.

While the second chapter addressed the business and technological environments for vehicle systems design in the aerospace industry, this chapter looks at the difficulty in “optimally” architecting the power systems. In order to determine this ‘optimality’, architecture models must be subject to accurate sets of requirements generated from conditions which drive the attributes at the unit level.

With increases in electrical power demand and design freedom being deferred to power systems developers, there is a greater need for the ability to explore architecture related solutions. The means for conception and decomposition, architecture complexity, information management, and requirements sensitivity must be addressed with the conceptualization of new architectures.

This chapter addresses two main challenges introduced by architecting power systems during conceptual design. The first stems from the traditional nature of aircraft platform level conceptual design. High levels of abstraction and hierarchical decompositions are difficult to reconcile with the a exploration of a highly flexible

network structure associated with prower systems architectures. Inherent architecture complexity and an intractable number of potential architecture solutions introduce difficulty in architecture exploration and requirements allocation. As seen with MOET and INVENT studies, once the architecture is fixed, complex analysis can be performed and the systems can be optimized. However, during the conceptual architecting of vehicle systems for revolutionary aircraft platforms, flexibility must be provided during the allocation of requirements throughout the system.

The second challenge emerges in the identification architecture specific sizing critical requirements. While requirements are traditionally allocated in a top down manner [210], requirements may be sensitive to architecture implementation. It is necessary to explore how architecture requirements are sensitive to unit and platform decisions in regards to power systems embodiment. Unit and platform level requirements must remain valid during the exploration of the highly flexible architecture tradespace.

This chapter discusses how requirements emerge during the design of complex vehicle systems. This is done by looking at the traditional aircraft conceptual design, defining what is meant by architecture, and exploring architecture complexity. Additionally, this chapter addresses the objectives of this thesis: namely, development of a systematic means for identifying architecture specific emergent requirements during architecture exploratory design.

3.1 Aircraft Conceptual Design

Aircraft systems are typically characterized by large, multidisciplinary architectures. The process of complex system design is made up of multiple steps, often concurrently across multiple organizations. The traditional steps of the design process include pre-design, conceptual, preliminary, and detail design.

Conceptual design is concerned with the formulation of the design problem. Although little to no hardware is produced, conceptual design is considered to be most critical [305]. During this design phase decisions have a large impact on overall incurred cost through the reduction of design freedom during the latter design phases. Early decisions impact future labor, materials, manufacturing required, as well as product performance and the overall product life cycle. These early design phases determines the ability of a company to introduce a viable product into the market quickly [76].

Conceptual design is not intended to guarantee optimal system performance [210]. Within this design phase, a framework is developed wherein engineers, manufacturers, and customers can operate comfortably and pursue a more detailed definition. Conceptual design considers the overall understanding of the primary functions of the system and investigates whether the requirements can be met in a viable manner. The product of the conceptual design process is generally seen as one or more possible high level solutions. The detail of these solutions depends on the maturity of the basic technologies put into operation and the type of the design project [288]. Conceptual design deliverables typically take the form of computer or paper-based descriptions, reports, and mathematical models [210].

This phase in product development generally includes three major steps: problem/project definition, alternative generation, and alternative selection [76, 288, 258]. Wheelwright and Clark visualize the process of design as a widemouth funnel depicted in figure 7 and Moir and Seabridge illustrate this design process in figure 8. The wide part of the funnel captures the magnitude of the product tradespace as driven by concept studies. Drawing from the tacit knowledge from the design team, information from previous projects, research and design studies, and help from suppliers, concept studies are performed and alternatives are generated. A series of screens are used to downselect concepts for further development. These screens denote a tradeoff and

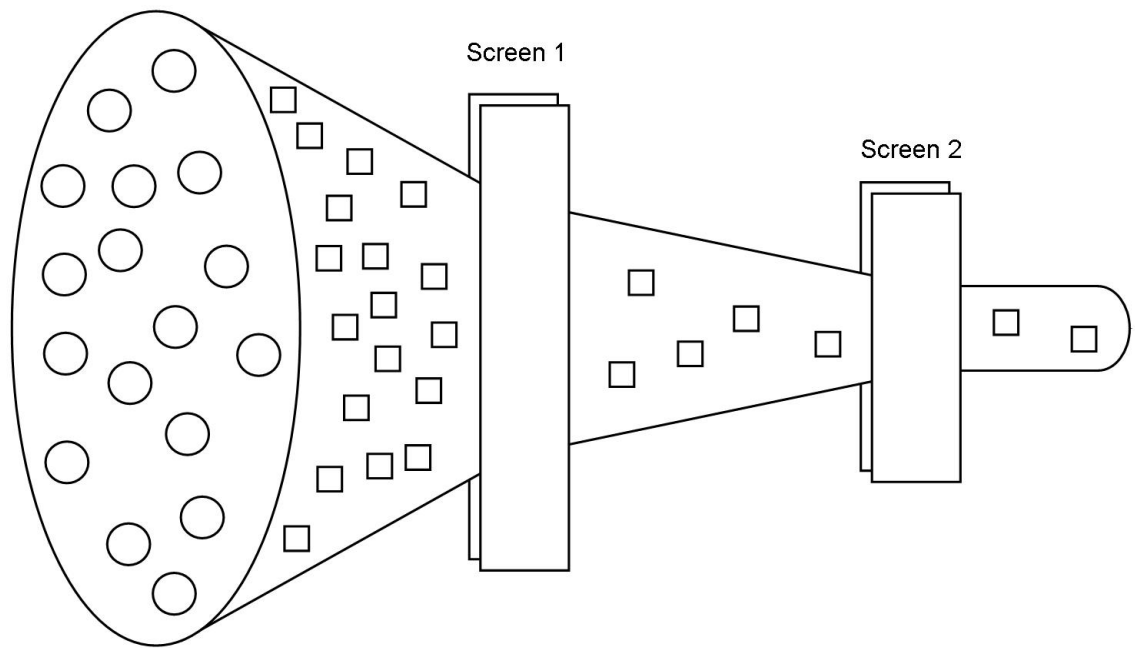


Figure 7: Wheelwright-Clark Product Development Process

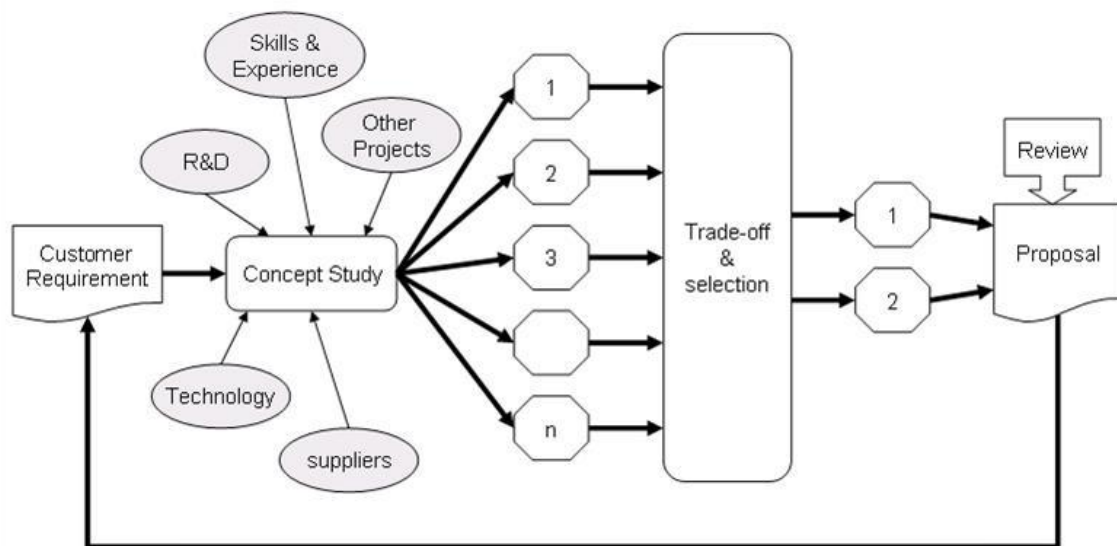


Figure 8: Moir and Seabridge Conceptual Design Process

selection process which evaluates and compares potential concept alternatives.

This process typically requires limitations of the design space based on assumptions on the part of the conceptual designers. Levis and Wagenhals write:

“The customer and the architect assume that these components will work properly because they will be constructed and installed in accordance with established codes and guidelines [293].”

It is difficult to capture all of the detail associated with an architecture considering the limited design knowledge available during conceptual design. According to Lockheed design engineers, Bond and Ricci, with aircraft level conceptual design there is no dedicated process for power systems architecture trades regarding electrical, environment control, and other vehicle subsystems. Aircraft systems conceptual design is occupied primarily with structures, weights, aeromechanics, and mission analysis for a specific configuration of fuel, stores, engine, onboard systems [24]. This includes the location of subsystems, units, structural members, and basic geometry and size.

At some point in conceptual design, when enough alternative designs have been considered and compared, and the company feels confident with the potential designs and are willing to invest more resources, a larger group of specialists are assigned to the design to develop the concepts further [47].

Thus, aircraft systems are traditionally defined through an evolutionary process. Faliero writes:

“Conventional aircraft systems on civil aircraft are a product of decades of development by systems suppliers. Each system has become more complex, as designers have striven to overcome interactions between equipment by increasing the efficiency of each system [93].”

While much work has been done toward incremental improvement of individual technologies and subsystem, there is natural resistance to solve the problem at the

whole aircraft level [93]. In the current aircraft design paradigm of best practices and axioms regarding the impact of high power electrical systems at the platform level do not exist. Complex systems design does not pose contained and well-formed problems [89] but "messy, indeterminate situations [261]."

Michael Sinnett, chief engineer of systems development for the Boeing 787 Dreamliner, spoke about the decision to change the cabin air pressurization method from engine bled to electrically compressed. This single conceptual change to the aircraft architecture imposed multiple dramatic changes to the predefined or assumed relationships within the system. Sinnett said:

"When we decided on electric pressurization, it lowered aircraft empty weight 1,000-2,000 lb. and fuel burn was down several percent, but the numbers got muddled as the 787 got integrated. It's hard to say where the weight has gone [78]."

The initial performance estimates did not take into account the multiple system level changes which needed to occur within the architecture and appropriate strategies to facilitate component integration. The avoidance of architecture exploration and "the use of electrical power components where possible [44]" in conventional or evolutionary architectures may yield incremental improvements to standard aircraft platforms. However, given the trends for electrical power demand, electrical and other power systems architectures are beginning to become central to total concept feasibility.

3.2 Conceptual Architecting

Addressing the composition and structure of power systems architecture during the conceptual design phase is difficult because of uncertainty in platform level requirements and a need to manage high levels of design freedom. The requirements for power systems architectures are typically dictated from the platform level during

preliminary and detail design. However, as power systems become more critical, requirements are generated during power systems design which impacting the platform level design. In order to explore the implications of electrical unit level technologies at the platform level there must be a thorough understanding of the architecture design space.

3.2.1 Architecture

Architecture is an important tool for systems design, concept trades and complexity management. It is communicated as a set of abstract views or models constituting the a blueprint for the design, development, and acquisition processes [293]. Architecting is the process by which a solution space is defined to satisfy system requirements. The International Organization for Standardization defines architecture design as the process to “synthesize a solution that satisfies system requirements ... (and) explore one or more implementation strategies at a level of detail consistent with the system’s technical and commercial requirements and risks [145].”

Architecture is a fundamental, defining characteristic of every complex system and has a large impact on its ultimate performance. Architecture design is crucial to the success of a project because of its impact on the ability of designers to efficiently and effectively develop new products [288]. As indicated by the POA [94] and initial Lockheed studies [56], architectural configuration is integral to achieving maximum benefit from electrical technologies.

Definitions of the term architecture vary depending on the perspective of the definition source. In general architecture denotes entities and their underlying structure whose combined attributes accomplish a task or sets of tasks. Crawley et. al. defined system architecture as a description of elements within a system and the interactions between those elements [53]. Other definitions portray system architecture with primary emphasis on structure and interaction. Maier and Sage describe architecture

as groupings of components joined together in a way to fulfill some task that no single element can fulfill individually, or the means by which proper communication and interaction between elements within a system is achieved [198, 258]. Ulrich and Eppinger place more emphasis on conceptualization and standards in architecture design. They define architecture as:

“the scheme by which the functional elements of the product are arranged into physical [element subsets] and by which the [element subsets] interact [288].”

Additionally, the Department of Defense defines architecture in terms of “major functional elements, interfaces, and design rules, pertaining as feasible to all simulation applications, and providing a common framework within which specific system architectures can be defined [60].” Similarly, The International Council of Systems Engineering (INCOSE) defines architecture as a the unifying system structure in terms of “elements, structure, interfaces, processes, constraints, and behaviors.”

For optimal implementation of electrical technologies, trades in the systems architecture must be performed. This involves the exploration of structural, operational, functional, and technological solutions pursuant to increased product performance. Each perspective provides information necessary to define the architecture and its interaction with the environment [74].

Predefinition plays a major rolls in the use and development of complex systems architectures. All products have a structure, fulfill functions, and in turn, are defined by an underlying architecture [245]. However, varying levels of architecture pre-definition cause architectural concepts to emerge during different portions of the design process [288]. Architectures can come forward through dedicated architecture definition exercises or can be altered and adapted from previous concepts. The means by which this architecture definition takes place is generally determined by the maturity of the technologies to be implemented and the level of definition to the project

previous to conceptual design.

Ideally, the complex system would be decomposed to a “harmonious state“, in which

“all elements are divided into unique modules and ... all intermodule relationships are ... completely described in interface descriptions that also fully describe the emergent system level characteristics [266].”

Traditional architecting processes are schemes for generalizing elements within a system and their relationships. This is enabled through the delineation of standards and interfaces. Functions are grouped together to form tightly linked “chunks“; a chunk being a subset of system elements, or subsystem [266], which represent the physical building blocks of the system [288]. These chunks are defined depending on their roles or functions within the system, or due to physical or disciplinary similarity. This decomposition assists in managing architectural complexity standardizing and minimizing the interactions between subsystems. This is called clustering [122]. In the definition of the subsets of system elements, system architects define where tight physical relationships will occur. This allows the architect to determine the limit and effect of a change within one subset on another. These subsystems are then laid out physically to determine the rough geometric relationships in which interactions are explored [288].

Most design practices assume a pre-existing architecture framework [6]. Redesign, evolutionary design, and derivative design are all exercises which generally require definition within a fixed architectural scheme. However, working within a fixed architecture imposes limitations on the performance of the system. Applying revolutionary technologies to previously defined architectures can introduce complex interactions which significantly change the predefined interfaces and relationships [6]. A breach of the architecturally dictated interactions can have detrimental impacts on the ability

of designers to predict the actual performance of the product. It follows that revolutionary systems require creative and innovative methods for architecture definition.

In order to accurately represent the product, architecture models must capture the relationships between the fundamental elements in a way which can describe the combined attributes and resulting performance of the product. Furthermore, these relationships should be described in a way which is not subject to the breaching of constructs or assumptions with the introduction of new elements into the system. The conceptual architecting of power systems introduces much complexity during the early stages of the aircraft design process.

3.2.1.1 Object-Oriented Vehicle Systems Architecture

Increased emphasis of vehicle systems capabilities has lead many to invest in flexible vehicle systems architecture modeling efforts. In order to explore the impact of architecture changes and avoid over-generalizations of system performance, object oriented approaches to systems modeling provide improvements over historical regressions and system generalizations. This is achieved by closing the semantic gap between model and reality [147]. Systems level performance approximations provide little visibility regarding the performance of a given unit or component in the fulfillment of specific requirements. For object oriented design, a modeling object is mapped directly to an object in reality following the level of abstraction adopted by the systems modeler.

While motivated by functional and operational requirements, most early development exercises for the more electric aircraft have focused on the improvements through the integration of advanced technologies in an existing platform. However, ‘more electric’, ‘all electric’, or ‘power/energy’ optimized concepts represented revolutionary impacts to the aircraft systems architecture, necessitating implementing new perspectives. Sinnett explained the change in perspective necessitated by the 7E7 systems design group. He said:

“In the past systems have kind of come along for the ride. We’ve never really made big functional improvements in systems over the past forty years... Typically we’d approach the aircraft from an ATA chapter perspective. But from a first-principles perspective we were able to set aside all our more typical prejudices [294].”

The POA study also addressed the necessity for a functional perspective in the exploration of architecture concepts. Lester Faleiro, research coordinator of Liebherr-Aerospace, and project manager of the POA project wrote:

“So far, the industry has concentrated on producing potentially revolutionary ideas by taking evolutionary steps. Things change if we begin to look at the aircraft as a functional solution to a problem... Eventually, various solutions, and combinations of solutions, that meet each of the functions of the aircraft, can be found. The beauty of this approach is that instead of providing a number of potential solutions to a problem, engineers can be shown the ideal direction in which they have to take their developments [91].”

A trend is emerging which breaks from the traditional method of defining systems through partition hierarchies or aggregation and is beginning to address the need for the modeling of architecture. Tools and models began to emerge which allowed for flexibility in the embodiment of the vehicle systems architecture intended to assist in early vehicle systems concept trades. Many examples of this trend to the integration of vehicle systems modeling and trades

Examples of this trend include the Air force’s Integrated Vehicle Energy Technology (INVENT) Power/Thermal Models, Airbus’ Aircraft System - Subsystem Inter-relationship Model for Technology Evaluation, United Technology’s Integrated Total

Aircraft Power Systems (ITAPS), DLR's Virtual Iron Bird, the EU's More Open Electrical Technology multiobjective platform level architecture trades. These are just a few of the numerous private and academic research efforts currently being pursued around the world, each pursuing the capability to generate, validate, and explore potential advanced electric systems architectures using integrated object modeling techniques.

3.2.2 Combinametric Complexity

Problematic to the idea of an object-oriented exploration of the vehicle system architecture concepts is the shear magnitude of decisions which must be made to configure an architecture concept. Each unit is characterized by its own complexity in terms of its behavior and performance when placed in an operating environment and given specific performance requirements. However, the environment in which a single unit must operate must be derived from the attributes of the architecture as a whole. As the fundamental architecture structure is made flexible during architecture exploration, unit level requirements will necessarily change. Therefore, determining the requirements at the unit level becomes sensitive to a combinametric design space.

Table 4: Notional Morphological Analysis for Platform Level Functional Fulfillment

Function	Alternatives			a
Propel	More Electric Engine	Conventional Engine		2
Control Yaw	HA	EHA	EMA	3
Control Pitch	HA	EHA	EMA	3
Control Roll	HA	EHA	EMA	3
Actuate Landing Gear	HA	EHA	EMA	3
Protect from Ice	Pneumatic	Electric		2
Environment Control	Conventional	Bleedless		2

a = number of single alternatives per function

Conducting vehicle system architecture trades also introduces a design space which is combinametrically complex. The number and diversity of elements which can ultimately support the platform level functions represents a design space consistent of

an intractable number of potential architecture solutions. Each one of these combinations represents a distinct way to fulfill architecture tasks, exhibits an independent set of physical and behavioral attributes, and may induce the need to address configuration dependent functional or operational design decisions. Consider the simple morphological decomposition representing solutions to platform level functions in table 4. Here conventional and ‘more electric’ technology alternatives are listed for six vehicle systems related platform level functions.

Table 5: Number of Potential Combinations of Solution Considering Redundancy

Functions	Number of Potential Solutions by Redundancy			
	None	≤Dual	≤Triple	≤ n $\left[\sum_{i=1}^n \binom{a+i-1}{a-1} \right]$
Propel	2	5	9	$\sum_{i=1}^n \binom{1+i}{1}$
Control Yaw	3	9	19	$\sum_{i=1}^n \binom{2+i}{2}$
Control Pitch	3	9	19	$\sum_{i=1}^n \binom{2+i}{2}$
Control Roll	3	9	19	$\sum_{i=1}^n \binom{2+i}{1}$
Landing Gear	3	9	19	$\sum_{i=1}^n \binom{2+i}{2}$
Protect from Ice	2	5	9	$\sum_{i=1}^n \binom{1+i}{1}$
Environment Control	2	5	9	$\sum_{i=1}^n \binom{1+i}{1}$
Combinations	648	8.2×10^5	9.5×10^7	$\left[\sum_{i=1}^n \binom{1+i}{1} \right]^3 \times \left[\sum_{i=1}^n \binom{2+i}{2} \right]^4$

a = number of single alternatives per function

n = level of redundancy

The number of potential combinations of solutions depends on the level of redundancy for the technologies fulfilling each function. In table 5 we see the number of potential solutions given the ability to select up to ‘n’ redundant elements to fulfill the function. For no redundant selections there are a total of 648 combinations which

can fulfill the six functions. Allowing up to dual or triple redundancy this total increases to 8.20×10^5 and 9.50×10^7 respectively. If evaluation of each of the 9.50×10^7 concepts required 1 millisecond, it would take over 26 days to evaluate the set. This the number of potential solutions can be reduced by limiting the architecture in terms of redundancy, and technology compatibility. However, even with this simple table the number of alternatives could be too large to handle.

Neglected in this simple analysis is the potential addition of new functions when a physical element is selection. Each alternative induces new requirements on the system. At a minimum, generation, distribution, transformation, storage, and protection equipment must be defined with adequate redundancy for each power type required by the equipment selected to support platform level functions. Safety and reliability functions will also be introduced with the selection of physical elements. Assume these functions and their system definition alternatives are listed in table 6.

Assuming conventional technologies are selected to fulfill aircraft functions with dual redundancy for control, propel, and environment control, specific functions are introduced. Pneumatic and hydraulic distribution and generation become necessary. Again, these functions must be fulfilled with adequate redundancy. As can be seen in table 6, with this specific technology set, the number of potential solutions expands dramatically. For the conventional architecture as defined above relationships between elements provide combinations of potential flows of functions on the order of 1×10^{13} . This variability is increased by allowing the allocation of functions to vary for each mission scenario.

Behavioral aspects also increase architecture dimensionality. The physical sizing of each element will be subject to how the physical objects are being used during each mission segment or operating scenario within the life cycle. Decisions must also be made regarding how the equipment will be supported and when. Functions can also be supported by any one or combination of elements during the various mission

Table 6: Notional Morphological Analysis for Derived Functional Fulfillment as Required by Functions from Table 4

Induced Function	Alternatives		Number of Solutions	
			Conventional	More Electric
1. Distribute Electric	Electrical Bus			n_1
2. Distribute Hydraulic	Hydraulic System		n_2	
3. Distribute Pneumatic	Pneumatic System		n_3	
4. Distribute Fuel	Fuel Distribution		n_4	n_4
5. Distribute Thermal	Cooling Loop		n_5	n_5
6. Generate Electric	Generator			n_6
7. Generate Hydraulic	Mechanical Pump	Electrical Pump	n_7	
8. Generate Pneumatic	Electric Compressor			n_8
9. Store Electric	Energy Storage			n_9
10. Store Pneumatic	Air Tank		n_{10}	
11. Store Fuel	Fuel Tank		n_{11}	n_{11}
Total			$\prod_{i=1}^{11} n_i$	

segments. This causes the design space grows even larger.

Furthermore, adequate reliability must be maintained during the mission. Decisions on how to provide support for architecture equipment, allocate requirements with mission scenarios, and ensure reliable performance greatly complicate task of defining a conceptual power systems architecture. All of these decisions must be made to determine the sizing critical requirements for each unit in the system. From this simple example and its shortcomings, we see how managing perspectives is critical to architecture design.

Whereas the traditional hierarchical breakdown of the aircraft design space allows for the definition of unit level requirements by a ‘flow down’ from higher to lower levels of abstraction [210], the varying structure and highly integrated nature of power systems architecture trades necessitates alternative methods for traditional top down requirements allocation. It is necessary to understand the effect that this complexity has on the definition and application of requirements.

Observation: *Vehicle systems architecture trades greatly increase the combinametric complexity of the aircraft platform concept design space.*

3.3 Requirements Definition

Requirements analysis precedes all definition of the product functions or physical attributes. It is the means of generating a valid description of desired product attributes or goals which are logically organized to guide product development. Requirements analysis considers what needs to be done by a product and is not troubled with how these are to be accomplished.

David Hays described discusses requirements as follows:

“It is important not to confuse requirements analysis with system design. Analysis is concerned solely with what some call the problem space... There is a common tendency for designers... to go into the effort with preconceptions of what the solution space is going to look like, so they seek out problems they already know how to solve [127].”

External influences driving the definition of requirements can be categorized into coherent groupings. Moir and Seabridge discuss typical design drivers that are present in the requirements analysis of an aircraft: safety, cost, environmental conditions, performance, quality, human/Machine interface, structure, crew and passengers, stores and cargo, functional performance, and standards and regulations [210].

These requirements drivers lead to the definition of expressed desirements regarding the system. These desirements are categorized in terms of scope and application to form requirements groups. The DoD recommends grouping these requirements in a database which lumps these design drivers into project requirements, mission requirements, customer specified requirements, and interface, environmental, and non-functional requirements [75]. This constitutes what INCOSE terms a concept of operations (CON OPS) [125], which gives a description of all product requirements

and performance metrics. The CON OPS acts to define platform level functions and sizing scenarios in terms of user and environment interfaces, missions, and constraints. It also may place limitations on the architecture embodiment and metrics for alternative comparison.

In their document “Systems Engineering Fundamentals,” the Department of Defense’s Defense Systems Management College defines requirements in terms of three distinct views: operational, functional, and physical [75]. Operations are responsible for determining the magnitude, duration, and environment for platform requirements. The functional view addresses what the system must do to fulfill carry out the operations, and the physical view focuses on specific means to fulfill the functions. Thus, requirements originate from the operational view and are allocated to the physical elements by means of functional relationships. During conceptual design, changes in the mission necessarily induce changes in the physical attributes of the system [118].

An operation can be defined as “the tasks, actions, and activities to be performed... to satisfy defined operational objectives” subject to “conditions, circumstances, and influences” affecting performance [227]. These tasks, actions, and activities can be generalized under the definition of a function [229, 282]. Thus, operations describe the sequence and magnitude of concurrent or serial sustained and discrete functions which must be fulfilled in support of objectives or users’ needs. Each specific combination of requirements allocated to the architecture at a specific state and subject to a specific operating environment represents an operational scenario.

Identifying appropriate functional requirements for a product begins with identifying the environment in which it is to operate throughout its life cycle. This must be done independently of the physical structure or implementation strategy of the product and the relationships of this environment to the product itself. A holistic view is necessary when eliciting requirements from the concept of operations. Rosson and Carroll argue:

“Requirements are often documented as individual features, specific functions that must be implemented in order to make available the required overall system functionality. This approach entrains the creation of voluminous specification documents couched at the level of individual operations. This tends to create ... abstractions at a fairly low level with respect to overall system functionality [255].”

Platform level requirements are often assumed independent of product architecture. The means by which these requirements are fulfilled by the physical solutions may change the way these requirements are deployed to the unit level. This follows the typical flow down of requirements as discussed earlier. However, during architecture definition do requirements flow up?

3.4 Emergent Requirements

The sensitivity of platform requirements to architecture changes is not a foreign concept [204]. Some requirements have already been identified which emerged with the implementation of electric technologies. These requirements have expanded the necessary scope in systems evaluation and has motivated the introduction of specific new architectures. The MOET and INVENT architectures have been introduced to address the emergent requirements induced by new technology insertion. As discussed in the motivation chapter, thermal and transient consideration began to emerge as sizing critical requirements. While in previous architectures these requirements were not sizing critical and typically not modeled or addressed in concept development, these considerations have been included or augmented with studies in high power electrical technology implementation.

As expressed by Casti:

“Complex processes display counter-intuitive, seemingly acausal behavior full of unpredictable surprises [42].”

With complex vehicle systems, requirements “cannot be fully explained mechanistically and functionally [107].” New requirements may emerge following architecture decisions.

Flake described emergence as follows:

“[Emergence] refers to a property of a collection of simple subunits that comes about through the interactions of the subunits... Usually, the emergent behavior is unanticipated and cannot be directly deduced from the lower-level behaviors. [104].”

Emergence is often held synonymous with subunits exhibiting individual knowledge or consciousness. While these attributes may not hold for power systems elements themselves, requirements may emerge in an ontological sense. Some requirements do not exist and can not be predicted until product definition takes place. Similar to emergent behavior, requirements may be emergent if they are unanticipated during the requirements definition process and are a product of the interaction between architecture specification through the physical embodiment and system operations and behavior. In addition, conceptual design is an emergent complex process. The elicitation of requirements assigns attributes of intentionality, foresight, purpose, and morality in the definition of architectures.

Emergent requirements, defined here, are requirements which can not be enumerated or quantified during the traditional requirements definition process, but which are the result of complex behavioral relationships between units in specific architecture implementations.

A distinction should be made between what is meant by an emergent requirement in contrast to a derived or induced requirement. A derived or induced requirement is a requirement which is not designated by a stakeholder but is identified during requirements analysis process and is based on the designers understanding of the

problem [123]. Derived requirements are often defined through a decomposition of the explicitly specified requirements [188]. Similarly, emergent requirements are also not explicitly defined by the stakeholder. However, these requirements may also not be defined during requirements analysis, but emerges as a result of the operational implimention of a physical architecture. Emergent requirements is similar to a constructed requirement, which is “an expression of domain knowledge [192],” but they again differ in the fact that they emerge due to the specific aspects of the embodied architecture interacting with the operational domain.

Unit level requirements are inherently emergent. The relationship between platform level requirements and unit level requirements depend directly on the physical definition of the architecture and complex behavioral relationships. Modularity in systems modeling pursues the ability to capture changes in the interplay between systems and captures requirements interactions. Techniques like functional induction, as will be discussed later, can handle variability in functional requirements as they are deployed from system to system. However, for new technologies, combinations of technologies, or new strategies for providing loads, other requirements areas are effected which are critical for sizing at the unit and system level.

Research Question: *What factors contribute to the operational/behavioral complexity lead to emergent requirements in aircraft vehicle systems?*

3.5 Thesis Objectives

Traditional means for concept development requires assumptions regarding architecture embodiment to limit the architecture design space. Greater flexibility in the design space means that assumptions regarding sizing critical scenarios and limiting requirements may no longer hold. With the increased complexity introduced with power systems conceptual architecting, requirements emerge which depend on the

specific embodiment of the design space. If new requirements emerge with the introduction of novel architectures, these must be identified in order to justify architecture selection.

Conceptual tools and techniques are required which allow designers to explore architecture concepts and simultaneously capture these emergent systems requirements to justify architecture selection. The objective of this thesis is to develop tools and methods which assist the system architect in systematically identifying emergent operational and reliability related architecture requirements while allowing for variability in architecture construction. This ability has the potential to aid the designers during architecture definition and allow for more accurate prediction of power systems architecture effectiveness.

Objective: *Development of tools and techniques for systematic identification of architecture specific emergent requirements during concept architecture validation.*

CHAPTER IV

SIZING CRITICAL EMERGENT REQUIREMENTS

New system level requirements are introduced following decisions about the structural or physical nature of the system. Allowing the requirements to be augmented following design decisions is necessary for revolutionary concept architectures. Sizing critical requirements emerge from operating scenarios not defined by the concept of operations. However, these requirements depend on the specific architecture implementation of the solution. In order to size the system, unit level requirements must be accurately predicted.

As discussed in the previous chapter, design perspectives play a large role in defining revolutionary architectures. Multiple perspectives must also play into the identification of emergent requirements. Drawing from research performed by Lisouët-Hanke, vehicle systems architecture complexity can be characterized in multiple dimensions: technology dependence, spatial topology dependence, operating mode dependence, safety and reliability dependence, and time dependence [190]. These categories frame the dimensions explored in this chapter towards understanding the emergence of sizing critical requirements.

The first two categories of complexity (technology dependence and spatial topology dependence) refer to the dimensionality of physical architecture embodiment as discussed in the third chapter. Variations in technologies, their relationships, and their spatial integration represent variations in the architecture definition. Much work has been done to understand and characterize technological dependence and its potential impact potential to effect architecture performance. These efforts and ‘more electric’ technology examples were discussed in the second chapter. Spatial topology

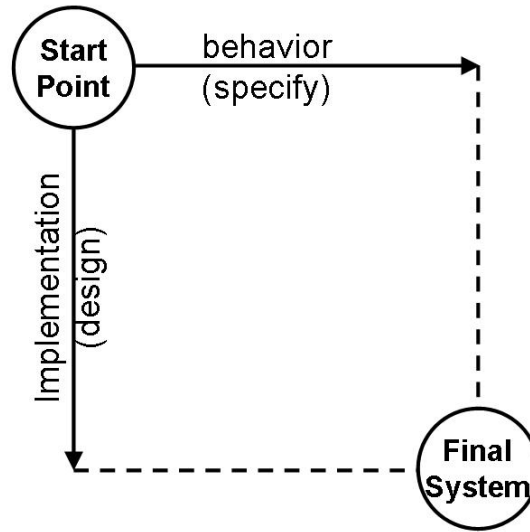


Figure 9: Harel’s Magic Square of System Development

also plays an important role in the physical definition of the architecture.

While not addressed directly in this thesis, layout and packaging concerns are of critical interest. Further information regarding these aspects of architecture design were addressed by Upton [289]. The physical embodiment, arrangement, and attributes of these units are assigned and derived from customer needs, operations, and safety/reliability considerations. However, the work presented in this thesis focuses on the latter categories introduced for characterizing architecture complexity which relate more directly to the behavioral space of the system. Primary focus is given to operating mode and safety and reliability dependence.

Emergence is a product of the behavioral complexity of units and systems. Behavioral requirements can be considered as orthogonal to the physical and implementation design space. This is expressed by Harel’s “Magic Square of Systems Development” displayed in figure 9. Arriving at some final system solutions requires progress in both the behavioral and implemenational dimensions of design.

The first behavioral dimension of complexity introduced by Liscouët-Hanke is time dependence. This chapter discusses time dependency in architecture modeling

with two main areas of focus. First, the definition of energy related requirements through integral of load demands. Second, the sizing critical nature of transient load, necessitating dynamic analysis

The last two behavioral dimensions of complexity (operating mode dependence and safety and reliability dependence) act to drive the requirements allocation to the unit level. Additionally, the concept of requirements emergence necessitates requirements feedback from the unit level. This is considered in terms of operating mode dependence and safety and reliability dependence. These two categories represent the primary focus for this thesis.

In order to address emergent requirements in the form of operation mode and reliability/safety dependence, it is necessary to benchmark against existing methods for operations definition and reliability analysis. Following discussions of time dependence, this chapter reviews tools and methods used in the identification and allocation of sizing critical requirements.

Research Question: *How does time dependence effect vehicle systems architecture trades?*

Research Question: *With varying vehicle systems architecture, how do sizing critical operating modes vary?*

Research Question: *With varying vehicle systems architecture, how do safety/reliability requirements vary?*

4.1 Time Dependence

Time dependence presents design challenges at multiple levels of abstraction during product development. For the traditional high level aircraft platform conceptual

designers, tasked with life cycle and mission analysis, time dependence may be considered on the order of minutes to decades. On the other extreme, unit level designers must take a much finer time dependence perspective. To ensure adequate stability and power quality power electronics and electric machine designers may consider switching and response rates on the order milliseconds or smaller. The high level time dependence perspective is insufficient for analysis at the unit level. Conversely the unit level perspective is far too detailed for assessment of the architecture at the platform level.

While a time scale adequate for mission analysis is also necessary for platform level sizing, it is necessary to determine what time perspective should be taken during unit and system level sizing. During early phases of power systems definition, models must be able to predict component size, weight, and other attributes while allowing for highly volatile physical relationships. Furthermore, changes in the way requirements are allocated, and take transient behavior must be taken into account.

4.1.1 Unit Level Time Dependence

Sterman observes:

“Models rarely fail because we used the wrong regression technique or because the model didn’t fit the historical data well enough. Models fail because more basic questions about the suitability of the model to the purpose weren’t asked, because a narrow boundary cut critical feedbacks, because we kept the assumptions hidden from the clients, or because we failed to include important stakeholders in the process [279].”

Not all modeling techniques are suitable for performing architecture trades. Box observed, “All models are wrong, but some are useful [279].” Models differ in their intended application with regard to the predictive capability towards the solutions of a given problem [147]. Identifying emergent vehicle systems architecture requirements

demand levels of modeling accuracy which provides confidence leading towards design decisions. However, there is little use for highly accurate dynamic models during conceptual design if they are not timely in both execution and construction. In order to implement such models, designers must often prematurely limit the number of degrees of freedom. There is a necessary tradeoff between efficiency and accuracy in the exploration of a vast architecture design space [169].

This section introduces four levels of vehicle systems abstraction used for modeling purposes: system level generalized modeling, steady-state modeling, reduced order/lumped parameter modeling, and switching level dynamic modeling. Each of these levels of abstraction include different levels of detail regarding the architecture embodiment. Some perspectives have the potential to yield more accurate predictions of systems behavior and requirements, but require larger computational resources and extended development time.

4.1.1.1 Systems Level Generalization

Systems level abstractions of vehicle system attributes represent one extreme in modeling system level performance and attributes, where time dependency is only exhibited through potential mission level analysis. With these techniques, the designer avoids the necessity to address unit relationships and specific architecture structures.

Well-established fields, like aerospace industry, benefit from a large historical database of aircraft concepts. This wealth of information provides a statistical reference for predicting system level attributes and performance. Traditional weights estimation techniques rely heavily on the historical database to predict system attributes. While these statistical approximations are continually being updated with new aircraft designs, published examples of statistical system weight approximation methods are provided by Nicolai [224], Raymer [244], Roskam [253], and Torenbeek

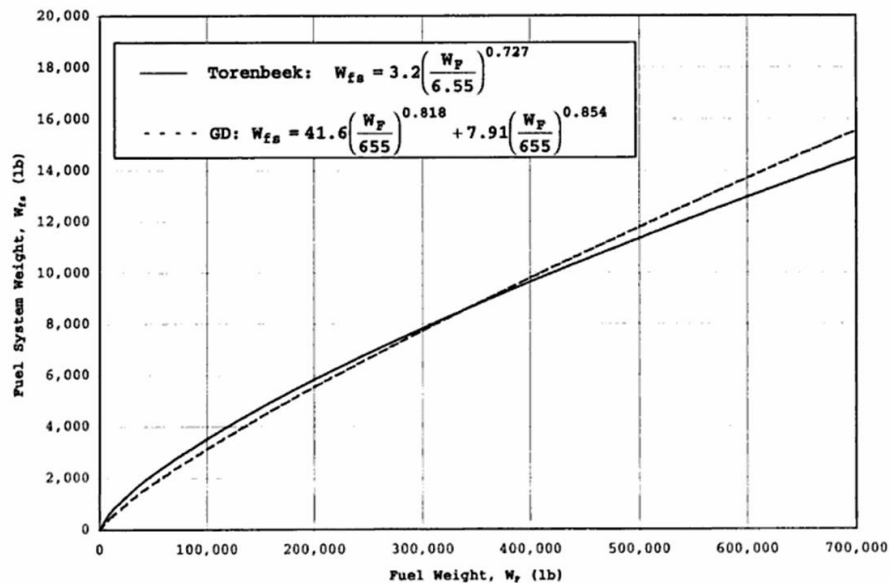


Figure 10: Comparison of General Dynamics and Torenbeek Equations for Fuel System Weight Estimation for Airplanes with Self-sealing Tank from Roskam [253]

[285]. These weight approximations identify the attributes in terms of the generally adopted hierarchical decomposition of the aircraft. Generalizations are made for each high level aircraft vehicle system. The attributes of structures, power plants, and equipment systems are approximated in terms of known generic attributes of the platform and mission. An example of such a regression is provided in figure 10. This figure displays two exponential regressions predicting the weight of a fuel systems based on fuel weight with self-sealing tanks.

The equations from figure 10 provides little information or representation of the physical systems itself. The attributes of this system are determined solely in term of fuel weight. While this statistical relationships may be valid for traditional systems concepts, revolutionary architectures require extrapolations from the historical database and remove the predictive power of the historical reference. Raymer expresses these limitation with historical weight estimation. He says:

“It should be understood that there are no ‘right’ answers in weights estimation until the first aircraft flies... Needless to say, these equations

are complicated, and it takes a lot of time to apply them successfully.
Mistakes are easy... [244]“

Novel architecture configurations and the introduction of advanced technologies undermine the accuracy and applicability of historical weight based regressions. Designing outside the traditional design space, as with the more electric aircraft, requires the use of “fudge factors [244]” which extrapolate from the existing databases. These fudge factors are qualitative estimates of the benefits or detriments to system attributes or performance based on engineering tacit knowledge, heuristics, and engineering reasoning [160, 245]. Performing power systems trades with this process of modeling may cause significant errors stemming from misunderstanding of assumptions made in regards to the regression itself due to the limited knowledge of the design team.

While these methods tend to fall short in accurately predicting vehicle systems attributes for novel concepts, they are often used during conceptual design due to their high level of abstraction and speed of execution. Assumed impacts from architecture trades and technology insertion can be easily represented as technological impact factors and be quickly augmented for architecture trades. Varying the technology impact factors presents little computational challenge for the statistical regressions. These tools allow conceptual designers to quickly generate platform level performance estimates and promotes optimization and robust design at the platform level [166].

4.1.1.2 Steady-State Modeling

Integrated, validatable, architecture specific models are required for conceptual architecting trades. NASA Glenn Research Center discussed new modeling necessities in 2003:

“[T]here is a need for more accurate models and validation of those models, especially at the systems level... Most of these tools exist in some

form, but the integration into a single, coherent systems model is not trivial. A dynamic model that investigates startup, takeoff, and other mission transients would also be valuable for such a system [106].”

The object oriented modeling approach implemented by most current vehicle systems integrators enables flexibility in the architecture design space. However, the question still remains regarding the level of time dependence necessary for unit modeling unit during conceptual architecting.

Kuhn describes three levels of electrical systems modeling which vary in detail and execution time. These levels can be described as architecture level steady state models, state space averaging/lumped parameter models, and switching level models [179].

This first level of abstraction typically involves algebraic balancing of power with no dynamic analysis. Time based relationships are not captured between components during steady-state analysis. However, many of the unit level requirements can be inferred from steady state analysis. While dynamic performance requirements have significant impact on the size and performance of power systems components, notional constructions of the transient signal may be communicated between devices through the specification of expected ramp rates and peak loads for given durations. These simplified abstractions of transient requirements coupled with a large time step mission analysis are termed “quasi-steady-state” models.

The advantage to steady state power balance relationships is their simplicity to specify and to execute in a model. Steady state models often exhibit execution times multiple orders of magnitude faster than switching level dynamic models [179]. The perspective taken during architecture level modeling of power systems allows the systems modelers to perform high level architectural trades and determine general unit level requirements. These concept level solutions provide justification for architecture decisions and select potential architectures for more detailed analysis. Naturally,

additional fidelity would be required during later phases of design refinement.

4.1.1.3 *Dynamic Modeling*

“Quasi-steady state” models can illicit many of the necessary sizing critical power requirements. However, considerations like voltage and current fluctuations, temperature variations, and control considerations require an understanding of system stability [87]. Dynamic models are required for each analysis.

Common techniques for dynamic analysis of aircraft power systems center around linearization, state space averaging, and evaluation for small disturbances [86, 62]. Complex dynamic systems can be represented by systems of first order linear differential equations to approximate the transient responses to perturbations around equilibrium conditions. An early process for system linearization and state space averaging of switching devices is developed by Middlebrook and Cuk [208].

Simplification techniques also apply transformations which allow the analysis of alternating current signals to be represented in terms of a time invariant or synchronously rotating reference frame (e.g. Park’s Transformation [116, 173]). This allows sinusoidal signals to be treated as time invariant linearizations which are precisely accurate under constant speed and load conditions. Additional estimation techniques exist for lumped parameter representations of other switching level considerations (e.g. ripple) [174].

Lumped parameter or state-space averaging evaluations are often sufficient for systems level modeling. As expressed by Kuhn, “Switching transients from power electronic devices do not normally have a significant influence on systems stability [179].” While this may be true for traditional power electronics loads, evaluations of high power actuators have indicated stability issues which can only be identified at the switching level. Linear time invariant systems evaluations of Routh-Hurwitz stability criterion, Nyquist criterion, and Eigen value and μ analysis, coupled with tools root

locus and Bode plots provide the ability to determine most small disturbance stability.

These state space averaged models are much more difficult to create and execute than architecture level power systems models. Differential equations must be generated, equilibrium points must be identified, linearizations must be generated. This must then be executed for all relevant operating conditions. Techniques for time averaging and linearization are heuristic in nature and are subject to sources of error. Stability can't be ensured with linearized systems representations. Actual waveforms, high frequencies, control issues, and response to large scale disturbances present problems which must be addressed using more accurate systems simulations.

Inherent trades between the development and simulation time versus accuracy must be addressed for architecture time dependence consideration. To enable faster evaluation of dynamic systems models pursuant to architecture development, the INVENT studies determined that state averaged systems models are sufficient for platform level performance simulations. The higher accuracy available from more detailed higher order models is forsaken in deference to the requirement for faster simulation time. Lower order models are used for platform level system analysis and higher order models are used for validation. As observed by Kuhn:

“Despite the highest level of model accuracy, the main drawback of [time varying nonlinear] modeling is the need for vast computational resources and time [178].”

Additionally, both switching level and state averaged systems models are typically intended for system analysis. Applying these tools during the design process would necessitate iterative processes of system definitions, redefinitions, and model executions. This process may be feasible for architecture level models with steady state relationships. However, for dynamic systems, tremendous amounts of effort may be necessary to simply construct the model and ensure convergence. Large cycle times

are necessary for even slight system modifications, let alone dramatic architectural alterations.

4.1.1.4 *Surrogate Modeling*

Nielsen writes, “In most projects, if the only available choice was that between nothing and perfection, nothing would win [225].” Detailed transient analysis is desired to validate vehicle systems concepts. However, it is unavailable during concept architecture trades. This is due to problems in modeling efficiency and flexibility. While “perfection” is unattainable, a third option is available; a “systematic approach to improving the usability of the user interfaces by applying a set of proven methods [225].” Alternative power systems modeling techniques can assist in gaining partial benefits through compromise between low accurate steady state architecture models and computation heavy dynamic systems modeling. This increasing the usability of steady-state and state averaged dynamic modeling.

The Aircraft Systems Validation Rig or “Copper Bird,” developed during the Power Optimized Aircraft research effort in Europe provided capability to validate system performance through lab test of a half aircraft [102]. This rig provided more accurate information than available through dynamic systems modeling. However, tests of the validation rig are very expensive and time consuming. Characterizing component performance in the validation rig for the range of potential load profiles was infeasible. In 2008, a joint research effort between Hispano-Suiza and the Aerospace Systems Design Lab and Georgia Tech released results and methodologies towards parametric models of generated data extracted from the Copper Bird [233]. Surrogate models which characterized the transient performance of the generators and electric power units were created. Dynamic power loads and network configurations were provided as inputs to these unit models and electrical responses were gathered.

The data gathered included steady state parameters as well as transient signal characteristics (ripple amplitude, voltage fluctuations, distortion spectrum). While these surrogate models did not generate the time dependent waveform structure, parametric assessment of dynamic performance was available. The dynamic performance of these units were accurately predicted using neural-network regressions.

Ensuring stability of the power system at the system level requires system level dynamic modeling. However, steady-state surrogates generated from dynamic models can provide local assurance of adequate unit level performance. Providing industrial standards require dynamic analysis [179]. However, similar to regressions fit to the Copper Bird components, surrogate models generated from the transient responses of dynamic models can provide some information regarding local stability, and maintain computational efficiency.

Surrogates of power systems components may benefit from the implementation of industrial standards. Partial assurance of systems stability can be enforced through the adoption of industrial standards like MIL-STD-704F for electrical systems performance [73]. These standards provide combined guidance towards system stability, power quality, and performance by way of constraints and conditions on dynamic responses. Enforcing local compliance with industrial standards through sizing constraints can assist the surrogate modeling of unit level components.

Observation: *Power system transient requirements are emergent.*

4.1.1.5 Time Dependence Observations/Conclusions

Time dependence adds to systems modeling complexity by requiring the identification of total mission energy requirements and time dependent system and unit level requirements. Traditional mission definition and systems level dynamic modeling address time dependence at different levels of abstraction.

The observations from this chapter can be characterized in figure 11. This figure

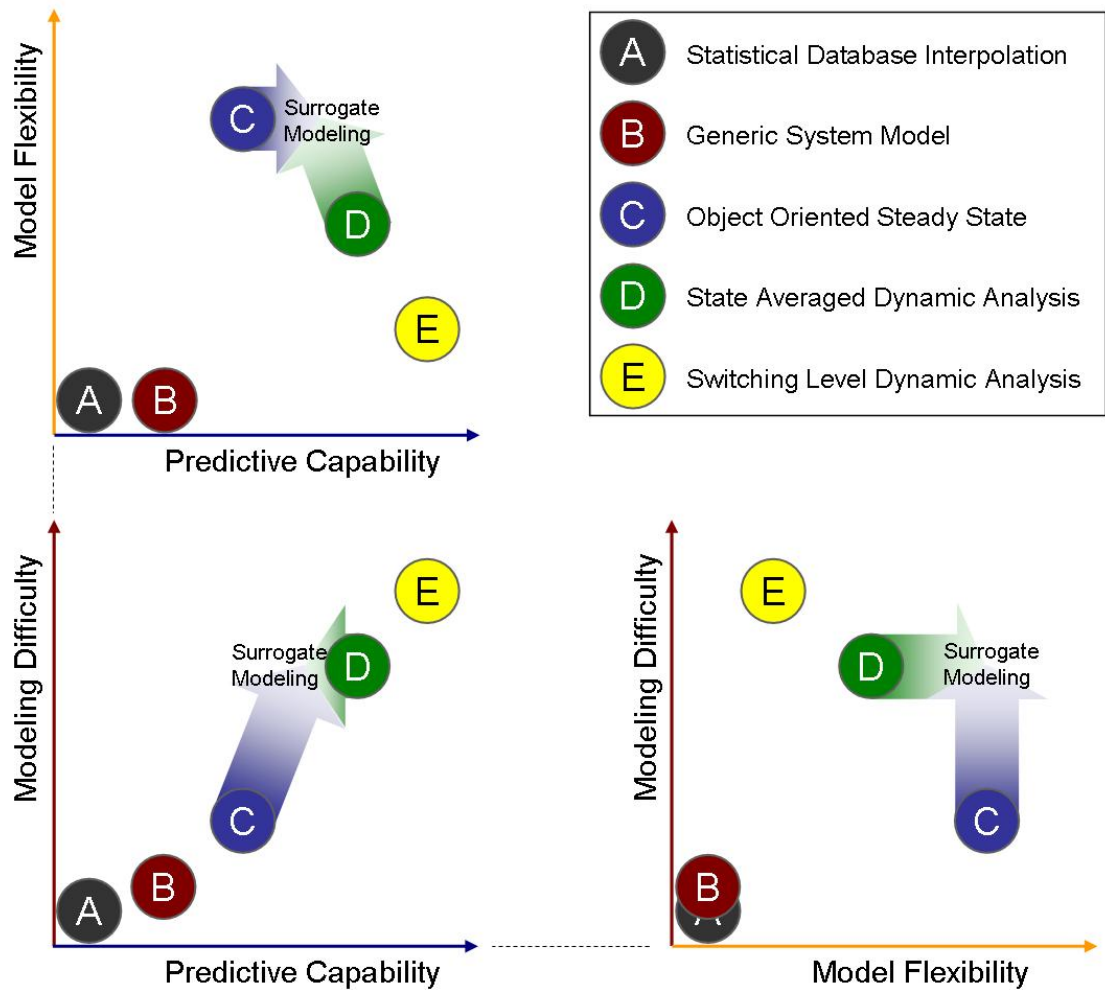


Figure 11: Tradeoff Between Predictive Capability, Model Flexibility, and Modeling Difficulty for Vehicle Systems Modeling Methods

notionally characterizes the types of modeling by their predictive capability, modeling flexibility, and modeling difficulty. Surrogate modeling attempts to achieve greater predictive capability while maintaining the flexibility of a steady state systems model.

Dynamic analysis is necessary to verify the fulfillment of all MIL-STD or other regulations. It is also necessary to amend platform requirements. During the conceptual design phase, with a multitude of potential architectural concepts, dynamic analysis are difficult to set up and execute for a highly flexible design space. Additionally, dynamic models are not typically intended to predict device size for exploration of high level architecture structure. Models are needed during early architecture development whose constructs and convergence are not endangered by major upheavals in product structure, and whose execution can be accomplished in a timely fashion.

Non time-domain modeling is insufficient for predicting detailed system attributes and requirements. “Quasi-steady state” models do not provide sufficient information regarding system level stability in regards to dynamic performance. Generalized transient considerations communicated by fixed values they can be used to assist in justifying the high level power systems architecture concept.

4.2 Operating Mode Dependence

Functional and physical perspectives are not sufficient to completely define architecture specifications. A complete set of design requirements are not guaranteed by simply completing functional specification [194]. Functions must be linked to the fulfillment of some higher level operational need.

An operating mode can be defined as the implementation and behavioral state of the system which governs performance and functionality in a given environment. With a varying architecture structure, sizing critical operating scenarios will force requirements to be deployed differently for different architecture concepts. Some scenarios which posed little problem with existing architectures may drive unit or

platform level requirements. Additionally, new functions may be introduced during a sizing critical scenario. A systematic means for identifying off-nominal sizing cases is necessary when exploring and justifying the pursuit of novel architecture concepts.

The traditional source for platform level systems operating requirements stem from the aircraft mission. In the previous section, the platform level energy requirements were discussed. Specific mission phases present potentially active constraints which drive the necessary physical attributes of the aircraft. Sizing critical scenarios generate active constraints on the attributes of the system. They represent the conditions which introduce the maximum demand in terms of load or energy requirements.

This section explores means for defining operating scenarios during aircraft conceptual design. Scenario based design techniques which have been adopted in model based systems engineering [MBSE] are discussed. The applicability of scenario based design tools to the identification of architecture specific emergent requirements during exploratory design is also considered.

Sizing critical requirements are often derived from off nominal operational considerations. Tools and theories like fault tolerance, contingency planning, failure management, and performance degradation techniques are traditionally used to configure or analyze the operating mode dependence of complex systems.

4.2.1 Scenario Based Design

Scenario based design is a “set of perspectives and approaches” integrated to provide an “object-oriented model of the user’s task domain [40]” and addresses the means for identifying system operating modes. These tools were initially intended to assist the computer systems engineering community in generating requirements [113], determining behavior and functions, and defining the concepts towards their fulfillment [180]. Additionally, scenarios based design techniques provide means for description, test, and validation of interfaces during design and implementation [295].

Kuutti describes a scenario as a sequence of acts [181], activity in narrative form [220], or situations or episodes with temporal elements [304]. Scenarios represent instances of use or intentional use of the system.

Potts has said:

“In the broad sense, a scenario is simply a proposed specific use of the system. More specifically, a scenario is a description of one or more end-to-end transactions involving the required system and its environment [234].”

Similarly, Kahn describes scenarios as follows:

“A scenario results from an attempt to describe in more or less detail some hypothetical sequence of events ... the scenario is an aid to the imagination [159].”

A scenario is characterized by an initial and final state connected by transitional actions, events, and other concurrent scenarios [9]. Uses, behaviors, user interactions, and environment conditions are all needed to define scenarios [180].

Go identifies four areas of application for scenario based design techniques. These include strategic planning, human-computer interaction (HCI), requirements engineering, and object-oriented analysis/design [113]. Table 7 outlines the uses of scenarios in these fields.

Different tools and perspectives are required with each of these four scenario based design communities. Determining the sizing critical operating scenarios which constrain the attributes of vehicle systems tends to focus more on the latter perspectives of scenario based design: requirements engineering and object-oriented analysis/design. The next sections discuss the perspectives taken with these scenario based design tools. Review of the fields of scenario based strategic planning and HCI are discussed in appendix A.

Table 7: Uses for Scenarios in Various Fields [113]

Field of Application	Scenario Based Design Uses
Strategic Planning	Envisioning uncertain future environment Providing communication tool Organizational learning Sharing a mental model among stakeholders
Human-Computer Interaction	Analyzing user tasks Envisioning future work Mock up and prototyping Evaluating the constructed system Deriving learning materials Developing design rationale
Requirements Engineering	Eliciting user requirements Deriving specifications Analyzing the current system usage Describing the current system usage Constructing test cases
Object-Oriented Analysis	Modeling objects, data structures, and class hierarchy Analyzing problem domain Providing a model of real-world objects

Scenario based requirements engineering presents systematic means for uncovering requirements similar to the process of mission analysis. Scenario based object-oriented analysis and design uses scenarios to apply requirements to a system in terms of functional structure.

Many scenario exploration tools and processes exist which attempt to encapsulate the users' requirements. Creative applications are needed in different development circumstances [194]. Many tools have been developed in order to manage scenarios for specific projects, but "no generally accepted tools exist [295]." Hsia states:

"Although much work has been done to apply [scenarios], there is still no systematic and formal methodology to automatically identify, generate, analyze, and verify the scenarios of a software system [139]."

Typical tools revolve around generating scenarios, using them effectively, and building complete operating scenario representations [194]. While tools specific to

strategic planning and human computer interactions are useful in other fields, the tools discussed in the next two subsections focus on the elicitation of requirements and the organization of a system in terms of fulfilling those requirements.

4.2.1.1 Requirements Engineering

Requirements engineering benefits from a systems viewpoint, which causes scenario based design to be more “concrete and process oriented [113].” Breaking from the traditional data flow model for deriving software requirements development, analyzing scenarios provides a means of describe necessary system attributes and behavior as directed by the user [139]. Requirements scenarios provide details regarding the specific uses of a system to produce technical specifications. Therefore, they necessarily include representations of sequences of operations [182]. One early approach implements scenarios to infer requirements in a sort of conceptual “prototyping” process. Hooper and Hsai write:

“In prototyping by use of scenarios, one does not necessarily model the system or any component thereof directly, but rather represents the performance of the system for selected sequences of events [136].”

Methods for scenario based requirements elicitation take many different perspectives. All provide logical approach to the analysis and description of system operations, function, and behavior. Nuseibeh and Easterbrook state:

“Since RE [requirements engineering] must span the gap between the informal world of stakeholder needs, and the formal world of software behavior, the key question over the use of formal methods is not whether to formalize, but when to formalize [226].”

Formalization of requirements definition requires some assumed structure to the requirements definition and architecting process. While the tools discussed in this

section provide formal approaches to requirements description, the perspective taken by these tools may or may not be applicable to the definition of requirements at the unit level.

Five tools and approaches are discussed here in terms of their applicability to the definition of emergent operational requirements. These are inquiry-based cycle models (IBCM), questions-options-criteria (QOC) methods, claims analysis, formal scenario analysis (FSA), and task analysis and modeling. The review of these tools is recorded in appendix B.

The aerospace engineering community takes a healthy scenario view in terms of mission and constraint analysis. Mission scenarios are critical to the definition of both load and energy requirements. There is a direct correlations between aircraft mission analysis and computer systems scenario based design techniques. Both are used in describing and constructing use cases which specify systems requirements during system architecture development [113].

4.2.1.2 Object-Oriented Analysis/Design

Scenario Based Object-Oriented Analysis/Design intends to create a “world model” by defining “objects, data structures, and model class hierarchy” [113]. As discussed in chapter three, an object oriented approach towards systems modeling has been adopted by many systems integration efforts.

Object-Oriented scenario based tools focus on the interrelationships between the system, system elements, and the environment. These tools may be used to define system level functions which are necessary in the accomplishment of some goal or requirement. They may also work towards understanding or defining specific relationships between system elements which do or must exist in the fulfillment of some system level objective. These methods define users, system elements, and the environment in terms of objects and different to explore how these objects interrelate

operationally. The attributes and performance of specific objects do not come into play. Jacobson argues:

“We therefore do not think the very first model of a complex system should be a object model. Instead, it should be a model that describes the system, its environment, and how it and its environment are related. In other words, it should describe the system as it appears from the outside; that is, a black-box view [146].”

Sufficient understanding of the requirements and potential relationships which exist between these “black-boxes” is necessary to construct appropriate operations models. These use-cases represent scenario classes which drive the system development and verification. Jacobson writes in regard to the use of scenarios during object-oriented systems engineering:

“The analysis process produces two models. From the requirement specification, a requirements model is created in which we specify all the functionality of the system. This is mainly done by use-cases in the use-case model which is a part of the requirement model ... The requirements model also forms the basis of another model created by the analysis process, namely the analysis model. The analysis model is the basis of the system’s structure [147].”

The specificity to which these models must be defined affects its applicability and flexibility to concept trades. According to Robertson, the goal for an object-oriented project is to “identify a set of classes and objects, specify their interrelations, and define their behaviors and responsibilities in such a way that they support a variety of activities within an application domain [248].” However, the degree to which the architecture must be predefined limits the ability of these tools to instantiate an

architecture while automatically identifying the sizing critical requirements associated with operations.

Developing use cases requires an understanding of objects and interactions with states, and transitions. The Object Management Group (OMG) see model based systems engineering in two domains: structural and behavioral. OMG's Unified Modeling Language (UML) expresses structure in terms of depends on classes, objects, component, packaging, and structures. Additionally it captures operational aspects in terms or behavior with activity, interactions, use case, and state Machine diagrams.

Thus as Go states with respect to OOA/D:

“Object-oriented analysis/design models an application domain. Its view is that of a system model [113].”

The tools and processes pursuant to scenario based OOA/D focus on the definition of objects which represent the system elements and users. Five tools (use-case diagrams, state and transition diagrams, interaction diagrams, activity diagrams, a responsibility driven approach, and automated modeling support) are discussed in this section. Tool overviews are given in appendix C.

4.2.1.3 Scenario Based Tools Evaluation

During the early stages of vehicle systems architecture definition and trades it is important for system architects to generate requirements which justify the selection of a specific technology or configuration over another. Similar to the trades regarding the level of accuracy of time dependent models, systems architects must determine what information regarding the interrelationships between systems elements is necessary for initial trades. Modeling operating modes in terms of logic level interactions between units or components is not feasible during large scale platform trades. On the other hand, the traditional mission profile may not be sufficient in generating requirements

which elicit the fundamental capabilities required at the unit level. Proper perspectives must be maintained during the exploratory design of aircraft vehicle systems.

These perspectives and modeling needs are discussed in terms of the classifications provided by the Cooperative Requirements Engineering With Scenarios (CREWS). The Basic Research Action, under the European Commission’s 4th Framework Programme and Rolland et. al. propose this CREWS framework for scenario tools classification. In their paper, *A Proposal for a Scenario Classification Framework*, they characterize scenario approaches in four categories: form, contents, purpose, and life cycle [251]. This characterization is shown in table 8. For the exploration of requirements which emerge from complex aircraft power systems, a scenario based tool would have attributes as indicated in this table.

Table 8: CREWS Scenario Classification Categories [251]

Form View: Descriptions and Presentations				
Notations	Formal*	Semi-formal	Informal	
Interactivity	Static	Animated	Interactive*	
Contents View: Kind of Information Captured				
Abstraction	Concrete*	Abstract	Mixed	
Context	System Functionality*	Enterprise		
Argumentation	Issues*	Positions*	Arguments	Decisions
Coverage:				
Functional	Structure*	Function*	Behavior*	
Intentional	Goal Dependence*	Problem*	Responsibility*	Cause*
Non-Functional	Constraints*	Capability*	Flexibility*	Portability
Purpose View: Capturing System Requirements				
RE Process Role	Descriptive	Exploratory*	Explanatory	
Life Cycle View: Scenario Capturing and Augmentation				
Lifespan	Transient	Persistent*		
Capture	From Scratch*	Reuse*		
Augmentation	Integration*	Refinement*	Expansion*	Deletion*

(* indicates necessary attribute for identification emergent scenarios of vehicle systems)

Form View: Using scenario based design techniques to determine operational requirements which emerge due to architecture changes requires a feedback between

operations definition and physical architecture definition. This presents difficulty when managing the assumptions adopted during scenario based design. The form of the tool must be formal and interactive. While illustrative, semi-formal and informal representations of scenarios, like textual descriptions, storyboards, and videos [195], are insufficient to support the flexibility necessary during the architecture trades process. For scenarios to emerge and expand depending on architecture decisions, a scenario tool must be interactive following specific structural guidelines.

Contents View: The contents of the scenarios must be concrete in accordance with requirements engineering scenarios. Scenario tools must also take a system functionality view as opposed to an enterprise view. With regards to argumentation, information regarding issues (“descriptions of problems or conflicts”) and positions (“descriptions of alternative solutions to a problem”) would be necessary [251]. However, definition decisions regarding the selection of a positions would fall into conceptual architecture definition and not be derived by the scenario tool.

Due to the nature of architecture complexity as discussed in chapter three, all functional and intentional coverage issues must be included in order to identify emergent requirements. This includes coverage of non-functional issues. This requires that constraints be managed for architecture sizing, adequate capability be ensured by the designers during architecture definition, and flexibility be provided in order to allow for architecture trades.

Purpose/Life Cycle Views: Determining emergent requirements during conceptual architecting necessitates an exploratory role for scenario based design. Information regarding new operational requirements must be provided by individual units, combinations of units, or specific relationships. This information must be readily available and programmable so as to automatically instantiate legitimate operational requirements during the physical definition and sizing of a specific architecture.

In exploring architecture trades, requirements emerge, are augmented, and disappear depending on changes to the system definition. Therefore, to support flexibility the scenarios must support all augmentation and capturing techniques. They must also be persistent because they drive requirements definition. Insight must be made available when emergent sizing critical scenarios are carried through to latter design stages.

Table 9: Evaluation of Scenario Based Design Tools for the Identification of Emergent Operational Requirements w.r.t CREWS Scenario Classification Views [251]

	Notation	Interactivity	Abstraction	Context	Argumentation	Coverage	RE Process Role	Lifespan	Capture	Augmentation
RE Methods										
IBCM	-	-	+	-	+	+	+	+	+	-
QOC	+	-	+	+	+	-	-	+	+	+
CA	-	+	+	+	+	+	-	+	+	-
FSA	+	+	+	+	+	-	+	+	+	+
TA&TM	+	+	+	+	+	-	+	+	+	+
OOA&D Tools										
Use-cases Diagrams	+	+	+	-	+	-	+	+	+	+
Interaction Diagrams	+	+	+	-	+	-	+	+	+	+
Activity Diagrams	+	+	+	+	+	-	+	+	+	+
State Transition Diagrams	+	+	+	+	+	-	+	+	+	+
Responsibility-Driven Approach	-	+	+	+	+	+	+	+	+	-

Each of the tools/approaches discussed in this section are evaluated in table 9 with respect to the operational dependence of the vehicle systems architecture as addressed during conceptual architecting. In classifying and comparing these tools using the CREWS classifications it was observed that many of the tools used for requirements engineering are insufficient due to informal notations and limited reconfigurability. Scenario based, object-oriented tools exhibit a more formal and interactive notation beneficial to an adapting architecture. However, the context of these tools focused

more on interactive exchanges primarily in the form of information. Ultimately, it was observed that formal scenario analysis, activity diagrams, and state transition diagrams are the most appropriate tools for expressing functional requirements towards concept architecture trades.

Through this qualitative assessment, it was additionally apparent that the tools reviewed lacked the ability to provide sufficient “coverage” in defining the emergence of requirements. Coverage includes the functional (structure, function, behavior) and intentional (goal dependence, problem, responsibility, cause) scope. It also includes additional non-functional aspects (constraints, capability, flexibility, and portability) [251].

Most methods and tools provide various levels of insight into structure, function, and behavior. They also exhibit different degrees to which flexibility, capability, and constraints are handled. However, all tools were limited in their management of intentional coverage issues. Indeed, intentional coverage is not often included in scenario based design. Rolland states:

“Intentional models are seldom included in scenario approaches... They are, so to speak, implicitly underlying the interfaces between the re-engineering company and its environment [251].”

There is no guarantee that the sizing critical operating scenario or use-case will be identified using traditional scenario-based design tools. With these tools, the user must specify specific cases during operations description. While object oriented scenario tools provide a more formal means for expressing operating modes, they are insufficient in their ability to capture deviations from nominal operations. Problems, causes, and responsibility are all attributes of the architecture which must be managed to understand emergent operational requirements.

The object oriented structure of operation mode requirement modeling tools prohibits easy exploration of off-nominal cases as necessitated by specific architecture

characteristics. When off-nominal scenarios must be identified the interactive, formal, and object oriented nature of these tools limit portability and flexibility when introducing new implementations. Furthermore, all aspects of functional and intentional coverage interact in development of these new scenarios. Informal and unstructured methods have adequate flexibility to explore exceptions originating by physical losses. However, these tools often require long iteration cycles to consider each off-nominal case and lack portability.

The “what if” approaches for strategic planning and requirements engineering is not currently integrated with formal and flexible structural relationships provided by scenario based object-oriented analysis/design tools. Allenby observes with respect to the Unified Modeling Language (UML):

“It is worth noting that there is little guidance available within the UML standard or accompanying guidance material for the systematic identification of either ‘alternative paths’ or ‘exceptional courses’ of events in scenario or use-case descriptions. Under these circumstances, the practitioner is left with little assurance of sufficient coverage. An impediment to adoption of a use-case approach in safety critical systems is the current lack of systematic method for identification of these alternative paths in association with failure condition [7].”

While UML is only one means for expressing the implementation and behavioral space of a system, Allenby generalizes his critique to include all use-case driven approaches in considering off-nominal operating conditions. The use of traditional scenario based methods for specifying the operations impact of off-nominal sizing cases proves insufficient. While these tools may remain the backbone to operations definition, alternative methods are used during the conceptual design phase which attempt to capture the emergent operational requirements.

4.2.2 Traditional Aircraft Operating Mode Identification

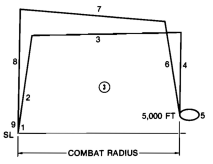
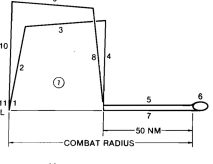
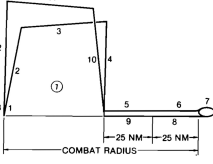
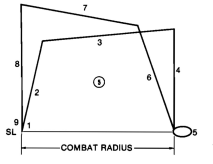

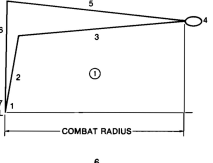
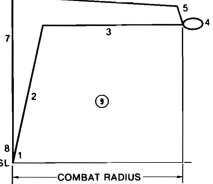
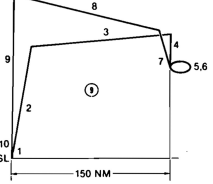
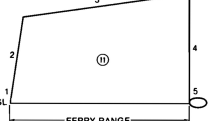
The aircraft mission is the primary source for requirements which drive aircraft sizing. This mission is cast as a group of sequential operations which must be fulfilled by the platform. Each phase/operation presents unique load and thrust requirements which may potentially drive platform level attributes. Additionally, the total sequence of operations determine the total energy requirements which govern the size of the platform. This sequence of operations produce time dependent requirements for aircraft sizing.

There exists a multitude of standard mission types for military and commercial aircraft. Each mission presents a unique set of requirements which must be fulfilled by the platform. The description of the mission can become very detailed in the level at which operations are specified. However, during conceptual design, mission analysis is typically performed at a high level. For example, a combat aircraft HI-HI-HI mission consists of 7 phases: warm up/takeoff/acceleration, climb, cruise out, combat, cruise back, descent, and reserve. This view of the mission does not constrain the physical means of fulfilling the operation, thus allowing for architecture flexibility. Table 10 displays pictorial overviews of alternative missions for the AV-8B Harrier II. While these mission can be performed by this specific platform, the Harrier is primarily designed around a Close Air Support missions. The CAS mission was therefore used as the primary source system requirements and drives the attributes of this platform.

In addition to the multiple mission phases, more information is necessary to declare the platform requirements. Information regarding the means of takeoff may be necessary. Examples of potential takeoff requirements include standard runways, deck launch, vertical takeoff, short fields, or undeveloped airstrips. Platform requirements vary widely due to specific maneuvers or conditions. In the example of the Harrier, vertical takeoff requirements dominate the performance capability of the platform.

The attributes of each platform are determined by the fulfillment of the power,

Table 10: Alternative Missions for the AV-8B Harrier II [1]

Mission	Pictorial Representation
Attack Configurations	<p data-bbox="743 489 971 520">Close Air Support</p>  <p data-bbox="743 657 930 688">HI-LO-LO-HI</p>  <p data-bbox="743 835 1060 867">Modified HI-LO-LO-HI</p>  <p data-bbox="743 1014 881 1045">HI-LO-HI</p>  <p data-bbox="743 1077 898 1108">LO-LO-LO</p> 
Air-to-Air Configurations	<p data-bbox="743 1266 865 1297">HI-HI-HI</p>  <p data-bbox="743 1486 1084 1518">Deck Launched Intercept</p>  <p data-bbox="743 1696 1003 1728">Combat Air Patrol</p>  <p data-bbox="743 1854 816 1885">Ferry</p> 

thermal, and energy requirements generated from the primary missions. Mission operations impose specific performance demands through the magnitude boundary function requirements. These requirements in turn size a portion of contributing vehicle systems. The sequence and sum of all mission operations also impose requirements on the architecture.

Traditional ‘sizing’ is occupied primarily with determining the takeoff gross weight of the aircraft by constraining platform scaling parameters and predicting the takeoff gross weight of the aircraft (W_{TO}) for a given mission. Mattingly’s constraint analysis derives loading requirements through a force balance on the aircraft. This force balance yields an equation relating the thrust-to-weight ration at sea level takeoff $\left(\frac{T_{SL}}{W_{TO}}\right)$ to the takeoff wing loading at takeoff $\left(\frac{W_{TO}}{S}\right)$ as displayed in equation 1 [201]. The required thrust capability (a) is expressed as a function of thrust lapse (α) and the installed thrust at sea level (T_{SL}) and is constrained by the aerodynamic forces (b) and excess power (c).

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

(a)
(b)
(c)

(1)

Manipulation of this sizing equation for each mission operation yields a constraint which limits the relationship between thrust to weight and wing loading. Thus, the first consideration for platform level sizing is the magnitude of the load requirements for a given scenario. These sizing critical sizing scenarios limit the design space and drive the physical attributes at the platform level. A carpet plot for a notional aircraft from Mattingly is seen in figure 12.

After completing the constraint analysis, the takeoff gross weight of the aircraft must be determined to obtain the size requirements of the platform. This is done through mission analysis. The attributes of all energy storage devices depend on the

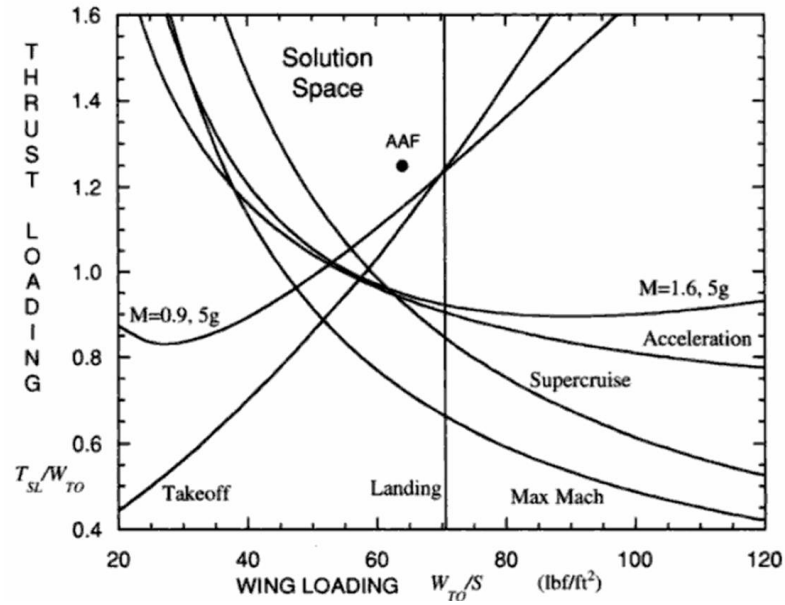


Figure 12: The Compete Preliminary Air-to-Air Fighter Constraint Diagram from Mattingly [201]

bulk of energy they must store to provide for future operations. Historical information [244], as well as tools like the Breguet range equations and max endurance equations [8] are used to estimate the fuel burn required to fulfill each portion of the mission.

Mission sizing is inherently iterative. Mission analysis is an process of estimating the takeoff gross weight following systems weight approximations, estimating the fuel burn for each portion of the mission, determining the block fuel, and iterating. This fuel weight is in turn used to augment the magnitude of the functional requirements on platform and vehicle systems (span, wing area, structures, control forces, etc). To determine energy storage requirements, load requirements for all segments must be applied in terms of the size and weight of the platform (e.g. β , or weight lapse for traditional constraint analysis). Once total fuel burn, weight lapses, and takeoff gross weight are obtained, the thrust requirements and physical dimensions are determined.

This process for platform level sizing provides the ability to estimate platform level performance. However, it gives little guidance as to how load requirements are allocated to the vehicle systems level. Additionally, models to determine the

attributes of the vehicle systems are not as easily obtained as the attributes estimated with Mattingly's equation. Additional information must be provided which deploy time sensitive requirements to the unit level. Vehicle systems attributes in turn impact the volumetric, weight, reliability, and power demand of vehicle systems. This would potentially require an integrated means for augmenting the drag polar, thrust lapse, weight lapse, and systems weights due to changes in vehicle systems concept.

4.2.2.1 Traditional Off-Design Systems Sizing

Traditional aircraft design operates within a comfort zone which typically deviates only slightly from previously designed architecture concepts. This allows conceptual designers to be secure in assumptions made regarding the impact of a given system failure. Systems architects are fairly certain when each system is active and necessary during the mission and potential contingencies which must be introduced given systems failures.

Working within the historical database allows the critical sizing scenarios to be dictated from previous experience. Traditional tools for expressing platform level mission requirements (CON OPS, Scenario Tools) can manage the typical sizing cases in a straight-forward manner. Typical mission sizing accounts for additional energy requirements during off-nominal operating conditions by means of the inclusion of a reserve mission segment. Other standard sizing scenarios like ETOPS (Extended-Range Twin-Engine Operations) [85, 100] or engine out on take-off are traditionally driving cases for the commercial two engine aircraft and have the tendency to drive unit level attributes. These cases present new mission phases and additional performance constraints. Corresponding alterations to the coefficients in Mattingly's constraint equation can be easily imposed in platform sizing.

During the conceptual design phase, sizing critical failure cases are often identified by inspection and inference. A more complete and detailed analysis takes place

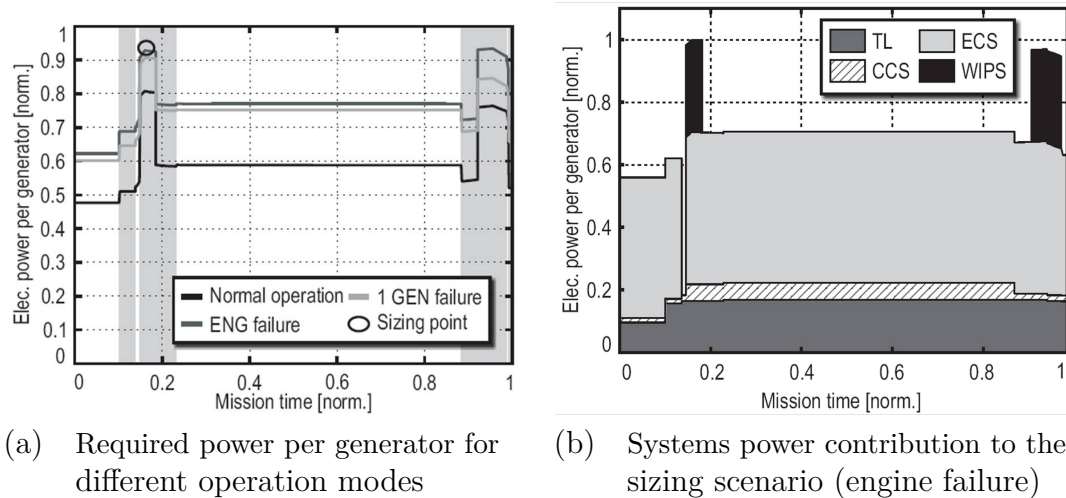


Figure 13: Liscouët-Hanke Bleedless Architecture Electric Power System Generator Contributing Power Requirements from Technical Loads (TL), Environment Control System (ECS), Commercial Control System (CCS), and Wing Ice Protection System (WIPS) [190]

later in the design process to ensure that an already defined architecture can meet reliability requirements and maintain maximum operational capability. Initially, however, rough estimates of unit reliability, symmetry, and necessary redundancy allow designers to assume which failure modes will be sizing critical. The selection of sizing critical cases correspond to losses of units or combinations of units which support the largest or most critical loads. Hence, typically adopted failure modes include engine and generator failures as illustrated in the results of the work by Liscouët-Hanke as illustrated in figure 13.

What is evident in figure 13 is the large increase in power requirements which are introduced by system failures. The peak power demand per generator increased by approximately 15% between the normal operations and engine or generator failure cases.

However, problematic to the exploration of a new architecture design space is the predefinition of performance degradation strategies applied during failure states. Increases in power requirements at the unit level are defined subject to specific predefined degradation profiles. The load degradations which yield the results illustrated

in 13 and are given table 11. Failures, and their subsequent effect on system operating modes impact the sizing of each element within the architecture. The behavioral impact of a specific failure is indeed manifest through the functional loss incurred by physical failures. In the cases addressed in table 11, reduction in behavioral requirements during degraded operating modes are dependent on the architecture concept.

With an unknown or flexible architecture, specific physical failure cases do not have discrete predefined effects on the change in magnitude of functional or operational requirements. When losses occur, the maximum available performance would be desired from the remaining systems so as to minimize deviation from the normal operating mode, and prevent further damage and cost. While these strategies are tacitly predefined, optimal strategies are necessarily emergent due to complex interactions between components. If the architecture is augmented, performance degradation strategies must be augmented accordingly.

Table 11: Liscouët-Hanke Operating Mode Degradations [190]

Considered Operation Modes	Load Shedding Scenario		
	Normal	1 Gen Failure	1 Eng Failure
Technical Loads (TL)	No Load Shedding		
Commercial Control System	No Load Shedding		50% Load
Wing Ice Protection System	Anti-Ice	Only De-Ice if Available	
Environment Control System	Normal	Normal	Minimum Airflow
Architecture	Number of Generators		
Conventional	2	1	1
Bleedless	4	3	2

The demand side reduction of requirements must reflect the minimum loss to the platform concept. The platform level functional loss incurred through the loss of a unit or group of units depends on the total embodiment of the architecture. Predefined assignments of contingency requirements are effective with traditional and evolving architecture concepts. However, the development of large quantities of revolutionary architectures requires more exploratory approaches to the identification of off-nominal

sizing cases. With revolutionary technologies and architectures, the criticality and behavioral effect of specific unit or combination of units should not be prematurely assumed.

Observation: *Off-nominal operating modes have the potential to present significant and architecture specific increases to unit level requirements.*

Observation: *Load shedding and performance degradation strategies are traditionally either predefined or tacitly identified during concept definition.*

4.2.3 Load Shedding and Performance Degradation

Unlike other complex systems, a loss of some aircraft level functions, even temporarily, may lead to loss of aircraft and life. The aircraft mission can not simply reboot, restart, or undergo immediate maintenance. The introduction of off-nominal operating modes during aircraft performance is based on the concept of demand response.

With reductions in the load providing capability through failure, the system must recover by reducing demand to a range which can be provided by the remaining intact systems. Naturally, by conservation of energy, the total power available must exceed total power required. Hsu et. al. write:

“For the steady-state operation of a power system, the total input mechanical power of all generators has to be equal to the sum of total connected loads and system loss [140].”

New systems architectures necessitate new strategies for load shedding, which in turn generate new sizing critical requirements. Catastrophic failures may result from neglecting the identification of appropriate load shedding schemes as illustrated by the 1992 China Steel Corporation plant failures. It was discovered that a plant blackout stemmed from an inadequate load shedding scheme following system modification and expansions [140]. Enumerating new operating modes due to failure cases in a flexible

architecting environment necessitates the an understanding of the functional losses incurred by physical failure.

For systems of systems like supply chains (e.g.- dairy products or consumer goods) or power networks (e.g - electrical or natural gas distribution), demand response involves the de-incentivizing at peak demand times through pricing and other controls. However, for a monolithic system like an aircraft platform load management systems demand response takes the form of load shedding.

The modern commercial aircraft uses an electric load management system (ELMS) to manage power for system faults [211]. With reductions in power available, the ELMS is tasked with shedding loads which are determined “non-essential [191].” The order and sequence of load shedding is determined based on the criticality of the service provided and the amount of power necessary to provide the service.

This concept of load shedding applies to more than just electrical power loads. Every function performed by aircraft systems can be made subject to a form of “function shedding.” Unit systems must be categorized by how their loss impacts the fulfillment of platform requirements.

In an atmosphere of architecture variability, accurate identification of the specific failure mode which drives unit and architecture level sizing proves difficult due to the increased size of the design space. Each architecture may exhibit a unique set of sizing critical operating scenarios introduced by unique failure states. Additionally, the effect of a unit level failure is a design decision.

The capacity of each generator is not just a functions of the total power consumption. Each generator is sized depending on the peak power required from the other systems, the capacity of all generators, the reliability of every generator, and the allowable behavioral outcomes of failures in terms of necessitated reliability and desired availability. Acceptable losses incurred with the failure of a unit or group of units are constrained by safety and reliability requirements. Within this constrained

operating space, the architect has the freedom to explore design options which may reduce cost in terms of operational benefits (e.g. availability) or performance and capability improvements (e.g. reduction in fuel burn).

With a flexible architecture design space, off-nominal sizing cases pose difficulties due to emergence. Operating scenarios introduced in response to failures place new requirements on the platform which drive the thrust and performance capability of the remaining undamaged engine and systems. Deviations to the mission also effect the energy requirements from the fuel tanks and secondary power systems and require the introduction of new functions. Off-nominal operational requirements placed on the vehicle systems with degraded capabilities often present size, weight, and capability driving constraints at the unit level.

In order to provide a reduction in the load requirements as necessitate by loss in capability, the augmented operating space designates new structural and behavioral requirements. Alterations to the physical state of the system, including failure states, may introduces new operating modes of the system. Depending on the magnitude of function loss and the reliability of the remaining system state, changes to mission may also occur. These new modes may range from continuing the mission unaltered, continuing under reduced requirements, reducing mission scope, aborting mission, or some undesirable loss.

Observation: *Traditional scenario based methods prove insufficient for specifying the operations impact of off-nominal sizing cases.*

Research Question: *How can emergent load shedding and performance degradation related requirements be identified and explored concurrent to conceptual architecture trades?*

4.3 Reliability/Safety/Criticality Dependence

The attributes of high-assurance systems, like aircraft vehicle systems, are driven by the need to be reliable, available, safe, secure, and timely [306]. Much of the weight and cost for aircraft systems would not be necessary with lax reliability requirements. However, the result from such reduced requirements would yield unacceptable consequences. In highly integrated systems operating in environment with a high cost of failure, much care must be taken to ensure the appropriate system performance.

Reliability is an attribute of the architecture as a whole and is sensitive to the relationship that all individual units have with platform level functions. These relationships are determined by the system architecture. With traditional aircraft systems design, reliability requirements could be hierarchically allocated from platform to systems, from systems to subsystems, and so forth. Once the systems was defined, it is assessed as to its safety and reliability merits. Therefore, safety and reliability considerations are often considered after an architecture is designed. These considerations act as metrics or filters for adopting a concept architecture.

Reliability considerations play a major role in determining both contingency scenario identification and the allocation of power requirements to the unit level through redundancy considerations. The previous section addressed the necessity to introduce additional operating modes in the behavioral space when the physical system is in a certain physical state. The techniques reviewed focused on the structuring of operational requirements. However, in contrast to scenario based design techniques, safety and reliability design tools rely on generalizations regarding the impact of system losses. This section considers the means for generating quantitative requirements on physical systems to avoid the need to specify all behavioral states. The techniques discussed in this section address means for expressing the fitness of an architecture concept with respect to given behavioral requirements.

Reliability requirements are derived by estimating the consequences of failures

			Occurrence				
			Extremely Improbable ($<10^{-9}$)	Extremely Remote (10^{-7} to 10^{-9})	Remote (10^{-5} to 10^{-7})	Reasonably Probable (10^{-5} to 10^{-3})	Frequent ($>10^{-3}$)
Hazard Level	Catastrophic	A					High
	Hazardous	B					
	Major	C			Med		
	Minor	D	Low				
	No Effect	E					

Figure 14: Low, Medium, and High Risk in Terms of Hazard and Probability of Occurrence

and depend directly on the relationships between unit level functions and platform level behavior. This section looks at reliability in terms function and unit criticality. It then looks at means for assessing unit level reliability performance.

4.3.1 Safety and Reliability

Safety and reliability requirements originate from the necessity to ensure that specific levels of hazards to not occur. Safety is defined as “freedom from unacceptable risk [145].” Designing for safety requires that requirements capture considerations for potential risks and their avoidance during the product life cycle.

Risk, as defined by ARP 4754, is “the frequency (probability) of an occurrence and the associated level of hazard [272].” This is illustrated in figure 14. The risk associated with the loss of a given system function or element is a product of an operational understanding of the system. In order to designate safety related requirements at the unit level, systems engineers must understand risk associated with unit/functional loss.

Because designing for safety entails ensuring freedom from an unacceptable probability of hazards, safety requirements (constraints) are primarily communicated in terms of reliability. Reliability is defined as:

“The probability that an item will perform a required function, under stated conditions, for a stated period of time. Reliability is therefore the

extension of quality into the time domain and may be paraphrased as ‘the probability of non-failure in a given period’ [270].”

Applying conditional probability, reliability $R(t)$ over a given time step dt is mathematically represented in terms of the failure rate ($\lambda(t)$) and probability density function ($f(t)$).

$$\lambda(t) dt = \frac{f(t) dt}{R(t)} \quad (2)$$

Manipulation and integration yields a direct relationship between reliability and failure rate.

$$R(t) = \exp \left[- \int_0^t \lambda(\tau) d\tau \right] \quad (3)$$

The failure rate may take various forms depending on the nature of the component. For preliminary reliability analysis and illustration, the failure rate is often assumed constant, reducing the reliability equation to:

$$R(t) = e^{-\lambda t} \quad (4)$$

Alternative distributions may also be used in determining the component reliability. The Weibull distribution represents reliability in terms of two parameters: the scale parameter, η , and the shape parameter, β . Component reliability for a Weibull distribution is given as:

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^\beta} \quad (5)$$

Table 12, represents the mathematical relationship between the probability of failure from time on the interval $(0, t]$ ($F(t)$), the failure probability density function ($f(t)$), the reliability (survivor) function ($R(t)$), and the failure rate ($\lambda(t)$).

Table 12: Probability Relationships for Failure and Reliability [243]

	$F(t)$	$f(t)$	$R(t)$	$\lambda(t)$
$F(t) =$	-	$\int_0^t f(u) du$	$1 - R(t)$	$1 - \exp \left[- \int_0^t \lambda(u) du \right]$
$f(t) =$	$\frac{d}{dt} F(t)$	-	$-\frac{d}{dt} R(t)$	$\lambda(t) \cdot \exp \left[- \int_0^t \lambda(u) du \right]$
$R(t) =$	$1 - F(t)$	$\int_t^\infty f(u) du$	-	$\exp \left[- \int_0^t \lambda(u) du \right]$
$\lambda(t) =$	$\frac{dF(t)/dt}{1-F(t)}$	$\frac{f(t)}{\int_t^\infty f(u) du}$	$-\frac{d}{dt} \ln R(t)$	-

These equations for reliability are fundamental in determining adequate system safety. When risk limitations are allocated to the functionality of individual components, this criticality requirement acts as a constraint on unit reliability. Unit criticality relates to the stringency of reliability requirements governing the performance of a task or operation.

FAR, SAE, DOD and other safety and reliability standards relate severity of a failure to some loss of ability to perform a basic function [272, 273, 95, 72]. MIL-STD-882D defines the term ‘safety critical’ as:

“A term applied to any condition, event, operation, process, or item whose proper recognition, control, performance, or tolerance is essential to safe system operation and support (e.g., safety critical function, safety critical path, or safety critical component) [72].”

Therefore, the more critical a unit is to platform level performance, the more stringent the reliability requirements.

Designers must take steps to provide adequate reliability by requiring increases in unit reliability, by ensuring safe execution of requirements in the presence of unit failure by way of redundancy, recovery [187], or by manipulating the operational

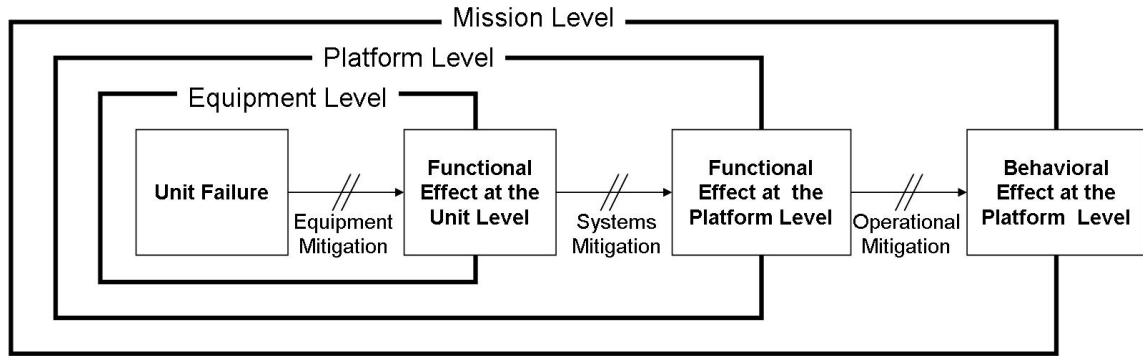


Figure 15: Adapted from EMMA’s [European Airport Movement Management by A-SMGCS (Advanced - Surface Movement, Guidance and Control systems)] Hazard Impact Assessed at the Boundary of Scope [231]

outcome of a failure. As seen in figure 15, a failure at the unit level only propagates to the change platform behavior when subsequent mitigation strategies are not applied or are unsuccessful. With new architecture design, systems architects must be aware of potential mitigation strategies at the unit, platform, and operational levels. Applying historical failure context to revolutionary architectures may place limits on these levels which do not allow for optimal integration of advanced technologies.

This concept is similarly illustrated by the FAA in their System Safety Handbook with figure 16. An adverse event does not occur due to the existence of hazards alone. Unsafe conditions of the system (failures, faults, anomalies, or malfunctions) must be coupled with less than adequate (LTA) controls for result mitigation.

Design for safety must manage multiple perspectives. Requirements engineers must first identify the hazards associated to the loss of platform level function during mission operations. Criticality must be allocated to the unit level during conceptual architecting by including decisions which ensuring safe operations. Finally, the architecture must be sized to ensure adequate reliability. The implementation of this process during exploratory design requires that long iteration cycles be avoided which are typically associated with safety assessment projects. This section discusses the framework for expressing criticality requirements, traditional means for allocating and

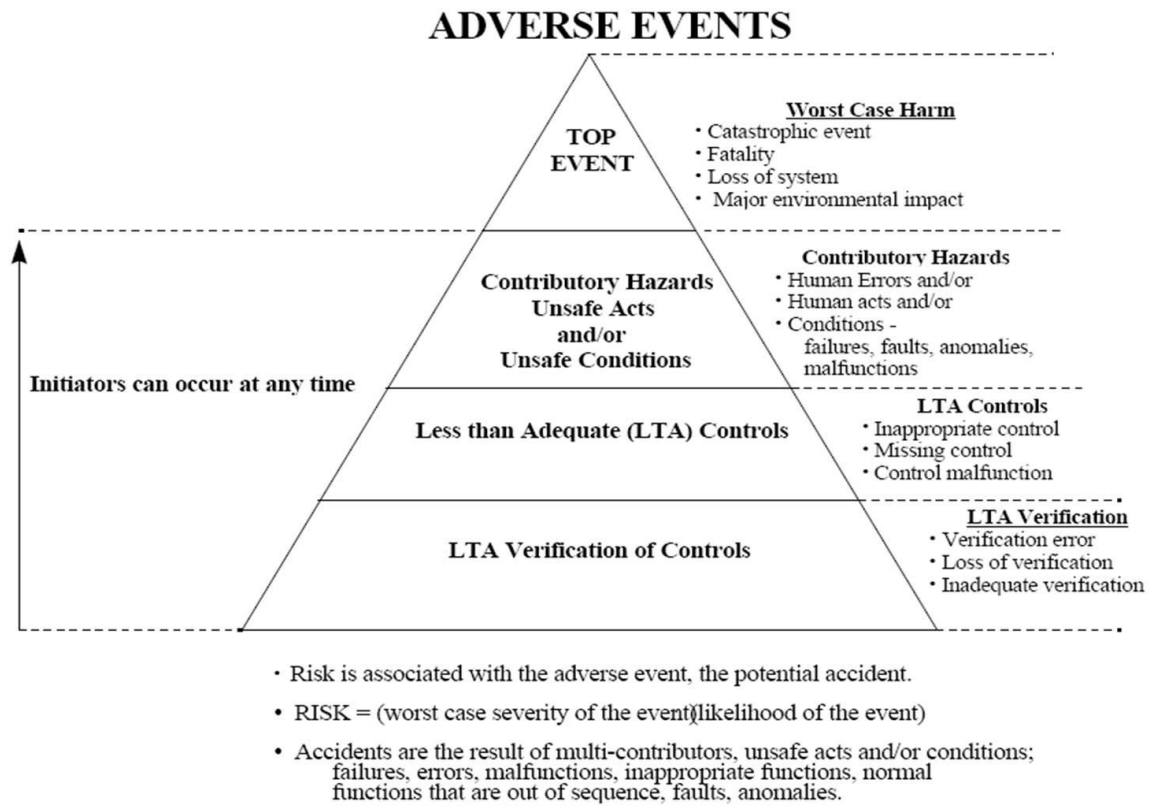


Figure 16: Relationship Between Contributory Hazards & Adverse Effects [96]

assessing systems in terms of these expressed requirements, and potential methods for flexibly addressing safety for complex architectures.

Observation: *Safety and reliability requirements are expressed as probability constraints on the behavioral space at the platform level.*

Research Question: *How are safety and reliability requirements determined and allocated to individual units?*

4.3.2 Aircraft Level Criticality Requirements

In 1988 the FAA released Advisory Circular 25.1309-1A which states:

“Many systems, equipment, and their installations have been successfully evaluated ... without using structured means for safety assessment. However, in recent years there has been an increase in the degree of system complexity and integration, and in the number of safety-critical functions performed by systems [95].”

As the complexity of the system increases and safety-critical functionalities become more integrated, more advanced techniques for structuring safety assessments become necessary. With the help of other documents, such as SAE ARP4754 [272] and ARP4761 [273], commercial industry practices were established to address safety and reliability concerns. The main goals of the tools and methods outlined in these documents are to ensure that an aircraft architecture can reliably operate without adverse effect on fundamental critical operations.

In order to understand the criticality of a given element within the system the designer must understand the result of the failure from that unit. The measure of its criticality is determined by the severity in which it adversely affects the platform’s ability to ensure safe execution of a given operation. AC-25.1309 states:

“Failure conditions adversely affecting non-essential functions would be minor, failure conditions adversely affecting essential functions would be major, and failure conditions adversely affecting critical functions would be catastrophic [95].”

To ensure safe operations, standards have been defined which limit the probability that an unfavorable result would occur. Failure results are characterized by a limiting probability that said result will occur. The FAA represents these probabilities in table 13.

Table 13: AC 25:1309-1A Failure Classifications [95]

Failure Classification	Description	Probability Condition
Minor	Probable	$p > 1 \times 10^{-5}$
Major	Improbable	$1 \times 10^{-5} > p < 1 \times 10^{-9}$
Catastrophic	Extremely Improbable	$p < 1 \times 10^{-9}$

p = probability of failure

SAE adopts a slightly different format and introduces another criticality category ‘Hazardous/Severe’ as seen in table 14.

Table 14: SAE ARP4754 Failure Classifications [272]

Failure Classification	Probability Condition
Minor	None
Major	$p < 1 \times 10^{-5}$
Hazardous/Sever	$p < 1 \times 10^{-7}$
Catastrophic	$p < 1 \times 10^{-9}$

In MIL-STC-882D the DOD defines mishap criticality in 4 categories as seen in table 15. Although no probability measure for the failure is indicated in this military standard, it does recommend that “... the qualitative mishap probability may be derived from research, analysis, and evaluation of historical safety data from similar systems [72].”

Additional safety objectives, like fail safe, impose additional constraints of systems embodiment. Fail safe requirements state that the loss of a single unit or connection

Table 15: MIL-STD-882D Mishap Categories [72]

Description	Category	Environment, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding \$10K but less than \$200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding \$2K but less than \$10K, or minimal environmental damage not violating law or regulation.

must be assumed during flight regardless of probability. Thus, every single point failure represents a necessary sizing scenario. Failure combinations must also be assumed unless the occurrence is extremely improbable.

These categorizations of criticality are the starting point for the allocation of criticality requirements to vehicle systems. Design for safety includes allocating reliability, identify the instigators of off-nominal modes, appropriately determining required capacity requirements with redundancy, and configuring the shedding of loads. This process begins the an understanding of the criticality of platform level functions. The rest of this section explores conventionally means for allocating these criticality requirements during the early design stages, as well as tools and methods for system safety and reliability assessment.

4.3.3 Allocation of Safety and Reliability Requirements

Safety and reliability assessment processes are typically applied in concert with traditional hierarchical system development processes. A generic guideline for safety assessment and design is provided in SAE Aerospace Recommended Practice (ARP) 4754 shown in figure 17 [272].

According to ARP-4754, there are 3 levels of abstraction which safety and reliability design must consider: aircraft platform, systems, and hardware level. Safety assessment begins with the development of safety requirements through functional hazard assessment (FHA) following the definition of aircraft level requirements. This is followed by traditional system decomposition and functional allocation. This process generates a platform level architecture decomposition. These generic systems groups then undergo a system level functional hazard assessment. The structure of the systems in turn determine the safety requirements at the unit level.

Functional allocation and system level FHA are performed concurrently, each contributing to the development of systems architecture. This is then followed by preliminary system safety analysis (PSSA). During PSSA quantitative tools (fault trees, reliability block diagrams, state based models) are used to verify that safety requirements are being met by the systems architecture. Requirements generated during PSSA and the resulting architecture definition allocates requirements to the unit level. Once these elements are integrated, a system safety analysis takes place in which the fulfillment of safety and reliability requirements are verified before undergoing certification.

Functional hazard assessments and each layer of system safety assessment are supported by the analysis of common cause failures. These types of failures present more stringent safety and reliability requirement due to concurrent unit or system failures originating from the same root cause. While these considerations are crucial to design for safety and reliability, they are not directly explored in this thesis.

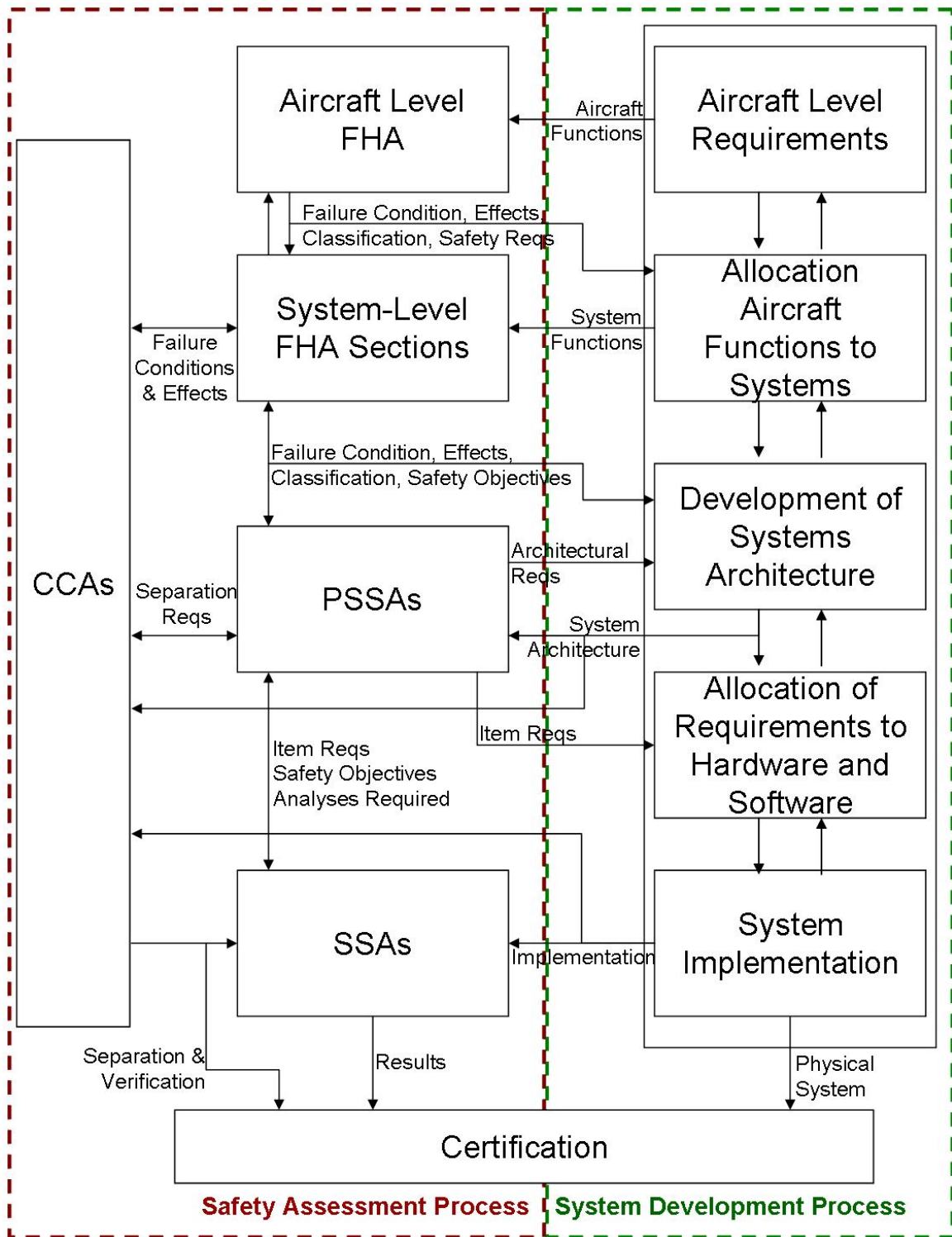


Figure 17: SAE ARP 4754 Safety Assessment Process Model [272]

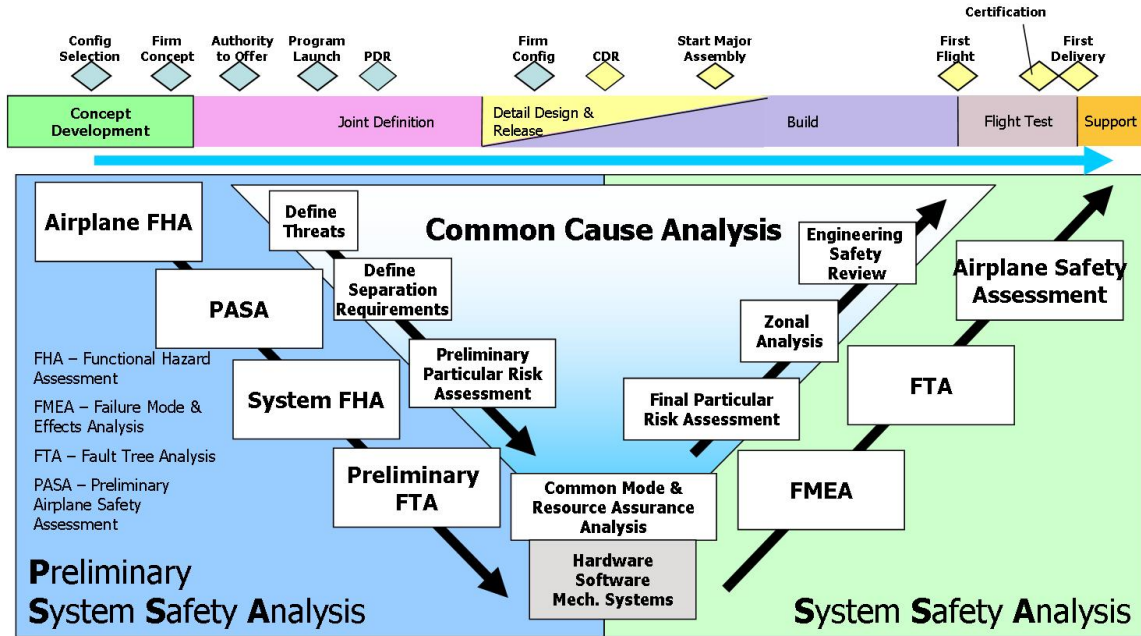


Figure 18: System Safety Analysis During the Design Process [61]

The process in figure 17 is a recommended practice and most practical implementations share similar tools and processes for determining safety and reliability requirements, allocating these requirements through architecture definition, and verifying that the requirements are fulfilled. An alternative conceptualization of design for safety is seen in figure 18. Along the top of this is the process for product development from conceptual design to delivery and support. Concurrent with this process, safety analysis takes place. This image, introduced by John Dalton, Technical Fellow Airplane Safety Engineering at Boeing Commercial, indicates that during concept development and early preliminary design is when preliminary system safety analysis takes place. This process includes functional hazard analysis, fault tree analysis, and common cause analysis [61].

Again, in figure 18, it is observed that the traditional allocation of reliability requirements to the system level follows the hierarchical decomposition of an aircraft architecture. At each level of the hierarchy a more refined system safety analysis takes place at lower levels of abstraction. Once these processes are complete further

decomposition occurs with additional detail.

Traditional processes for safety engineering suffer from the difficulty to manage large amounts of information regarding system definition, safety requirements, and certification.

Kritzinger writes:

“The hope is often that the weight (quite literally) of such evidence will be accepted as an overwhelming demonstration that the system has been adequately proven. But as systems become more complex and software intensive, assessment of the completeness and consistency of such information becomes more difficult. What is needed is a far more rigorous approach to safety, which provides logical arguments with supporting evidence and has clearly defined objectives, strategies, assumptions, and justifications [176].”

While this statement is in reference to the means from proving compliance to safety requirements, this difficulty also exists for integrating safety and reliability requirements into the definition of the system. This is magnified in an environment which allows adaptations to the systems fundamental architecture. As power systems become more central to the platform concept and the need for rapid alternative architecture concept exploration increases. Alternative processes are introduced for system architecting which break from the traditional hierarchical decomposition and functional hazard identification.

Flexible design perspective tools and processes become necessary for the application of safety and reliability requirements which may adapt with varying architecture embodiments. The field of safety and reliability is inundated with tools, methods, and approaches have been developed for defining, deploying, assessing fulfillment of safety and reliability requirements. From reviews gathered by Kritzinger there exists over 160 published generic or discipline specific tools, methods, and techniques

for addressing system safety [177]. Neglecting specific best practices, specific tools and software specified for very specific applications, table 16 summarizes the types of methods and generic tools used in designing for safety.

Table 16: Overview of Non-Discipline Specific Tools, Methods, and Techniques List Supplied by Kritzinger [177]

Focus of Reviewed Practice	Methods	Design	Math.	Eval.
		Tools	Tools	Crit.
Hazard Analysis	7*	5*		
System Evaluation	11	6*	4	1
Common Cause Analysis	3	1		
Operations	5			
System Structuring	1	6		
Incident Evaluation	9	2		
Human Factors	15		3	9
Decision Analysis & Methods	7	3		
Fault Management & Mitigation	5	1	1	
Product Test	3			

*Primary scope

Having already addressed the operational perspective and applying a system structuring based on functional induction, this section reviews mean for mathematically manipulated and augmenting the allocation of criticality criteria with changes in architecture. These tools need to be integrated and augmented to allow the designers to automatize capture of information regarding physical and behavioral reliability trades. Referring to these processes in figure 17 and figure 18, assuring system safety is a process of determining the impact of specific system losses and then ensuring that adequate probability that success will be assured.

Table 17 outlines traditional reliability tools which were evaluated towards their ability to identify off-nominal performance requirements. Focusing on preliminary system safety analysis tools implemented early in the design process further limits the state of the art review for common tools used during concept development and trades.

Table 17: Means for Reliability Allocation and Analysis

Conceptual Design Needs	Alternatives				
Hazard Analysis	Root Cause Analysis	HAZOP	SWIFT	Bow Tie Analysis	
Hazard Analysis Tools	Event and Causal Factor Charting	Functional Hazard Assessment	FME(C)A	Dependence Diagrams	...
System Evaluation Mathematical Tools	Markov Analysis	Petri Net Analysis	Reliability Block Diagram	Fault and Event Trees	SyRelAn

4.3.3.1 Hazard Analysis

A hazard is defined as “any condition, event, or circumstance, which could induce an accident, a potentially unsafe condition, a situation which has the potential to lead to harm [186].” Once the platform level functions are understood and structured, and the operational context is defined, the designer now has enough information to begin assessing the safety and reliability implication of the system. Hazard analysis is intended not to evaluate a system for its effectiveness in fulfilling safety requirements but to identify specific hazards that impose reliability requirements.

Hazard analysis can be either inductive or deductive in form. Inductive reasoning is bottom-up and typically works from a known potential cause of failure and traces it to the predicted outcome. Deductive analysis is top-down and begins with specific hazardous conditions and explores failures which must take place for such an outcome to occur. Both perspectives are necessary in the design process.

Like many tools and methods applied during early conceptual design stages traditional tools suffer from an inappropriate perspective. During concept development, and in an environment where the physical structure of the system is unknown and flexible, the hazard impact of specific physical device failures on the system as a whole is also non-static. In such an environment, specific events at the technology level have an unknown impact on system performance and behavior.

HAZOP

Hazard and operability studies (HAZOP) is a structured means for examining an existing well-defined process or operation through exposing potential hazards [103] which originated from the design of petrochemical plants in the mid 1960's and extended into the domain of software development. The original focus for HAZOP was the characterization of the flow of material throughout a chemical plant. Once normal operations are identified, deviations from this ideal point are characterized by a series of guidewords as outlined in table 18.

Table 18: Descriptions of Deviation Guide Words for HAZOP [168]

Guide Word	Deviation
NONE	No forward flow when there should be - ie, no flow or reverse flow
MORE OF	More of any relevant physical property than there should be - eg, higher flow (rate or quantity), higher temperature, higher pressure, higher viscosity, etc
LESS OF	Less of any relevant physical property than there should be - eg, lower flow (rate or quantity), lower temperature, lower pressure, etc
PART OF	Composition of system different from what is should be - eg, change in ratio of components, component mission, etc
MORE THAN	More components present in the system than there should be - eg, extra phase present (vapor, solid), impurities (air, water, acids, corrosion products), etc
OTHER THAN	What else can happen apart from normal operations - eg, start-up, shut-down, uprating, low rate running, alternative operation mode, failure of plant services, maintenance, catalyst change, etc

A subsequent method based on HAZOP, Software Hazard Analysis and Resolution in Design (SHARD), augments these guidewords for applicability to software developments. These alternative guide words are characterized by flow type. Service flow deviations are characterized by omission and commission. Timing flow error types are early and late. And finally, value errors are subtle and coarse [103].

Once normal operations are identified and appropriate flows have been defined, deviations of each type are explored in terms of possible causes, consequences, and action required. These actions consist of deviation operations with potential new assets required. The result is a “word picture” of what should be happening in the

presence of deviations [54] and usually takes a tabular form.

For flexible architectures, HAZOP, like most safety design processes, suffers from lack of general applicability and adaptability. When considering a new design, HAZOP is intended to be performed by a large team. In the example of a chemical plant design, this team is recommended to consist of at least six members: a project or design engineer, a process engineer, a commissioning manager, a control system design engineer, a research chemist, and an independent team leader [168]. Each major item within the system typically demands 1.5 to 3 hours of consideration, thus requiring weeks of evaluation from a relatively large team for a concept system [168].

HAZOP is not intended as a redesign exercise but a means for defining the appropriate operation envelope for a system [54]. Adaptations in the architecture may potentially negate the required actions and introduce new consequences. Thus, HAZOP is limited by its ability to quickly and accurately respond to alternative configurations.

SWIFT

Developed as an alternative to HAZOP, the structured what-if technique (SWIFT) takes a higher level perspective to inductive analysis. While HAZOP addresses deviations on a “item by item, procedure-by-procedure” basis for the complete system. SWIFT focuses on the top level perspective of the system [197]. It benefits by its flexibility and general applicability. There is no generally accepted means for “what-if” questioning. However, a general decomposition is displayed in figure 19.

Previous knowledge informing the team engaging in the SWIFT process could include previous hazards or incidents, known issues, regulations, etc. Macguire suggests organizing questions in specific categories. These categories include material problems, external influences, operating errors and other human factors, analytical or sampling errors, equipment or instrumentation malfunction, process upsets of unspecified origin, utility failures, integrity failure or loss of containment, emergency

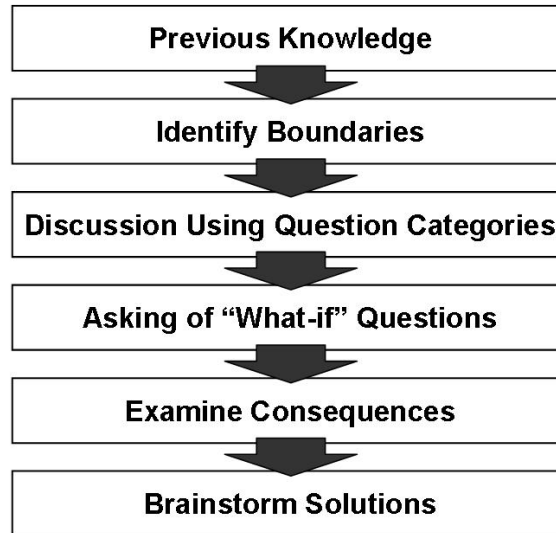


Figure 19: Process for Structure What-If Techniques [197]

operations, and environmental release [197].

‘What if’ questions are not intended to predict formal future scenarios but to bound the operating space of the system and explore potential future changes. The advantage to SWIFT over HAZOP is a free form structure and non-distinct wording for hazard discussion. However, this advantage becomes an issue when attempting to systematically allocate hazard related requirements to a flexible structure.

Root Cause Analysis

Causal analysis, widely applied during incident evaluation, tries to determine the *why* behind the *what* and *how* of a failure by defining the root causes [252]. As stated in the Department of Energy’s Order 5000.3A:

“The basic reason for investigating and reporting the causes of occurrences is to enable the identification of corrective actions adequate to prevent recurrence and thereby protect the health and safety of the public, the workers, and the environment [71].”

The US Department of Energy identifies six application specific methods used in the field of cause analysis: event and cause factor analysis, change analysis, barrier analysis, management oversight and risk tree (MORT) analysis, human performance evaluation (HPE), and Kepner-Tregoe problem solving and decision making [71]. Since the focus of this work is on the conceptual architecting of a flexible physical, the scope reduces to the tools reviewed in table 19.

Table 19: Root Cause Identification Methods as Reviewed by the DOE [71]

Method	When to Use	Advantages	Disadvantages	Remarks
Events and Causal Factor Analysis	Use for multifaceted problems with long or complex causal factor chain.	Provides visual display of analysis process. Identifies probable contributors to the condition	Time-consuming and requires familiarity with process to be effective.	Requires a broad perspective of the event to identify unrelated problems. Helps to identify where deviations occurred from acceptable methods.
Barrier Analysis	Use to identify barrier and equipment failures and procedural or administrative problems.	Provides systematic approach	Requires familiarity with process to be effective.	Based on the MORT Hazard/-Target Concept.
MORT	Use when there is a shortage of experts to ask the right questions and whenever the problem is a recurring one. Helpful in solving programmatic problems.	Can be used with limited prior training. Provides a list of questions for specific control and management factors	May only identify area of cause, not specific cause.	If this process fails to identify problem areas, seek additional help or use cause-and-effect analysis.

In addition to limitations incurred due to a post-failure incident evaluation perspective taken with all of these methods, each individual method suffers from its flexibility and scope. For example, barrier analysis primarily addresses all procedural and physical safeguards “barriers” which were breached in order for a failure to occur. These safeguards are imposed at the system level and are products of unit and system level attributes, environment interfaces, human interactions, and other system considerations. It is inherently analytical and detailed in view and structure; focusing on very specific breaches of existing barriers. The information may introduce new requirements regarding additional physical or procedural safeguards to be added

to a system. However, it does not assign actionable quantitative requirements to the unit level. Instead, it focuses on the development of procedural and administrative changes to an existing process.

Events and causal factor analysis focuses on specific sequences of interactions with a defined systems which introduced the failure. This single failure event and human error perspective gives this analysis process the informal title of “walk-through” analysis. Causal factor charting does provide a general tool used in cause consequence analysis. This tool provides formal logical structure to tracking the effect of a failure in the form of a cause and effect chart. This diagram is essentially a state transition diagram. Each action relates to the preceding action or state. The sequence of actions end in a failure state. In figure 20, Rooney includes questions regarding the details of each state. Once this sequence of events is clear, the root causes can be identified in order to be rectified [252].

While causal analysis does identify critical factors which drive requirements, the traditional perspective is tactical in nature. Once the physical system is in place and procedures for operations have been outlined, these tools act to remedy deviations from the procedural requirements. When an event or incident occurs, a team is formed to manage the problem, identify its cause, and implement corrections to prevent it from happening again (e.g. Ford 8-D method [193]).

This tactical perspective limits the direct benefit to the conceptual architecting design process. During concept development previous causal analysis do assist in mitigating potential incidents by introducing additional required functions and unit and platform level performance standards which reduce the likelihood for root causes to occur. However, structuring the architecture following functional induction assists in managing when these additional functions must be applied.

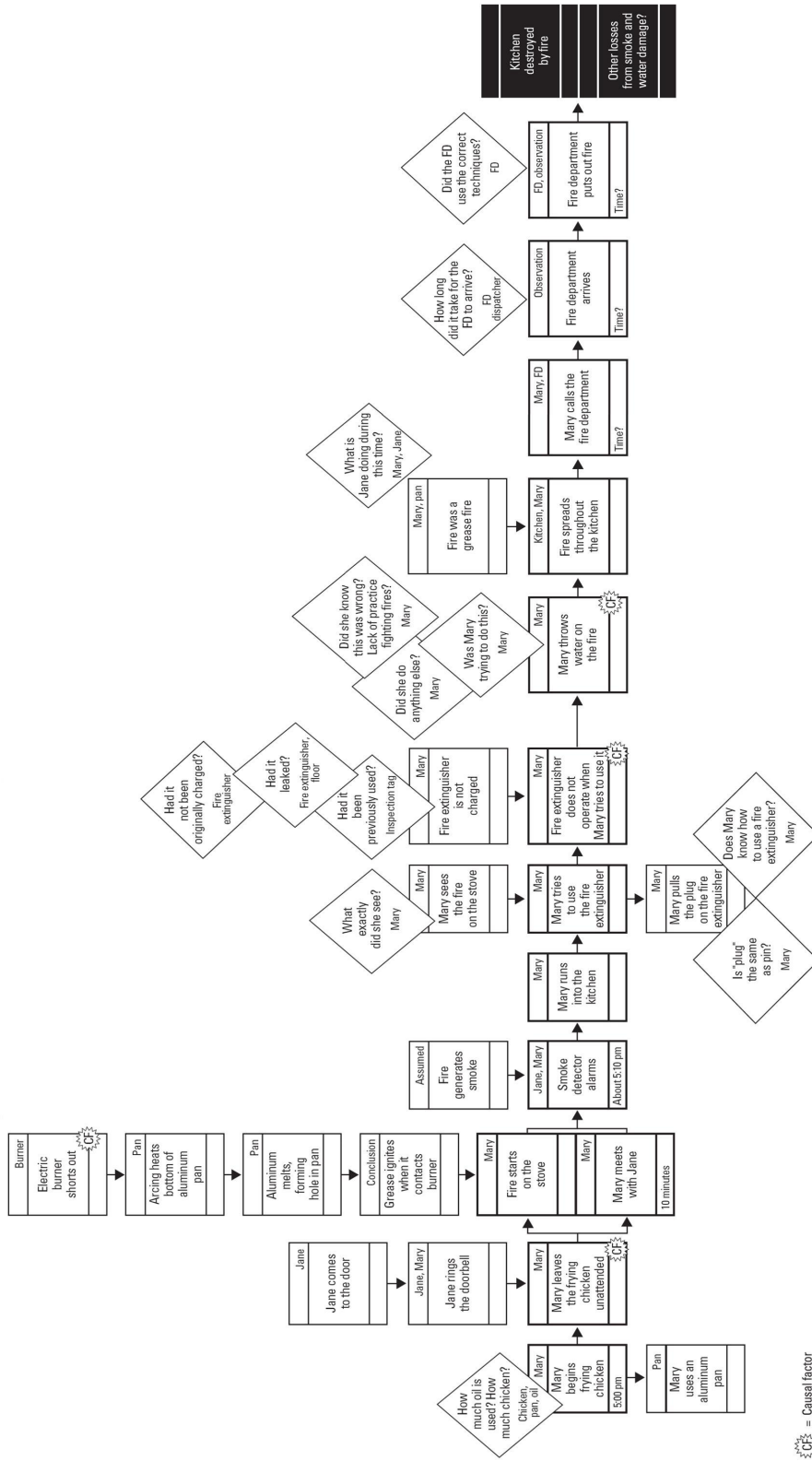


Figure 20: Notional Causal Chart for a Fire from Rooney [252]

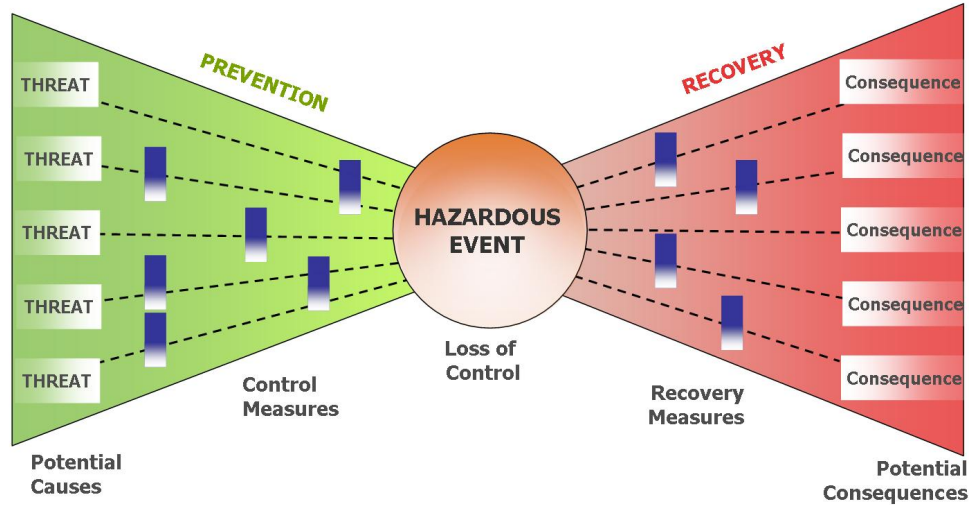


Figure 21: Expanded Risk Bow-Tie [284]

Bow-Tie Analysis

The risk bow-tie, seen in figure 21, displays the causal relationship between potential causes (threats), hazardous events, and potential consequences with respect to control and recovery measures. While hazard analysis takes place on the right portion of the bow-tie, this perspective of risk mitigation highlights the failure condition as the connection between two areas of safety and reliability: avoidance of a hazardous event, and mitigation of detrimental consequences. This separation of the behavioral and implementation space is advantageous in addressing a flexible architecture environment. Careful definition of the right side of the bow-tie can be established independent of the physical implementation.

Hammer et. al. define three distinct steps in performing safety assessment using the bow-tie model: operational hazard identification, operational hazard assessment, and allocate safety objectives and requirements [117]. This expansion of the bow-tie model is seen in figure 22. The first two steps are synonymous with traditional platform level functional hazard assessment. Assigning the left portion of the bow-tie to implementation space and the right portion to the behavioral space, Hammer et.al. term these internal and external mitigation means (IMM, EMM).

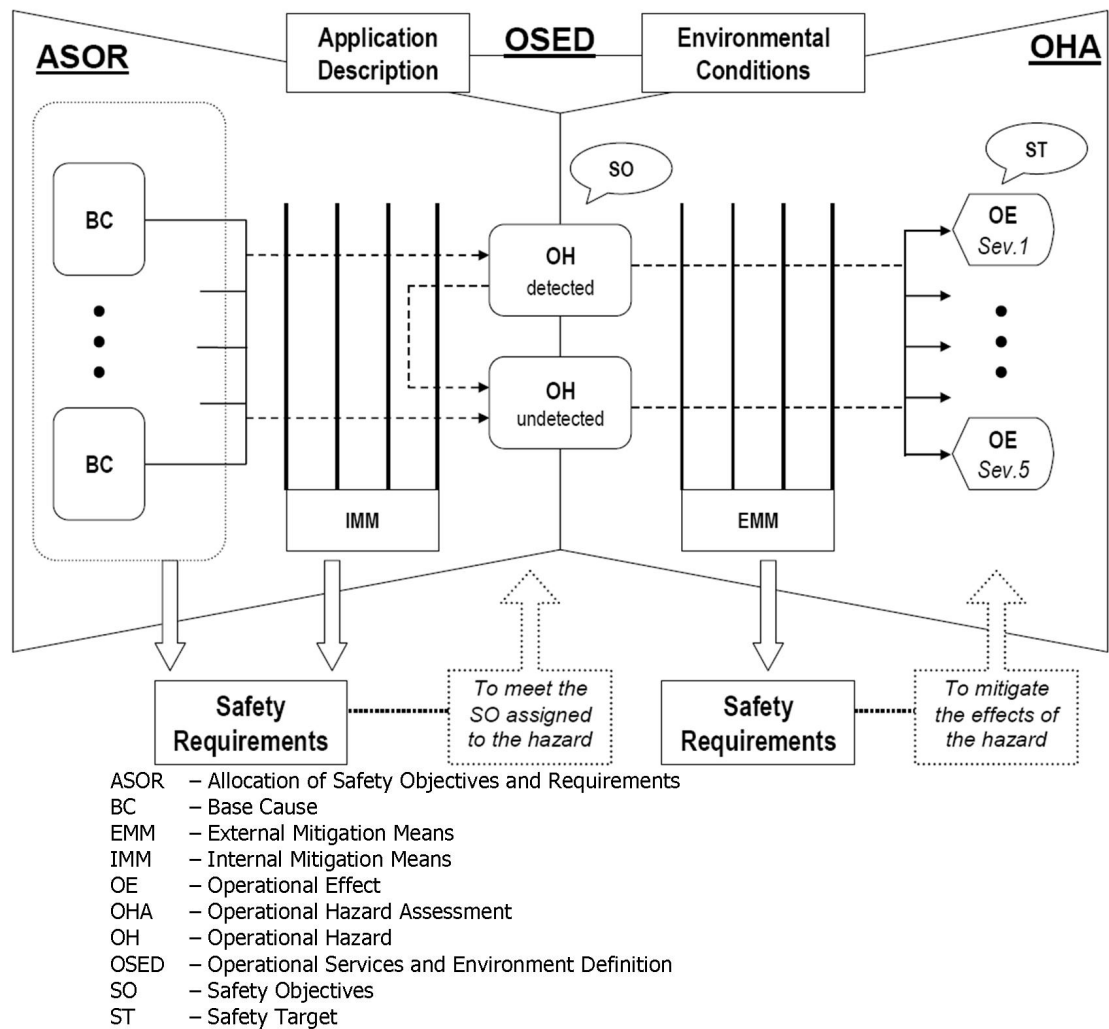


Figure 22: Operational Safety Assessment Process Overview from Hammer et. al. [117]

External mitigation means are accomplished through functional hazard assessment (FHA). FHA is a complimentary approach to HAZOP. Both processes focus on identification of potential hazards. However, FHA attempts to remain abstract, avoiding the necessity to characterize all types of functional lapses [7]. The number of guidewords is reduced from six or more to three: loss of function, too much function, and incorrect operation of function.

ARP 4754 presents Functional Hazard Assessment (FHA) as a preliminary system safety assessment tools to predict and explore functional failure and their impact of system compliance and performance [272]. FHA is a systematic technique for exploring and classifying functional importance, potential failure modes, and the criticality of their impact for system operations. The inputs to this process therefore include a description of the system under study, a specific operating environment, regulatory frameworks, and standards [186]. The goal of FHA is the identification of risk associated with each functional failure and responding with appropriate reliability requirements.

ARP 4761 decomposes the process of functional hazard assessment in 5 main steps. First, the functions of the system must be identified to the desired level of abstraction. Next, specific failure conditions associated with these functions are identified. The effect of each failure condition is determined and classified at the platform level. This finally results in a requirements allocation regarding the specific failure condition [273]. As indicated in figure 18, the FHA process may be repeated many times at subsequent lower levels of abstraction following the traditional structure for systems hierarchical decomposition.

Functional hazard assessment takes external mitigation procedures into account. Inappropriate fulfillment of a platform level function is assessed regarding its impact on operational effects. These failure modes are specific to each mission phase and environment condition and each operational hazard (a.k.a. functional failure) is

assigned a criticality measure based on the criticality measures introduced earlier.

Like HAZOP, FHA typically takes a tabular form. Figure 23 displays a conventional functional hazard analysis worksheet developed by Ericson [90]. To characterize a functional failure this worksheet lists the type of function loss with associated hazard number, the effect on the platform behavior, potential causal factors, the initial mishap risk index (IMRI), any recommended actions, the final mishap risk index (FMRI), any applicable comments and its assessment status. The initial and final mishap risk index refer to the risk associated with the failure as categorized by MIL-STD-882D [72].

While functional hazard analysis, pictured in figure 23 analysis techniques to determine the probability of a given functional failure, functional hazard assessment addresses only the effect of the failure and not the probability that the functional failure will occur. Traditional FHA recording formats only include information regarding the functions, the failure conditions, the flight phase, the effect of failure, the class of failure, and verification [300].

A benefit to FHA as described and implemented in the bow-tie model is its focus on the fulfillment of functions, not on the performance of specific architecture implementations. Maintaining independence between the operational requirements in terms of hazards and allocating physical failures to function in terms of fault tolerance in a given architecture allows for the systems architecture to be flexible. It also assists in the definition of system operating modes during hazard conditions. With information provided through functional induction, namely the relationship between unit level and platform level functionality, and generic criticality associated with the loss of platform level functions, load shedding strategies may be tailored to the specific architecture.

One shortcoming often encountered with functional hazard assessment and other

System: Aircraft		Functional Hazard Analysis					Analyst:		
Subsystem: Critical Functions							Date:		
Function	Hazard No.	Hazard	Effect	Causal Factors	IMRI	Recommended Actions	FMRI	Comments	Status
Control flight path (pitch and yaw)	F-1	Fails to occur, causing aircraft crash	Inability to control flight path (e.g. elevator hard over)	Loss of hydraulics; flight controls; software	1C			Safety critical function	Open
	F-2	Occurs erroneously, causing aircraft crash	Elevator hard over	Software	1C				Open
Control touchdown and rollout	F-3	Fails to occur, causing aircraft crash	Inability to control flight path (e.g. elevator hard over)	Loss of hydraulics; flight controls; software	1C			Safety critical function	Open
	-	Occurs erroneously, causing aircraft crash	Not applicable		1C				Open
Control thrust (engine speed and power)	F-4	Fails to occur, causing aircraft crash	Loss of aircraft thrust when needed	Engine hardware; software	1C			Safety critical function	Open
	F-5	Occurs erroneously, causing aircraft crash	Incorrect aircraft thrust	Engine hardware; software	1C				Open
Control cabin environment	F-6	Fails to occur, causing passenger becomes sick	Passenger comfort	Computer fault; software	2D				Open
	F-7	Occurs erroneously, causing passenger	Passenger comfort	Computer fault; software	2D				Open
Provide spatial orientation	F-8	Fails to occur, causing aircraft crash	Pilot loses spatial orientation during critical flight	Computer fault; software; displays fail	1C	Provide three independent displays		Safety critical function	Open
	F-9	Occurs erroneously, causing aircraft crash	Pilot loses spatial orientation during critical flight	Computer fault; software; displays fail	1C				Open
Fire protection	F-10	Fails to occur, causing aircraft crash	Unable to extinguish onboard fire	Computer fault; software	1C			Safety critical function	Open
	F-11	Occurs erroneously, causing equipment	Equipment damage	Computer fault; software; displays fail	3C				Open

Figure 23: Functional Hazard Analysis Worksheet from Ericson [90]

hazard analysis techniques is perspective. FHA often occurs in multiple stages following traditional systems decomposition. In order to perform FHA at the lower level there must be a consensus as to the traditional functional decomposition, the interfaces between functions, and interfaces with the environment. With a flexible architecture structure composed following functional induction this is not often guaranteed. The columns in figure 23 indicating causal factors and recommended actions are architecture specific. A conceptual architecture perspective denies the capability to identify cause and internal mitigation means in a generic fashion.

Temporal information is also not adequately supplied tabular FHA. Sustained function loss has much more potential to incur hazardous effects than temporary lapses in capability. Additionally, as with HAZOP, SWIFT, and other hazard assessment techniques, FHA is developed and collated in tabular form. This leads to a discrete allocation of functional hazard results. Depending on the redundancy in the system and the means for load shedding, the percentage of the function loss is an analog relationship.

Observation: *Traditional methods for hazard identification assign static or discrete hazard value to the loss or excess of a given function.*

Observation: *The traditional approach to hazard assessment generalize expected result of failure, avoiding exploration of the scenario tree.*

4.3.4 System Safety Assessments

Architecting for system safety is a question of providing adequate fault tolerance. To ensure that a system reliable performs its functions, designers must have two options. The first is to prevent any fault from occurring, and the second is allowing faults to occur, but limiting their severity [187]. According to Yen:

“Fault tolerance focuses on how to exploit spatial and temporal redundancies to deal with failures [306].”

Ensuring that adequate reliability has been provided through a specific design turns attention to the left side of bow-tie in figure 21, once the hazards associated with specific functional failures have been defined, the implications of these hazards must be allocated to the unit level. This typically takes the form of constraints on the necessary reliability of each unit or group of units. Qualitative and quantitative assessment techniques are necessary when a system may exhibit failure conditions exceeding the minor categorization, when the system is complex [95].

Preliminary system safety analysis (PSSA) as defined in ARP 4761 is proposed as a set of tools and practices to validate that the architecture can meet safety requirements, and establishing new safety related requirements. Each unit must be characterized by a development assurance level (DAL). This measure classifies the most severe impact of the unit failure [273]. Additionally, PSSA is tasked with identifying emergent safety requirements. This includes managing architecture specific component interactions and the identification of critical failure modes for new designs [65]. This must take place in an environment in which the architecture is non-static. While PSSA occurs early in the design process, Dawkins highlights flexibility issues with PSSA. He writes:

“To meet its (PSSA’s) objectives we want to do PSSA early and thus influence the design, but we will then be faced with the cost of updating 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 [65].”

In order to determine sizing critical effects of safety and reliability requirements during conceptual architecting, flexible system safety assessment tools are preferable

generated simultaneously architecture implementation object models. Rausand and Høyland introduce four concept level tools for quantitative systems safety analysis of non-repairable, temporally independent component failures: fault tree analysis, Bayesian belief networks, event tree analysis, and reliability block diagrams [243].

The primary focus of tools and methods discussed in this section is on fault trees and reliability block diagrams. Both event trees and Bayesian belief networks are useful in system evaluation. However, these tools require a detailed understanding of inferred component and unit relationships which may not be available during conceptual architecting. Event trees focus on safety mitigation procedures and functions and very specific instigating events which occur in a configured system. These are similar to scenario trees as discussed earlier. Bayesian belief networks use conditional probability to determine the probability of specific technical failures with relationship to human and organizational factors. While more flexible than the fault tree, due to its non-binary representation, it is more similar to a cause and effect analysis with quantitative outputs [243].

Analogous to object oriented behavioral modeling discussed in the previous section, fault trees and reliability block diagrams are discussed here in terms of their underlying structure. These reliability models can take a form similar to object oriented activity diagrams or state transition diagrams.

4.3.4.1 Function/Action Based Assessment Tools

The fault tree and reliability block diagrams are recommended processes for qualitatively assessing the ability of a system to fulfill safety requirements. Advisory Circular 25.1309 describe as follows:

“(Fault trees and reliability block diagrams) are structured, deductive, top down analyses which are used to identify the conditions, failures, and events that would cause each defined failure condition. They are graphical

methods of identifying the logical relationship between each particular failure condition and the primary element or component failures, other events, or combinations thereof what can cause it [95].”

The fault tree and reliability block diagram take opposite perspectives in assessing system reliability from a failure and success perspective, respectively. The reliability block diagram graphically represents units and functional relationships whose probability of working contribute to the overall probability of success for a given function. On the other hand, the fault tree graphically relates fault events whose probability of occurrence contribute to the probability occurrence of a top level failure event.

Fault Tree Analysis (FTA)

Fault tree analysis is a widely accepted method for system safety assessment. The perspective taken is one of what and how a system experiences failure. Originating with the development and evaluation of the Minuteman Launch Control System in the 60's by Bell Labs, FTA and was recognized by Boeing as an advantageous tool to system safety assessment. Since that time, FTA has been widely adopted in many industries, primarily in high risk fields including nuclear power, chemical, and aerospace. The fault tree is an object model which takes a top down perspective to architecture evaluation which calculates the probability of occurrence of some undesirable top level event. Each top level event is contingent upon basic events which form the necessary and sufficient conditions. These then allow the top level event to occur.

The top down expansion of the top level error is facilitated by logical gates and events. Logic gates and event types are reviewed in tables 20 and 21. Each event type is characterized by its probability of occurrence. ‘AND’ and ‘OR’ logic gates use union and intersection probability calculations to determine the probability of each intermediate event. Applying these calculates allows for the probability of the top

Table 20: Fault Tree Logic from Andrews and Moss [10]

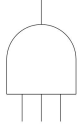
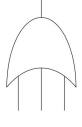
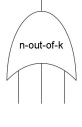
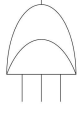
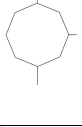
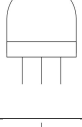







Logic Gates		
Type	Symbol	Causal Relation
AND gate		Output event occurs if all input events occur simultaneously.
OR gate		Output event occurs if at least one of the input events occurs.
k-out-of-n (voting gate)		Output event occurs if k-out-of-n input events occur.
Exclusive OR gate		Output event occurs if one, but not both, of the two input events occurs.
Inhibit gate		Input produces output when the input event and the conditional event occur.
Priority AND gate		Output event occurs if all input events occur in the order from left to right.
NOT gate		Output event occurs if the input event does not.

Table 21: Fault Event Objects from Andrews and Moss [10]

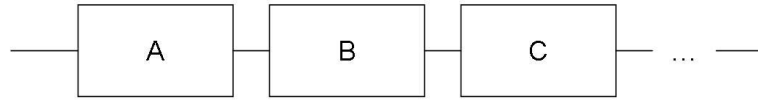
Events		
Type	Symbol	Description
Intermediate event		Event incurred dependent on gate logic
Basic event		Component Failure characterized by failure rate or probability
Undeveloped event		Externally caused failure characterized by failure rate or probability
Conditional event		Attached to an intermediate event establishing conditions on gate logic
House event		Events with fixed probability (0 or 1)
Transfer		Connects branches used elsewhere in the tree.

level event to be calculated.

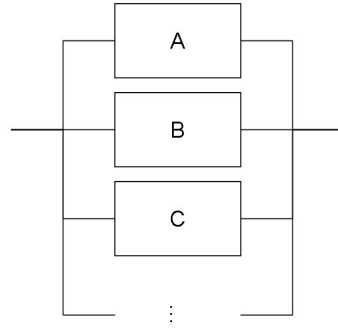
FTA benefits from a simple structure which generates quantitative evaluation of system reliability. It is widely accepted and easily implemented. However, the FTA is an analysis tool which is typically generated requiring a robust understanding of the system. Additionally, its object oriented structure can be a benefit or a detriment. With complex systems, the ‘and’ and ‘or’ structure of fault tree composition present a vast hierarchical structure which can be difficult to reconcile with the functional relationships between units.

Reliability Block Diagram (RBD)

The reliability block diagram (RBD) is a more functional and dependence driven approach to visualizing and assessing system reliability. Taking a success based approach, the reliability block diagram is implemented to determine the probability of being able to perform a given top level function. Avoiding complex logic structures, the RBD visualizes the system in a functional or dependency diagram. The traditional reliability block diagram presents the reliability of the system as a function of



(a) Blocks in Series



(b) Blocks in Parallel

Figure 24: Series and Parallel Components in Reliability Block Diagram

the reliability of individual systems aligned in series and parallel. Assuming element failures are independent, reliability of blocks in series and parallel as depicted in figures 24 are calculated in the by the following equations [270]. Blocks in series are equivalent to a fault tree intermediate event driven by an ‘OR’ gate and blocks in parallel are equivalent to a fault tree intermediate event driven by an ‘AND’ gates.

$$\text{Series : } R_{sys} = R_A \cap R_B \cap R_C \dots = R_A \cdot R_B \cdot R_C \dots \quad (6)$$

$$\text{Parallel : } R_{sys} = R_A \cup R_B \cup R_C \dots = 1 - (1 - R_A)(1 - R_B)(1 - R_C) \dots \quad (7)$$

The reliability of the individual units and the structure of the system contribute to overall reliability of fulfilling the function. Formulating system structuring using the reliability block diagram assists in considering the effect of redundancy in system composition. Redundancy entails providing multiple means of performing required functions. This is represented as parallel tracks in the reliability block diagram.

Active, warm, or standby redundancy are all intended to increase overall system reliability with varying failure rates [20].

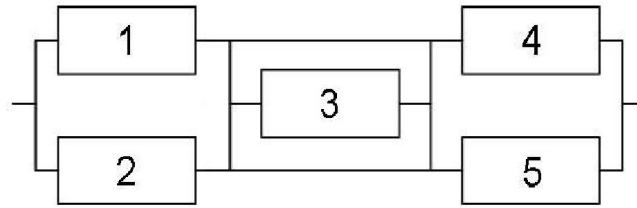
Another form of redundancy takes the form of load sharing. Load sharing requires that multiple elements be available to fulfill architecture reliability requirements. Combinations of elements must be identified which can fulfill functional requirement. For independent parallel systems with identical components the reliability of a minimum of k-out-of-n is determined through probability calculations of combinations:

$$R_{sys} = \sum_{i=k}^n \binom{n}{i} \cdot R^i \cdot (1 - R)^{n-i} \quad (8)$$

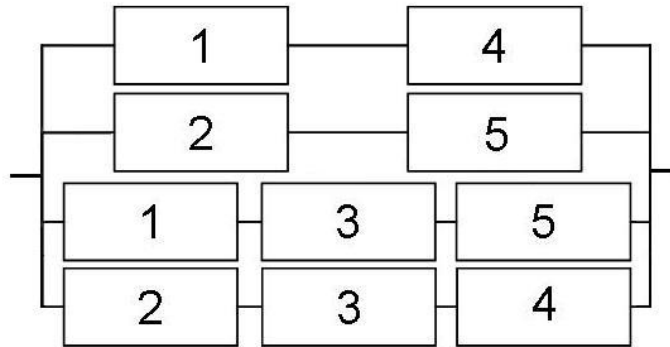
The appropriate combination of elements organized in fulfillment of the function must be identified for a continuous range of probabilities. The process of identifying ‘minimal path sets,’ the traditional parallelizing during load shedding scenarios, and logical operators regarding necessary capacity are applied in this process.

Handling the load sharing problem can be viewed as a restructuring of the reliability block diagram by replacing the ‘n’ parallel components with parallel paths, each including a different series of ‘n’ units. This is similar to the concept of identifying a minimal path set. A minimal path set is the minimum number of elements which must be active so as to support system functionality and restructures a complex reliability block diagram so as to create a strictly parallel relationships. This process is illustrated in figure 25. Identification of these minimal path sets simplifies the calculation of the reliability requirements.

Parallelizing the load sharing relationship requires previous knowledge regarding the number of necessary elements to fulfill requirements by assuming that a given ‘n’ blocks can provide functionality with a static reliability. Each combination of ‘n’ blocks provides an independent parallel path as displayed in figure 26.

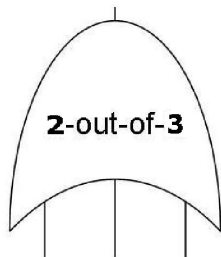


(a) Minimal Path Sets for Notional Reliability Block Diagram

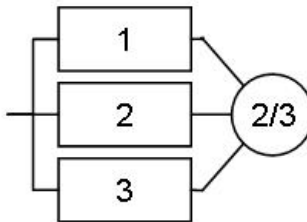


(b) Parallel Minimal Paths

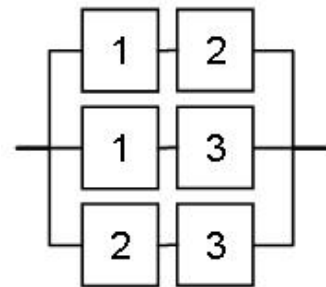
Figure 25: Conversion of Complex Graph to Minimal Path Sets



(a) Fault Tree Load Sharing Element



(b) Reliability Block Diagram Load Sharing Element



(c) Parallelized Load Sharing Element

Figure 26: Load Sharing Reliability Structuring

Performing PSSA with the reliability block diagram produces a quantitative reliability assessment of the architecture. This value is used to verify that safety requirements can be fulfilled. An advantage of the RBD is its form. The RBD takes a similar form to a dependency diagram. Parallel and serial paths more visible correlate with the physical interrelationships between system elements. This visualization relates more directly to the dependency structure used during functional induction. In highlighting necessary extension to PSSA while addressing analog functional hazard requirements reliability block diagrams will be used for illustration purposes.

Observation: *Traditional PSSA are limited by assumptions regarding the failure states of units and functions.*

4.4 Emergent Requirements Overview

Multiple sources of emergent requirements were identified and discussed in this chapter. The first section of this chapter addressed time dependency in architecture sizing. Time dependency was first discussed in the context of traditional constraint and mission analysis. This is necessary for determining power and energy requirements at the platform level. To capture and identify sizing critical scenarios and operations, a more detailed and flexible means for mission definition.

Next, time dependency in the context of vehicle systems modeling was addressed. While all modeling techniques may provide information necessary for the engineering of the vehicle systems, not all are applicable during architecture conceptualization and trades. This section provides justification for the modeling strategy implemented in the research plan. The level of time dependency of a vehicle system model depends on the design phase in which it is implemented.

Traditional statistical methods for predicting systems weight and other attributes during conceptual definition was discussed. This is followed by a review of modeling

efforts towards increased predictive capability and insight obtained through object-oriented systems modeling and transient analysis. Finally, steady state surrogates were introduced as a means to increase model fidelity without incurring the computational cost of dynamic analysis.

The second section of the chapter explored the means for identifying emergent requirements in terms of operating mode dependency. In order to accurately size the power systems architecture, models must be subject to the appropriate conditions which generate the most stringent performance requirements. Model based systems engineering techniques characterized by scenario based design are reviewed. Failure considerations oftentimes dominate the sizing requirements for a high assurant system. Off-nominal cases introduce the concepts of load-shedding in the power system, and performance degradation.

The final section of this chapter looks at the dimension of safety and reliability dependence. Fault tolerance and other methods for requirements identification operate within the framework of reliability analysis. These considerations must interact with the operational perspective in identifying potential sizing critical requirements. Therefore, this section reviews applicable tools and theories for addressing reliability, criticality, safety, and risk during concept development and assessment.

The complexity of an vehicle systems architecture design space does not exclusively stem from the complexity of physical attributes. While requirements concerning the nominal operations can be defined independent of physical implementation, unit level requirements must be made sensitive to behavioral attributes specific to the architecture. A complete exploration of all potential sizing scenarios is necessary to generate unit level load profiles. Time, operating mode, and safety and reliability related requirements must be specified to accurately size architecture units. These three domains intersect in the generation of requirements through off-nominal sizing case consideration as depicted in figure 27.

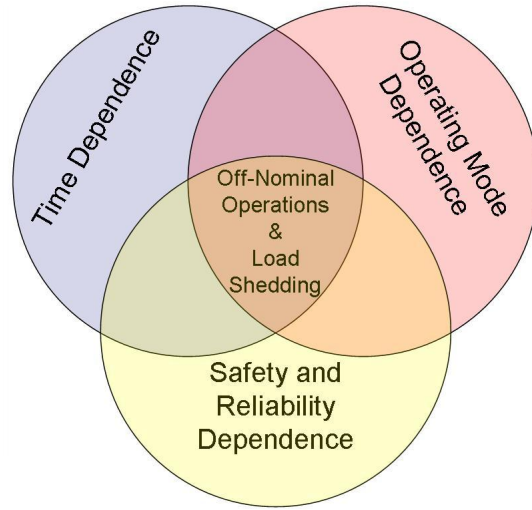


Figure 27: Interacting Dependence Domains

In order to understand the specific requirements for equipment in a given architecture there must be a fundamental understanding of the functions of that equipment with relation to operations and their associated criticality. The criticality associated with a given piece of equipment is only discernible in the context of the specific architecture in which it is operating, including its functional and physical relationships with other components. The system operational criticality imposes reliability requirements on each grouping of elements dedicated to the fulfillment of a given function in the architecture. The units utilized to fulfill a given function, must provide adequate reliability based on the criticality of each provided function.

Due to their sizing critical nature, a flexible means for the identification of architecture specific unit level behavioral requirements is necessary during early conceptual design. This includes understanding and defining the operational implications of unit failures. Systematizing the identification of off-nominal sizing considerations is necessary.

Many tools exist which support the formulation of operating modes and reliability requirements. However, limitations exist which limit their ability to interface

in formulating architecture specific behavior related requirements. Traditional constraint and mission analysis formalizes the means for determining power and energy requirements. However, it presents a limited number cases which can pose sizing critical requirements on unit performance in terms of hard capability constraints. Scenario based design tools provide a means for exploring the behavioral space of the system. However, they face challenges when addressing the combinatoric nature of off-nominal scenario exploration. Safety requirements and assessment tools provide quantitative assessment of system performance. They state reliability in terms of fixed metrics, treat failure in terms of discrete “on or off” states, and provide limited information regarding the implications of proportional function loss. These limitations hinder the ability of these tools to assess and optimize the probability and impact of partial system level failures for specific architecture concepts. In order to systematize the identification and allocation of architecture specific sizing critical behavioral requirements, tools must be introduced which systematically identify the impact of off-nominal operational requirements.

Objective: *Provide systematic risk and reliability based means for the identification of off-nominal operational requirements which can be rapidly implemented during concept architecture trades.*

CHAPTER V

METHOD

The exploratory design of vehicle systems architectures requires the identification of sizing critical requirements for revolutionary architectures. As was discussed in the previous chapter failure scenarios pose more stringent unit level performance requirements than those derived from nominal operations. Standard performance degradation heuristics give estimations of unit level requirements but are insufficient for predicting requirements for revolutionary vehicle systems concepts. Addressing design for safety requires that operational mitigation strategies are in place, the probability of proportional functional losses are known, and the consequences of these failures are understood. This chapter proposes extensions to the standard safety and reliability tools as a means for exploring the operational impact of unit level functional failures at higher fidelity in order to identify emergent off-nominal requirements.

The ability to appropriately identify beneficial degradations of platform level functions during failure states allows better prediction of unit level requirements. However, when vehicle systems attributes and alternative architectures are introduced, the operational effects of unit level failures are ambiguous. Determining the probability of an given operational consequence necessitates adaptively relating the reliability of all system units to the partial or complete fulfillment of platform level functions. If physical units support multiple loads, the effect of a unit level loss may be felt as a reduction of capability among one or multiple platform level functions. Load shedding involves the reduction in platform level capability by selective reductions in functional capabilities to minimize operational losses.

Hypothesis 1: *Optimizing load shedding strategies yields more accurate predictions of unit level requirements than heuristically defined performance degradation during the exploratory design of revolutionary vehicle systems architectures.*

The identification of load shedding strategies during the exploratory design trades requires a systematic means for identifying and assigning these minimum effects to unit level failures in a manner unique to each architecture concepts. This chapter focuses on formulating this optimization schemes which will leverage operational and physical means for ensuring architecture reliability. Specifically, this chapter explores expansions to the traditional functional hazard assessment in generating an analog hazard function relationship.

The aerospace recommended practices and bow-tie model, as discussed in the previous chapter (traditional functional hazard assessment (FHA) and preliminary system safety analysis (PSSA)), provide the framework for identifying off-nominal requirements in this thesis. However, In order to minimize the severity of operational effects, meet the hazard probability constraints, and reduce overdesign for safety, the designer must provide more information regarding which functional loads are more or less critical. Traditional safety and reliability tools are therefore extended to capture the effect of proportional function losses. This requires a continuous extension of the traditional FHA process and an analog assessment of system safety.

Continuous FHA explores the severity of operational consequences (hazards) in terms of the magnitude of the system level functional losses. This yields a reliability constraint which is continuous in terms of loss percentage. Additionally, system safety must be explored in an analog fashion. Assessing system safety in terms of this continuous hazard constraint requires that the operational effect of unit level failures must also be identified in terms of the magnitude of losses which they impose. The methods discussed in this chapter (continuous FHA, load shedding optimization, and analog SSA) constitute a process defined for the systematic identification of

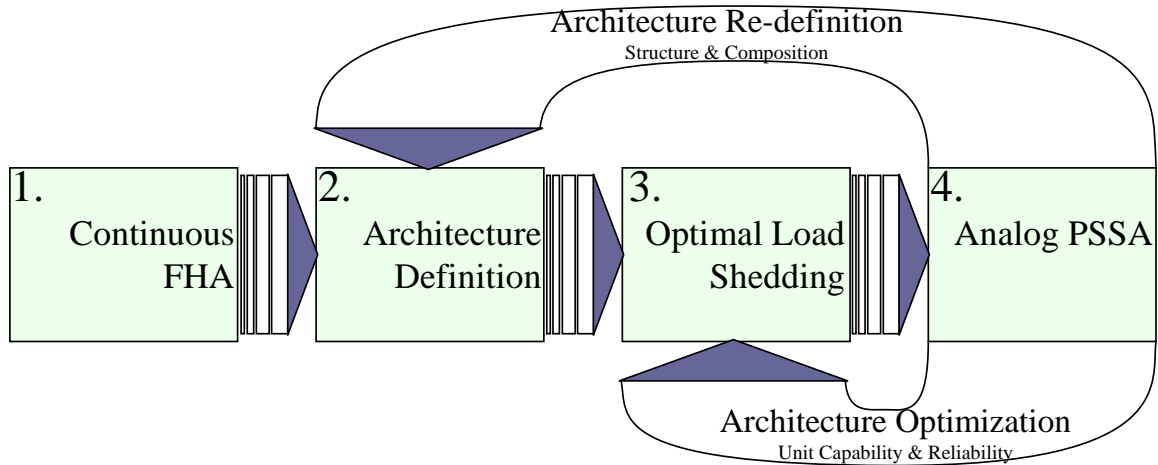


Figure 28: SONOMA (Systematic Off-NOMinal Requirements Analysis)

emergent off-nominal requirements. This process is entitled SONOMA (**S**ystematic **O**ff-**N**OMinal **R**equirements **A**nalysis) and is illustrated in figure 28.

As seen in this figure, this process involves the continuous definition of the function loss vs. hazard relationship, the optimization of capability allocation for unit level failures, and an analog assessment of system risk. This requirements assessment process identifies off-nominal considerations which inform the optimization and augmentation of the vehicle systems architecture concepts during exploratory design. The methods introduced in this chapter facilitate the identification of these requirements architecture specific emergent requirements. The tools and methods posed were developed and applied primarily for independent unit level failures. Extending this method to address common cause failures is a matter for future investigation.

5.1 Continuous Functional Hazard Assessment

The means to define an appropriate constraint function limiting the allowable probability of function loss and an objective function is discussed in this section. This function is minimized in order to facilitate load shedding. Continuous FHA is based around the hazard analysis methods discussed in the previous chapter. It was observed in the last chapter:

Observation: *Traditional methods for hazard identification assign static or discrete hazard value to the loss or excess of a given function.*

Extensions to traditional discrete hazard assessment methods are addressed with the following hypothesis:

Hypothesis 2: *Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements.*

The approach to characterizing hazard effect as an analog relationship with platform level function loss can be compared to the Taguchi loss function's approach to quality control and robust design as introduced in 1978. Taguchi expressed quality as a loss to society in terms of costs incurred through production and consumption [254]. Breaking from the traditional discrete method for applying specification limits, Taguchi introduced a continuous relationship (quadratic function) between deviation from target and loss. Breyfogle defines this function as follows:

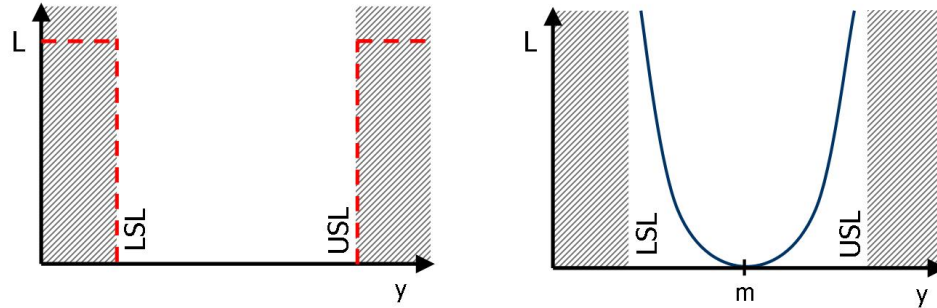
“The loss function describes the loss that occurs when a process does not produce a product that meets a target value. Loss is minimized when there is ‘no variability’ and the ‘best’ response is achieved in all areas of the product design [29].”

This is mathematically expressed as follows:

$$L = k(y - m)^2$$

In this relationship L is the loss, m is the target value, y is the independent variable, and k is the cost factor. Taguchi's idea behind quality was targeted towards to minimizing the loss. This change in perspective is illustrated in figure 29.

While Taguchi's intent was to minimize loss in the form of cost, the intent of



(a) Traditional Loss Function for Given Manufacturing Limits (b) Taguchi Loss Function for Given Target and Manufacturing Limits

Figure 29: Perspective Change from Traditional to Taguchi Quality Control

hazard analysis is to minimize loss by avoiding unwanted operational effects due to component, unit, or functional failure. Similar to the difficulties encountered with the traditional quality control loss function, discrete or stepwise representations of hazard level do not provide adequate information to weigh the impact of a unit level failure with respect to the desired target. Graphically interpreting the traditional criteria posed by functional hazard assessment resembles the charts in figure 30.

Safety and reliability requirements are sizing critical. As was illustrated in the previous section, off-nominal sizing cases drive the unit level requirements. Safety requirements drive the reaction to off-nominal operating modes by governing the demand side management, the architecture specific load shedding strategies, and the trades between internal and external mitigation means.

Traditional functional hazard assessment (FHA) is applied in a tabular fashion. Discrete functional failure states are evaluated as to the level of severity for which they may be responsible. These discrete setting give a loss hazard relationship as seen in figure 30a. A more detailed FHA may provide information regarding loss in terms of proportional loss. However, because of its tabular implementation, the hazard function becomes a set of discrete steps (figure 30a).

In order to know which loads to shed in addressing off-nominal sizing cases, one

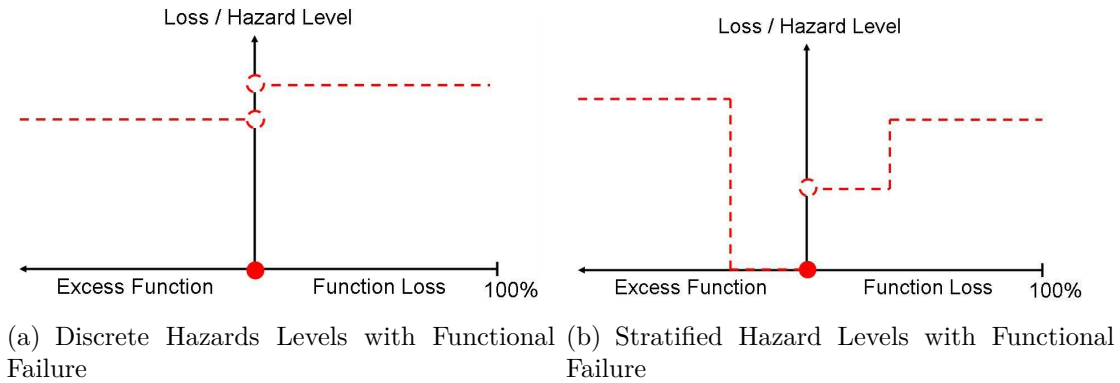
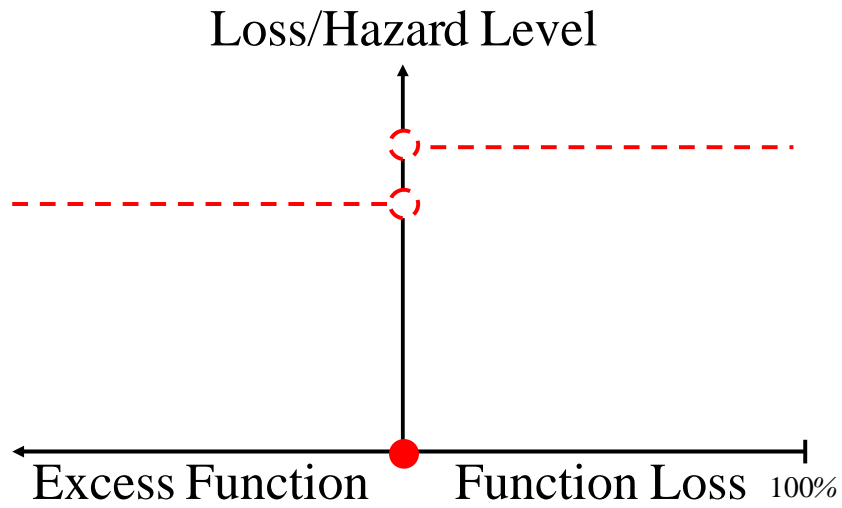


Figure 30: Notional Representation of Functional Hazard Assessment Result

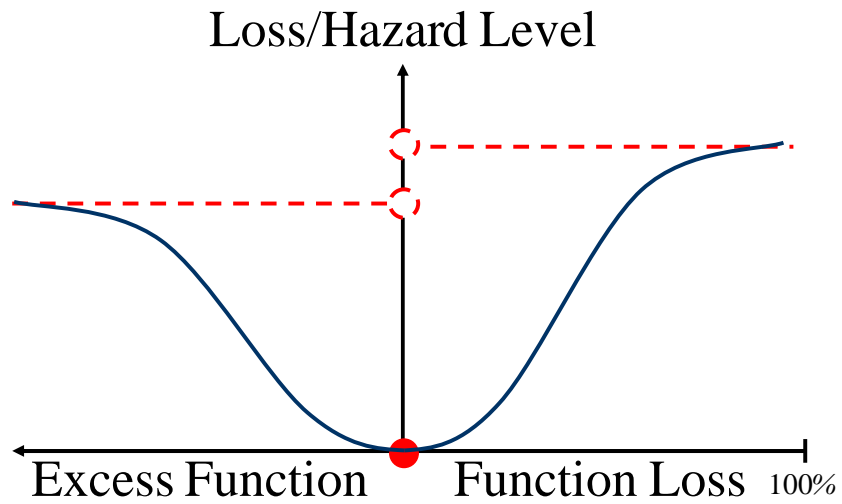
must determine the criticality of the functions which demand the loads. These criticality measures are architecture specific; depending on the relationship between the unit and platform level functions. In order to generate requirements which are safety and reliability dependent during the consideration of a new architecture, and in an environment in which the architecture will be augmented during conceptual trades, these considerations must be addressed in a formal and automated manner. This requires the designer to know at what point one function becomes more critical than another.

Three changes to the manner in which functional hazards are introduced to improve its flexibility in the identification of emergent operating mode requirements.

An initial improvement to FHA is the application of an analog representation of the hazard levels in terms of the loss or excess of some function. The degree to which a function is lost impacts the operational effect. Superimposing this hazard function on the notional graphs in figure 31 is shown in figure 30. While a continuous relationship between functional failure and hazard effect is not necessary or applicable, constructing the hazard effect as a function of % function loss or gain provides a more systematic means for determining load shedding strategies driven by specific unit level failures during conceptual architecting.



(a) Notional Continuous Hazard Relationship with Functional Failure



(b) Notional Stratified Continuous Hazard Relationships with Functional Failure

Figure 31: Notional Representation of Functional Hazard Assessment Result

For various architecture configurations a unit could be supporting multiple platform level functions to various degrees. With a loss in unit capability and depending on the levels of redundancy used, some proportion of the vehicle system's ability to perform platform level functions may be lost. Depending on the magnitude of the loss and the criticality of the platform functions, load shedding and performance degradation can be systematically identified through minimizing the hazard impact of a given unit loss through loss of one function above another. This would simply be done by minimizing the loss (or hazard) in the presence of a given failure.

The second improvement to the standard FHA is the inclusion of temporal considerations in the characterization of a failure. The length of time during which a function has failed impacts the operational significance of a functional failure. Thus, the operational effect of functional failure will be expressed in terms of % function loss and failure duration. This concept is illustrated in figure 32. The surface represents the variability of hazard level with the magnitude of functional failure and the duration of the failure. At zero failure duration there is no effect. However, as the duration and magnitude of the failure increases, the hazard level necessarily increases. A hazard function must be defined for each function at each mission phase.

This safety and reliability tradespace highlights the available design recourse to minimize operational hazard. Consider failure cases A and B in figure 33, where these specific failures breach the probability limits associated with the hazards at a given function loss. Point A represents a notional failure scenario. In this situation a unit level failure introduces a percent loss in platform level function for a given time. Taking a design perspective; in order to reduce the operational implications of the failure, the designer may increase the functional reliability, increase the speed of functional restoration, or alter the contours through operational effect mitigation. Assuming a fixed hazard/function/duration relationship leaves two options, increase functional reliability or decrease repair time.

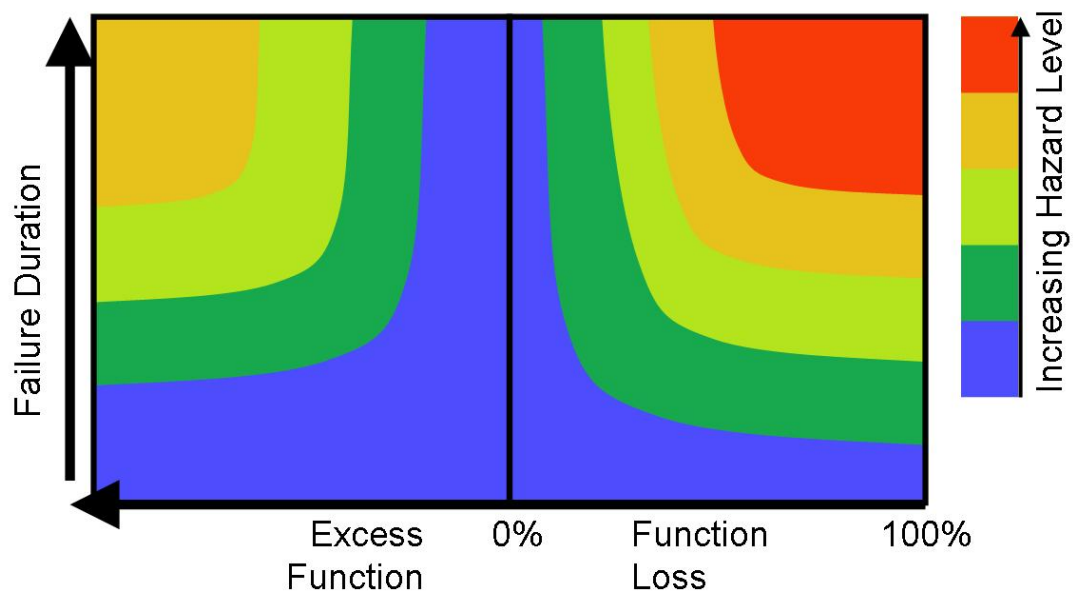
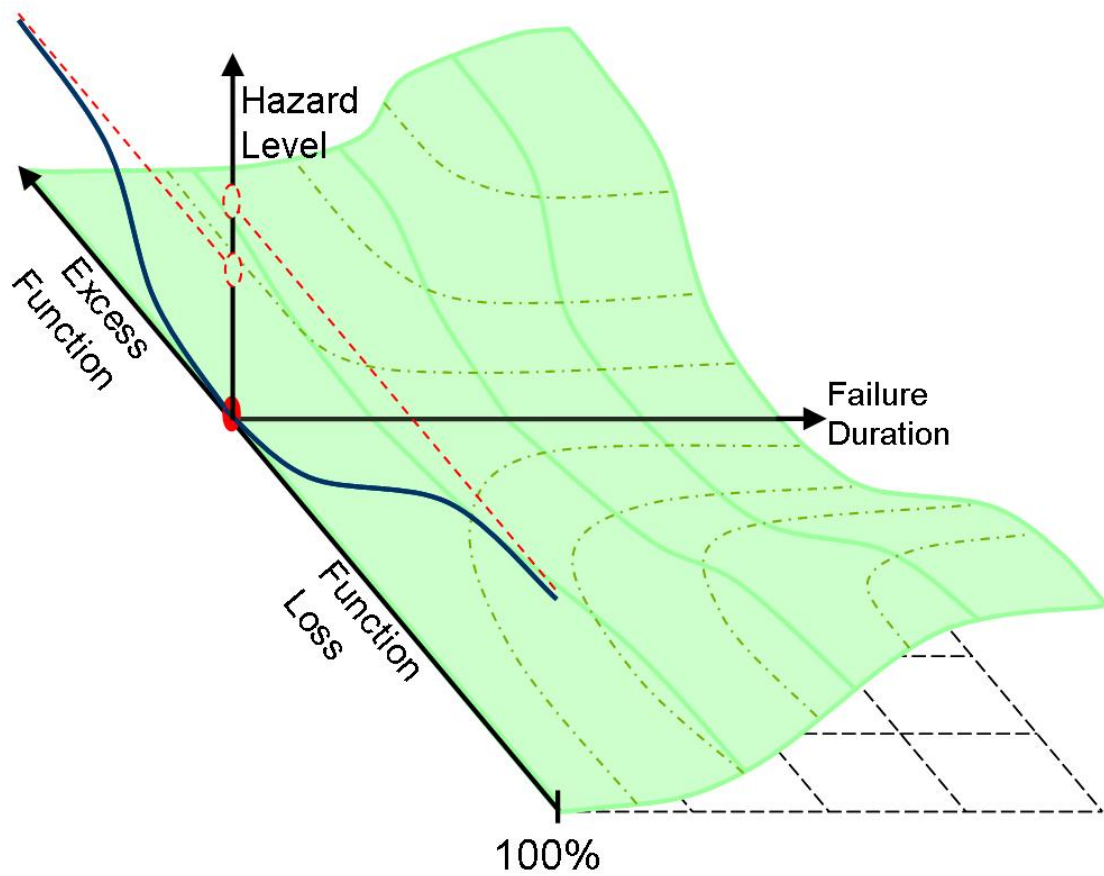


Figure 32: Notional Relationship Between Hazard Level, Function Failure, and Fault Duration

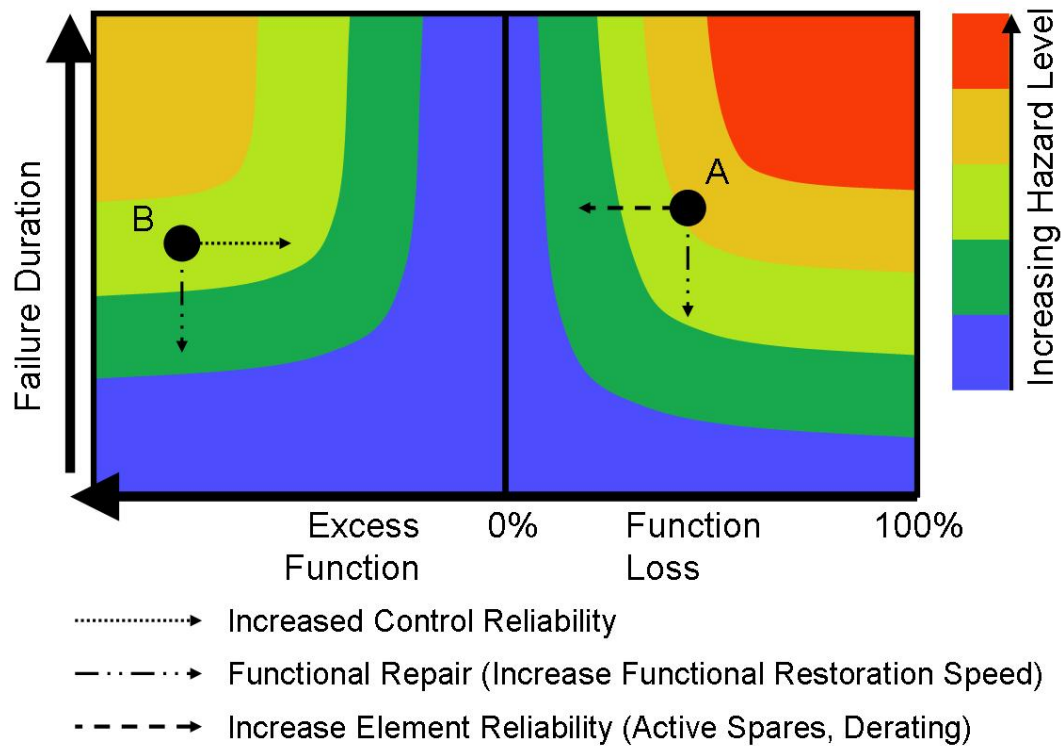


Figure 33: Hazard Effect Mitigation for Notional Physical System (A) and Control (B) Failure

Point B represents a notional control failure. Here capability exists to fulfill adequate functionality, however, a control failure has introduced an excess of functionality (e.g. too much thrust). In this circumstance, recourses include an increase in control reliability, or an increased speed of restoration to original functionality. A third option also exists through augmentation of the function/hazard relationship.

If the assumption is made that the operational space (hazard effect function) is independent of architecture definition, the three means to ensure appropriate reliability for a function loss must be defined in order to accurately size the architecture. The challenge presented by addressing reliability in this fashion is identifying when system reliability breaches hazard constraints during each flight phase and when the architecture may be overdesigned in terms of reliability.

Lastly, the potential dimension of reliability requirements configuration may require considering combinations of platform level functional failures during the functional hazard assessment. As electrical power begins to support more of the platform level functions, loss in load capacity will impact the fulfillment of multiple platform functions simultaneously. The architect must be aware of the implication of concurrent platform level functional failures. While the majority of the work done in this thesis assumes independent criticality of platform level functions. The formulation of the hazard function may be expanded to include combined functional failures.

Continuous representations of top down operational criticality requirements allows for more insightful architecture trades regarding load shedding and performance degradation than traditional fixed reliability requirement measures during conceptual architecting. The function/hazard relationship must be expressed in a form which allows for considerations of load shedding, fault tolerance, and mission analysis. This relationship takes the form indicated in equations 9 and 10. At any point in the mission (time t) the level of hazard incurred is a function of the available system level capability (X).

$$Hazard(t) = h[\{X\}, \tau, \{Op(t)\}] \quad (9)$$

$$\{Op(t)\} = \langle alt(t), M(t), dist(t), \dots \rangle \quad (10)$$

This hazard function is also calculated in terms of the duration of the failure (τ). There are multiple means by which the designer can ensure that the appropriate functional reliability is achieved. Fault tolerance is applied preventatively through the configuration of an architecture with “spatial and temporal redundancy” ([306]). Temporal redundancy takes the form of replication or repair. Replication is a sequential performance of some action and can achieve higher reliability in the performance

of discrete tasks. Repair, on the other hand, is the restoration of some original capability. Total loss of thrust for a $\Delta t = 30$ seconds is much different than a total loss of thrust for $\Delta t = 10$ minutes. Allowing for engine restart can reduce hazard severity by reducing duration. With the inclusion of temporal redundancy for increased reliability, new architecture specific functions and operations must be introduced which enable functional restoration.

Finally, the hazard must be made sensitive to operating conditions ($Op(t)$). These operating conditions are time variant as the platform progresses throughout the mission. For example, the operational effect of a loss in thrust for 30 seconds is much more hazardous during low altitude flight and takeoff than for higher altitude operations. A loss of thrust yielding marginal excess power is minor during high altitude cruise, but may prove catastrophic during low altitude obstacle clearance or takeoff.

Research Question: *How does taking an continuous approach to functional hazard identification impact the means by which these requirements are allocated to the unit level?*

5.1.1 Functional Hazard Relationships Definition

The hazard function relationships can be defined heuristically by the architect, following prescribed limitations dictated by certification requirements, or be derived from constraint analysis. Heuristic definition is applied for rough conceptual studies conducted with limited information regarding actual system implementation. This takes a form similar to traditional FHA by requiring the manipulation of surface plots instead of the discrete hazard assignments.

Necessary performance requirements and hazard responses are often dictated based on historic aircraft performance data. Certification requirements can provide direct limits and information towards the characterization of functional criticality. However,

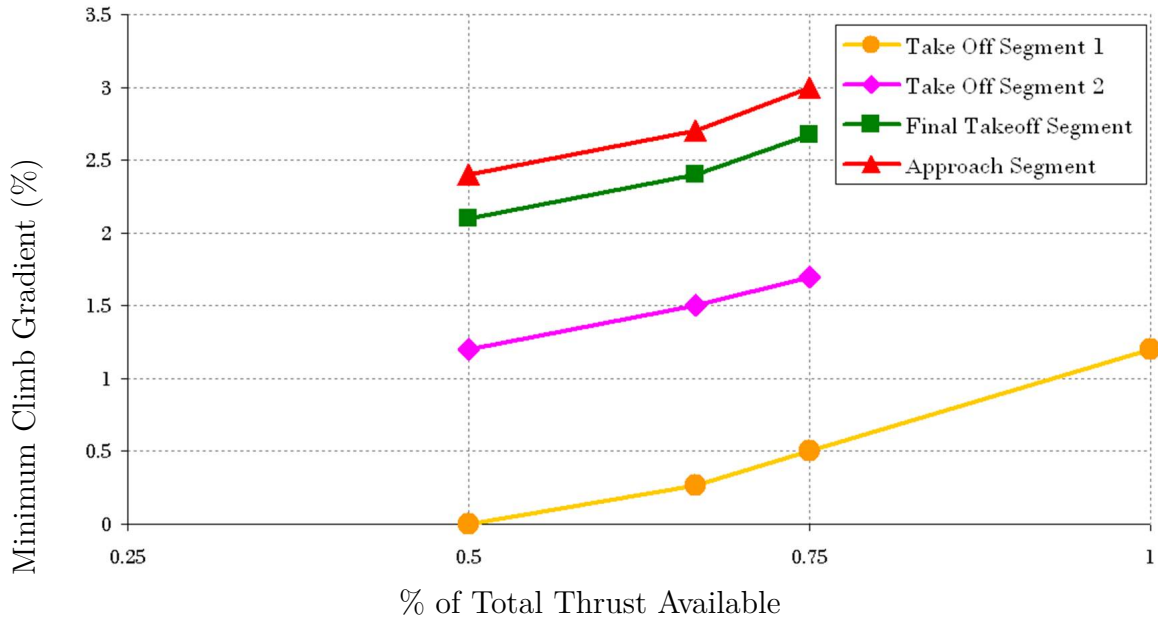


Figure 34: Reduction in Rate of Climb Requirements for loss of engine in FAR 25 [69]

constructing hazard function relationships requires extensive decomposition and reformulation of the Federal Aviation Regulations (FAR) and other design certification standards ([69]).

An example stating requirements through generalized operational impacts is cited by de Tenorio [69]. With figure 34 he graphically displays information scattered between multiple sections of FAR 25 certifications requirements regarding the impact of rate of climb requirements due to engine loss during takeoff and landing.

FAR 25 specifies the minimum reduction of climb rate incurred with a loss of engine. Loss of propulsion functionality induces a reduction in the rate of climb operational requirement. This is necessitated by constraints imposed by operations within commercial aerospace. FAR 25 regulations state these changes in the behavioral attributes due to functional failure at specific mission points at discrete percent loss values. Additionally, while thorough, the FAR 25 regulations are not presented in a directly usable fashion. Developing the figure 34 representation of climb gradient limits for thrust loss during takeoff and approach required reference to twelve FAR

25 sections. While FAR provides minimum requirements, additional capability may provide enhanced availability or performance.

Physical analysis assists the assignment of failure by linking functional fulfillment to fundamental requirements. Constraint analysis is often used to identify the bounds on the solution space for the system. Each operation which the system performs introduces a constraint which limits the design space. For aircraft design, constraint analysis acts to limit the thrust to weight ratio (T_{SL}/W_{TO}) and wing loading (W_{TO}/S) often in the form of motion equations or energy relationships ([201],[219]). While system attributes are set so as to operate within the constraints, hazard analysis can be accomplished by exposing hazards incurred from breaching the defined constraints and defining appropriate probability limits.

$$\frac{\alpha T_{SL}}{\beta W_{TO}} = \frac{1}{\beta} \frac{qS}{W_{TO}} \left[K_1 \left(\frac{n\beta W_{TO}}{q S} \right)^2 + K_2 \left(\frac{n\beta W_{TO}}{q S} \right) + C_{D0} + C_{DR} \right] + \frac{1}{V} P_s \quad (11)$$

Consider the form of Mattingly's aircraft motion relationship in given previously by equation 1. The hazard associated with a loss of thrust becomes a question of the allowable reduction of system capabilities (velocity (V), altitude (h), maneuverability (n and P_s)) at each initial flight phase. This constraint relaxation due to system level failure requires that the each requirement must no longer be perceived as hard limit ("go, no-go"), but rather as a limit with accompanied assurance of fulfillment. This assurance takes the form of a function loss probability limit.

Relaxation of a high altitude maneuver constraint is depicted in Figure 35 for a twin engine, 15 pax, commercial aircraft with a wing loading of $76 \text{ lbf}/\text{ft}^2$ and max T_{SL}/W_{TO} of 2.2. The aircraft drag polar was characterized by $K_1 = 0.085$, $K_2 = 0$, $C_{D0} = 0.02$. For this plot the weight lapse is assumed to be 0.8 and the thrust lapse is allowed to vary with altitude and Mach number. The design point for this aircraft is indicated as A. Applying constraint analysis provides a visual tool for identifying the effect of a functional failure. With a loss of thrust the point begins to drop towards

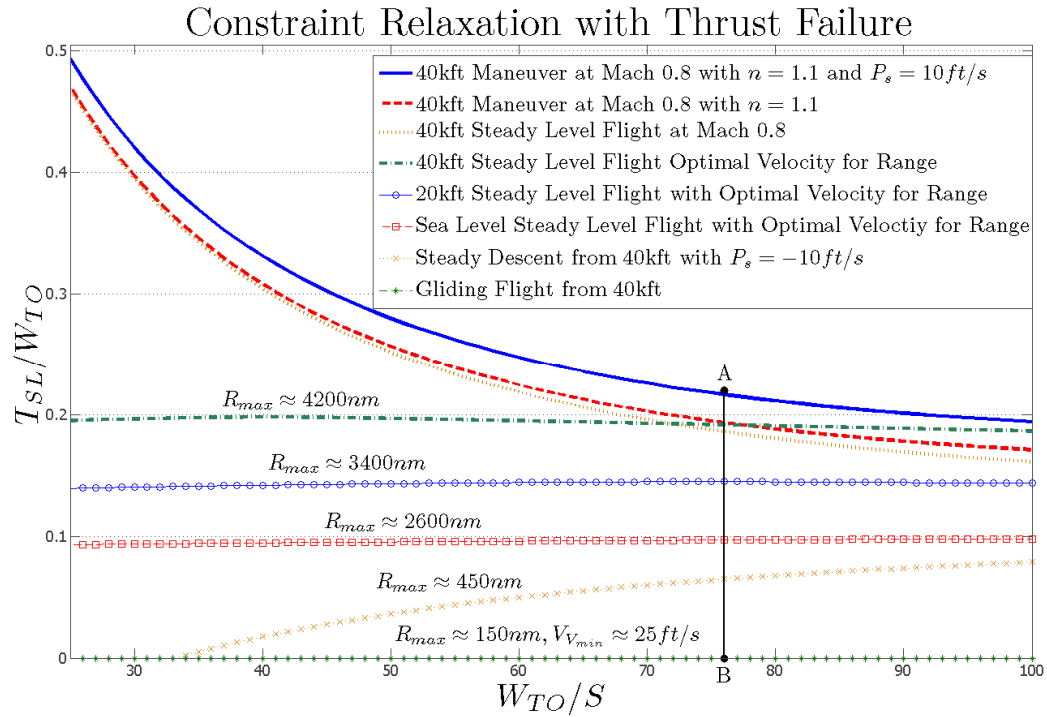


Figure 35: Effect on performance constraint given a loss of thrust

B and the aircraft no longer can sustain some requirements. This is seen as a breach of operational constraints.

Figure 35 indicates how hazards can be mitigated by augmenting flight performance. As the thrust available diminishes the system begins to lose capability. This may initially entail a loss of specific excess power and maneuverability (reductions in P_s and n) or require a change in velocity. Ultimately, the criticality associated with a loss of thrust relates to the aircraft's ability to reach a suitable landing site and safely approach it. Performance limits corresponding to the maximum range for a given thrust available are displayed on the chart. The magnitude of thrust loss yields decreases in range. Additionally, with a total loss of thrust the minimum descent rate is also fixed.

The function/hazard curve for thrust loss as prescribed by the analysis above yields hazards with various degrees of severity depending on altitude, Mach number,

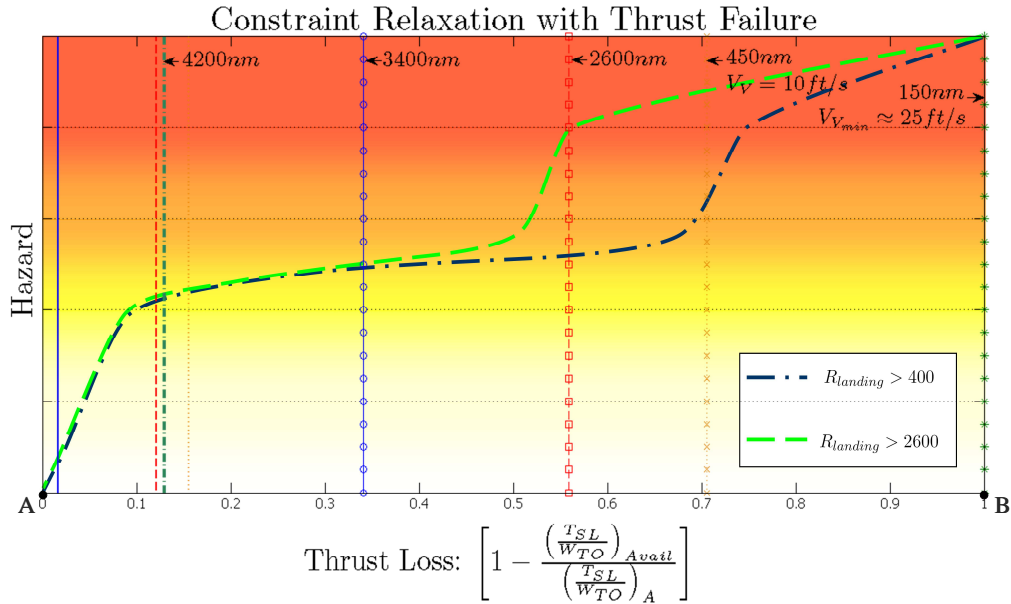


Figure 36: Thrust loss hazard relationship as informed by analysis results seen in Figure 35

desired maneuverability, and distance from landing field. Figure 36 shows a monotonically increasing hazard with magnitude of thrust loss. In this figure, the horizontal axis represents the magnitude of a thrust loss failure. The vertical axis represents the operational hazard. Catastrophic hazards are indicated by red coloration, critical hazards by orange, major hazards by yellow, and so forth.

As thrust begins to reduce the maneuverability it is no longer negligible. Additionally, if the distance to a landing field requires more thrust than available the hazard becomes catastrophic. Non-catastrophic performance losses must also be characterized by their associated hazard. As displayed in the figure, failures which require mission augmentation are deemed marginal and transition to catastrophic as the thrust capability for max available distance is approached. The rigidity of the performance constraint can be enforced through the magnitude of the associated hazard.

This hazard function is defined only in terms of cruise and maneuverability operations. Other thrust hazard limits must be derived for other applicable constraints (i.e. taxi, landing, takeoff, stop on ground). Expressing the hazard function as a

direct relationship to platform operations requires a more systematic means for exploring the effect of functional loss. These relationships are critical to load shedding optimization.

Further formulation of function hazard relationships will be discussed in the next chapter while considering the platform capabilities of a medium/long range business jet.

5.2 PSSA Continuous Expansion

Presenting reliability requirements in terms of % function failure and failure duration presents challenges in the implementation of traditional system safety analysis tools. These challenges stem from reliability requirements which are no longer being expressed as a static metric. Traditional quantitative reliability tools determine reliability as a single reliability metric (system reliability as a function of time) which is compared to a constant reliability objective. Fault trees and reliability block diagrams operate under the assumption that components operate in two states: functional, and failed [243] as observed in the previous chapter.

Observation: *Traditional PSSA are limited by assumptions regarding the failure states of units and functions.*

The exploration of load shedding schemes necessitates that unit and system reliability be determined in terms of function loss and failure duration. The question changes from “How reliable is the system?” to “How reliable is the system at providing a specific load, under specific conditions?” Therefore, unit and intermediate reliability must be defined in with respect to the magnitude of the failure.

5.2.1 Proportional Function Loss

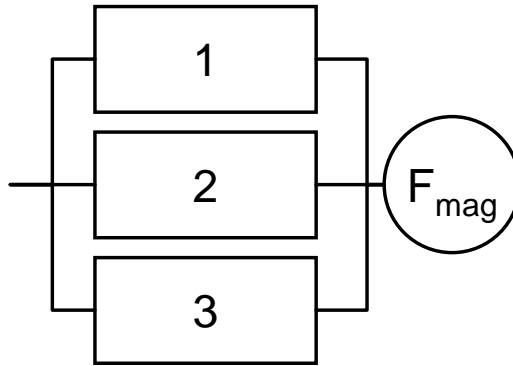
The two failure state representation (functioning or failed) of an failure events does not adequately express the probability of a proportional functional loss. This is primarily

evident when multiple unit share responsibility for the provision of functionality. the probability of failure increases with increased magnitude of load for these load sharing relationships. Determining the reduction of reliability with increasing load requires an augmented form to traditional load sharing calculations.

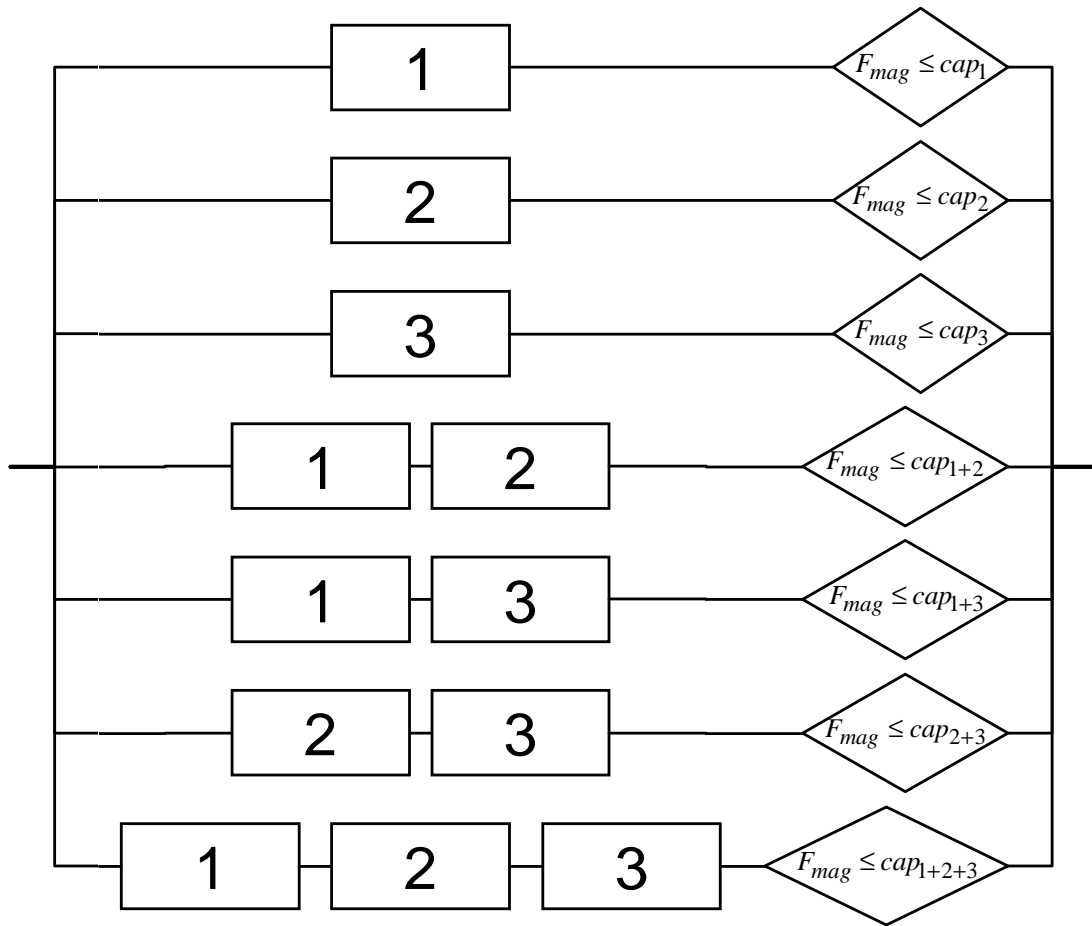
Limitations are imposed due to the fact that load-sharing is often provided by dissimilar components or systems. These components may vary in potential load capacity and reliability. In order to consider continuous representation of reliability objectives among units with varying embodiment, traditional tools must be augmented to provide information verifying that reliability targets are met for a non-constant reliability requirement. For a conceptual architecture which can potentially utilize dissimilar means for the fulfillment of a single function, one cannot assume independent and identical parallel units for load sharing.

When load sharing can be provided by dissimilar components with various functional capacities, the problem can be restructured as illustrated in figure 37. Initially assuming that any combination of components can fulfill the required level of functionality yields $\sum_{i=1}^n \binom{n}{i}$ parallel paths. Restructuring three parallel load sharing components which provide a function at magnitude F_{mag} creates multiple parallel paths each active when the capacity of the contributing blocks meets or exceeds the functional requirement [242].

Determining the reliability for load sharing between multiple components through parallelizing and checks is illustrated through the example of the reliability of three notional units providing the same function: providing steady state electrical power. Assume no functional restoration available on these units (fault duration $\gg 0$). The reliability to load relationship for each of these elements is shown in figure 38. Assume element $U1$ has a 3 kW load capacity with a reliability of 80% (given in blue), element $U2$ can support 5 kW with at 90% reliability (given in green), and element $U3$ can support 6 kW at 99% reliability (given in red).



(a) 3 Parallel Load Sharing Units Required to Fulfill Function at Magnitude F_{mag}



(b) Reformulated RBD for 3 Parallel Load Sharing Units

Figure 37: Reposing Load Sharing Reliability Block Diagram

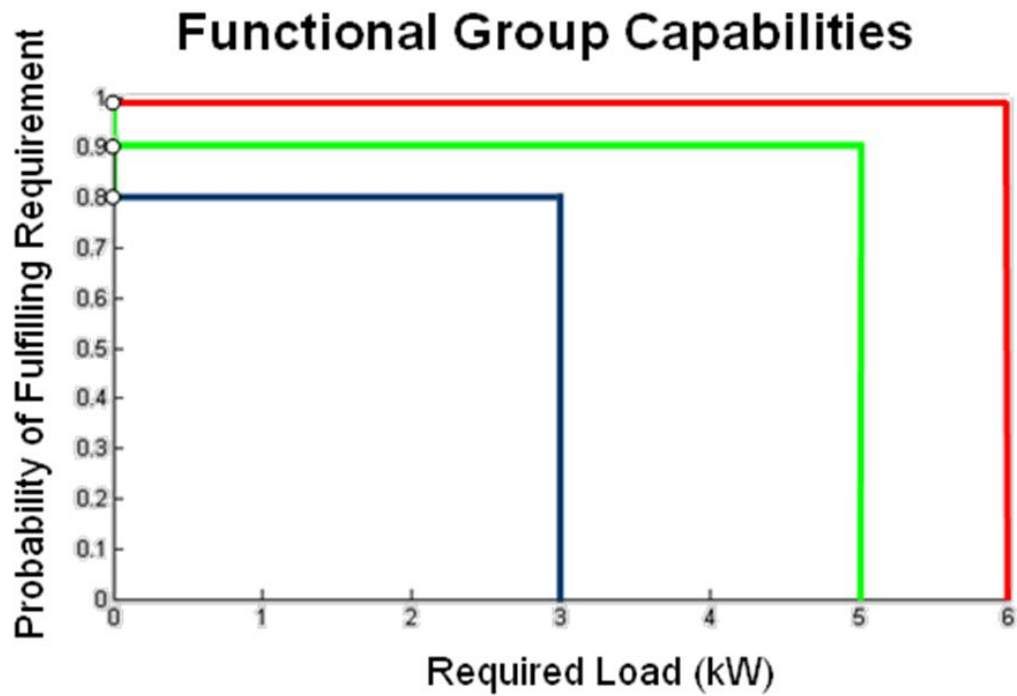


Figure 38: Notional Reliability Curves for Load Sharing Elements

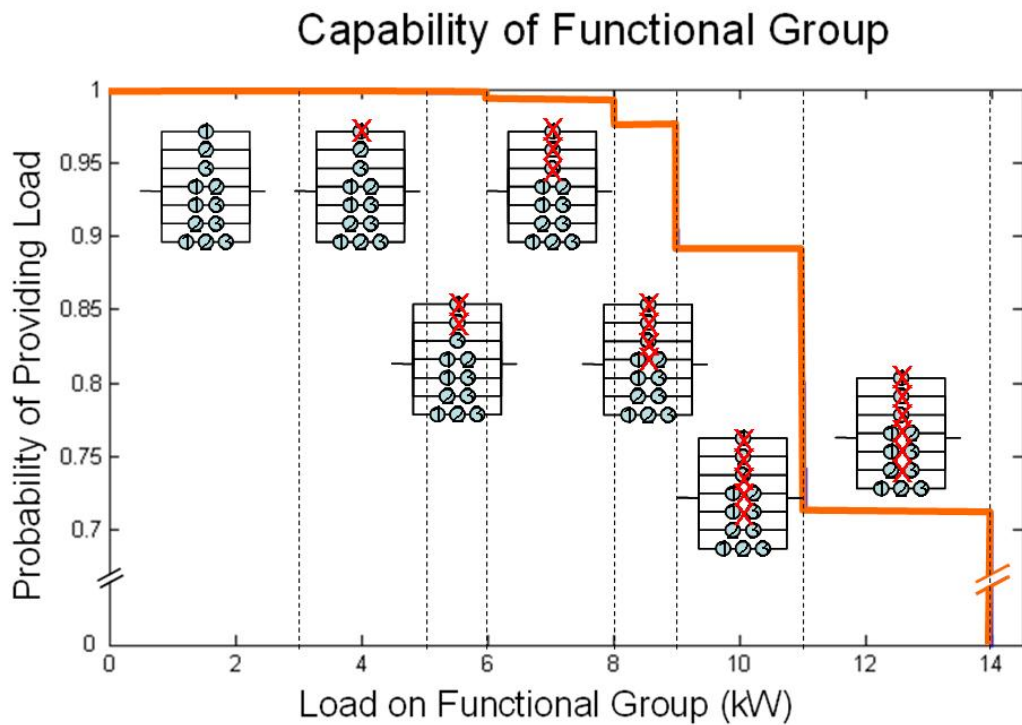


Figure 39: Load Sharing Reliability of the Functional Group A,B,C with Reliabilities as Illustrated in Figure 38

For kW loads requirements less than 3 kW any individual element or combination of elements are capable of fulfilling the requirement. Thus, the reliability for loads under 3 kW can be provided by any combination of elements. Above a 3 kW load requirement and below 5 kW all combination of elements besides $U1$ can provide the necessary capability. Between 5 and 6 kW $U1$ and $U2$ alone are insufficient. Thus, the load sharing reliability reduces until the limit load of 14 kW. Loads over 14 kW can no longer be supplied by this combination of systems. The new reliability relationship for the functional group $U1, U2, U3$ is illustrated in figure 39.

Assigning continuous safety requirements to the fulfillment of functions imposes a constraint on the probability of a given loss of functional capacity. Assuming this relationship is given by the inverse exponential function as displayed in figure 40 it can be seen in figure 41 that the unit group ($U1, U2, U3$) does not provide sufficient reliability throughout the range of reliability requirements. The reliability requirement given in red exceeds the system capability shown in blue in this figure. The ability to a minimum capability under rare failure conditions is constrained more stringently than the large load requirements under standard operation. The larger the loss of functional capability, the more stringent the failure incurred. While these three parallel systems exhibit adequate reliability for large load requirements, they fail to fulfill the more critical lower load levels with sufficient reliability.

In order to meet reliability and capability requirements, the attributes of the function group must be augmented. Using the constraint graph given in figure 41 the system architect gains insight as to which failure combinations contribute most to constraint violation and in what manner this violation can be remedied.

Consider the graph in figure 42. The fulfillment of functional requirements can be represented by points 1 through 7. Each of these points (x_i, y_i) is subject to the constraints $y_i \leq H_{MaxLimit}(x_i)$, where $H(x)$ is the value of the constraint at point x . Meeting the constraints can be achieved by moving the points in either the x

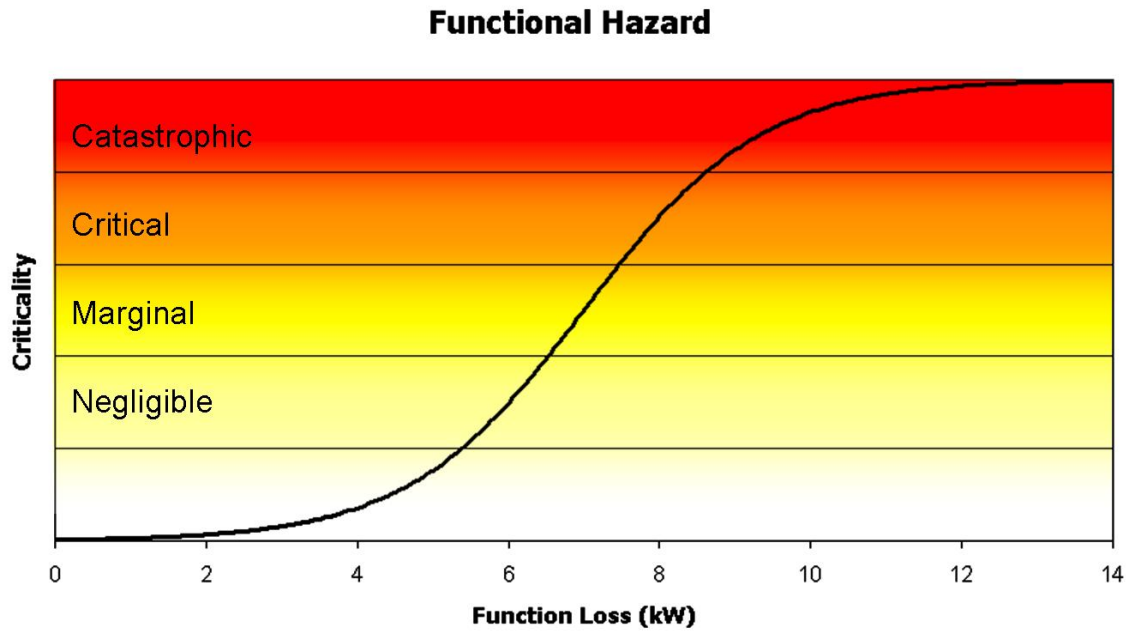


Figure 40: Notional Function Loss Criticality Curve

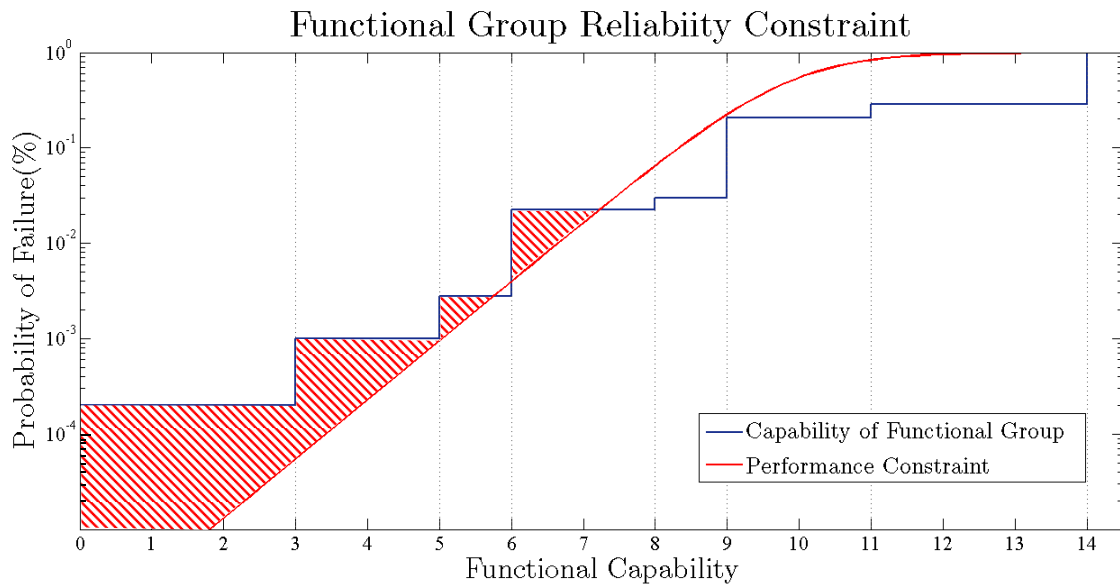


Figure 41: Comparison of Functional Group Reliability from Figure 38 Compared with Functional Criticality Constraint from Figure 40

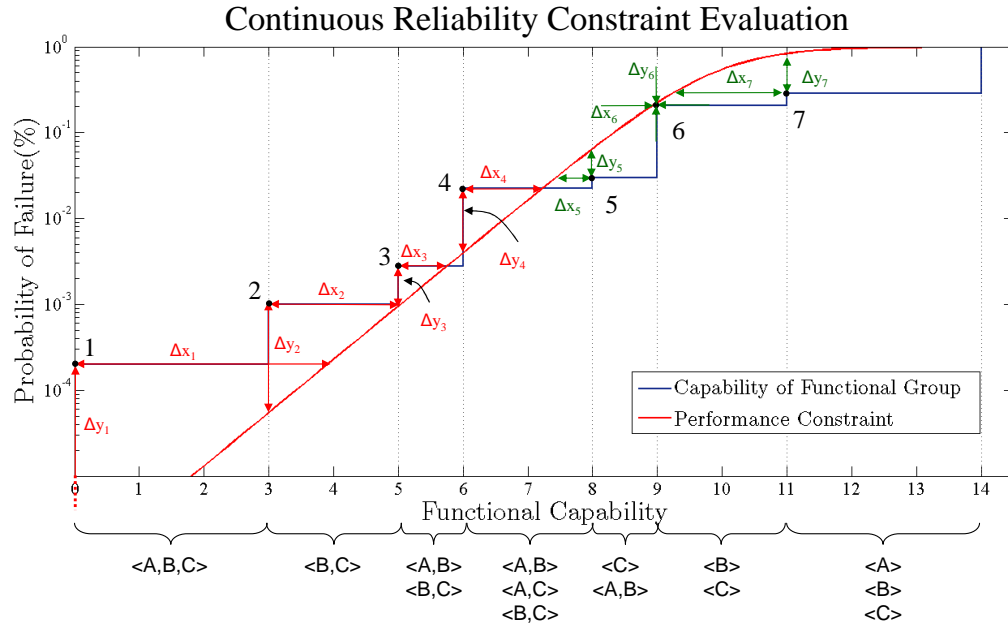


Figure 42: Continuous Reliability Assessment/Optimization

or y directions. Sufficient reliability can be achieved by augmenting the capacity of the elements, increasing the reliability of each unit, including additional redundancy, or reducing failure duration through functional repair. A change in the y direction (Δy_i) is achieved by increasing unit reliability. A change in the x direction (Δx_i) is achieved by increasing the capability of the redundant units. For example, point 2 can be moved in y by increasing the reliability of units B or C . It can also be moved in x by increasing the capability of the only other redundant unit A (unit a not belonging to the set contributing to the failure ($\langle B, C \rangle$)).

System design/optimization takes the form displayed in equation 12. Here, **Cap** represents the capabilities of system units, η and β represents Weibull parameters for the unit hazard functions, and **MTTR** represents the maintenance schedule. The points can not be translated in this space independently of each other. The x positions are functions of the capabilities of all of components fulfilling similar functions. The y positions are functions of the failure probabilities of all contributing failure combinations.

Min:	Cost= $f(\mathbf{Cap}, \eta, \beta, \mathbf{MTTR})$				
<table border="1" style="border-collapse: collapse; width: 50%; text-align: center;"> <tr> <td style="padding: 2px;">\mathbf{Cap}</td> </tr> <tr> <td style="padding: 2px;">η</td> </tr> <tr> <td style="padding: 2px;">β</td> </tr> <tr> <td style="padding: 2px;">\mathbf{MTTR}</td> </tr> </table>	\mathbf{Cap}	η	β	\mathbf{MTTR}	<i>s. t.:</i> $y_i - H_{Lim}(x_i) \leq 0$
\mathbf{Cap}					
η					
β					
\mathbf{MTTR}					
<hr style="border-top: 1px dashed black;"/> Where: $x_i = f_{x_i}(\mathbf{Cap})$ and $y_i = f_{y_i}(\eta, \beta, \mathbf{MTTR})$					

(12)

In the case described here adding capacity does not effect the reliability of low functional loads (point 1). Insufficient reliability for the system at $x = 0$ must be remedied through increases in reliability. This can be achieved by increasing unit reliability through design or dispatch or by augmenting the architecture through the inclusion of additional redundant units). Extending safety and reliability methods in this fashion yields additional design insight towards optimal fault tolerant solutions.

5.2.2 System Level Implementation

Formulating load shedding optimization requires a detailed understanding of how functional requirements flow throughout a system. Every point in the architecture where multiple loads are placed on a single unit or group of units necessitates load prioritization. When generating concept architectures these points must be systematically identified with sufficient information to format function/hazard relationships for upstream systems in terms of unique shedding strategies.

Function/hazard information must be made available at all points in the architecture where these shedding decisions must be made. Additionally, all unit level continuous functional/reliability requirements must be traceable to the support of platform level functions and operations in light of optimal performance degradation strategies.

Complex unit interactions and highly interdependent structures of aircraft vehicle systems architectures pose difficulties in the traditional hierarchical flow-down

of functional and reliability requirements. Therefore, a systematic means for the management of architecture relationships in the communication of requirements is necessary.

Functional dependency relationships communicate requirements from the platform to each individual unit or groups of units. The system can be represented by a directed graph which depicts the communication of functional requirements between subsystems or components. These directed graphs use edges to communicate requirements upstream from the system boundary (load, hazard) and capability downstream for the system nodes (capacity, reliability).

$$\{\mathbf{X}\}_{i+1} = f([\mathbf{A}] \times \min(\{\mathbf{X}\}_i, \{\mathbf{K}\}), \{\mathbf{Op}\}) \quad (13)$$

The adjacency matrix for this complex graph, $[\mathbf{A}]$, propagates capabilities between system units from the upstream to the downstream unit. System capabilities are iteratively determined by equation 13. In this relationship, $\{\mathbf{X}\}$ represents all input and output capabilities seen by unit edges, the function $f(\{\mathbf{X}\}, \{\mathbf{Op}\})$ captures all relationships between the capability provided to each unit and its downstream capability during the operational state $\{\mathbf{Op}\}$. Figure 43 illustrates the formulation of the capability propagation. The $\{X\}$ vector and $[A]$ matrix are sized by the number of upstream and downstream interrelationships. The output capabilities of unit b and c are calculated by the f function in terms of the upstream capability relationships.

$$\sum_{i=1^n, i \neq j} a_{ij} = 1, \quad \forall j \in \{\mathbf{C}\} \quad (14)$$

Additionally, $\{\mathbf{K}\}$ represents limitations placed on the unit capabilities by failure conditions, unit design limits, or external constraints. Energy balances introduced by the constraints in equation 1 are maintained by the adjacency matrix as shown in equation 14. Each column associated with the downstream relationships from combination elements ($\{\mathbf{C}\}$) is equal to unity. Additionally, diagonal values (a_{ii})

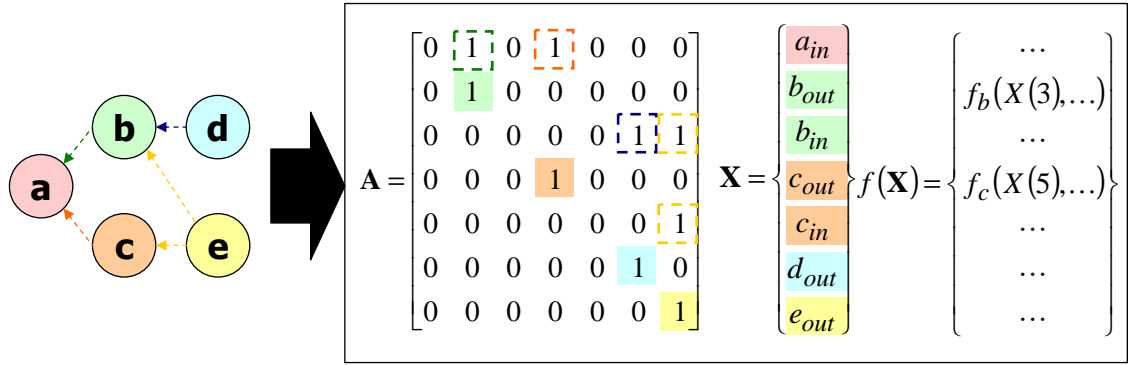


Figure 43: Formatting Propagation of Capabilities

corresponding to the downstream output from physical elements are also set equal to unity in order to retain information generated by querying unit sizing models.

Optimizing the response to a given failure state (capacity limit $\{\mathbf{K}\}$ and operating state $\{\mathbf{Op}\}$) is achieved by varying the proportional loading on each shedding column ($\{\mathbf{C}\}$) in $[\mathbf{A}]$ and shedding proportions for each node with multiple downstream outputs. The associated operational hazard is determined in terms of the capabilities in the capability matrix $\{\mathbf{X}\}_n$ which interact with the system boundaries and the operational state $\{\mathbf{Op}\}$.

Load shedding optimization takes the form of equation 15.

$$\begin{array}{l|l} \text{Min:} & \text{Operational Hazard} = H(\{\mathbf{X}\}_\infty) \\ \left[\begin{array}{c} \alpha_{x_1,y_1} \\ \alpha_{x_2,y_2} \\ \alpha_{x_3,y_3} \\ \vdots \end{array} \right] & s.t.: \quad \sum_{j=1, j \neq i}^n \alpha_{i,j} = 1, \quad \forall i \in \{\mathbf{C}\} \\ & \alpha_{i,j} \geq 0, \quad \forall i, j \end{array}$$

(15)

5.3 Architecture Definition

In order to determine the optimal allocation of failures for a concept, the architecture must be structured following equations 13.

$$\{\mathbf{X}\}_{i+1} = f([\mathbf{A}] \times \min(\{\mathbf{X}\}_i, \{\mathbf{K}\}), \{\mathbf{Op}\}) \quad (15)$$

A mapping of all functional relationships between systems must be defined ($[A]$), and appropriate transfer functions ($f(\{X\}, \{Op\})$) must be organized and updated as the architecture is augmented and redefined.

Systematic load shedding optimization and off-nominal performance analysis require architecture concepts to be expressed in a manner which efficiently expresses the functional interdependencies of the architecture. When performing exploratory architecture design, the aggregation and composition of the architecture must be allowed to change. However, the customer requirements are the same regardless of the product architecture. A functional perspective provides a consistent platform whereon the designer can define architecture alternatives. While the traditional conceptualization of architecture relies on systems generalization, clustering, and functional allocation, structuring the process following a functional perspective avoids many constraining assumptions regarding systems structure and unit responsibilities.

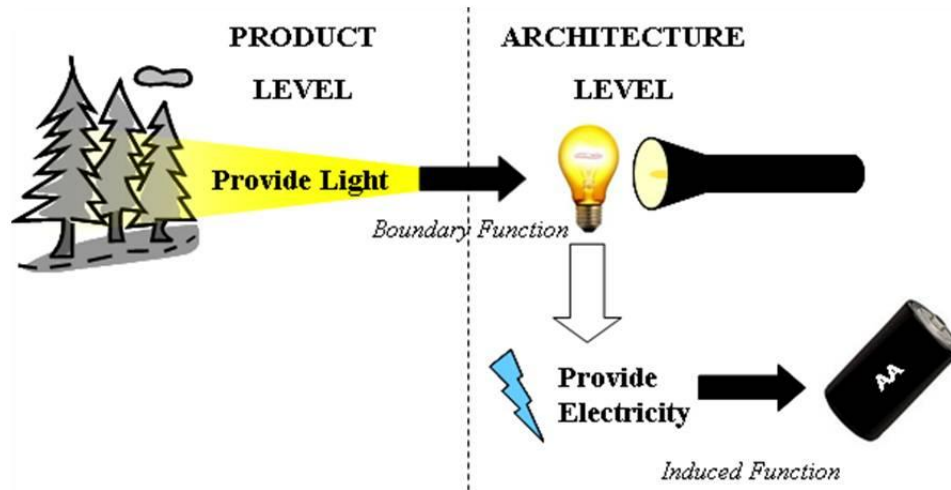
The Energy Optimized Aircraft and Aircraft Equipment Systems Program Committee from the America Institute of Aeronautics and Astronautics was formed to support research towards novel approaches to integrating aircraft equipment systems. This support led to the development of a robust functional perspective and process for organizing architecture formulation of trades called functional induction [203]. This process of facilitates adaptive architecture definition and enables the concurrent definition of concept architecture, sizing model generation, and the formulating of the load shedding optimization process. Toolsets based on this process were developed at the Aerospace Systems Design Lab (ASDL) and Georgia tech.

Functional Induction is a means to facilitate the process of architecture design and allows for flexible structuring of the design solution [67]. Functions are used as the means of defining and communicating requirements by addressing what system elements are “supposed to do.” Typically, functions are described as a minimum of two

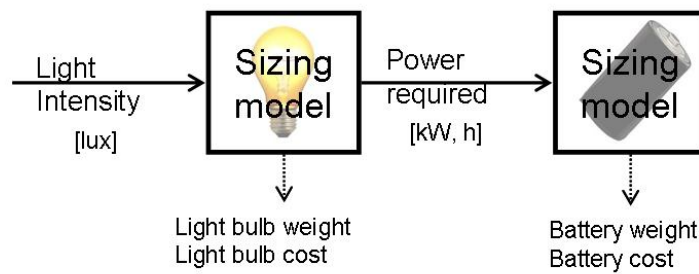
specific characteristics: action and magnitude. In addressing load shedding and safety and reliability requirements, the attributes are expanded to include reliability. Thus, to completely specify functional requirements the capacity must be characterized by a given magnitude at a desired security.

Functional Induction provides conceptual structure to the architecture and frames the means for architecture assessments, including safety and reliability calculations. This method for concurrent concept and model definition tracks the functional dependency between units or systems through the systematic definition of functional relationships. Functional induction defines two distinct types of functions: boundary, and induced. The boundary functions are platform level functions which relate the platform to its operating environment ('inter' functions). This type of function is independent to architecture embodiment. Induced functions describe the relationships between system components ('intra' functions). Mavris et. al. illustrate functional induction with the notional flashlight example shown in figures 44 [203]. While the function to provide light remains fixed at the product level, choices regarding the means of providing that light induce additional functions within the architecture. As these elements are designated to fulfill functional requirements unit models are instantiated which determine the magnitude of induced functional requirements and unit level attributes.

In a given architecture, there may be many distribution, transformation, or source elements which can fulfill given functional requirements or loads. The source used may vary with mission segment or operation. In order to define the sizing requirements for the architecture units, these complex functional relationships must be defined. Tools were developed to managing the relationships between function, physical element, and structure. The primary tool developed for functional induction is called the Architecture Design Environment (ADEN).



(a) Boundary and Induced Functions



(b) Instantiated Model Relationships Following Functional Induction

Figure 44: Notional Flashlight Functional Induction Example [203]

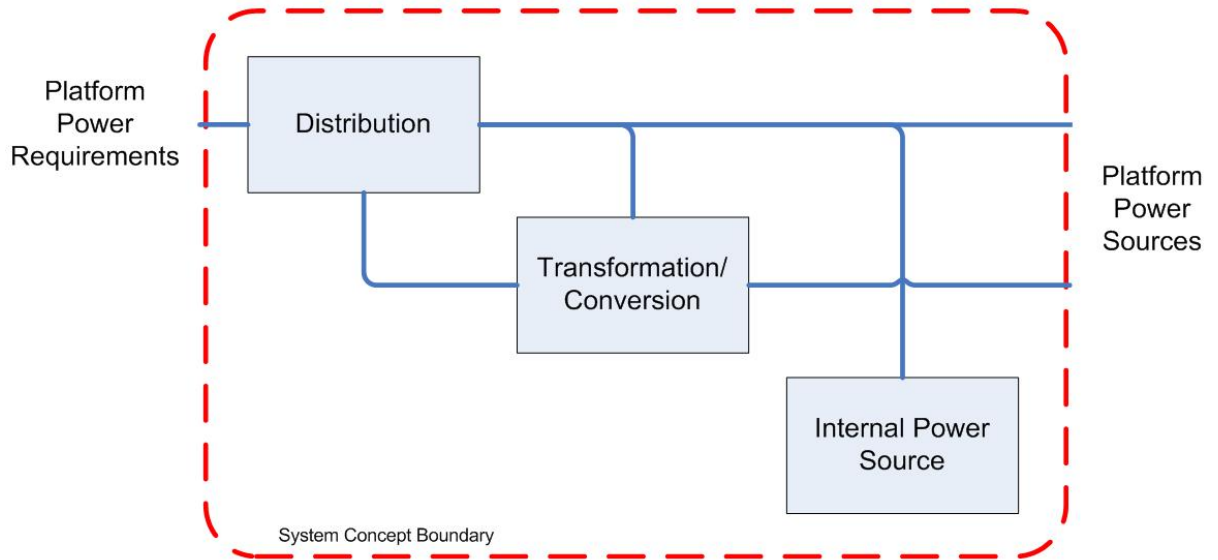


Figure 45: Types and Requirements Relationships for Systems Architectures

The process of ‘functional induction’ addresses the inadequacy of traditional systems design tools like the morphological and design structure matrix due to complexity introduced by allowing the architecture to vary. It allows the design space to augment as decisions are made for the fulfillment of architecture functions. The platform level environment introduces architecturally independent functions to the vehicle systems. Acting across system boundaries terms these functions ‘boundary functions.’ As instances of physical elements are introduced to fulfill known defined functions, new function are introduced. These ‘induced functions’ depend on the specific implementations of functional requirements. Each physical elements is characterized in terms of the functions they fulfill and the functions they induce. The process of architecture definition using functional induction includes iterative introductions of functions and definition of physical fulfillment.

In the development of functional induction, four distinct groupings of elements were identified to facilitated decomposition and definition: distribution elements, transformation or conversion elements, source elements, and storage elements. These physical elements are characterized by the functions they perform. Load elements and

introduce functional requirements on other system units [271]. Figure 45 illustrates these elements and the functional requirements flow between them by means of a design structure matrix.

Distribution elements fulfill the function of providing energy, information, material, etc. in the support of some load. The distribution element in turn places a load requirements of the same energy, information, material, etc. on a load provider. The load providers are sources, or transformation/conversion elements. Transformation and conversion elements fulfill some load requirements while inducing requirements for loads of a different type. Sources are the ultimate suppliers of energy, information, material, etc. to support the platform level loads. These sources can be internal or external to the system (e.g. ram air is external source, fuel tank is an internal source). One element which complicates architecture definition is a storage element. A storage may act as a load or a source depending on what is necessary to support platform level functions during the mission. The charge/discharge scheduling of the storage elements necessitates introducing iterative methods for handling time in the sizing.

Additional information may also be required at the unit level concerning the attributes of the system as driven by the functional requirements. These attributes may include any information which is necessary to evaluate overall platform level effectiveness. Typical attributes which are desired are weight, volume, and cost. Other attributes, like heat generated and such, may be managed as induced functional relationships, or may be tracked as metrics depending on the architecting scope of the system.

A functional perspective and the use of functional induction provide an important framework for this thesis. Tacit knowledge, engineering judgment, independent assessment of the various architecture dimensions, and baseline architectures greatly reduce design freedom. Understanding the complexity of the design space and the

way design decisions impact the reduction of that space highlights the impact of design decisions on the variability of the architecture solution. Functional induction also provides the functional framework whereby criticality requirements can be allocated.

Functional induction is facilitated by the integration of morphological analysis and the design structure matrix. Managing the information necessary to integrate architecture conceptualization and model generation is achieved through the Architecture Design Environment. This tool is used to automatically instantiate architecture models following conceptual architecture definitions. For more information regarding the ADEN toolset and functional induction, see previous publications [12, 11, 67, 68]. This toolset is the framework by which architecture concepts are defined and analysis models are created for this thesis.

5.3.1 System Level Example

Consider a notional system which provides for the completion of two system level functions as depicted in Figure 46. For this system, two system level functions are provided: provision of 28V DC power (F_1) and the provision of 120V AC power (F_2). The 21×21 adjacency matrix for this simple graph is displayed in Figure 47 a. This matrix represents the communication of capabilities from one unit to another. The design limits for all unit capabilities is given with the $\{\mathbf{K}\}$ array shown in Figure 47 b. The initial values in the matrix $\{\mathbf{X}\}_0$ are zeros except for $X(19)$, $X(20)$, and $X(21)$. These values are set to equal the corresponding capability limit: $K(19)$, $\{K\}(20)$, and $K(21)$ respectively.

The transfer function (f) is given by a series of transfer functions for each node as displayed in equation 16. For this notional example problem the transfer function takes the form of simple efficiency relationships where all efficiencies (η_i) equal to 90%. The capabilities transferred through the system boundaries, $X(1)$ and $X(2)$, are in turn used to determine the level of hazard incurred with system losses, ($H(\{\mathbf{X}\}, \{\mathbf{Op}\})$).

$$\mathbf{f}(\mathbf{X}, \mathbf{Op}) = \left\{ \begin{array}{l} X(3) = f_1(X(4), \{\mathbf{Op}\}) = \eta_1 X(4) \\ X(6) = f_2(X(7), \{\mathbf{Op}\}) = \eta_2 X(7) \\ X(9) = f_3(X(10), \{\mathbf{Op}\}) = \eta_3 X(10) \\ X(11) = f_4(X(12), \{\mathbf{Op}\}) = \eta_4 X(12) \\ X(13) = f_5(X(14), \{\mathbf{Op}\}) = \eta_5 X(14) \\ X(16) = f_6(X(17), \{\mathbf{Op}\}) = \eta_6 X(17) \end{array} \right. \quad (16)$$

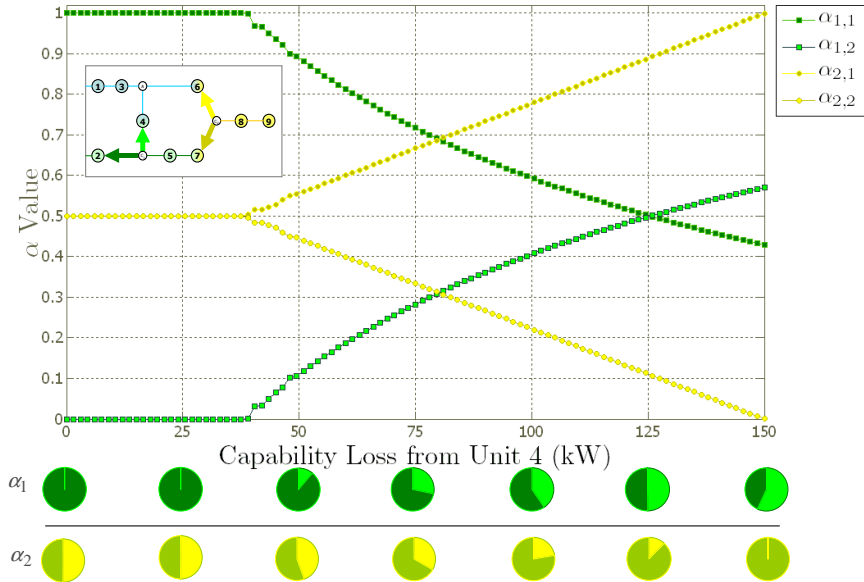
This simple graph includes two nodes at which load shedding decisions must be made (node C_1 and C_2). The proportion of the load transferred upstream from these nodes are regulated by the variables $\alpha_{1,1}$, $\alpha_{1,2}$, $\alpha_{2,1}$, and $\alpha_{2,2}$. Optimal load shedding is achieved by determining the appropriate combinations of the α variable in order to minimize the hazard. Different criticalities for the system level functions drive different responses to unit failures.

Failures occurring on parallel paths within the system require intelligent shedding of loads. Consider a failure of the unit at node 4 (120V DC to 28V Power Converter Unit) whose maximum downstream capability equals 150kW DC power ($K(11)$). Each proportional failure of this unit may yield a different optimal load allocation. Under non failure conditions the load allocation $[\alpha_{1,1}, \alpha_{1,2}, \alpha_{2,1}, \alpha_{2,2}]$ is equal to $[1, 0, 0.5, 0.5]$. The optimal failure allocation is determined over the range of capacity limits in $K(11)$ from 0 to 150kW. The results of these optimizations are shown in the results in Figure 48.

The hazard is expressed on the range $[0, 1]$ with 0 indicating no operational impact of functional loss and 1 indicating catastrophic results incurred. Depending on the risk mitigation index [90] for these hazards the limiting probability corresponding to values on this range may change. For this example it was assumed that a system level loss of 28V DC electrical power is independent of the loss of 120V AC power. This assumption holds when the functions supported by these two power types are

Failure Allocation at Nodes (C_1 and C_2)

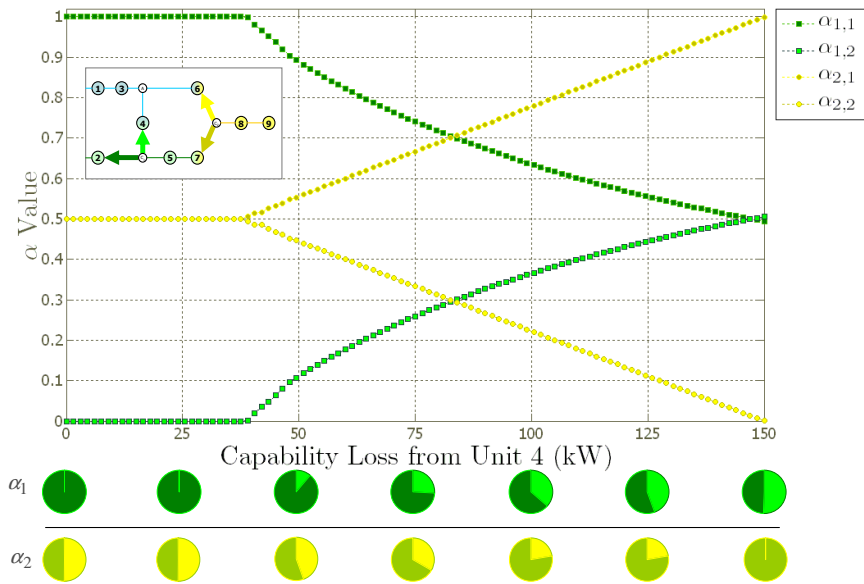
$$H_1 = \max \left[\left(1 - \frac{X(1)}{100}\right), \left(1 - \frac{X(2)}{100}\right) \right]$$



(a) Optimal Failure Allocation for Hazard Functions H_1 (Equation 17)

Failure Allocation at Nodes (C_1 and C_2)

$$H_2 = \max \left[\left(1 - \frac{X(1)}{100}\right), \left(1 - \frac{X(2)}{100}\right)^{\frac{1}{10}} \right]$$



(b) Optimal Failure Allocation for Hazard Functions H_2 (Equation 18)

Figure 48: Failure Allocation for Load Shedding Optimization with Failure of Node 4 of the System Graph in Figure 46

independent. If these capabilities are not independent the objective function must reflect their relationship. Additionally, the system of interest could be expanded to capture the interactions between these capabilities.

The load shedding optimization was performed considering two objective functions. These objective functions are displayed in equations 17 and 18. The hazard associated with the loss of DC power was assumed to be proportional to percent loss with an initial 100kW DC power capability $[1 - X(1)/100]$. The first hazard function (equation 17) assigns hazard values as the maximum percent loss of functionality. In order to illustrate the change in optimal load shedding with variation in system level hazards, the hazard associated with loss of AC power was increased in the second hazard function (equation 18). The hazard associated with this loss of $X(2)$ in equation 18 increases exponentially from 0 and 1. This notional relationship between hazard and capability loss is intended only illustrate the variation in load shedding during various operating states. More useful objective functions must be derived using the continuous functional hazard assessment.

$$H_1 = \max \left[\left(1 - \frac{X(1)}{100} \right), \left(1 - \frac{X(2)}{100} \right) \right] \quad (17)$$

$$H_2 = \max \left[\left(1 - \frac{X(1)}{100} \right), \left(1 - \frac{X(2)}{100} \right)^{\frac{1}{10}} \right] \quad (18)$$

Evaluating the probability in which a system level loss will occur must take optimal response to the failure into account. The optimal response determines the relationship between the unit capability loss, the magnitude of system failure, and the associated hazard.

Optimal reliability allocation favors one boundary function over another. Thus, more critical boundary functions are provided with higher probability. Figure 48 indicates that optimal shedding prescribes the original allocation to be maintained with Node 4 failures of less than approximately 40 kW. As the failure increases,

functional dependency relies more on AC distribution and the AC to DC 28V power converter. Depending on the magnitude of this failure, the efficiency of the units, and the hazards associated with functional loss, the optimal allocation proportions are ascertained. As illustrated in Figure 48(c), hazard function H_2 places more emphasis on the fulfillment of the function F_2 (or $X(2)$) by driving increased $\alpha_{1,1}$ values.

5.3.1.1 Failure Cases

Determining this reliability requires the evaluation of each optimal failure response for all statistically significant unit failures or unit combination failures. For larger architectures the number of failure combinations increases exponentially. However, the failure probabilities also decrease exponentially with the number of concurrent failures. Assuming independent failures, combinations of probability orders of magnitude smaller than the typical 1×10^{-9} probability limit for catastrophic failures on aircraft platforms may be neglected. Additional simplifications to reliability evaluations are achieved by managing of common cause and cascading failures failures through identification of functional dependencies.

The probability of a failure with a given magnitude is determined by finding the union of all applicable failure combinations. The maximum number of concurrent failures which are required for statistical significance (n) is given by equation 19, assuming that catastrophic failures are limited by a probability of 1×10^{-9} . In this relationship x is the total number of independent failures and P_{max} is the largest independent failure probability.

$$P_{max}^n \cdot \binom{x}{n} \leq 1 \times 10^{-10} \quad (19)$$

If P_{max} is greater the largest independent failure probability then for any failure intersection then equation 20 applies.

$$P(F_1 \cap \dots \cap F_i) \leq P_{max}^i \quad (20)$$

Additionally, because probabilities take on values from 0 to 1, the union of independent probabilities is bounded by:

$$P(F_i \cup F_j \cup F_k) \leq P(F_i) + P(F_j) + P(F_k) \quad (21)$$

Combining equations 20 and 21, the probability of all cases including i concurrent failures, P_i , is bounded by equation 22. Additionally, the overall probability of failure, P , is bounded by equation 23, where n is the total number of independent failures

$$P_i \leq P_{max}^i \cdot \binom{x}{i} \quad (22)$$

$$P \leq \sum_{i=1}^n P_{max}^i \cdot \binom{x}{i} \quad (23)$$

With knowledge regarding the minimum significant probability required (1^{-9} for catastrophic failures), the required value of n can be determined in equation 23. This decreases the number of cases which must be run. However, to afford rapid optimization of failure allocations, computational resources should be made available for large architecture structures with complex hazard functions. More details into the algorithm which identifies statistical significance is available in appendix D.

5.3.1.2 Analog PSSA

Table 22 displays the failure probabilities for all system nodes. All non-redundant elements which operate under nominal conditions operate with a maximum probability of failure of 1×10^{-9} . All other elements exhibit a maximum probability of failure of 1×10^{-6} .

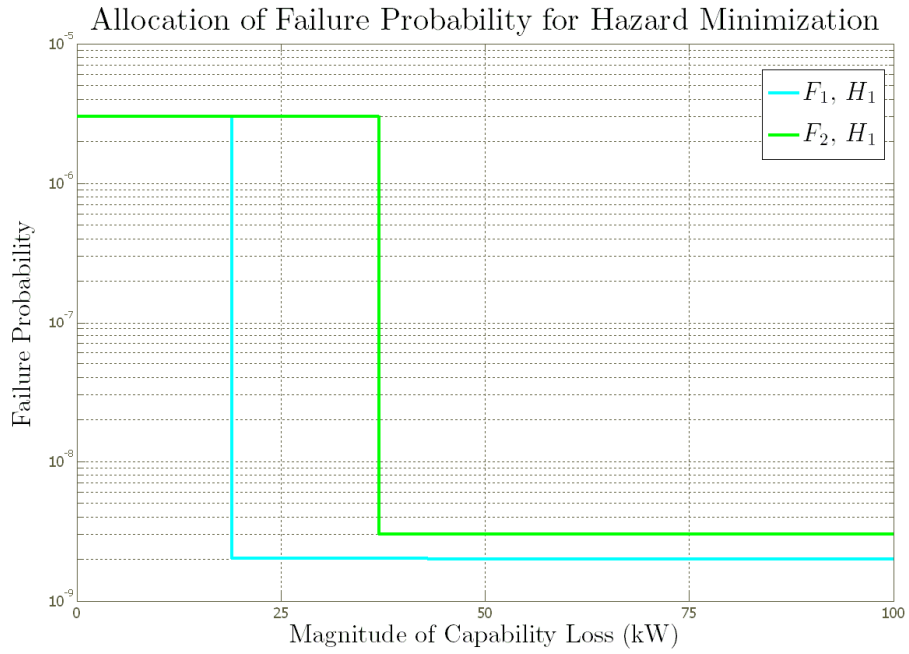
Table 22: Node Failure Probabilities for the Notional System in Figure 46

Node Number	Max Probability of Failure ($P_{max}(t)$)
1	1×10^{-9}
2	1×10^{-6}
3	1×10^{-9}
4	1×10^{-9}
5	1×10^{-9}
6	1×10^{-9}
7	1×10^{-6}
8	1×10^{-6}
9	1×10^{-6}

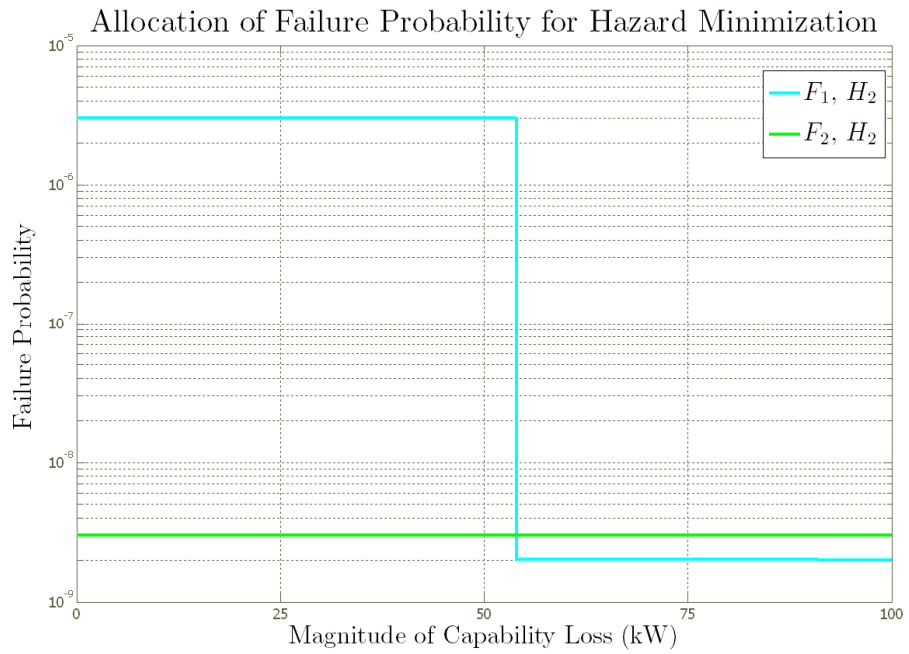
With these unit level probabilities and all failure combinations, the reliability of this notional system is displayed as a function of the magnitude of functional capability. This is shown in Figures 49 and 50.

As illustrated in Figure 49, the probability of failure for each individual system level function depends on the associated hazard functions. With a hazard function which favors losses to F_2 above those to F_1 (H_1), F_1 operates with higher reliability for a larger range of capability loss. Conversely, H_2 favors losses to F_1 and drives lower probabilities of loss for F_2 .

Although performance degradation is optimized, the system must still be evaluated in relation to reliability constraints. The probability of failure occurrence must not exceed the probability prescribed by failure classifications as outlined earlier. The function/hazard relationships H_1 and H_2 both yield failure probabilities exceeding the typical probability constraints (as per MIL-STD-882D, FAA-AC-1309, SAE-ARP-4754) as indicated by the red dashed line in Figure 50. However, the most driving reliability requirements do not necessarily act under the highest criticality classifications as seen in the figure for hazard function, H_2 . Depending on the stringency of the hazard probability constraints (indicated by a shift in the red dotted line to the yellow line), a marginal failure for the system operating under the second hazard function would require design augmentation. With the constraint given by the yellow



(a) Hazard Functions H_1 (Equation 17)



(b) Hazard Functions H_2 (Equation 18)

Figure 49: System Level Function Failure Probabilities with Optimal Shedding

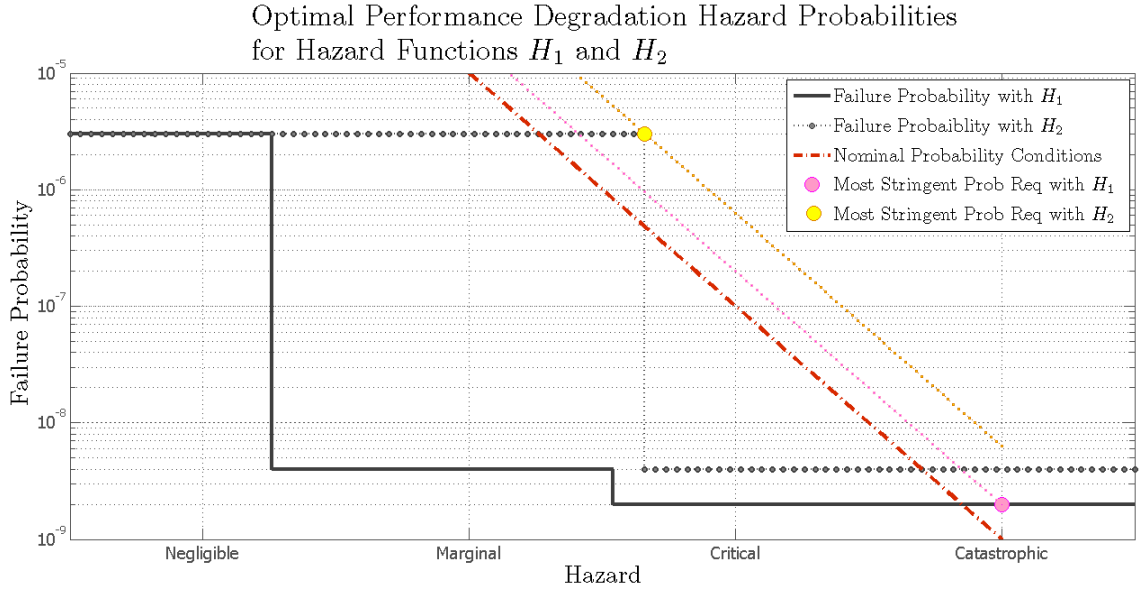


Figure 50: Hazard Probabilities with Optimal Shedding for Hazard Functions H_1 (Equation 17) and H_2 (Equation 18)

dotted line the catastrophic condition demands no redesign.

The notion that less hazardous conditions provide more sizing critical unit level requirements is not surprising. Nominal operating states typically pose the largest load requirements on the system as a whole. Depending on the allocation of these loads, these nominal requirements direct proportional load requirements on redundant systems. With the failure of redundant systems new requirements allocations must be used in order to provide the maximum amount of capability possible. Considering the complex structure of the system and optimal allocation of capabilities the magnitude of unit level requirements is emergent. Changing the structure or composition of the architecture concept changes this optimal allocation and changes the hazard probability curve. For novel architecture concepts, the internal operating states in which sizing critical reliability requirements emerge are unique.

Sizing critical requirements depend both on the shape of the failure vs probability curve as obtained by optimal load shedding and analog PSSA and the criticality vs probability constraint curve as determined by mission analysis and continuous

FHA. When comparing system reliability to the probability limits as defined by the hazard functions, it can be determined which failure combinations contribute most significantly to inadequate insurance of performance for all proportional functional fulfillment. This then can be used to inform augmentation to the system to meet constraints or reduce overdesign. Additionally, this approach reduces the necessity to rely on predefined rules of thumb regarding the impact of off-nominal operations on unit level requirements.

5.4 Method Overview

Two hypotheses were introduced pursuant to the thesis objective of integrating the identification of off-nominal operational requirements during architecture exploration.

Hypothesis 1: *Optimizing load shedding strategies yields more accurate predictions of unit level requirements than heuristically defined performance degradation during the exploratory design of revolutionary vehicle systems architectures.*

Pursuant to this goal, two needs were addressed. First, load shedding optimization requires the development of an objective function which captures the operational impact of platform level failure. Second, the relationship between these consequences system level failures must be defined within a framework in which the optimal allocation of failure consequences can be determined.

The objective function for load shedding optimization requires the adaptation of traditional Functional Hazard Assessment. In order to perform trades between various platform level failure allocations the relationship between hazard and functional failure is expressed as a continuous function of capability loss. As discussed in this chapter, this relationship can be defined anecdotally, or follow a physics based assessment of platform level capability requirements. The benefit to this strategy of failure characterization is expressed in Hypothesis 2.

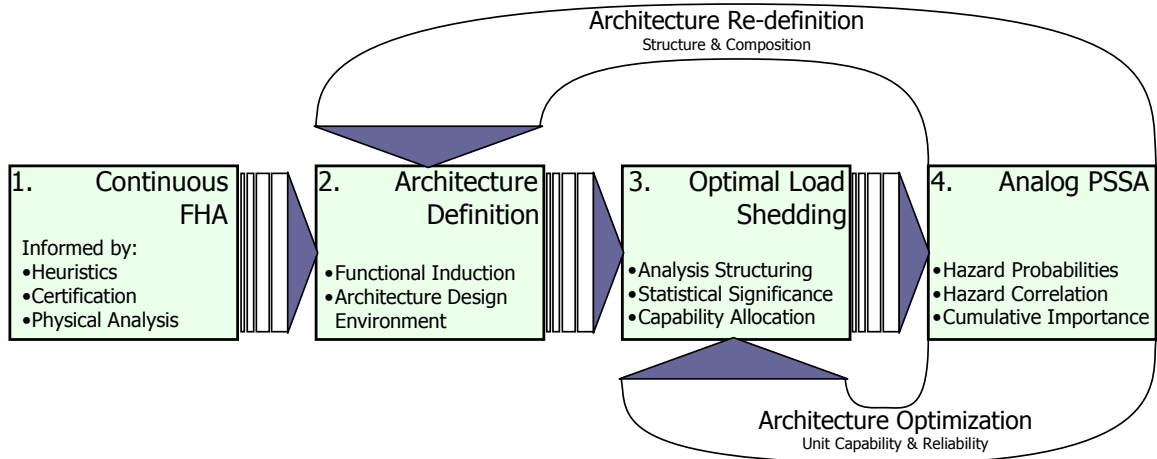


Figure 51: Process Used for Integrating Emergent Operational Requirements During Architecture Design, **SONOMA**

Hypothesis 2: *Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements.*

Capturing the effect of optimal load shedding on system architecture conceptualization is achieved in four steps as illustrated in figure 51. Three original methods are introduced to assist in off-nominal design:

1. Continuous FHA

Method 1: *The severity of system level failures are expressed continuously in terms of the magnitude of the functional failure.*

Addressing system performance in this fashion provides is superior to the traditional two state representations. It informs optimal load shedding and enables performance degradation analysis. Function/Hazard relationships are defined generic to the platform level and must be defined in a continuous fashion. These relationships maintain independence between overall functionality and the implementation space. Generating these relationships can be achieved anecdotally or by analytically assessing the effects of the failures.

2. Architecture Definition

Functional induction and the Architecture Design Environment are used to generate the matrices implemented during numeric load shedding optimization.

3. Optimal Load Shedding

Method 2: *Optimal load shedding is to be performed for all statistically significant unit failure cases to ensure adequate coverage of off-nominal requirements.*

Optimal Load Shedding identifies the preferred operational responses to unit failures in terms of function loss. Two approaches were explored which relate the platform level hazards to systems. The first, an analytical formulation for propagating criticality relationships, helps develop an understanding of how criticality must be assigned throughout the system as discussed in appendix E. This approach is limited in its applicability to larger, complex systems. The second, a numeric optimization approach was adopted for further implementation. While the analytical approach focuses on the flow of criticality from requirements to system, the numeric approach focuses on the flow of failure from system to platform level requirement. This allows for the assessment of any failure state which the system architect deems statistically significant. The numerical approach is implemented for the hypothesis testing. This optimization follows equation 15.

$$\begin{array}{l|l}
 \text{Min:} & \text{Operational Hazard} = H(\{\mathbf{X}\}_{\infty}) \\
 \left[\begin{array}{c} \alpha_{x_1, y_1} \\ \alpha_{x_2, y_2} \\ \alpha_{x_3, y_3} \\ \vdots \end{array} \right] & s.t.: \quad \sum_{j=1, i \neq j}^n \alpha_{i,j} = 1, \quad \forall i \in \{\mathbf{C}\} \\
 & \alpha_{i,j} \geq 0, \quad \forall i, j
 \end{array}$$

Where: $\{\mathbf{X}\}_{i+1} = f([\mathbf{A}] \times \min(\{\mathbf{X}\}_i, \{\mathbf{K}\}), \{\mathbf{Op}\})$

4. Analog PSSA

Method 3: *The probability of systems failure is expressed in terms of the magnitude of functional loss (% functional failure).*

Analog PSSA highlights necessary trades between design capability and reliability. Preferred solutions are identified following equation 12.

$$\begin{array}{|l}
 \text{Min:} \\
 \hline
 \begin{array}{l}
 \mathbf{Cap} \\
 \eta \\
 \beta \\
 \mathbf{MTTR}
 \end{array} \\
 \hline
 \text{Where: } x_i = f_{x_i}(\mathbf{Cap}) \text{ and } y_i = f_{y_i}(\eta, \beta, \mathbf{MTTR})
 \end{array}
 \quad
 \begin{array}{l}
 \text{Cost} = f(\mathbf{Cap}, \eta, \beta, \mathbf{MTTR}) \\
 \hline
 \text{s.t.:} \\
 y_i - H_{Lim}(x_i) \leq 0 \\
 \hline
 \hline
 \end{array}$$

Examples were given in this chapter which identify potential benefits available with the implementation of this load shedding optimization approach. Visually inspecting the continuous relationship between hazard and loss acts as a design tool which highlights potential fault tolerant design solutions. While these results are promising, further work will be presented in applying these tools to larger more representative systems. Validating these hypothesis lays the framework towards automatic definition and management of off-nominal operational requirements concurrent to architecture exploratory design.

The next chapter illustrates the implementation the first steps of the method illustrated in figure 51 for the aircraft vehicle systems architecture. The last step of this method (Continuous preliminary system safety analysis) for the aircraft vehicle system architecture is illustrated in the Analysis Results chapter.

CHAPTER VI

HYPOTHESIS TESTING

Hypothesis 1: *Optimizing load shedding strategies yields more accurate predictions of unit level requirements than heuristically defined performance degradation during the exploratory design of revolutionary vehicle systems architectures.*

Hypothesis 2: *Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements.*

Emergent requirements are a product of the combined behavioral impact of the units in a complex system. In performing system safety assessment for complex systems concepts, these emergent attributes must be considered while identifying new architecture specific safety and reliability requirements. The validity of assumptions concerning the structure of the function loss/hazard relationship are evaluated in terms of the architecture to which they are applied. In order to test these hypothesis it must be shown that the design conclusions reached for asimilar architecture concepts must differ significantly when applying assumptions regarding the application of operational requirements.

These two hypotheses are centered around gaining fidelity in vehicle systems sizing through changing the form of system level requirements and evaluating an architecture concept with respect to off nominal requirements. Hypothesis testing must include load shedding optimization on differing architectures concepts under similar platform level requirements. Additionally, it must be shown that increased accuracy of the platform level function/hazard relationship adds value to the design process by providing insight not otherwise available.

Concept architectures for hypothesis validation took the form of object oriented vehicle systems models for a short to medium range business jet. This platform was selected due to its well understood mission level requirements and a limited functional scope compared to military platforms. However, the vehicle systems architecture remains complex and exhibits emergent requirements.

Load shedding optimization was performed with objective functions at various degrees of fidelity. This was done to assess the impact that inaccurate representations of hazards have on architecture design. In order to consider the unique impact of platform level requirements on architecture concepts, load shedding optimization executed for two vehicle systems concepts: conventional and ‘more-electric’ vehicle systems architectures.

This chapter discusses the process for testing of these two hypothesis. It outlines the two architecture concepts to which load shedding optimization is applied and introduces the platform level function/hazard requirements used for this optimization.

6.1 Hypothesis Testing

As illustrated in figure 52, the two hypotheses address different impacts of load shedding optimization. The first hypothesis addresses the effect of implementing load shedding for dissimilar architecture concepts. The second addresses the effect of increasing the fidelity of the function/hazard relationship in terms of continuous functional hazard assessment. In order to validate these hypotheses a minimum of three load shedding optimization cases must be performed. One set of test cases addresses the differences between optimal load shedding strategies between architecture concepts. A second set of cases are then compared with additional cases evaluated with higher fidelity FHA.

A total of eight load shedding optimization cases were performed in support of these hypothesis. Requirements for two mission scenarios and two function/hazard

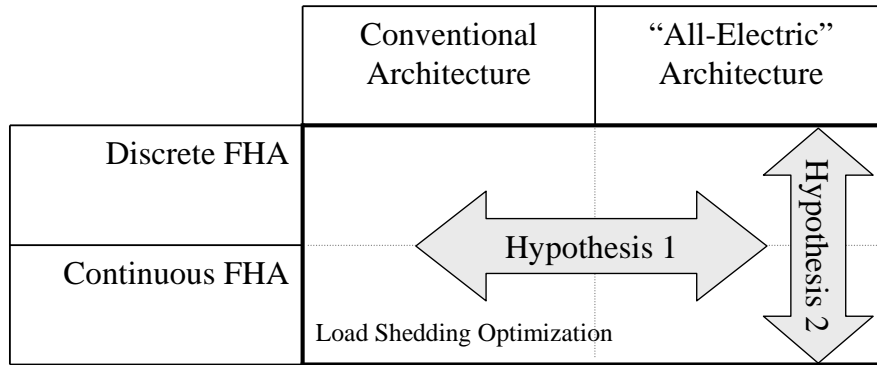


Figure 52: Focus of the Two Hypothesis Regarding the Application of Load Shedding Optimization

approximations were applied to the two vehicle systems architecture concepts. The limiting cruise and a takeoff scenarios were applied to evaluate sizing critical system performance. Variations in the structure and composition of the architecture were applied to address Hypothesis 1 and varying degrees of fidelity of the hazard objective function provide insight towards the claims of Hypothesis 2.

6.2 Hypothesis 1 Testing

There are three stages to the verification of Hypothesis 1. According to the hypothesis, the sizing critical requirements and associated load shedding strategies generated through the minimization of operational hazards will differ for alternate architecture concepts. By defining two different architectures and optimizing their load shedding strategies, sizing critical requirements and their associated load shedding scenarios can be compared.

The first step in validating this hypothesis is the definition of the roles for which the systems architecture is responsible. The hazards associated with loss of functional capability are then characterized. These function/hazard relationships will act as the objective functions for load shedding optimization. Hazards are minimized by optimally allocating system capabilities. All statistically significant failure states must be evaluated to assess system reliability.

Comparative assessments are made for two vehicle systems concepts: a conventional architecture and a ‘more-electric’ architecture. These alternative architectures are initially defined and sized by the engine failure heuristics outlined in table 23.

Table 23: Architecture Sizing Shedding Heuristics

Load	Load Percentage with One Engine Failure
Base Loads	85%
Actuation	50%
Windshield Ice Protection	60%
Wing Ice Protection	40%
ECS	50%

Load shedding optimization is performed for both concepts. The sizing critical unit failure scenarios are compared. Differences in the load shedding strategies for similar component failures will be discussed. Significant variation in both the shedding strategy and unit level requirements will validate that load shedding optimization enables a more accurate prediction of unit level requirements.

Hypothesis 1 is tested as follows:

1. Apply heuristic for system sizing
2. Optimize load shedding for the baseline aircraft
3. Optimize load shedding for the ‘more-electric’ aircraft
4. Compare preferred load shedding strategies for the different concepts and the original heuristic
5. Perform Analog PSSA
6. Compare Analog PSSA results regarding the importance level of risk at the system and functional level

Undesirable performance risk for these concepts will indicate whether the heuristic applied for the sizing of these two architectures adequately captures requirements.

Additionally, differences between the magnitude of this risk indicates an applies bias in the application of the requirements. The validity of this hypothesis will be further shown by comparing the system level functions which produce the highest performance risk for each architecture concept.

6.3 Hypothesis 2 Testing

The second hypothesis addresses increased accuracy in requirements identification using a higher fidelity function/hazard relationships. Similar to the validation of hypothesis 1, this hypothesis will be addressed by comparing requirements generated using traditional methods (FHA) to those generated by higher fidelity continuous hazard analysis.

The same ‘more-electric’ architecture defined for hypothesis 1 validation will serve as the test case for the validation of this second hypothesis. While the architecture remains the same, the hazard function will be varied as illustrated in figure 53.

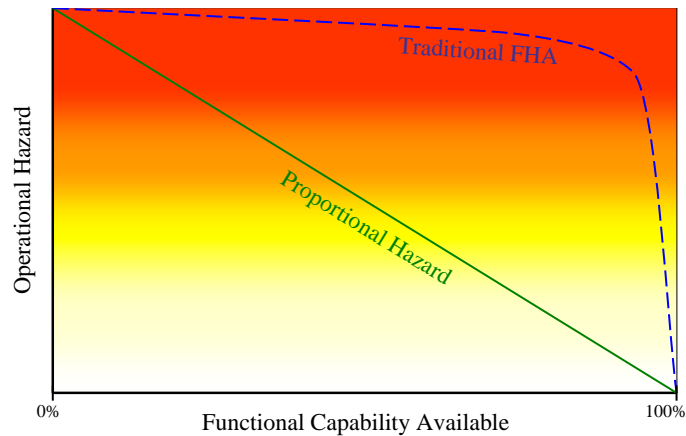


Figure 53: Comparative Baseline Hazard Relationships

A function/hazard relationship is applied for load shedding optimization which mimics the information available following traditional FHA. This is illustrated with the blue dashed line in figure 53. With little information qualifying the relationship between loss and hazard, traditional FHA only indicates that hazard occurs with failure. Therefore, small losses in functional capability yield large operational effects.

The second function/hazard objective function defined for load shedding optimization is illustrated with the green line in figure 53. This relationship assumes that hazards are directly proportional to the percent loss of system functionality.

Finally, a higher fidelity functional hazard assessment (discussed later) will be performed to define hazards which continuously vary with % loss in system functionality. These non-linear hazard relationship reflect the actual operational hazards which occur following system level function losses. Continuous system safety assessment is applied to the results of all load shedding optimizations.

Hypothesis 2 is tested as follows:

1. Apply heuristic for system sizing
2. Optimize baseline/"more-electric" aircraft architecture with discrete function/hazard relationship
3. Optimize baseline/"more-electric" aircraft architecture with higher fidelity function/hazard relationship
4. Perform Analog PSSA
5. Compare Analog PSSA results with varying function/hazard fidelity

Any significant overpredictions or underpredictions of system risk obtained by implementing lower fidelity hazard characterizations indicates inadequacies in the traditional function hazard definition tools. Additionally, changes in the perceived risk associated with the fulfillment of the vehicle functions generates may place undue emphasis on certain units which is not warranted. Variations in design bias indicate validation of this hypothesis.

6.4 System of Interest

As discussed in chapter three, the design space for a vehicle systems architecture is extremely vast. Even with a fixed set of technologies, architectures vary in terms of

the level of redundancy applied and the structure of functional flow. It is not possible to exhaustively explore the architecture design space. Indeed, the intent of this work is not to provide evidence for the application of one specific aircraft vehicle systems architecture concept over another. The goal of this thesis is to illustrate the benefits achieved by applying the extensions to safety and reliability tools discussed in the previous chapter. Assessing the benefits attained by applying the SONOMA process for varying architecture concepts requires that the architectures to which it is applied exhibit significant differences in structure and composition.

While many of the more electric studies have focused on large commercial applications or military platforms, the “More-Electric” concepts have made inroads to business jets class aircraft [88]. The vehicle systems architecture of a mid-size, two-engine, medium range business jet platform was selected for load shedding and continuous system safety analysis. The business jet mission is much simpler than those required from military platforms. However, these aircraft exhibiting similar subsystem functional requirements structure as larger commercial class aircraft. While providing similar functionalities at the platform level, the vehicle systems of business jets exhibit less complexity than those for large scale commercial transports. This platform affords the necessary size and scope to illustrate the benefits of optimal load shedding.

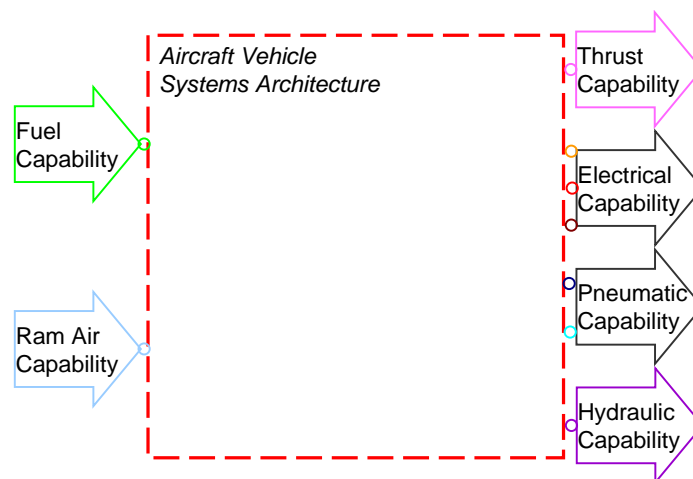


Figure 54: Boundaries of the Business Jet Vehicle Systems Architecture

Figure 54 shows the vehicle systems generalized in terms of the four primary requirements they provide. They are primarily tasked with providing electrical power, high temperature and potable pneumatic airflow, hydraulic flow, and thrust. The inputs to this system of interest include ram air and fuel (cooling capability is another potential input to the system). These vehicle systems capabilities are to the fulfillment of platform level functions, including environmental control, ice protection, actuation, avionics, and base aircraft loads.

6.4.1 Electric Technologies

Electrical technologies have impacted all aircraft systems and increased demand for electric non-propulsive power. However, the ‘more electric aircraft’ architecture focuses primarily on ‘vehicle systems’ functions as listed in table 1. This section reviews the specific technologies associated with the conventionally accepted ‘more electric aircraft’ architecture concept. These technologies involve actuation, environment control, ice protection technologies, engine auxiliaries, and electrical generation, distribution, and management systems. Assessing the benefits of ‘more electric aircraft’ must include some or all of these considerations in architecture optimization.

6.4.1.1 Actuation Technologies

There are two typical categories for actuation functions: flight control actuation and utility actuation. Flight control actuation is tasked with maintaining appropriate aircraft motion by creating yaw, pitch, and roll moments. Pilot control inputs drive actuators, which deflect control surfaces and induce aerodynamic forces. Utility actuation is tasked with applying forces necessary to fulfill many other aircraft functions. Landing gear extension and retraction, braking and steering systems, cargo and weapons bay doors articulation, and thrust reversers are all included in utility actuation.

Electro-hydrostatic actuators [EHA] and electro-mechanical actuators [EMA] are

the primary actuation technologies considered for the more-electric aircraft. Both the EHA and EMA eliminate the requirement to distribute hydraulic power. This has the potential to decrease systems weight and volume as well as provide improvement by eliminating maintenance issues concerning central hydraulic system. However, these devices must be supplied by an uninterrupted high power electrical distribution system.

In contrast to hydraulic actuators, EHA's utilize a localized hydraulic force. These actuators use a hydraulic piston to provide translational force. However, this piston is not connected to a central hydraulic system as is the case for traditional hydraulic actuators. Each actuator has an isolated supply of hydraulic fluid and its own pressure/flow generating device. This pressure/flow device often takes the form of an electrically driven fixed displacement hydraulic pump. Each EHA is also far more complex than a simple hydraulic actuator. It not only requires its own built in power transformation device, but it also becomes a source of thermal energy which must be managed.

The EMA is made up of a mechanical gear and screw system which converts rotational torque from an electric motor into a translational force. These actuators can receive either AC or DC electrical power to drive their motors. Due to limitations in force, response time, and jamming issues with EMA's, their application in aerospace systems was initially limited to non-flight critical utility actuation. However, advances in rare earth material for high power DC motors, solid state switching devices, and lightweight controls have increased the viability of using EMA for flight control applications [211]. With application of these technologies, failures can be potentially reduced with penalties in complexity, cost, and weight. For these reasons the EMA is typically not used for primary actuation. However, with technology advances, performance may increase to the point of increased feasibility [28].

6.4.1.2 Environment Control

The environment control system is tasked with providing a comfortable and safe passenger environment under potentially dangerous conditions. This environment manipulation includes elevating temperatures and pressures higher than those present at cruise altitudes and removing ozone and other particulates from the incoming airflow. Cabin pressure must be maintained at a minimum of 8000 ft pressure altitude with temperatures ranging between 65 and 73 °F. Humidity is also managed in order to prevent ice from forming in the pneumatic tubing and ducting, condensation from occurring inside the cabin, and fungus and bacteria from growing within the cabin and ECS systems. FAR regulations also stipulate that 0.55 lbs per minute of outside air must be provided per passenger. These requirements are met by providing external air and filtering and recirculating spent air back into the ECS system. As a result, the aircraft has a completely new cabin full of air every 2 to 3 minutes [48].

The ECS system is very complex. It is comprised of multiple physical elements, each fulfilling individual functions of the system (mix, filter, cool, remove O₃, etc). All of these functions are generalized by the single function to condition air. Although this function could be decomposed further, applying a higher level of abstraction allows the architect to simply compare different types of environment control system concepts; bleed, and bleedless.

In contrast to the conventional ECS, a ram compressed ECS system does not rely on pneumatic power from the engine to drive the system. Air is received by ram ports located in the belly fairing of the aircraft and is compressed to much lower temperature and pressure than that provided by the engine compressor. In so doing, the need for a precooling is eliminated. The pressure and temperature is directly determined by the electrically driven compressor. However, with lower operating temperatures, elements tasked with ozone removal and heat exchange must adapt and generally grow in size.

6.4.1.3 Ice Protection

Ice buildup can have detrimental and hazardous effects on aircraft performance. Icing occurs at altitudes and conditions where there is enough moisture in the air and temperatures are such that water begins to freeze on the skin of the aircraft. This generally only occurs during low altitude maneuvers, when the amount of moisture in the air can be problematic (e.g. takeoff, climb, descent, approach, holding, and landing). Ice buildup on the lifting and control surfaces can lead to flight instability, lack of control, and an inefficient production of lift. Systems must be used in the aircraft which either prevent ice formation from occurring (anti-icing) or remove ice when present on the aircraft skin (deicing).

Conventional ice protection devices on large scale commercial aircraft utilize the high temperature air available in the pneumatic system to heat the leading edges of the wings in order to protect the wing from icing. This heated air is directed along the surface of the leading edge of the wing, providing thermal energy to melt the ice or increase the temperature of the surface of the wing to prevent ice from forming. After the thermal energy has been used, this air is discarded overboard, representing a loss in thermal energy.

Pursuant to the removal of bleed systems, the 'more electric' aircraft utilizes electrical energy to provide the functionality to protect from ice. Many ice protection devices utilize electricity. Electro-impulsive, and electro-expulsive deicing elements use electrical energy to provide a mechanical force which moves the wing surface, breaking up accumulated ice [98]. Electrical anti-icing devices also exist which prevent ice from forming on the wing. Electro-thermal device convert electrical energy into heat which protects the critical lifting and control surfaces. Heaters do not require a stable electrical signal. Therefore, variable frequency signals, which are more efficient to generate, are often used to power electrical heating [211]. Eddy current devices have also been proven able to provide ice protection [98].

6.4.1.4 *Electrical Systems Technologies*

Multiple advances in electrical system technologies have contributed the capability to handle increased power requirements. The thrust of these advances go towards increasing capacity, reliability, and ‘ruggedness’ of electrical systems in supporting multiple types of power while decreasing weight and volume. Much of the improvement in electrical systems technologies can be attributed to advances in materials (insulation, dielectric, magnetic material) and low level components (capacitors, and inductors) [297].

The 90’s saw the development of high-power solid-state switching technologies enabling Variable-Speed/Constant Frequency (VSCF) generation. However, with increases in the magnitude and diversity of of flight critical electrical loads, current trends are pointing towards the adopting 270 VDC as the primary electrical power type. Conversion devices must then be used to support alternative electrical power types [211]. Specific developments in the electrical systems technologies include high-power shaft-mounted switched-reluctance starter generators, superconducting generators, fault protection/prediction systems, regenerative load management distribution systems, solid state distribution switching, high current intelligent power controllers and converters, and high power/energy density electrical storage technologies [44].

Additional considerations which have been raised following increases in electrical power requirements involved the means for providing adequate thermal management. Reductions in aircraft block fuel requirements, and increased thermal loads can potentially render the fuel tank insufficient as the sole thermal sink. Advanced inerting systems (e.g. OBIGGS), phase change materials, external air heat exchange, and insulation technologies are currently being pursued as alternatives for the management of heat produced by increases in electrical loads.

6.4.2 Proof of Concept Architectures

As discussed in the hypothesis testing, two architecture concepts must be evaluated and compared. The first vehicle systems architecture concept can be considered conventional. Environment control and ice protection are performed through customer bleed and control and utility actuation are supported by engine driven hydraulic systems (this is illustrated in figure 55). For the conventional aircraft architecture electrical power is used to support base aircraft loads (28V DC), and windshield ice protection (120 VAC).

The ‘more-electric’ architecture eliminates hydraulic and high pressure/temperature pneumatic requirements entirely. Hydraulic actuation is replaced by electrical actuation and ice protection is achieved through electric heating. While the customer bleed requirements are eliminated from the engine, pneumatic requirements are fulfilled by ram compression. Higher voltage (270V) electrical distribution and generation is used to reduce current requirements. Vehicle systems are supported entirely by electrical power generation. The ‘more-electric’ vehicle systems architecture is illustrated in figure 56.

These architecture concepts reflect the fundamental changes to the vehicle systems architecture which occur for the ‘more-electric’ aircraft. Again, these concepts represent two embodiments of this vast architecture design space. However, the differences in structure and composition are sufficient to address the claims made by both hypotheses. Significant variations in the emergent off-nominal requirements observed for these architecture concepts are observed in the next chapter.

In order to determine the available off-nominal capability of the system, the system model is formulated by equation 13.

$$\{\mathbf{X}\}_{i+1} = f([\mathbf{A}] \times \min(\{\mathbf{X}\}_i, \{\mathbf{K}\}), \{\mathbf{Op}\}) \quad (15)$$

Both concept architectures must be represented in terms of the adjacency matrix

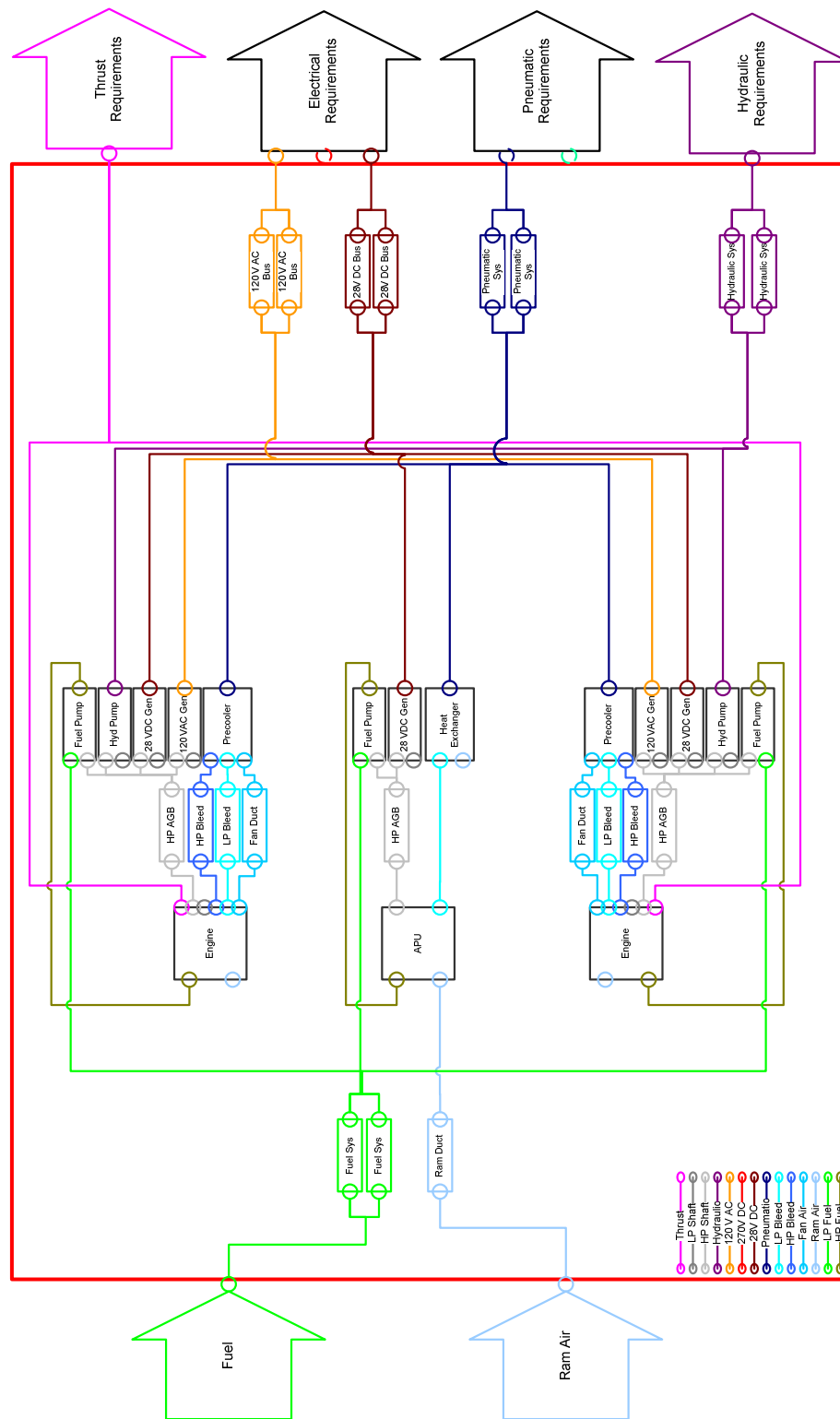


Figure 55: Conventional Architecture Diagram

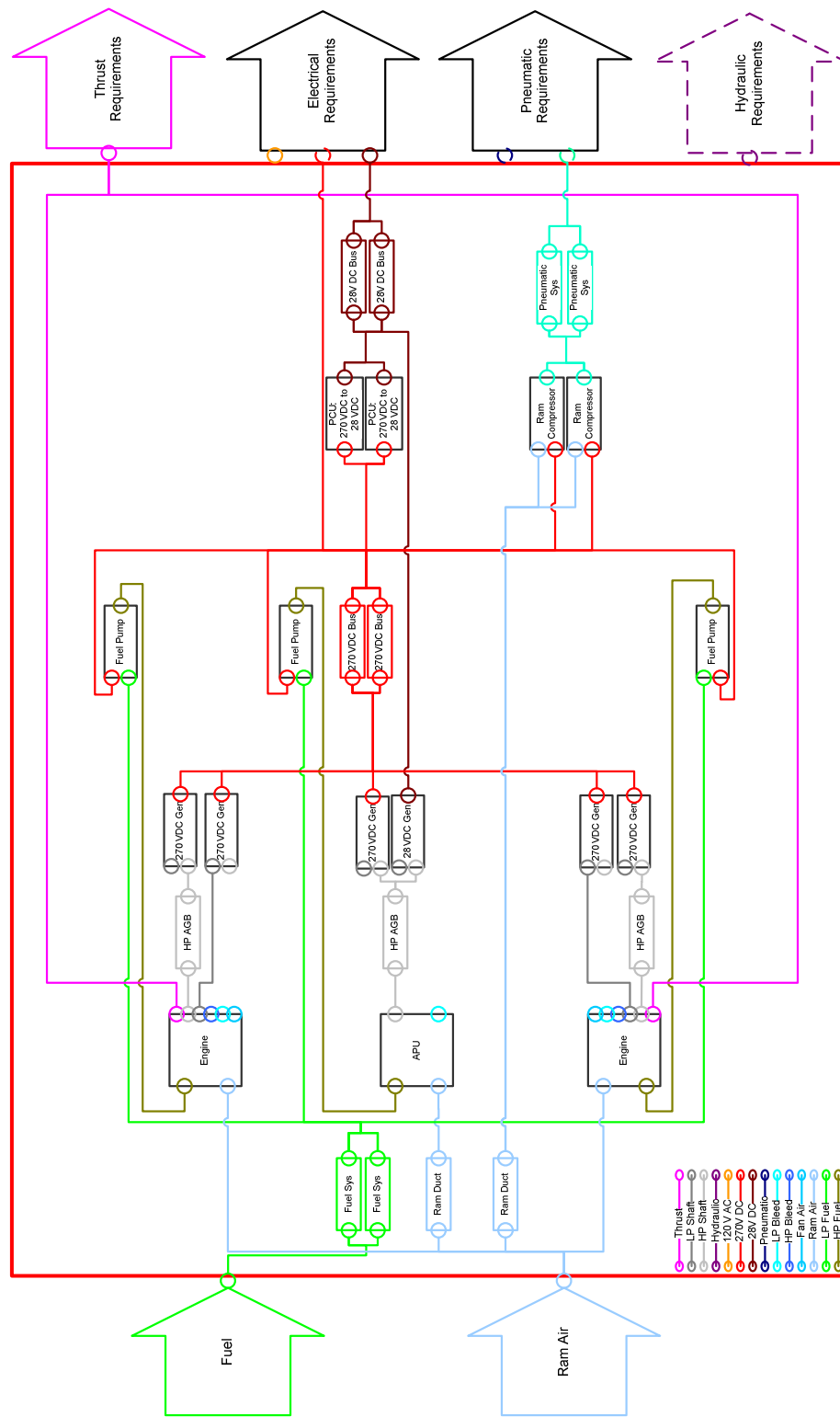


Figure 56: "All-Electric" Architecture Diagram

([A]) and unit capability transfer functions ($f(\{X\}, \{Op\})$). The transfer functions for these two concept architectures are discussed in the following section and the adjacency matrices for these concept architectures are given in appendix F.

Each architecture exhibits a unique set of design variables ($\alpha_{i,j}$) which assign capabilities during failure conditions. These represent the flow of functionality through every point in the architecture in which a single functional source provides for multiple downstream requirements. The number of decision points and potential functional capability flows throughout the architecture depends on its structure and composition.

The conventional architecture has 47 allocation variables as listed in table 24. The ‘more-electric’ architecture has 52 allocation variables as listed in table 25. Load shedding optimization is performed by identifying ideal combinations of these allocation variables. The proportional values of these variables determines how functionality flows throughout the systems.

6.5 *Function/Hazard Relationships*

The function/hazard relationships are the mechanism by which operational considerations impose performance requirements on units within a system. Misrepresentation of the function/hazard relationship leads to inappropriate allocation of failure. This biases architecture evaluation by imposing false requirements.

To show the benefits of higher fidelity function/hazard relationships informing load shedding, continuous functional hazard assessment is performed with three levels of detail. These three resulting function/hazard relationships for both the conventional and ‘more-electric’ architecture are depicted in table 26. Continuous system reliability is then evaluated by optimizing the load shedding strategies for each of these hazard objective functions. While the higher fidelity function/hazard relationships

Table 24: Conventional Architecture Allocation Variables

Source	Load	Source	Load
Ram Duct	$\alpha_{1,1}$: Ram HX $\alpha_{1,2}$: APU	R Eng AGB	$\alpha_{2,1}$: R HS 120V AC Gen $\alpha_{2,2}$: R HS 28V DC Gen $\alpha_{2,3}$: R Hydraulic Pump $\alpha_{2,4}$: R Fuel Pump
L Eng AGB	$\alpha_{3,1}$: L HS 120V AC Gen $\alpha_{3,2}$: L HS 28V DC Gen $\alpha_{3,3}$: L Hydraulic Pump $\alpha_{3,4}$: L Fuel Pump	APU AGB	$\alpha_{4,1}$: APU HS 28V DC Gen $\alpha_{4,2}$: APU Fuel Pump
Fuel Sys 1	$\alpha_{5,1}$: R Engine Fuel Pump $\alpha_{5,2}$: L Engine Fuel Pump $\alpha_{5,3}$: APU Fuel Pump	Fuel Sys 2	$\alpha_{5,1}$: R Engine Fuel Pump $\alpha_{5,2}$: L Engine Fuel Pump $\alpha_{5,3}$: APU Fuel Pump
R Eng HS 28V DC Gen	$\alpha_{7,1}$: 28V DC Bus 1 $\alpha_{7,2}$: 28V DC Bus 2	L Eng HS 28V DC Gen	$\alpha_{8,1}$: 28V DC Bus 1 $\alpha_{8,2}$: 28V DC Bus 2
APU HS 28V DC Gen	$\alpha_{9,1}$: 28V DC Bus 1 $\alpha_{9,2}$: 28V DC Bus 2	R Hyd Pump	$\alpha_{10,1}$: Hyd Sys 1 $\alpha_{10,2}$: Hyd Sys 2
L Hyd Pump	$\alpha_{11,1}$: Hyd Sys 1 $\alpha_{11,2}$: Hyd Sys 2	R Precooler	$\alpha_{12,1}$: Pn Sys 1 $\alpha_{12,2}$: Pn Sys 2
L Precooler	$\alpha_{13,1}$: Pn Sys 1 $\alpha_{13,2}$: Pn Sys 2	Ram HX	$\alpha_{14,1}$: Pn Sys 1 $\alpha_{14,2}$: Pn Sys 2
L Engine	$\alpha_{15,1}$: Thrust $\alpha_{15,2}$: Fan Bleed $\alpha_{15,3}$: HP Bleed $\alpha_{15,4}$: LP Bleed $\alpha_{15,5}$: LS Shaft Power	R Engine	$\alpha_{16,1}$: Thrust $\alpha_{16,2}$: Fan Bleed $\alpha_{16,3}$: HP Bleed $\alpha_{16,4}$: LP Bleed $\alpha_{16,5}$: LS Shaft Power
APU	$\alpha_{17,1}$: Thrust $\alpha_{17,2}$: HS Shaft Power $\alpha_{17,3}$: LS Shaft Power		

Table 25: 'All-Electric' Architecture Allocation Variables

Source	Load	Source	Load
270V DC Bus 1	$\alpha_{1,1}$: Aircraft 270V DC Loads $\alpha_{1,2}$: 270 to 28V DC Trans 1 $\alpha_{1,3}$: 270 to 28V DC Trans 2 $\alpha_{1,4}$: Ram Comp 1 $\alpha_{1,5}$: Ram Comp 2 $\alpha_{1,6}$: L Engine EMP $\alpha_{1,7}$: R Engine EMP $\alpha_{1,8}$: APU EMP	270V DC Bus 2	$\alpha_{2,1}$: Aircraft 270V DC Loads $\alpha_{2,2}$: 270 to 28V DC Trans 1 $\alpha_{2,3}$: 270 to 28V DC Trans 2 $\alpha_{2,4}$: Ram Comp 1 $\alpha_{2,5}$: Ram Comp 2 $\alpha_{2,6}$: L Engine EMP $\alpha_{2,7}$: R Engine EMP $\alpha_{2,8}$: APU EMP
Ram Duct	$\alpha_{3,1}$: Ram Comp 1 $\alpha_{3,2}$: Ram Comp 2	APU AGB	$\alpha_{4,1}$: HS 270V DC Gen $\alpha_{4,2}$: HS 28V DC Gen
Fuel Sys 1	$\alpha_{5,1}$: L Engine EMP $\alpha_{5,2}$: R Engine EMP $\alpha_{5,3}$: APU EMP	Fuel Sys 2	$\alpha_{6,1}$: L Engine EMP $\alpha_{6,2}$: R Engine EMP $\alpha_{6,3}$: APU EMP
L Eng HS 270V DC Gen	$\alpha_{7,1}$: 270V DC Bus 1 $\alpha_{7,2}$: 270V DC Bus 2	R Eng HS 270V DC Gen	$\alpha_{8,1}$: 270V DC Bus 1 $\alpha_{8,2}$: 270V DC Bus 2
APU HS 28V DC Gen	$\alpha_{9,1}$: 270V DC Bus 1 $\alpha_{9,2}$: 270V DC Bus 2	L Eng LS 270V DC Gen	$\alpha_{10,1}$: 270V DC Bus 1 $\alpha_{10,2}$: 270V DC Bus 2
R Eng LS 270V DC Gen	$\alpha_{11,1}$: 270V DC Bus 1 $\alpha_{11,2}$: 270V DC Bus 2	APU HS 28V DC Gen	$\alpha_{12,1}$: 28V DC Bus 1 $\alpha_{12,2}$: 28V DC Bus 2
270 to 28V DC Trans	$\alpha_{13,1}$: 28V DC Bus 1 $\alpha_{13,2}$: 28V DC Bus 2	270 to 28V DC Trans	$\alpha_{14,1}$: 28V DC Bus 1 $\alpha_{14,2}$: 28V DC Bus 2
Ram Comp 1	$\alpha_{15,1}$: Pneumatic Distr. Sys 1 $\alpha_{15,2}$: Pneumatic Distr. Sys 2	Ram Comp 2	$\alpha_{16,1}$: Pneumatic Distr. Sys 1 $\alpha_{16,2}$: Pneumatic Distr. Sys 2
L Engine	$\alpha_{17,1}$: Thrust $\alpha_{17,1}$: HS Shaft Power $\alpha_{17,2}$: LS Shaft Power	R Engine	$\alpha_{17,1}$: Thrust $\alpha_{17,1}$: HS Shaft Power $\alpha_{17,2}$: LS Shaft Power

do not represent reality, they provide justification for the development of higher fidelity characterization of the consequences of loss. This process is repeated for both architecture concepts.

The functional hazard relationships displayed in table 26 are abstractions of the relationship between system level functionalities and the operational space of the architecture. Loss of capability has a direct impact on the occurrence of undesirable events.

All of these capability hazard relationships are defined so as to decrease monotonically with system capability. As the magnitude of a loss in capability increases the hazard will naturally increase in severity. Distinctions are not typically made regarding gradations of failures within a specific class (e.g.- How major is a major failure?). However, expressing these relationships continuously allows for the implementation of gradient based optimization in the identification of optimal failure allocation.

The first function/hazard relationship used mimics the level of fidelity provided by traditional FHA. FHA gives little information regarding the consequences of intermediate failure conditions. Assuming that no additional information is applied than that provided by traditional FHA, this form of the hazard function could be applied while considering optimal load shedding. No distinctions are made in terms of loss magnitude. Low levels of loss are equivalent in consequence to total losses in functionality. However, In order to use gradient based optimization methods a step function is not implemented. A continuous relationship between hazard and loss is applied which rises quickly and yields catastrophic failures for small functional losses. It is unrealistic that such an objective function would be used for load shedding optimization. These pseudo-step objective functions act as a baseline by mimicking the information available during traditional FHA.

The second function/hazard relationship applies a linear relationship between hazard and loss. The magnitude of the hazard associated with total loss of functionality

Table 26: Hazards for Conventional and 'All-Electric' Architecture Concepts

System Capability	Conventional Architecture	"All-Electric" Architecture
Potable Air		
HP Bleed		
120VAC		
28VDC		
270VDC		
Hydraulic		

as prescribed by FHA and is the same magnitude of hazard incurred with any failure using the first hazard function described. This loss function makes the assumption that the magnitude of the hazard is equivalent to the proportion of the loss incurred.

The third function/hazard relationship applies nonlinear relationships between hazard and function loss. These non-linear relationship reflect degraded performance available through the reduction of platform level capability (de-ice instead of anti-ice, reduced control responsiveness, etc.).

The conventional and ‘more-electric’ architecture concepts associate different operational hazards with the provision of different functionalities. While the conventional architecture fulfills system level functions by utilizing multiple power types (hydraulic, AC electric, high pressure bleed) the ‘more-electric’ concept places more emphasis on the 270VDC power. The hazard associated with the loss of each capability stems from its support of the system’s fundamental capabilities.

The nonlinearity of the function/hazard relationships for system capabilities is derived from these relationships. For the conventional architecture, each capability maps to the loss of a single system level function. However, the ‘more-electric’ architecture allocates multiple system level functions to the capability of providing 270VDC power.

6.5.1 Thrust Loss Hazards

The non-linear function/hazard relationships displayed in table 26 were defined anecdotally. It is therefore necessary to illustrate how physical analysis can and should be applied in defining the impact of capability loss. This is performed here for the function to propel. In order to capture the effect of a loss of thrust the functional loss must be mapped to the operational consequences. Hazards are then assigned according to the operational impact of the functional loss.

As discussed in the previous chapter, the fundamental consequence of a loss of

thrust on a commercial aircraft is the inability of reaching and landing at a suitable landing location. Furthermore, thrust requirements are also derived by the aircraft's ability to perform maneuvers to avoid additional undesirable consequences. The hazard associated with a loss in thrust is addressed in two separate analyses: mission analysis and takeoff performance analysis. At any point during the flight, a loss in thrust imposes undesirable limitation on aircraft range [85, 100, 240]. During takeoff, sufficient thrust must provide the ability to safely clear a 35 ft obstacle with one engine out or perform a safe abort given a limited takeoff distance [101, 97].

Mattingly's equation provides the relationship between propulsion requirements and aircraft attributes. Additionally, the engine model which will be discussed later in this chapter is also used to estimate fuel flow rate for mission analysis.

6.5.1.1 Takeoff

The hazard associated with loss of thrust at takeoff is determined in terms of the required take off field length (TOFL). This distance is determined by decomposing the takeoff in four segments: ground roll (s_g), rotation (s_R), transition (s_{TR}), and climb (s_{CL}). Ground roll distance (s_g) is the displacement required to accelerate the aircraft from rest to the safety speed (V_{safety}). Rotation distance (s_R) is the distance required to increase the aircraft angle of attack for takeoff. Transition distance (s_{TR}) is the horizontal distance the aircraft travels while changing the flight path angle to the climb angle. Finally, climb distance (s_{CL}) is the horizontal distance the aircraft travels while climbing to an altitude equal to the obstacle height (h_{obs}).

These segments are characterized by two velocities (V_{fail} and V_{safety}). V_{fail} is the velocity at which the failure occurs and V_{safety} is the velocity at which the takeoff can be safely achieved with one engine operational. In the event that a loss of thrust occurs before the decision speed (V_{dec}), the balanced field length (BFL) is calculated in terms of the velocity at which the failure occurs (V_{fail}) and the distance required

to stop once the failure occurs (s_{BR}). If V_{fail} is greater than V_{dec} , the pilot must continue with the takeoff.

The total required take off distance is illustrated in figure 57.

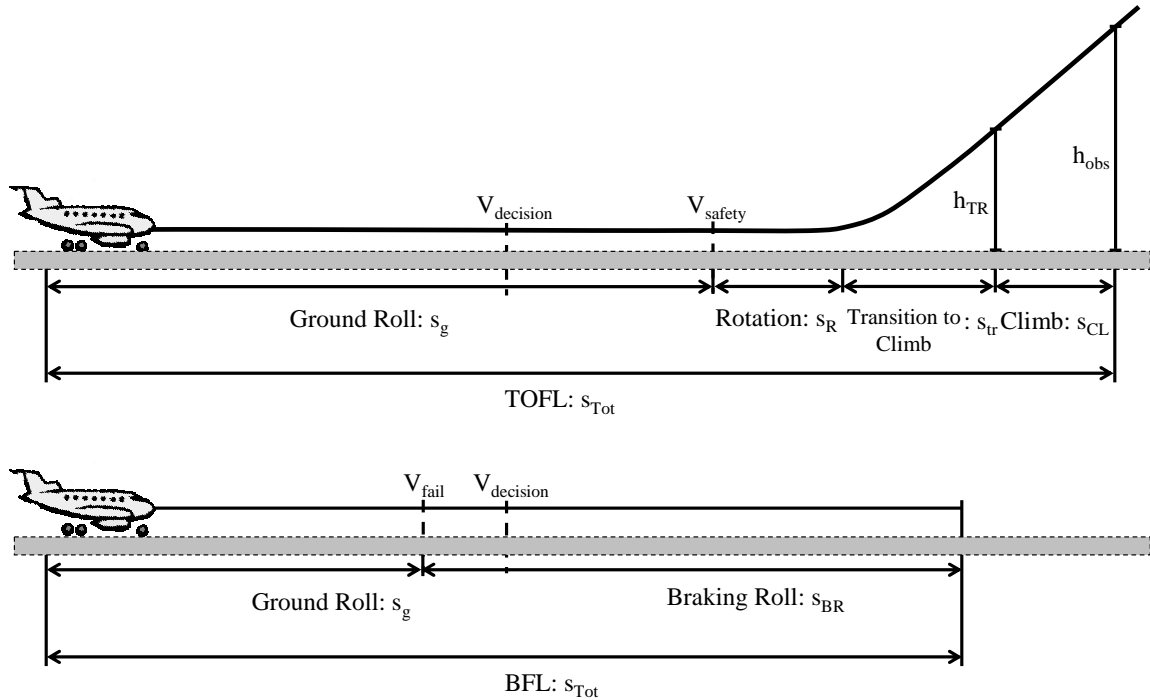


Figure 57: Takeoff Field Length and Balanced Field Length Compositions

The total displacement required is the maximum of the takeoff field length and balanced field length. This is calculated by equation 24.

$$s_{Tot} = \max \begin{bmatrix} TOFL \\ BFL \end{bmatrix} = \begin{bmatrix} s_g + s_R + s_{TR} + s_{CL} \\ s_{V_{fail}} + s_{BR} \end{bmatrix} \quad (24)$$

This formulation makes several assumptions. The first assumption is that the thrust loss failure occurs instantaneously and $V_{failure}$. The second assumption is that any failure occurring before the decision speed yields a total takeoff distance equal to the BFL.

Calculating each of these displacement values implements a form of Mattingly's

thrust equation given in equation 1.

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

This equation can be reduced to equation 25 by eliminating dh/dt from the excess power term (P_s) and lumping all drag and rolling resistance parameters ($\zeta_{TO} = C_D + C_{DR} - \mu_{TO}C_L$).

$$\frac{T}{W} = \zeta_{TO} \frac{qS}{W} + \mu_{TO} + \frac{1}{g} \frac{dV}{dt} \quad (25)$$

Recognizing that $dt = V/ds$ and rearranging this relationship overall displacement can be calculated.

$$\int_{s_0}^{s_1} ds = \int_{V_0}^{V_1} \frac{\frac{1}{g} V}{\frac{T}{W} - \frac{\zeta_{TO} qS}{W} - \mu_{TO}} dV \quad (26)$$

Substituting the definition of dynamic pressure ($q = \frac{1}{2}\rho V^2$) and replacing $u = \frac{T}{W} - \frac{\zeta_{TO} qS}{W} - \mu_{TO}$, equation 26 reduces to equations 27.

$$\Delta s = -\frac{W/S}{g\rho\zeta_{TO}} \int_{V_0}^{V_1} \frac{du}{u} \quad (27)$$

The final form of this displacement equation is achieved by integration.

$$\Delta s = -\frac{W/S}{g\rho\zeta_{TO}} \left[\ln \left(\frac{T}{W} - \zeta_{TO} \frac{\frac{1}{2}\rho V_1^2 S}{W} - \mu_{TO} \right) - \ln \left(\frac{T}{W} - \zeta_{TO} \frac{\frac{1}{2}\rho V_0^2 S}{W} - \mu_{TO} \right) \right] \quad (28)$$

Substituting equation 28 into equation the TOFL expression in equation 24 and assuming that, the total ground roll distance (s_g) becomes:

$$s_g = -\frac{W/S}{g\rho\zeta_{TO}} \left[\ln \left(\frac{T_0}{W} - \zeta_{TO} \frac{\frac{1}{2}\rho V_1^2 S}{W} - \mu_{TO} \right) - \ln \left(\frac{T_0}{W} - \mu_{TO} \right) \right] - \frac{W/S}{g\rho\zeta_{TO}} \left[\ln \left(\frac{T_F}{W} - \zeta_{TO} \frac{\frac{1}{2}\rho V_S^2 S}{W} - \mu_{TO} \right) - \ln \left(\frac{T_F}{W} - \zeta_{TO} \frac{\frac{1}{2}\rho V_F^2 S}{W} - \mu_{TO} \right) \right]$$

Combining the logarithm terms yields equation 29 as the final expression for take off ground roll where $q_F = \frac{1}{2}\rho V_{failure}^2$, $q_S = \frac{1}{2}\rho V_{safety}^2$, T_0 is the initial thrust available, and T_F is the reduced thrust capability incurred at velocity $V_{failure}$.

$$s_g = - \left(\frac{W/S}{g\rho\zeta_{TO}} \right) \ln \left[\left(\frac{T_0 - W\mu_{TO} - \zeta q_F S}{T_0 - W\mu_{TO}} \right) \left(\frac{T_F - W\mu_{TO} - \zeta q_S S}{T_F - W\mu_{TO} - \zeta q_F S} \right) \right] \quad (29)$$

It is assumed that rotation and transition each take approximately 3 seconds and obstacle clearance distance is given by equation 30. Therefore, the total distance needed for takeoff given a given a loss of the loss of thrust $T_0 - T_F$ is given by equation 31.

$$s_{CL} = \frac{h_{obs}}{\frac{T_F}{W} - \frac{q_S C_D}{W/S}} \quad (30)$$

$$TOFL = -\frac{W/S}{g\rho\zeta_{TO}} \ln \left[\frac{T_0 - W\mu_{TO} - \zeta q_F S}{T_0 - W\mu_{TO}} \frac{T_F - W\mu_{TO} - \zeta q_S S}{T_F - W\mu_{TO} - \zeta q_F S} \right] + 6V_{safety} + \frac{h_{obs}W}{T_F - q_S C_D S} \quad (31)$$

The Balanced Field Length (BFL) is calculated similarly and is used to determine the decision speed. For a braking roll Mattingly's equation is reduced to equation 32 by assuming zero reverse thrust and lumping all drag and resistance parameters ($\zeta_{BR} = C_D + C_{DR} + \mu_{BR}C_L$).

$$0 = \zeta_{TO} \frac{qS}{\beta W_{TO}} - \mu_{BR} + \frac{1}{g} \frac{dV}{dt} \quad (32)$$

After substitution for dt, integration, and simplification similar to the derivation of TOFL, the balanced field length is given by equation 33.

$$BFL = -\frac{W/S}{g\rho\zeta_{TO}} \ln \left[\frac{T_0 - W\mu_{TO} - \zeta q_F S}{T_0 - W\mu_{TO}} \right] + \frac{W/S}{g\rho\zeta_{BR}} \ln \left[\frac{W\mu_{TO} - \zeta q_F S}{W\mu_{TO}} \right] \quad (33)$$

Assuming a known maximum allowable BFL, numerically solving this equation for q_F yields an expression for the decision speed: the maximum speed at which at which the takeoff can safely be aborted. Failures prior to the decision speed can be operationally mitigated through abort. However, failures after this point may result in TOFL overruns. The reason the decision speed was chosen as the critical failure point is also due to the fact that partial thrust losses are less stringent the nearer the aircraft velocity is to the safety speed. In order to assess the maximum operational consequence of the loss of thrust during takeoff it is assumed that the failure occurs directly after the decision speed.

Figure 58 gives the expected takeoff field length considering the decision speed calculated from equations 33 and the TOFL determined with 31. This was calculated for the aircraft described in the previous section with flaps at 15°.

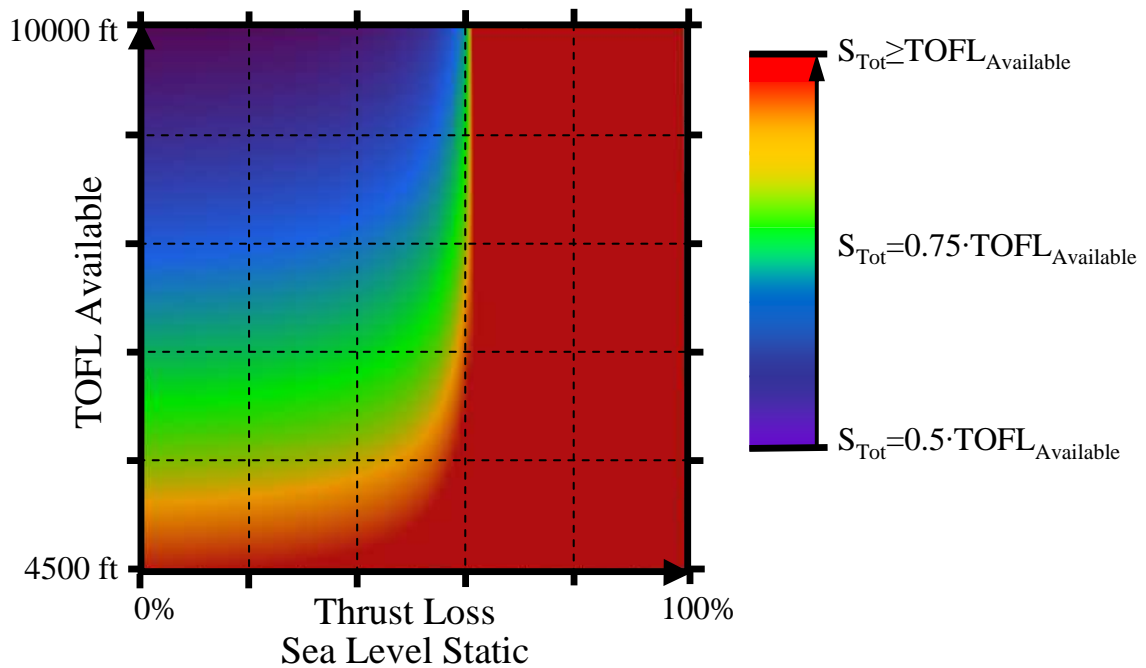


Figure 58: Take Off Field Length for Business Jet with Variation in Thrust Available

This graph reflects the the necessity to design the aircraft with adequate capability to takeoff with one engine out. More specifically, this analysis shows that for any TOFL available a 60% loss in thrust yields fieldlength overruns. With this knowledge

in hand, the criticality of the function to produce thrust can be recast in terms of the expected TOFL required. This analysis links the functional loss to its actual operational impact, which is an inability to perform the take-off within the available distance. This hazard is described as a function of the amount of field length overhead which is available during the failure case ($\Delta s = TOFL_{available} - s_{Tot}$). This hazard relationship calculated using equation 24 is depicted in figure 59.

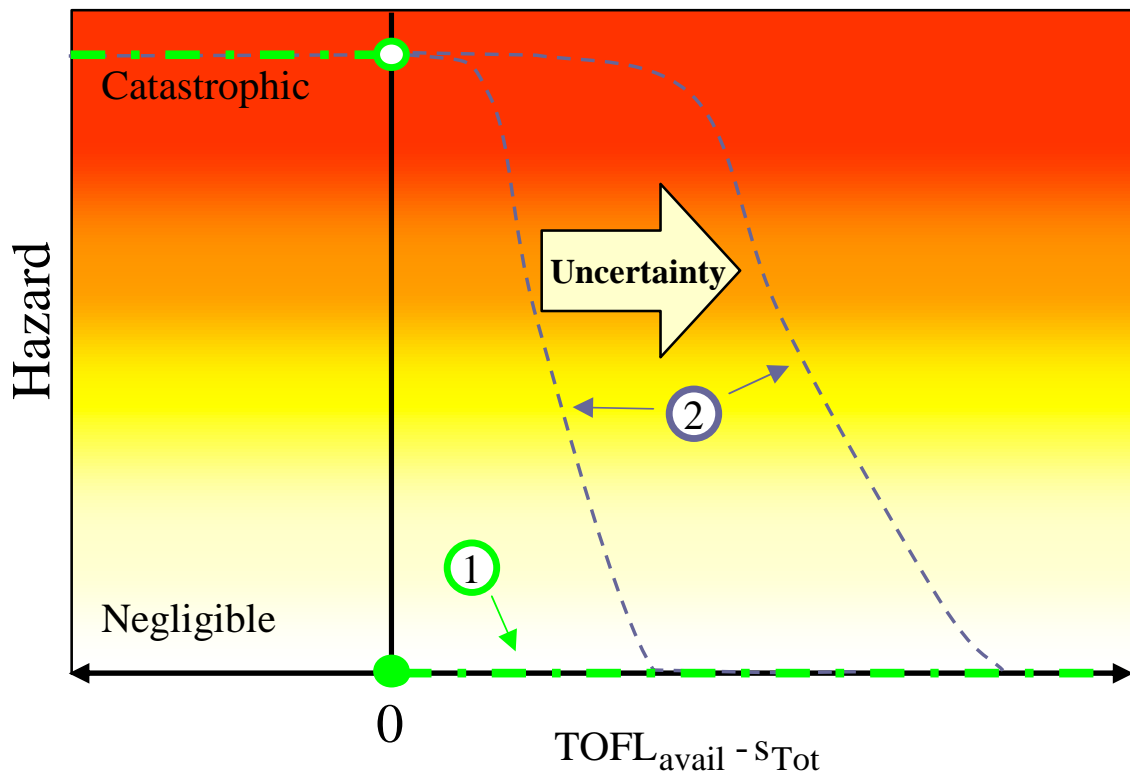


Figure 59: Hazard Associated with the Required TOFL for a Business Jet During Thrust Loss Conditions

The hazard associated with an runway overruns is discrete. It can be directly asserted that negative Δs values will yield catastrophic hazards. Additionally, very large positive values of Δs assign no hazard in performing the takeoff operation. Assuming that the analysis performed to determine the required TOFL directly captures reality, and that the pilot has the ability to perform optimally during engine failure conditions, the transition between zero hazard and catastrophic hazard would be a step function (function 1 in figure 59). However, hazard characterizations are

essentially probability constraints. The relationship between required TOFL and available TOFL must account for the probability that a consequence will occur given the expected performance available.

Overhead introduced between known operational consequences essentially acts as a safety factor in allocation of requirements. The shape of this transition region is affected by multiple sources of uncertainty. The first source of uncertainty is the analysis itself. Variations in the aircraft attributes and the level of fidelity in which the functional performance analysis was performed may prompt the inclusion of safety factors in the formulation of this hazard relationship. Each assumption made in this analysis can introduce variability in the definition of required TOFL which must be reflected in the definition of this transition region (functions labeled 2 in figure 59).

The probability that external factors will aid in the occurrence of hazards must also be included in the definition of this transition region. This can be defined heuristically or anecdotally depending on the level of confidence the requirements engineer has in the analysis performed. Further studies may be performed to describe this transition region in greater fidelity (e.g. human factors analysis or uncertainty analysis).

6.5.1.2 *Cruise*

Much like the takeoff hazard analysis, loss of thrust during the cruise segment must be linked to is operational effect. The operational effect of a loss in thrust is a reduction in the ability to maintain desirable flight conditions. This leads to reductions in the effective range of the aircraft. Therefore, the hazard associated with thrust loss during cruise must be described in terms of the range available during thrust loss (R) and the range required (R_{req}). The range required is determined by considering the design range, the portion of the mission already completed, and the distance to alternate runways. The range available is determined by identifying the optimal failure response in terms of flight path which maximizes range.

The value which is used to characterize the operational impact of thrust loss is $\frac{R_{req}}{R}$. If this value is larger than 1, the thrust loss scenario causes the aircraft to lose the ability to reach a suitable landing site. For values less than 1, analysis shows that the required range is available. However, depending on the level of confidence in the analysis results, values of $\frac{R_{req}}{R}$ close to 1 may be characterized as incurring hazards also.

Aircraft range is given by equation 34.

$$R = \int_0^{t_{final}} V(t) \cos(\theta(t)) dt \cong \sum_{i=1}^{t_{final}/\Delta t} V_i * \cos(\theta(t_i)) \Delta t \quad (34)$$

Determining the maximum range available (R) during thrust loss scenarios was determined by optimizing the flight path of the aircraft for failures of various magnitudes. These failures may occur at different points in the flight envelope and under varying customer load requirements. A design of experiments was used to characterize this thrust loss, range relationship. Space filling Latin hypercube and full factorial sample points were used to develop a neural network of the relationship in equation 35. The variable β in this expression represents the amount of fuel remaining in the aircraft $\left(\beta = \frac{W - W_{empty}}{W_{TO} - W_{empty}}\right)$.

$$R = f \left(\begin{array}{l} Alt, Mach, \beta \\ Engine1 [ThrustLoss, FuelCap, CustomerLoads] \\ Engine2 [ThrustLoss, FuelCap, CustomerLoads] \end{array} \right) \quad (35)$$

In order to determine the maximum range for each point in the DOE, the required velocity and climb angle ($\theta(t)$) needed to be identified throughout the mission. The definition of $\theta(t)$ and $V(t)$ are discussed. Relevant variables for this study are indicated in the free body diagram for this aircraft in figure 60.

The climb angle can vary continuously during the flight. Assuming small angle approximation for α is calculated by equation 36.

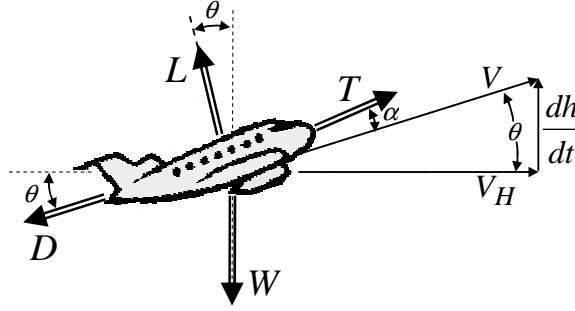


Figure 60: Business Jet Free Body Diagram for Climbing Flight

$$\theta(t) = \min \left\{ \begin{array}{ll} \frac{A}{(1 + e^{-B(t+C)})} & (a) \\ A \sin \left(\frac{T_{avail}}{W(t)} - \sqrt{4KCD_0} \right) & (b) \\ \max \left[0, A \tan \left(\frac{h_{max} - h(t)}{V(t) \Delta t} \right) \right] & (c) \end{array} \right\} \quad (36)$$

The first θ calculation (equations 36a) is varied by the optimization routine. Variables A , B , and C in this equation are the design variables accessed for range optimization. This equation is used to calculate the aircraft trajectory throughout the mission. A determines the vertical scaling, B determines the slope, and C determines the time offset of the inverse exponential (s-function).

The second θ equation (36b) calculates the maximum climb rate available given cruise velocity for optimal range. Derivation of this equation begins with the thrust equation 1. Substitution for lift and drag coefficients given equation 37.

$$T_{avail} \geq K \frac{W^2}{\frac{1}{2} \rho V^2 S} + \frac{1}{2} \rho V^2 S C_{D0} + W \sin(\theta) \quad (37)$$

Multiplying by V^4 and applying the quadratic formula yields equation 38.

$$0 \geq \frac{1}{2} \rho C_{D0} \frac{S}{W} V^4 + \left[\sin(\theta) - \frac{T_{avail}}{W} \right] V^2 + \frac{2K}{\rho} \frac{W}{S}$$

$$V^2 \leq \frac{\frac{T_{avail}}{W} - \sin(\theta) \pm \sqrt{\left[\frac{T_{avail}}{W} - \sin(\theta)\right]^2 - 4KC_{D0}}}{\rho C_{D0} \frac{S}{W}} \quad (38)$$

In order to obtain feasible solutions to V^2 , the value under the radical must be greater than zero. Solving for theta in the radicand yields equation 36b.

$$\theta = A \sin\left(\frac{T_{avail}}{W} - \sqrt{4KC_{D0}}\right)$$

The third equation (36c) calculates the limiting θ given the maximum allowable cruising altitude. If an external max operating altitude is imposed by the operating envelopes of other aircraft systems, the climb rate is limited so as to keep the altitude under this limit.

This velocity for maximum range is calculated by equation 39.

$$V(t)^2 = \frac{W(t)/S}{\rho(t)C_{D0}} \min \left\{ \begin{array}{l} \sin(\theta(t)) + \sqrt{\sin^2(\theta(t)) + 12KC_{D0}} \quad (a) \\ \left[\frac{T(t)}{W(t)} - \sin(\theta(t))\right] + \sqrt{\left[\frac{T(t)}{W(t)} - \sin(\theta(t))\right]^2 - 4KC_{D0}} \quad (b) \end{array} \right\} \quad (39)$$

The thrust limited aircraft velocity (equation 39b) is determined with equation 38.

Derivation of equation 39a (velocity for maximum range) begins with the equation for time rate of change in aircraft weight, as seen in equation 40. This change in weight is directly proportional to the thrust specific fuel consumption (T_{SFC}).

$$\frac{dW}{dt} = -T_{SFC}(t) T(t) \quad (40)$$

Assuming a steady rate of climb (load factor, $n=1$) and substituting the drag coefficients ($D = \frac{1}{2}\rho(t)V(t)^2SC_D$), the drag polar ($C_D = KC_L^2 + C_{D0}$), and the lift coefficient ($C_L \cong \frac{W}{\frac{1}{2}\rho(t)V(t)^2S}$) this relationship is augmented as follows:

$$\begin{aligned}
\frac{dW}{dt} &= -T_{SFC} [D + W \sin(\theta)] \\
&= -T_{SFC} \left[\frac{1}{2} \rho V^2 S C_D + W \sin(\theta) \right] \\
&= -T_{SFC} \left[\frac{1}{2} \rho V^2 S (K C_L^2 + C_{D0}) + W(t) \sin(\theta(t)) \right] \\
&= -T_{SFC} \left\{ \frac{1}{2} \rho V^2 S \left[K \left(\frac{W}{\frac{1}{2} \rho V^2 S} \right)^2 + C_{D0} \right] + W \sin(\theta) \right\}
\end{aligned}$$

Recognizing that $\frac{ds}{dt} = V \cos(\theta)$, the change in aircraft weight per displacement is given by equation 41.

$$\frac{dW}{ds} = \left[\frac{-T_{SFC} K W^2}{\frac{1}{2} \rho S \cos(\theta)} \right] V^{-3} + \left[\frac{-T_{SFC} W \sin(\theta)}{\cos(\theta)} \right] V^{-1} + \left[\frac{-T_{SFC} \frac{1}{2} \rho S C_{D0}}{\cos(\theta)} \right] V \quad (41)$$

The velocity in which maximum range is achieved is determined by evaluating $\frac{d\left(\frac{dW}{ds}\right)}{dV} = 0$. Simplification of this expression is given in equation 42.

$$0 = \left[\frac{1}{2} \rho C_{D0} \right] V^4 - \left[\frac{W}{S} \sin(\theta) \right] V^2 - 3 \left[\frac{2K}{\rho} \left(\frac{W}{S} \right)^2 \right] \quad (42)$$

Application of the quadratic formula yields equation 43.

$$V^2 = \frac{\left[\frac{W}{S} \sin(\theta) \right] \pm \sqrt{\left(\left[\frac{W}{S} \sin(\theta) \right]^2 + 4 \left(\left[\frac{1}{2} \rho C_{D0} \right] \right) \left(3 \left[\frac{2K}{\rho} \left(\frac{W}{S} \right)^2 \right] \right) \right.}}{2 \left(\left[\frac{1}{2} \rho C_{D0} \right] \right)} \quad (43)$$

This can be simplified to equation 39a.

$$[V(t)]^2 = \frac{W(t)/S}{\rho(t) C_{D0}} \left[\sin(\theta(t)) + \sqrt{\sin^2(\theta(t)) + 12K C_{D0}} \right]$$

With these equations in hand, maximum range was identified for all DOE points. These results are displayed in figure 61 for an initial flight altitude of 35 kft, nominal customer loads, and a maximum operating altitude of 50 kft.

This figure displays available range (R) in terms of the remaining fuel $\left(\beta = \frac{W - W_{empty}}{W_{TO} - W_{empty}} \right)$ and % thrust loss. As expected, the remaining range available decreases with less fuel burn available. Additionally, large losses in thrust also reduce the remaining range.

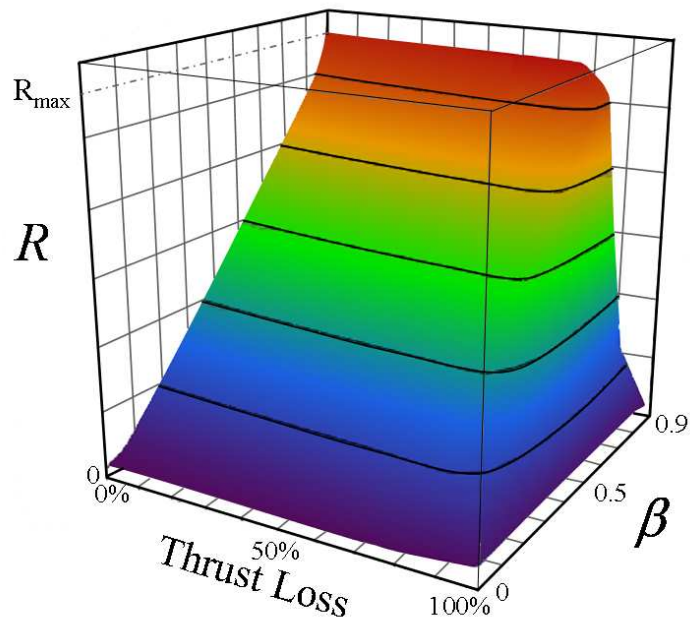


Figure 61: Aircraft Range with Variations in Thrust Loss and Fuel Consumed ($alt = 35kft, alt_{max} = 50kft$)

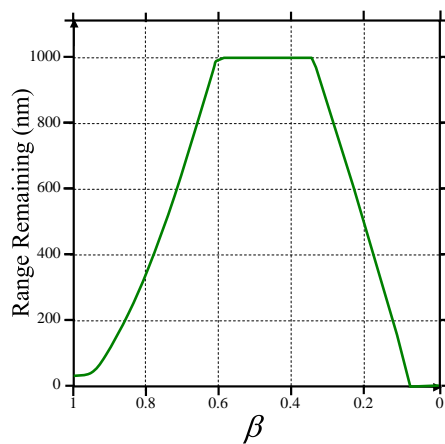


Figure 62: Range to Landing Field with Variations in Fuel Spent

The required range also changes throughout the mission. The distance to a suitable landing field is illustrated in figure 62. While the US Federal Aviation Administration provides does not require ETOPs certification of private jets, the Joint Aviation Authority. The JAA has qualified private jets to ETOPS requirements of 120 to 180 minutes [240]. Under these certification requirements, a private business jet must be able to reach an alternate landing site within the specified time. As such, the divert distance used for this study as assumed to be 1000 nm. Assuming this divert distance remains at a maximum throughout the duration of the mission, the distance to a landing field length increases as the aircraft moves away from the departure field and decreases as the aircraft approaches the destination field. The maximum remaining range is given by the divert distance.

With range available and range required varying throughout the mission, thrust loss criticality subsequently varies with β . Figures 63a and b illustrate the ability to fulfill range requirements in terms of functional losses and remaining fuel. Figure 63a shows range limitations in terms of thrust loss percent and figure 63b shows range limitations in terms of percent fuel capability loss. For practically all values of β , large thrust losses result catastrophic failures. For both functional losses, the most stringent criticality requirements occur at β values of $\frac{1}{3}$.

The magnitude of the thrust hazard is determined by its impact on the loss of available range. It can be safely assumed that values of $\frac{R_{req}}{R}$ greater than 1 yield catastrophic hazards. In this scenario, the minimal required range is greater than the range attainable under the failure state. Values of $\frac{R_{req}}{R}$ much less than 1 yield no failures. Similar to the assignment of *TOFL* hazards, the transition region must be defined.

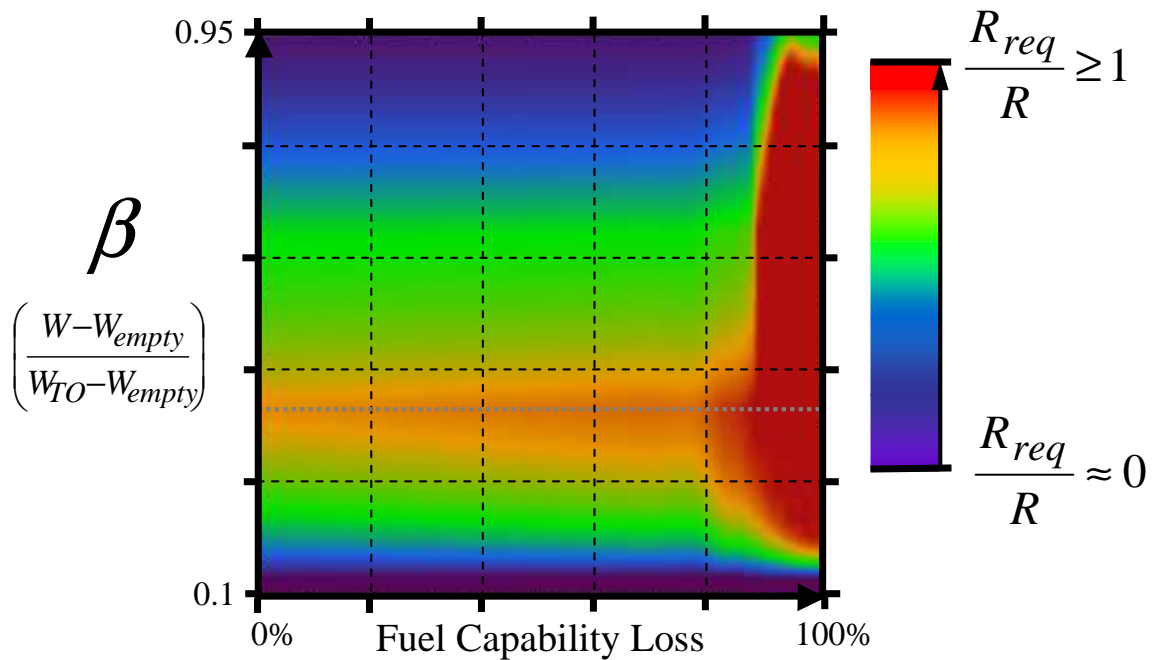
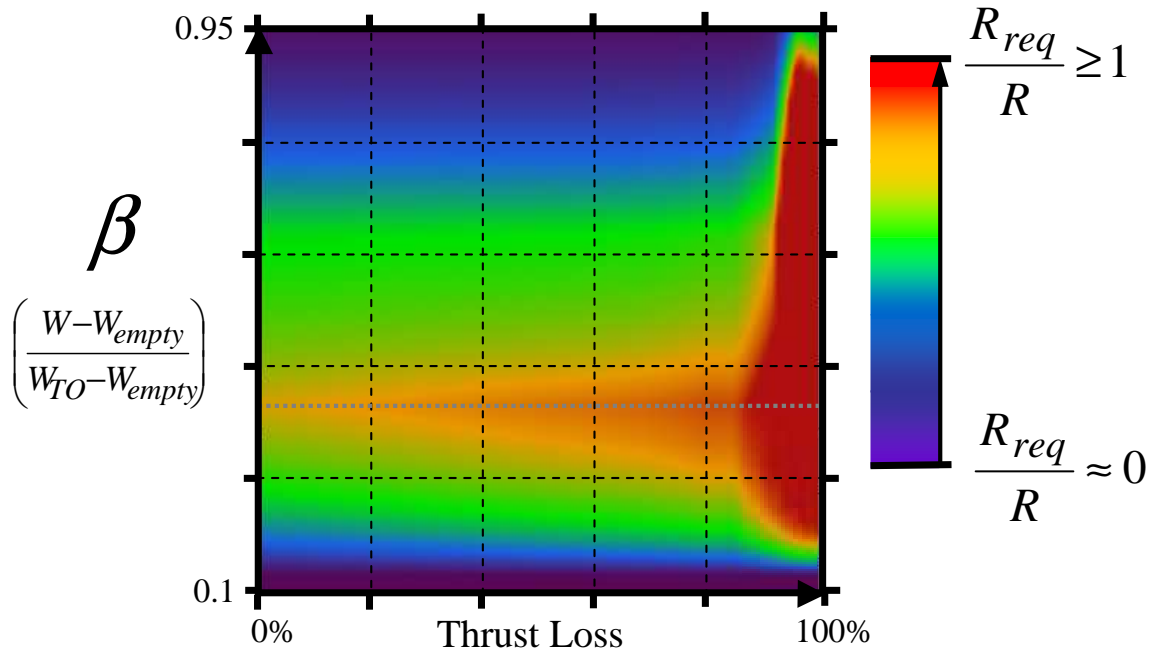


Figure 63: Range limitations due to Functional Failures

6.6 System Models

In order to model the concept architecture, transfer functions were developed which determine the available capability of a unit given the environment in which the unit is operating and the functional capabilities made available to that unit by other units in the system. In order to represent these architectures 25 transfer functions were defined with various degrees of fidelity. The unit transfer functions used for each concept architecture are outlined in table 27. The columns labeled conventional and 'more-electric' in this table indicate the number of these units present in each architecture.

Table 27: Unit Models (Capability Transfer Functions)

Unit Type	Unit	Conventional	More-Electric
Electric	120V AC Distribution	1	
	28V DC Distribution	2	2
	270V DC Distribution		2
	270 to 28V DC Transformer		2
	HS 120V AC Generator	2	
	HS 270V DC Generator		3
	HS 28V DC Generator	3	1
	LS 270V DC Generator		1
Hydraulic	Hydraulic Distribution	2	
	Hydraulic Pump	2	
Pneumatic	Pneumatic Dist	2	2
	Ram Heat Exchanger	1	
	PreCooler	2	
	Ram Duct	1	2
	Ram Compressor		2
Power Plant	AGB	3	3
	HP Bleed System	2	
	LP Bleed System	2	
	Fan Duct	2	
	Turbofan Engine	2	2
	APU		1
Fuel	Fuel System	2	2
	Fuel Pump	3	
	EMP		3

The fidelity of the transfer functions for each of the units within the architecture depends on the amount of knowledge available during architecture trades. As discussed in chapter three, surrogate models of system elements provide sufficient fidelity during conceptual trades. The following sections discuss the models developed for these load shedding optimization studies.

6.6.1 Electrical

The focus of this study focuses on providing adequate steady state capability. Therefore, it is assumed that each electrical component will be configured in a manner which provides meets transient performance constraints (e.g. MIL-STD-704). The capability equations for electrical systems components take one of two forms: distribution element or transformation element. Distribution units convey functional capability between multiple physical locations. Transformation units convert functional capability from one form to another. While device controllers can be managed as independent functional elements. However, for the purposes of this study it is assumed that a transformation units include both transform and control elements.

6.6.1.1 Distribution Elements: Electric Buses

The capability provided by the distribution element (Cap_{out}) is determined in terms of capability of the electrical sources (Cap_{in}), the required distribution length (L), and the peak design capability (Cap_{des}). The output capability for each of the three electrical distribution element models is calculated by assuming a constant efficiency (η_L) of 98% [69]. While this linear representation of bus efficiency is sufficient for the purposes of addressing the validity of the proposed hypothesis, additional merit may be achieved by higher fidelity representation of the electrical distribution system (capturing the effect of allowable fusing current, required shielding attributes, etc.). The relationships developed for these models are given in table 28.

Table 28: Electrical Distribution Capability Transfer Functions

Unit	Transfer Function
120V AC Dist:	
$AC120VCap_{out}$	$= AC120VBusCaps(AC120VCap_{in}, AC120VCap_{des}, L)$ $= \min \left[\begin{array}{l} AC120VCap_{des}, \\ \eta_L \cdot AC120VCap_{in} \end{array} \right]$
28V DC Dist:	
$DC28VCap_{out}$	$= DC28VBusCaps(DC28VCap_{in}, DC28VCap_{des}, L)$ $= \min \left[\begin{array}{l} DC28VCap_{des}, \\ \eta_L \cdot DC28VCap_{in} \end{array} \right]$
270V DC Dist:	
$DC270VCap_{out}$	$= DC270VBusCaps(DC270VCap_{in}, DC270VCap_{des}, L)$ $= \min \left[\begin{array}{l} DC270VCap_{des}, \\ \eta_L \cdot DC270VCap_{in} \end{array} \right]$

6.6.1.2 Transformation Elements: Generator, Power Converter

The structure of the transfer function for electrical transformation elements is similar to that developed for the distribution elements. However, unit capability is determined in terms of these two upstream functional capabilities available. The output capability of the DC to DC converter is calculated in terms of input electrical power and available cooling. Generator output capability is calculated in terms of the available shaft power and cooling. The shaft power functional relationship includes a vector of attributes characterizing the form of the function available. For this study the shaft power relationship is decomposed into a vector of two attributes: available horsepower and shaft speed ($ShaftPowerCap_{in} = [HPAvailable, ShaftSpeed]$). Relaying both of these variables downstream is valid assuming that generator torque loads do not significantly impact engine shaft speeds. This assumption holds for the ‘more-electric’ and conventional vehicle system architectures for typical business jet aircraft customer loads. Typical customer shaft horsepower extraction for these aircraft does not significantly impact engine shaft steady state operating speeds.

The transfer function for the electrical generator calculates the available electrical power in terms of expected shaft speed and load provided. The efficiency (η_G) of

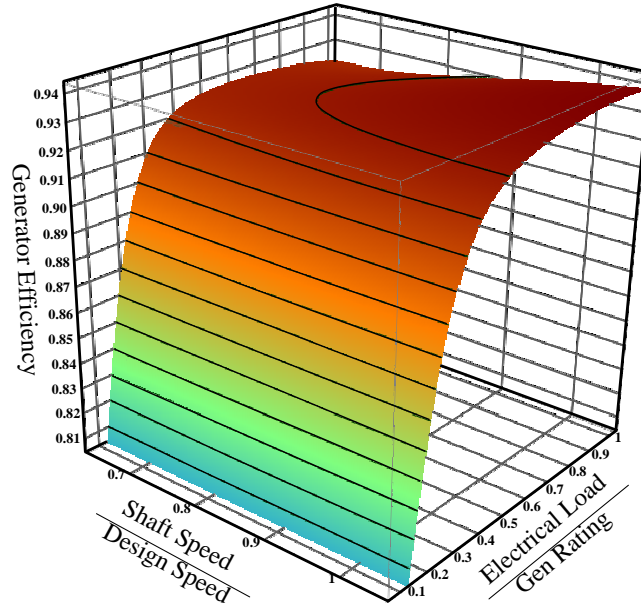


Figure 64: Generator Efficiency Relationship

a 270V DC, Mosfet rectified, six-phase, brushless generator is illustrated in figure 64. The effect of speed on efficiency is minor compared to the effect of electrical load. Generator efficiency drops dramatically with reductions in desired load, while variations of the peak Machine efficiency due to speed do not exceed $\pm 2\%$ for large variations in shaft speed. These trends are typical for efficiency calculations of electric Machines [45, 141].

The transfer functions for electrical transformation elements are outlined in table 29. The available capability from these electrical units can be limited by three values. The first limit is imposed by the max unit design capability. The second limit is imposed by the supply of the primary source of upstream power. For a generator, the output is limited by available input shaft speed. For a power converter, the output is limited by the upstream power available. The third limitation stems from a reduction in cooling capability. With a reduction in cooling capability, the level of sustainable steady state load is limited. These considerations are reflected in the transfer functions in table 29.

Table 29: Electrical Transformation Capability Transfer Functions

Unit	Transfer Function
DC-DC Converter:	
$DC28VCap_{out}$	$= DCtoDCCaps(DC270VCap_{in}, CoolingCap_{in}, DC28VCap_{des})$ $= \min \left[\begin{array}{l} DC28VCap_{des}, \\ \eta_{Gen} \cdot AC120VCap_{in}, \\ \left(\frac{\eta_{Gen}}{1 - \eta_{Gen}} \right) \cdot CoolingCap_{in} \end{array} \right]$
Generator:	
$ElecCap_{out}$	$= GenCaps(ShaftCap_{in}, CoolingCap_{in}, ElecCap_{des})$ $= \min \left[\begin{array}{l} ElecCap_{des}, \\ \eta_{Gen} \cdot ShaftCap_{in}, \\ \left(\frac{\eta_{Gen}}{1 - \eta_{Gen}} \right) \cdot CoolingCap_{in} \end{array} \right]$

6.6.2 Hydraulic

As discussed in the second chapter, hydraulic power has been considered the default means for power assisted actuation since the 1930's and 40's. The primary function the hydraulic system is to deliver pressurized hydraulic fluid flow to actuation systems. The traditional source for hydraulic power is the engine. Shaft power is delivered to the engine driven pumps (EDP) by way of the accessory gear box (AGB). Moir and Seabridge's rudimentary illustration of the hydraulic system is shown in figure 65.

While multiple elements are involved in the compilation of the hydraulic system (reservoirs, filters, accumulators, etc), the composition adopted for this study is outlined in figure 65. The capability of the hydraulic system is determined by two transfer functions. The hydraulic distribution system (outlined in red) delivers hydraulic fluid to the actuators and the pump (outlined in blue) provides pressure and flow to the distribution system. These transfer functions are given in table 30.

Modeling of this hydraulic distribution system assumes delivery of hydraulic fluid at 3000 psi with allowable pressure losses (20-25%). Under this assumption this distribution unit becomes a functional pass through. The amount of flow provided from the pump is equal to the flow available at the actuators. Additional fidelity

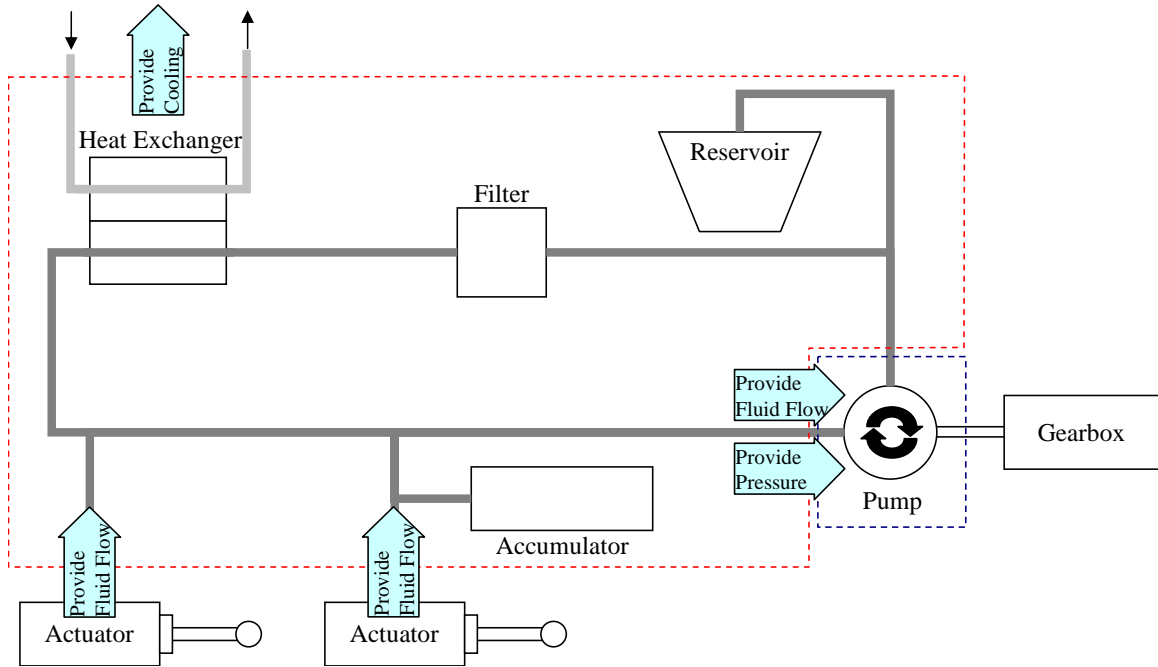


Figure 65: Rudimentary Hydraulic System [211]

Table 30: Hydraulic Capability Transfer Functions

Unit	Transfer Function
Hydraulic Dist:	
	$HydCap_{out} = HydSysCaps(HydCap_{in}, CoolingCap_{in}, HydCap_{des})$ $= \min \left[\begin{array}{c} HydCap_{des}, \\ HydCap_{in}, \\ k \cdot CoolingCap_{in} \end{array} \right]$
EDP:	
	$HydCap_{out} = EDPCaps(ShaftCap_{in}, HydCap_{des})$ $= \min \left[\begin{array}{c} HydCap_{des}, \\ \frac{ShaftCap_{in}}{\eta_p (P_{High} - P_{Return})} \end{array} \right]$

to the functional model could be included which calculates the expected pressure loss and the functional effects of loss of cooling capability. However, for illustrative purposes, the functional representation of the system here is adequate. The hydraulic system capability is limited by the system attributes ($HydCap_{des}$), the input flow ($HydCap_{in}$), and limitation due to lack of cooling ($k \cdot CoolingCap_{in}$).

Constant pressure, variable flow pumps convert shaft power to fluid flow at a constant pressure. Following Bernoulli's equations, pump power is given by equation 44. The fluid volumetric flowrate is given by Q , the difference between the high and return pressure is given by ΔP , and the hydraulic efficiency is given by η_p .

$$Power = \frac{\Delta P Q}{\eta_p} \quad (44)$$

Assuming a fixed operating pressure and return pressure the flow, Q , is calculated with the relationship given in table 30. For this study a fixed pump efficiency (η_p) was assumed. This is sufficient in addressing the hypotheses. However, higher fidelity is available by defining this efficiency in terms of a pump curve efficiency map.

6.6.3 Pneumatic

The conventional aircraft utilizes customer bleed air to fulfill multiple functionalities on an aircraft. Pneumatic air must be characterized by flow, pressure, and temperature. This high temperature and pressure air is used to provide ice protection to the nacelle and wing surface. First order approximations of unit performance were used for this study. The unit capability transfer functions employed for this analysis are outlined in table 31.

Bleed air is further conditioned to maintain cabin pressurization, regulate cabin temperature, and provide necessary airflow. The temperature of this bleed air is maintained around $175^\circ C$ through heat exchange with air bled from the engine fan [48]. The "more-electric" vehicle systems remove customer bleed requirements by

compressing ram air for cabin environmental control and replacing pneumatic ice protection with electrical heating.

Table 31: Pneumatic Capability Transfer Functions

Unit	Transfer Function
Pneum Air Dist:	
PnC_{out}	$= PnDuctCaps(PnC_{in}, PnC_{des}, L)$
$PnC_{out} (1)$	$= \dot{m} = \min \left[\begin{array}{c} PnC_{des}, \\ PnC_{in} \end{array} \right]$
$PnC_{out} (2)$	$= P_{out} = P_{Tin} - f_r \frac{Le}{D} \frac{1}{2} \left[\frac{\dot{m}}{\rho \pi D^2} \right]^2$
$PnC_{out} (3)$	$= T_{out} \approx T_{in}$
Heat Exchanger:	
PnC_{out}	$= HXCaps(HotPnC_{in}, ColdPnC_{in}, HotPnC_{des})$
$PnC_{out} (1)$	$= \min \left[\begin{array}{c} PnC_{des}, \\ HotPnC_{in}, \\ DependsonColdPnC_{in} \end{array} \right]$
$PnC_{out} (2)$	$= P_{out} = P_{in} - \Delta P_{HX}$
$PnC_{out} (3)$	$= T_{out} = \min \left[\begin{array}{c} HotPnC_{in} (3), \\ 175^\circ C \end{array} \right]$
Ram Compressor:	
$PnC_{out} (1)$	$= RamComCaps(RamAirC_{in}, ElecC_{in}, PnC_{des})$
	$= \min \left[\begin{array}{c} PnC_{des}, \\ RamAirC_{in}, \\ MaxFlow(ElecC_{in}, RamTemp, RamPress) \end{array} \right]$

6.6.3.1 Distribution Element: Pneumatic Tubing/Ducting

Assuming no pneumatic leakages and adiabatic flow, pneumatic distribution systems are assumed to provide flow up to the design limit at the input temperature but subject to head loss. Loss of head (h_l) is given by equation 45. In this equation, f_r is the friction coefficient, Le is the straight pipe length equivalent for the system capturing all major and minor losses, \dot{m} is the fluid flow rate, and D is the pipe diameter.

$$h_l = f_r \frac{Le}{D} \frac{1}{2} \left[\frac{\dot{m}}{\rho \pi D^2} \right]^2 \quad (45)$$

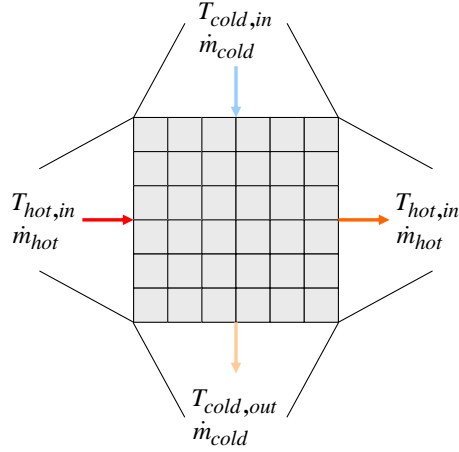


Figure 66: Cross Flow Heat Exchanger Diagram

The friction coefficient is given by the Colebrook equations [46]. In the equation Re is the Reynolds number ($Re = \dot{m}/\pi\mu D$), and e/D is the relative roughness (assumed at 5×10^{-6} for drawn tubing).

$$\frac{1}{(f_r^{0.4})} = \left(-2 \log \left(\frac{e/D}{3.7} + \frac{2.51}{(Re f_r^{0.5})} \right) \right) \quad (46)$$

6.6.3.2 Transformation Elements: Heat Exchanger

The second unit capability transfer function defined for this study is a precooling heat exchanger. See the diagram in figure 66. The maximum pneumatic air capability is a function of available high temperature air, the design capability of the heat exchanger, and limits in the amount of low temperature air available to sufficiently reduce the temperature of the high temperature air. This hot flow limit depends on the total amount of heat that can be extracted by the cooling flow. This heat transfer rate (q) is determined by equation 47. Ideal counter flow heat exchange indicates that the output of the high temperature side approaches the input temperature of the cold side. The effectiveness of the exchange (ϵ) expresses the relationship between the actual heat exchange provided and the maximum heat exchange possible.

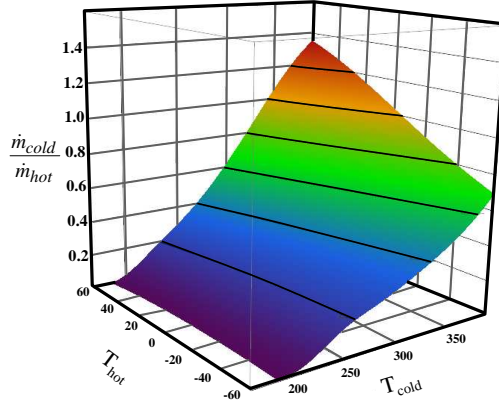


Figure 67: Heat Exchanger Flow Requirements

$$\epsilon = \frac{q}{q_{max}} = \frac{\dot{m}_{hot} c_p (T_{hot,in} - T_{hot,out})}{\min(\dot{m}_{hot}, \dot{m}_{cold}) c_p (T_{hot,in} - T_{cool,in})} \quad (47)$$

The effectiveness-NTU method for a cross flow single pass heat exchanger analysis calculates effectiveness in terms of the number of transfer units (NTU). This is given in equation 48.

Assuming minimal variation in the specific heats of the hot and cold sides, NTU is calculated by $NTU = UA / (\min(\dot{m}_{hot}, \dot{m}_{cold}) c_p)$ and the heat capacity ration is given by $C_R = \min(\dot{m}_{hot}, \dot{m}_{cold}) / \max(\dot{m}_{hot}, \dot{m}_{cold})$.

$$\epsilon = 1 - \exp \left[\left(\frac{1}{C_R} \right) (NTU)^{0.22} \left\{ \exp \left[-C_R (NTU)^{0.78} \right] - 1 \right\} \right] \quad (48)$$

With known input temperatures and available mass flows and by fixing the maximum allowable output temperature ($\approx 200^\circ C$) [48] equations 47 and 48 are used to numerically determine the maximum available hot massflow. The ratio of cooling flow to hot flow required is displayed in figure 67 as a function of input temperatures for a given overall heat transfer coefficient.

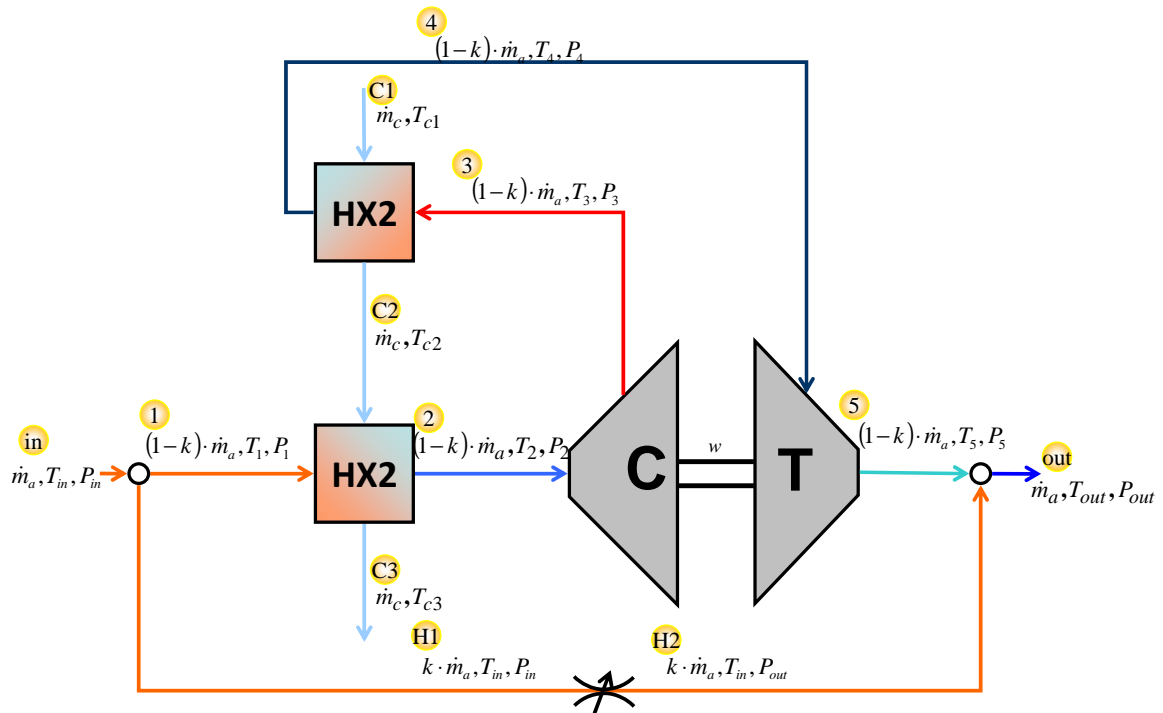


Figure 68: Bootstrap ACM System Diagram

6.6.3.3 Transformation Elements: Ram Compressor

The third type of element modeled for the pneumatic system is the electrically driven ram compressor. One benefit to replacing bleed ECS with ram compressor is the gained ability to regulate the pressure of the air independent of the engine thrust settings. This reduces the amount of wasted energy used for precooling and the operating temperatures of the pneumatic distribution system. The capability of the ram compression is characterized as the amount of mass flow that can be provided to the air cycle Machine (ACM) which can be regulated in support of environmental control. Therefore, in order to determine the capability limits of the ram compressor, the inlet airflow pressure and temperature requirements of the ACM must first be understood.

It was assumed that air conditioning is achieved by the bootstrap air cycle as illustrated in figures 68 and 69. The bootstrap air cycle Machine conditions compressed ram air through a process of cooling, compression, and expansion. Two heat

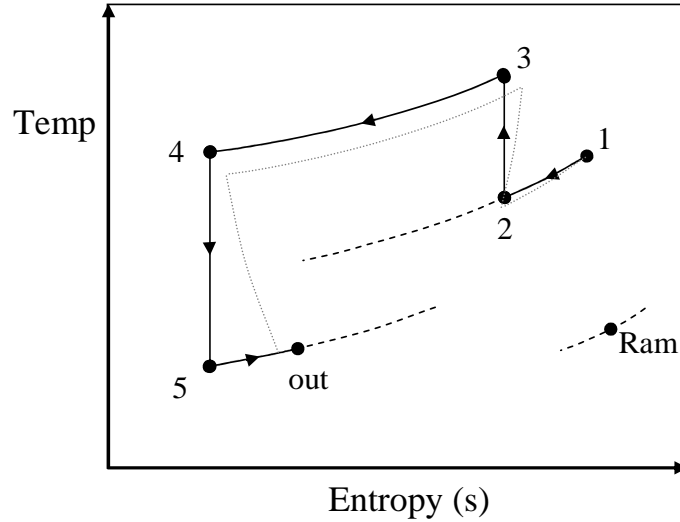


Figure 69: Bootstrap ACM T-S Diagram

exchangers are used to regulate temperature separated by a bootstrapped compressor/turbine to regulate pressure. Additional heat is available from air which bypasses the ACM and is throttled to cabin inlet pressure. It is assumed that the ACM Machine provides air to the aircraft ventilation system at a max pressure-altitude of 8000 ft and is mixed with an equal mass flow of recirculated air. Maintaining the required cabin temperature ($22^{\circ}C$) requires air delivered to the cabin diffusers at $\approx 15^{\circ}C$ [48].

Assuming a fixed air cycle Machine design, the minimum required input temperature and pressure (P_{in}, T_{in}) from the ram air compressor was determined by fixing the output flow conditions required and identifying the bounds on these variables for different cooling flow attributes. This was performed with the system of equations listed in table 32. The ability of this bootstrap ACM to meet the output flow conditions was assessed for each input case.

This analysis limits the allowable output flow conditions for the ram compressor, thereby specifying required pressure ratio and compressor efficiency. The capability transfer function for the ram compressor enforces the limits imposed by the ACM.

Compressor capability is determined in terms of the available ram air inflow and

Table 32: Bootstrap ACM System of Equations

Eq	Function
1:	$P_1 = P_{in}$ $T_1 = T_{in}$
2:	$P_2 = P_1 (1 - hl_{HW1})$ $T_2 = T_1 - \epsilon_1 \frac{\min((1-k)\dot{m}_a, \dot{m}_c)}{(1-k)\dot{m}_a} (T_1 - T_{c2})$ $T_{c2} = T_{c1} + \frac{(1-k)\dot{m}_a}{\dot{m}_c} (T_3 - T_4)$
3:	$P_3 = \pi_{comp} P_2$ $T_3 = T_2 \left[1 + \frac{1}{\eta_{comp}} \left(\pi_{comp}^{(\frac{\gamma-1}{\gamma})} - 1 \right) \right]$
4:	$P_4 = P_3 (1 - hl_{HX2})$ $T_4 = T_3 - \epsilon_2 \frac{\min((1-k)\dot{m}_a, \dot{m}_c)}{(1-k)\dot{m}_a} (T_3 - T_{c1})$ $T_{c1} = T_{Ram}$
5:	$P_5 = P_{out}$ $T_5 = T_4 \left[1 + \eta_t \left(\left(\frac{P_{out}}{P_4} \right)^{(\frac{\gamma-1}{\gamma})} - 1 \right) \right]$
out:	$T_{out} = (1 - k) T_5 + k T_{in}$

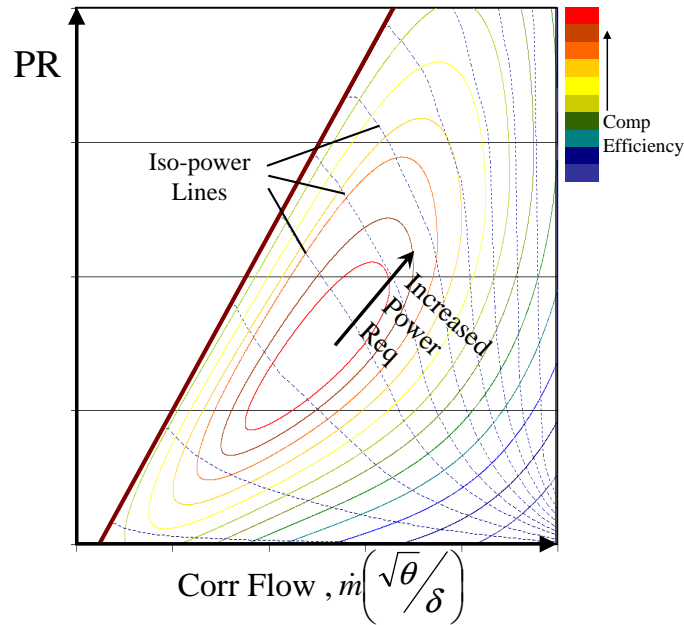


Figure 70: Typical Centrifugal Ram Compressor Map

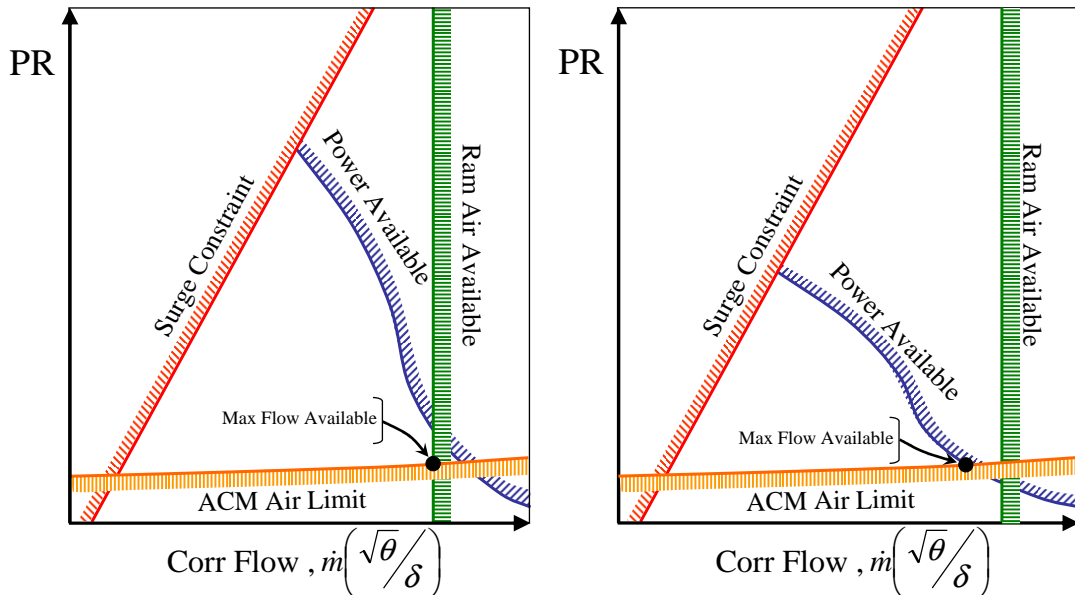


Figure 71: Ram Compressor Operating Envelope

power. The operating limits of this centrifugal compressor is provided by the compressor map shown. A typical centrifugal compressor map is given in figure 70. This compressor map also shows iso-power lines. Assuming the ability to control compressor rpm, increasing the power available allows higher pressure ratios for a given mass flows.

The massflow capability of the ram compressor is effected by power available, ram air available, and ACM flow requirements. This constrained operating envelope is shown in figure 71. The green flow constraint changes with increases and decreases in ram mass flow capabilities. The blue power constraint varies with losses in electrical power capabilities. Pressure ratio limits (orange constraint) stems from the operating envelope of the ACM.

The compressor transfer function is illustrated in figure 72 with ram compression at 0.7 Mach number. The definition of this transfer function takes all limitations into account as imposed by the ACM and compressor performance map.

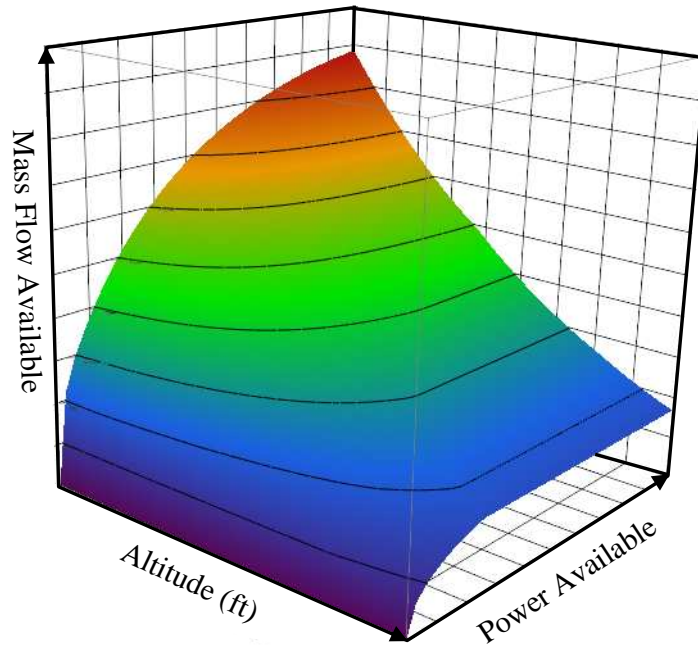


Figure 72: Centrifugal Ram Compressor Transfer Function

6.6.4 Powerplants

Unlike the other transfer functions introduced previously, the powerplant units (engine and auxiliary power unit (APU)) are used to provide multiple capabilities. Both the engine and APU are tasked to transform fuel and ram air capabilities to the provision of both shaft power and bleed air. Additionally, the engine is responsible for the system level function to propel. With multiple output capabilities, optimal allocation of capability requires input regarding which output capability is preferred. These preferences are set by a matrix of values accessible by external optimization routines ($[\alpha]$). The sizes of these matrices are given by number of output capabilities provided by the unit. Table 33 gives the form of these transfer functions.

6.6.4.1 Transformation Element: Turbofan Engine

The engines employed for this business jet architecture study are two shaft, high bypass ratio, turbofan engines. Shaft power extraction is available from either the HP or

Table 33: PowerPlant Capability Transfer Functions

Unit	Transfer Function
TurboFan Engine:	
$\begin{bmatrix} ThrustCap_{out} \\ FanAirCap_{out} \\ HPPnCap_{out} \\ LPPnCap_{out} \\ HSShaftCap_{out} \\ LSShaftCap_{out} \end{bmatrix}$	$= EngineCaps \begin{pmatrix} RamAirCap_{in}, \\ CoolingCap_{in}, \\ FuelPressCap_{in}, \\ Alt_{in}, \\ Mach_{in}, \\ [\alpha] \end{pmatrix}$
APU:	
$\begin{bmatrix} PnCap_{out} \\ ShaftCap_{out} \end{bmatrix}$	$= APUCaps \begin{pmatrix} RamAirCap_{in}, \\ FuelCap_{in}, \\ PnCap_{des}, \\ ShaftCap_{des}, \\ [\alpha] \end{pmatrix}$

LP shaft and bleed is provided in three types (high pressure bleed, low pressure bleed, and fan bleed). In all, the capability allocation matrix for the engine unit is 6 variables in length. Additionally, engine output capabilities depend on mission variables (altitude, Mach number) which determine the ram air input total pressure, output static pressure, and input total temperature. The total temperature and pressure are determined by isentropic ram compression at standard atmospheric conditions.

The engine capability transfer function developed for this study is a neural-network surrogate generated from a detail level model of a two shaft high bypass turbofan model with a sea level static thrust class of approximately 7000 lbf. The data used for this regression was acquired by sampling the operating space of the engine model with 40,000 space filling DOE sample operating points. Half of these cases were executed by solving to fuel flow provided and half were executed by solving for thrust provided. Customer loads (shaft hp and air flows) and flight conditions were set as inputs. The model was then tasked to solve for available thrust, shaft speeds, surge margins, and bleed flow conditions. Figure 73 shows the relationship between

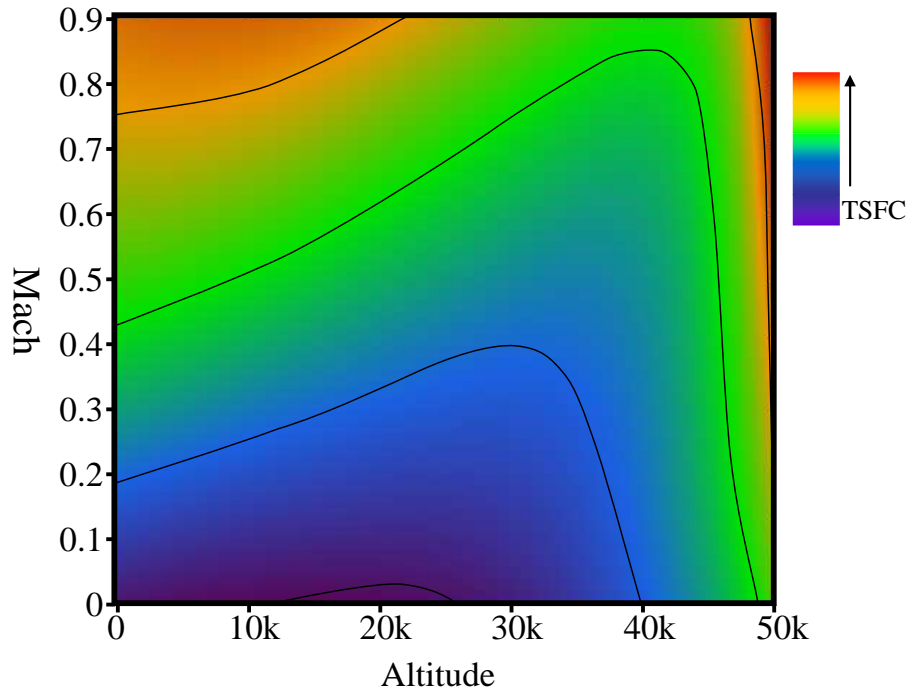


Figure 73: Thrust Specific Fuel Consumption Variation with Flight Conditions

thrust capability and available fuel flow for this engine model at the indicated flight and load conditions.

Not all combinations of these input variables yield feasible model outputs. The levels to which auxiliary output capabilities are available are limited for different regions of the operating envelope (altitude, Mach number). Additionally, provision of one capability impacts the ability of the unit to provide additional capabilities. By sampling this space, capability limits were defined for each customer load in terms of flight condition. The allocation variables ($[\alpha]$) were then used to specify the magnitude of the capability provided as a proportion of capability available.

These limits are displayed in figures 74 and 75. Figure 75 displays the maximum allowable low pressure customer bleed and figure 74 displays the maximum limits for all other customer loads. All loads are subject to limitations with reductions in fuel flow available. Additionally, LP bleed is also limited with increases in altitude. The capability transfer functions for the customer load capabilities are given by the

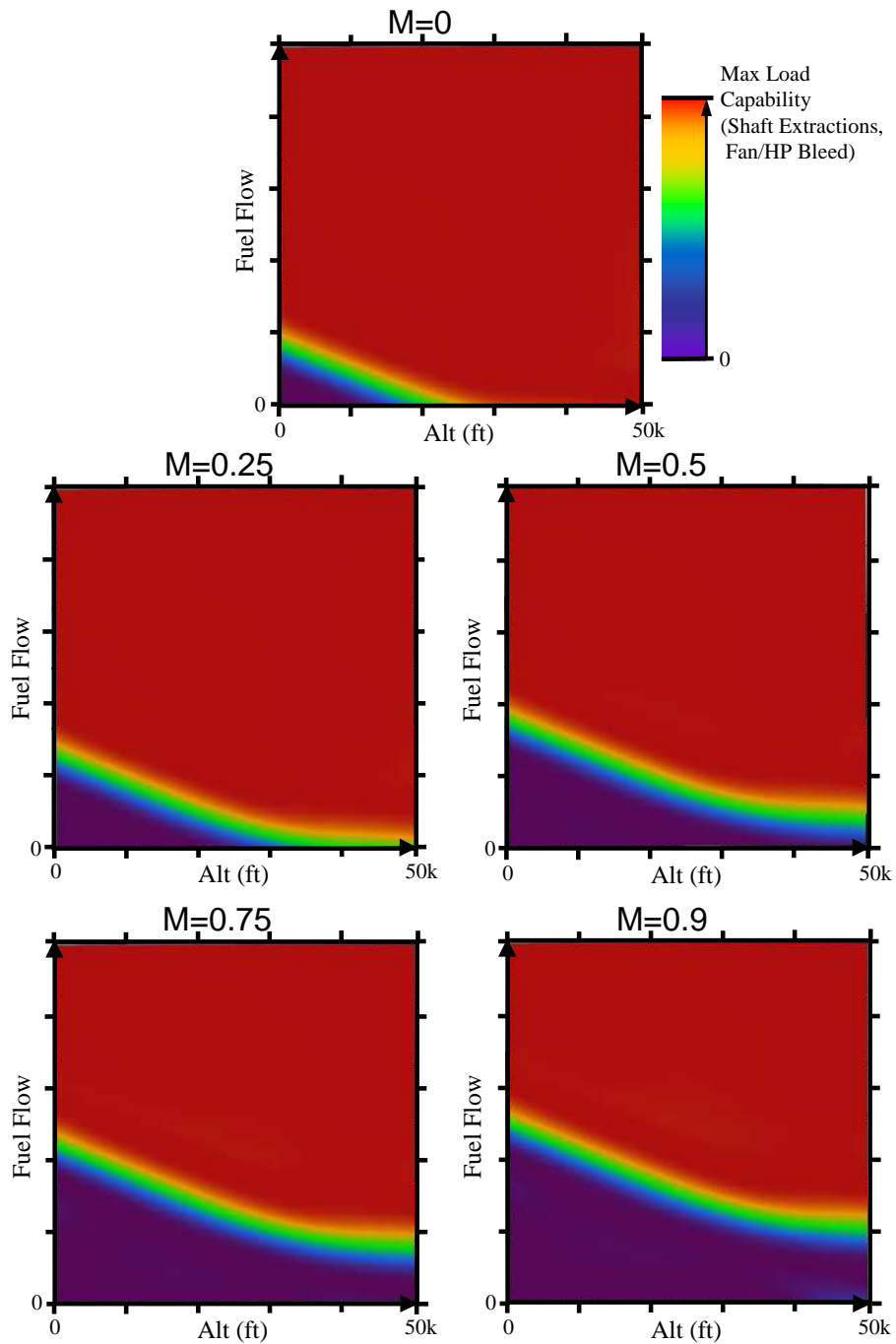


Figure 74: Limits to Engine Auxiliary Load Available with Variation in Available Fuel Flow, Altitude, and Mach Number

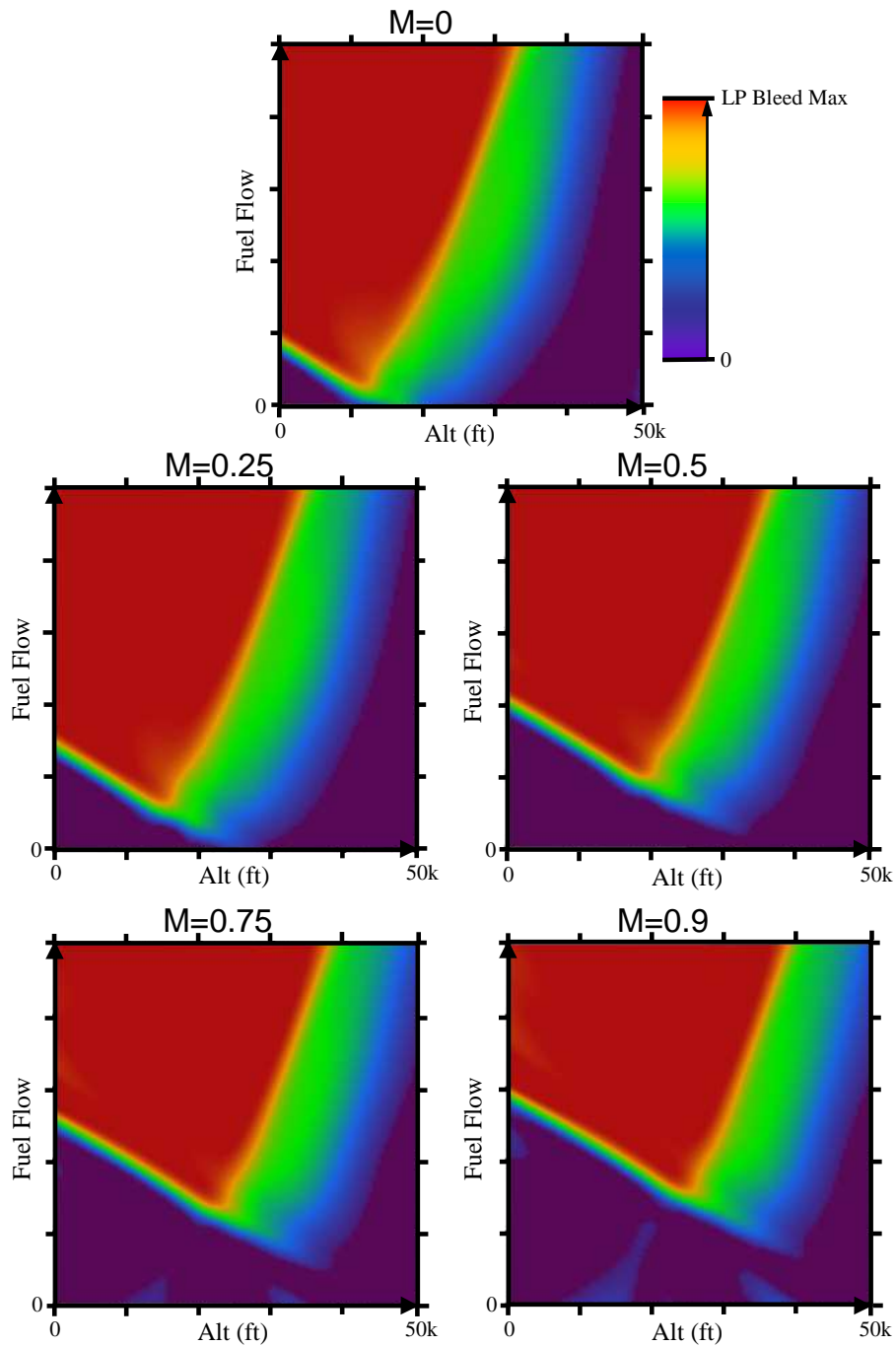


Figure 75: Limits to Engine LP Bleed Available with Variation in Available Fuel Flow, Altitude, and Mach Number

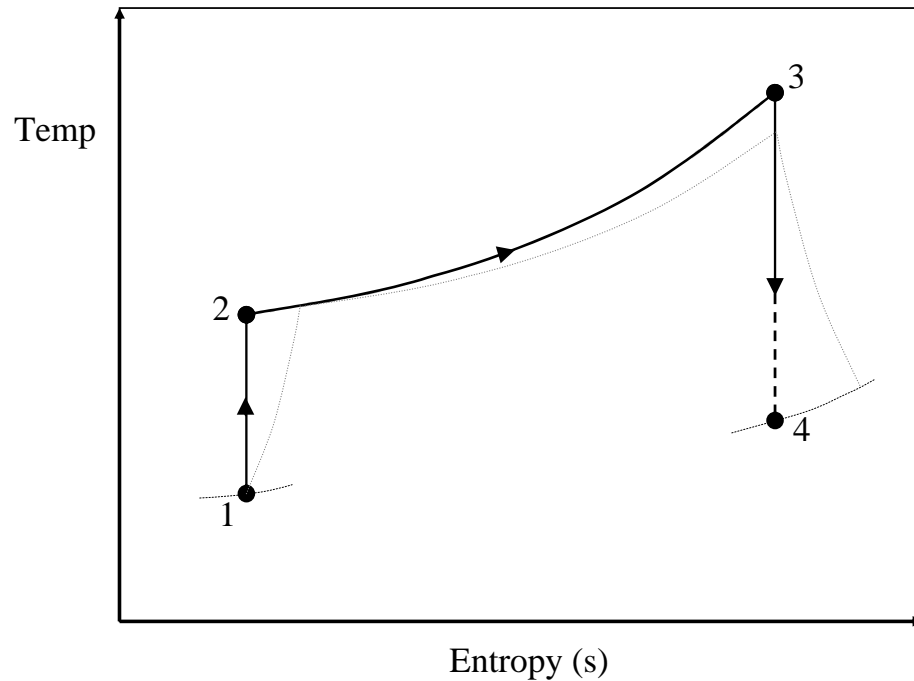


Figure 76: Ideal and Actual Brayton Cycle T-S Diagram Used for APU Modeling

feasibility limits, the allocation matrix ($[\alpha]$), and the capability transfer function for the thrust capability is given by the the thrust capability surrogate.

6.6.4.2 Transformation Element: Auxiliary Power Unit

The second transfer function in table 33 calculates the capabilities provided by the auxiliary power unit. As indicated in the table, the APU provides shaft power and pneumatic air while relying on input bleed air and fuel. This relationship is calculated as an ideal Brayton cycle with a fixed pressure ratio available as displayed in figure 76.

High pressure bleed air is extracted following the compression portion of the cycle (point 2). The air that remains is heated through combustion (2-3). This high pressure air is then expanded through a turbine which provides both power for the compressor and for shaft power customer loads (3-4). The maximum amount of bleed air is fixed by the minimum amount of air which must remain in the cycle in order to sufficiently compress the air for customer bleed. The maximum amount of shaft power

available occurs when no air is extracted for bleed. Preference of one capability type to the other governs how much air is bled from the APU. The system of equations which determines the magnitude of these capabilities is displayed in table 34.

Table 34: Brayton Cycle APU System of Equations

Eq	Function
1:	$P_1 = P_{Ram}$ $T_1 = T_{Ram}$
2:	$P_2 = \pi_{Comp} P_1$ $T_2 = T_1 \left[1 + \frac{1}{\eta_{Comp}} \left(\pi_{Comp}^{\frac{\gamma-1}{\gamma}} - 1 \right) \right]$
3:	$P_3 = P_2$ $T_3 = \max \left[T_{max}, \frac{h\nu \cdot \dot{m}_f}{\dot{m}_{air} (1 - k_{bleed}) cp} + T_2 \right]$
4:	$P_4 = P_{out}$ $T_4 = T_3 \left[1 + \eta_{Turb} \left(\left(\frac{P_{out}}{P_3} \right)^{\frac{\gamma-1}{\gamma}} - 1 \right) \right]$

In these equations, the variable k_{bleed} determines the proportion of the airflow which is bled from the compressor. This value is limited by the amount of heated air necessary to drive the compressor with no horsepower extraction. The maximum value of k_{bleed} is graphed in figure 77 with inlet flow characteristics fixed by ram compression. This graph was generated with an inlet massflow of 0.2 kg/s, an altitude of 25kft, Mach number of 0.5, and a T_3 operating at T_{max} . The maximum k_{bleed} is also sensitive to variation in available massflow, and available fuel

Optimal allocation of capability requires a decision to be made as to which output, bleed air or shaft power, will be provided for each failure conditions. The α variable input sets the preference between these two capabilities. An α value of 1 corresponds to the maximum allowable k_{bleed} value. This yields maximum bleed air capability with no shaft power. An α value of 0 corresponds to a k_{bleed} value of 0. This yields a maximum shaft power capability with no bleed air. Figures 78 a and 78 b illustrate the capability transfer function for APU bleed air and power available with variations

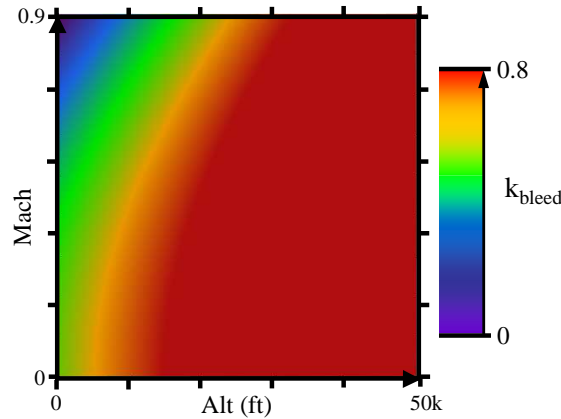


Figure 77: Maximum Bleed Air Mass Flow Proportion (k_{bleed}) with Input Airflow of $\dot{m}_{in} = 0.2 \text{ kg/s}$

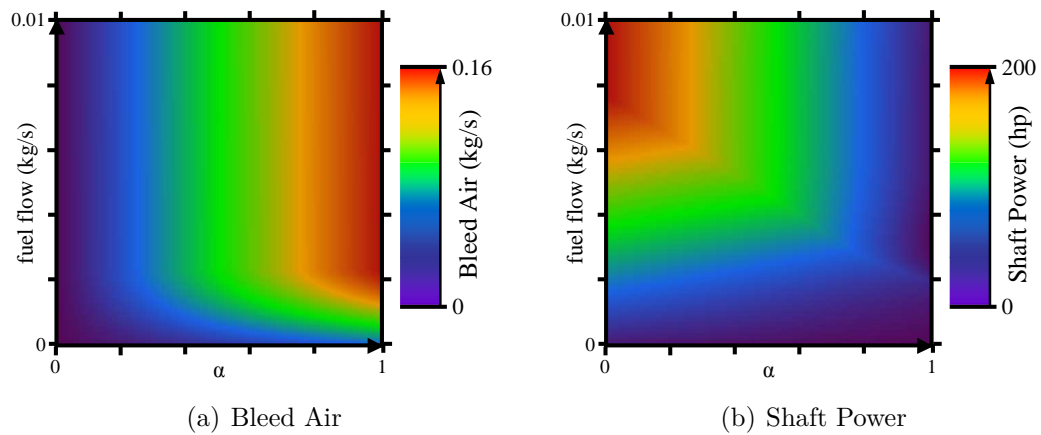


Figure 78: Transfer Functions for Auxiliary Power Unit Output Capabilities

in fuel flow available and α . These graphs are also generated with an inlet massflow of 0.2 kg/s , an Altitude of 25000 ft , and a Mach number of 0.5 .

6.6.5 System Reliabilities

In order to perform trades between the unit capability and reliability in meeting operational performance constraints, the reliability of each of the units described above must be defined. In defining the reliability of each of these units it was assumed that the reliability is uniform over the range of functional requirements as illustrated in figure 79.

The structure of this relationship between failure rate and magnitude of functional

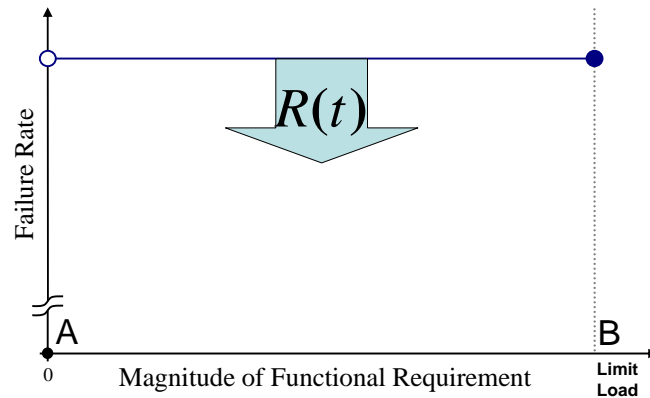


Figure 79: Assumed Relationship Between Reliability and Functional Requirement Magnitude

requirements makes three fundamental assumptions. The first assumption is that the all units are perfectly reliable at providing no functional requirements (the failure rate at $x = 0$ is zero). The second assumption is that the unit is entirely incapable of providing for functional requirements in excess of the limit load (B). Therefore, for functional requirements higher than this load, $Req > B$, the failure rate is infinite.

The third assumption is that at any instant in time, the failure rate is uniform over the whole range of functional requirements. Revisiting equation 3 from chapter four, unit failure rates vary in time depending on unit mission loading.

$$R(t) = \exp \left[- \int_0^t \lambda (Req(\tau), \tau) d\tau \right]$$

Reliability is a function of load history. As stated by Smith, reliability is the “probability of non-failure in a given period [270].” Reliability at one instant in time is therefore sensitive to loading during all previous timesteps. This failure rate is therefore architecture and mission specific. Loading at a given time only affects $\lambda(t)$ and future reliability. This assumption is illustrated in figure 80.

The failure rate for each unit is a function of time. “Infant Mortality” Failures

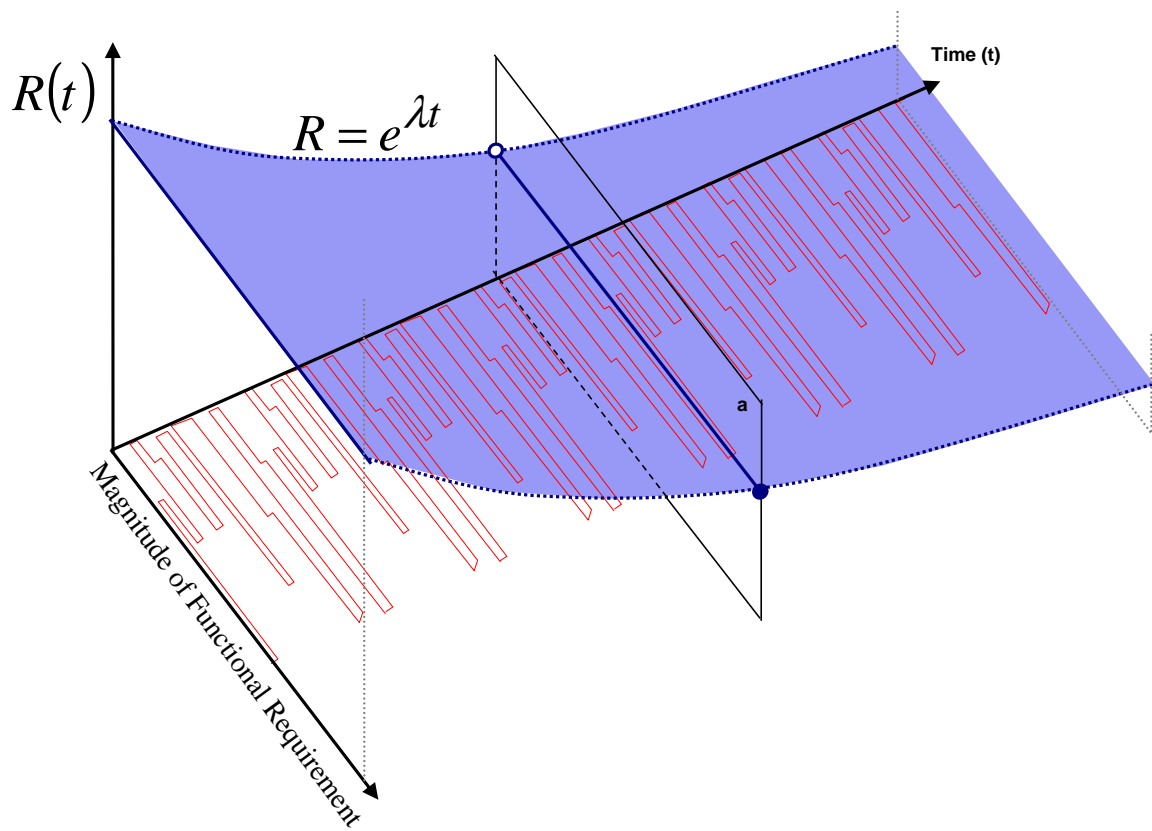


Figure 80: Reliability Degradation for a Unit with Uniform Reliability

and wear out failures impact variations in failure rate in time. Additionally, the duty cycle and load profile for each unit effects its failure rate. In figure 80 the red line on the x, y plane represents the cyclical loading of a unit throughout its life. The load requirement profile ($Req(\tau)$) causes the unit reliability to degrade over time. This does not negate the assumption that at a given instant in time, reliability is uniform for any functional requirement (figure 79).

For this study, it is assumed that unit reliabilities are given by Weibull distributions. The minimum reliability is of interest for this analysis. Therefore, assuming that repair reinitializes the reliability calculations, the unit reliability used for criticality analysis is given by equation 49. In this equation λ is the failure rate and t_{max} is given by the Mean Time to Repair.

$$R_{min} = e^{-\left(\frac{t_{max}}{\eta}\right)^\beta} \quad (49)$$

A table of the assumed Weibull parameters for all units in this model is given in table 35. The parameters used here were made following literature review and are meant for illustrative purposes. The values of these parameters were defined within reasonable ranges considering literature sources [21, 148, 308, 70]. Actual failure calculations must be derived from vendor specific sources. The values as indicated are sufficient in highlighting potential trades between redundancy, capability margin, and maintenance schedule.

6.6.5.1 Load-Independent Uniform Reliability

The load-independent uniform reliability assumption yields inaccuracies with increased unit complexity. Each unit can be considered as a self-contained system with internal redundancies. As such, these units exhibit reliability profiles which decrease with unit capability. Representing unit reliability in this fashion reduces

Table 35: Hazards for Conventional and ‘All-Electric’ Architecture Concepts

Unit	η	β	$t_{max} = MTTR(hrs)$	$F(t)_{max} = 1 - e^{-\left(\frac{t_{max}}{\eta}\right)^\beta}$
AC Bus Failure	1400000	2.25	5000	3.12E-06
AC Gen Failure	200000	2.1	700	6.96E-06
AGB Fail	662500	3.25	5000	1.27E-07
APU Fail	80000	4.5	5000	3.81E-06
DC Bus Failure	1400000	2.25	5000	3.12E-06
DC Gen Failure	160000	2.1	700	1.11E-05
Engine Fail	80000	4.5	5000	3.81E-06
Fan Duct Failure	80000	2.7	1500	2.17E-05
Fuel Pump Fail	125000	2.1	700	1.87E-05
Fuel Sys Fail	80000	2.7	1500	2.17E-05
HP Bleed Failure	80000	2.7	1500	2.17E-05
Heat Ex. Failure	80000	2.7	1500	2.17E-05
Hyd. Pump Failure	125000	2.1	700	1.87E-05
Hyd Sys Failure	250000	2.05	700	5.84E-06
LP Bleed Failure	80000	2.7	1500	2.17E-05
PCU Fail	200000	2.05	1500	4.40E-05
Pn Sys Failure	80000	2.7	700	2.78E-06
Ram Comp Fail	120000	2.45	1500	2.17E-05
Ram Duct Fail	80000	2.7	1500	2.17E-05

the number of optimization points needed to characterize the probability of fulfilling partial system capabilities.

It is also assumed that the reliability of two units are each given by a tiered load/reliability relationship as illustrated in figure 40 from chapter five. The reduction in the number of design points required to characterize proportional losses for two unit failure combinations is illustrated in figure 81. Each independent reliability relationship corresponds to the intersection of xz and yz planes at x=14kW and y=14kW respectively. The combined capability of these complex units is characterized by a multidimensional tiered reliability relationship.

With these triple-redundant complex units, a total of 64 points would be necessary to characterize the relationship between combined capability and failure probability. These points are indicated with yellow circles in figure 81. Assuming a uniform reliability capability relationship, only 4 combinations of failures must be assessed. These

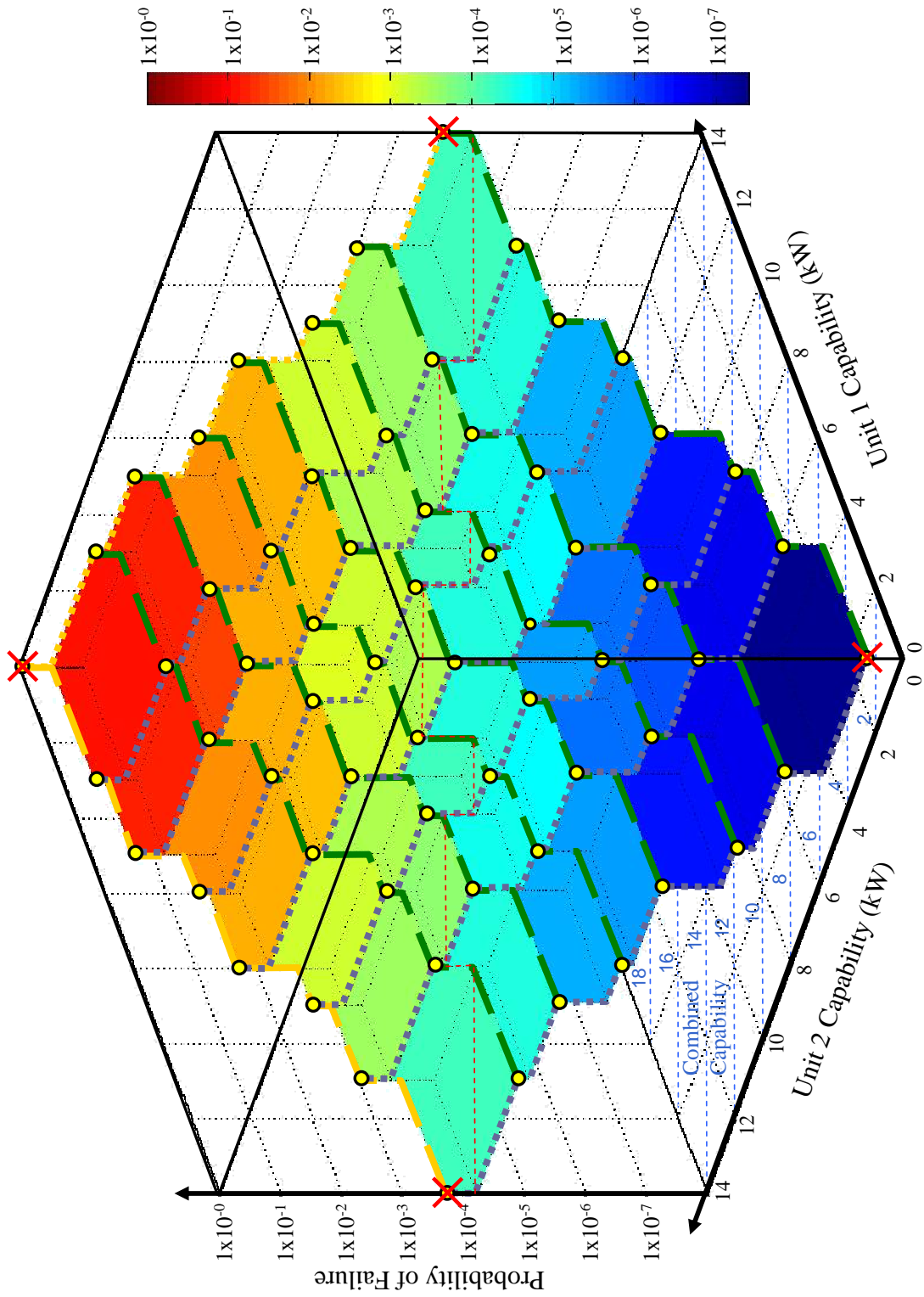


Figure 81: Reliability of Combined Unit Capabilities with Complex Unit Reliability Structure

four combinations are indicated with red x's in figure 81. While this introduces inaccuracies in the continuous reliability assessment of the architecture, it also simplifies the reliability evaluation.

Questions also arise regarding the identification of the reliability which characterizes a combined capability of a given magnitude. The four representative points for the uniform approximation assume independent unit failures. However, the multiple points which characterize partial unit failure must consider interdependent internal unit failures which are masked at the system level. Consider the combined level of capability indicated by the contours on the xy plane in figure 81. The combined capability of $14kW$ is projected on the reliability relationship with a red dashed line. This isocapability line cuts across multiple combined failure states. The final probability measure of a given capability must capture the total probability of failure considering all interdependent states that generate that failure.

Applying complex unit reliability/capability relationships requires the ability to identify or approximate multidimensional step functions for the combined failures of multiple complex units. These challenges are allayed by assuming uniform reliability relationships. Augmenting this assumption introduces ancillary research opportunities.

6.6.5.2 Eliminating Inconsequential Failure Combinations

The last assumption made to reduce the number of optimization cases is the elimination of all statistically insignificant failure combinations. Failure conditions which exhibit the highest probability of occurrence are single point failures. Increasing the number of concurrent independent failures decreases the probability of occurrence. The limiting recognized probability of failure was determined by organizing the unit failures by magnitude of failure probability. These failure cases are organized from least probable to most probable. Assume that all failure states contribute to a system

failure and that all failure combinations are independent. (Note: This assumption is not used for actual probability calculation but only for limiting the number of optimization cases). With the least likely recognized failure case given as P_n and the most likely failure case given as P_1 , the probability of failure is given by equation 50.

$$P = 1 - \prod_{i=1}^n (1 - P_i) \quad (50)$$

Minimum recognized independent failure probability is illustrated in figure 82.

The x axis in this figure represents the probability of failure for any failure case. The y axis represents the union of all failure probabilities less than x , given by equation 50. The dark and light blue dots are calculations performed for the conventional architecture. The dark blue dots begin calculations with $P_n \ll 1 \times 10^{-15}$ and the light blue dots begin with $P_n \geq 1 \times 10^{-14}$ indicated by the blue vertical line. The green dots are calculated from all failure cases from the ‘more-electric’ architecture. The light green dots begin union calculations at the green vertical line, $P_n \geq 1 \times 10^{-13}$.

The minimum recognized probability of failure (P_n) is selected to limit the failure cases to those with probabilities greater than 1×10^{-11} (indicated by the horizontal line in figure 82). As illustrated in figure 50, a P_n of 1×10^{-14} for the conventional architecture is necessary to capture are failure probabilities greater than 1×10^{-11} . Over 775 cases must be calculated to maintain this level of fidelity. Following similar analysis over 475 failure cases must be considered for the ‘more-electric’ architecture with a limiting P_n of 1×10^{-13} . These results are obtained using the maximum probabilities of failure, $(F(t)_{max})$, from table 35.

This analysis assumed that the union of failure case is given by the following equation under the assumption that each failure case is independent.

$$P(X \cup Y) = P(X) + P(Y) - P(X \cap Y) = 1 - (1 - P(X))(1 - P(Y))$$

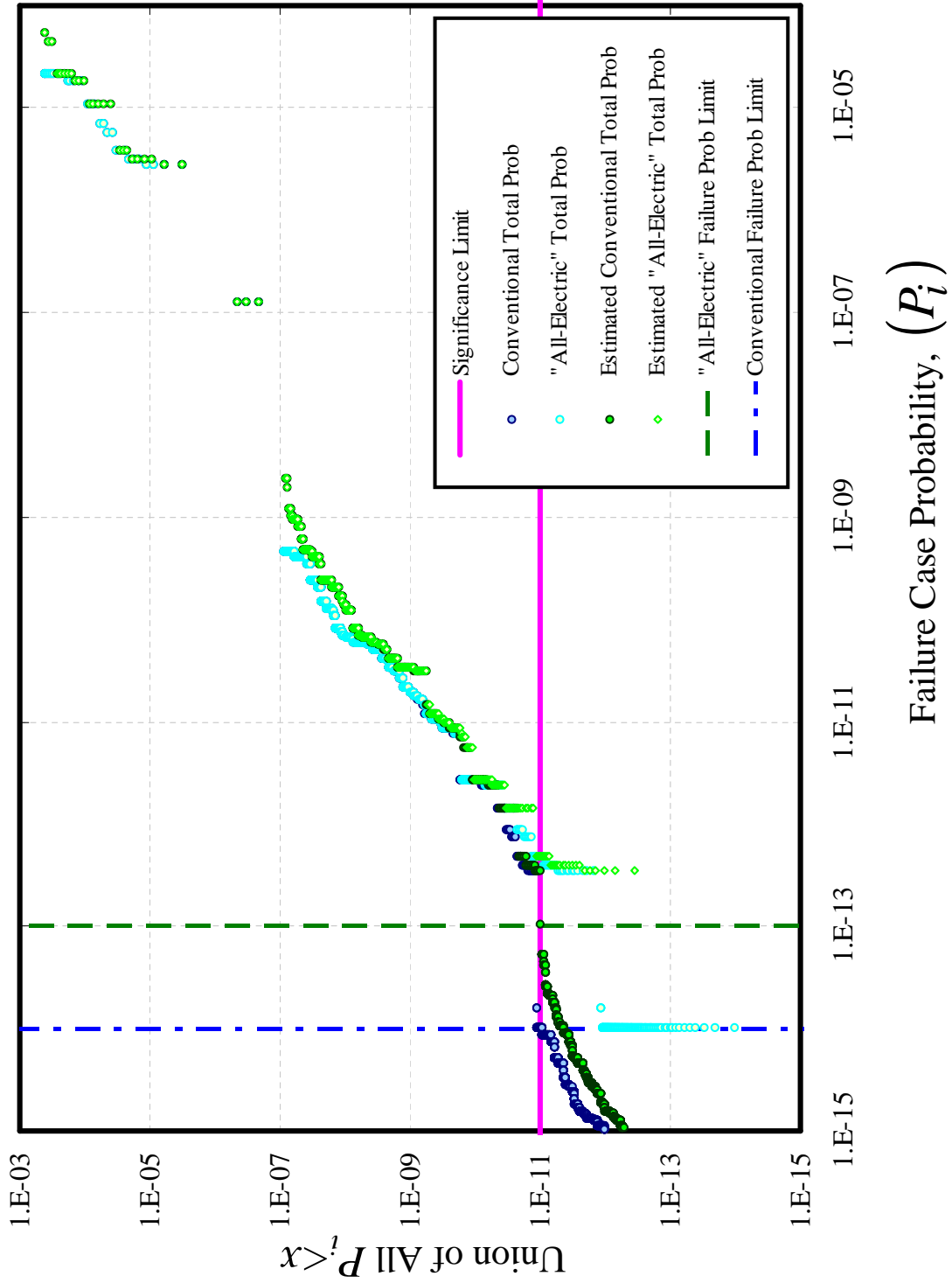


Figure 82: P_n limits for Conventional and 'All-Electric' Failure Cases

However, the actual calculation of unions of potentially non-independent failure intersections was accomplished by two corrections.

The first consideration must recognize that the union of the probability of event X with event $X \cap Y$ is equal to the probability of event X [$X \cup (X \cap Y) = X$]. If the union of the probability of event X is already used in reliability calculations then event $X \cap Y$ may be excluded in the union calculations. All of these exclusions can be identified and considered in reliability calculations.

Unions of intersections must also be monitored for potential interdependencies. Consider the case where failure state X represents the intersection of two unit failures, A and B ($X = A \cap B$). Additionally, Y represents the the intersection of unit failures A and C ($Y = A \cap C$). In this scenario, $P(X \cap Y)$ is not equivalent to $P(X) \cdot P(Y)$ [$P(A)P(B)P(C) \neq 1 - (1 - P(A) \cdot P(C)) (1 - P(B) \cdot P(C))$]. These interdependencies are maintained in the reliability calculation algorithm by requiring all exponents to be equal to unit. The reliability equation is posed in its entirety and all repetitive multiplications are removed.

The algorithm and computer code used for determining the actual system level failure probability calculations is given in appendix D. This code addresses the considerations discussed regarding the non-independence of failure cases.

6.7 Optimization Formulation

As is evident in this analysis, the same percent loss of thrust yields different consequences depending on when it occurs in the mission. Loss of thrust at takeoff is more critical than loss of thrust during cruise. Additionally, environmental and operating conditions influence the criticality relationships.

Sizing critical requirements must be derived during the most stringent operating conditions. Since both thrust loss and ECS loss hazards vary with altitude, load

shedding optimization must be performed for multiple operating conditions. To illustrate the effect of varying function hazard relationships two operating states are considered: takeoff at 6000 ft, and cruise at 35kft $\beta = 1/3$.

The function hazard relationships illustrated in table 26 and discussed in this section act as the objective functions for load shedding optimization. The operational hazard function from equations 15 (Operational Hazard = $H(\{\mathbf{X}\}_{\infty})$), is found in terms of all function/hazard relationships for a given unit level failure (equation 51). Load shedding optimization tries to minimize the maximum incurred operational hazard by advantageously allocated capabilities.

$$\text{Operational Hazard} = \max \left\{ \begin{array}{l} H_{Thrust} \left(\frac{R_{req}}{R}, TOFL_{avail} - s_{Tot} \right) \\ H_{Bleed} \left(\frac{BleedAir_{cap}}{BleedAir_{req}} \right) \\ H_{Hydr} \left(\frac{Hydr_{cap}}{Hydr_{req}} \right) \\ H_{120VAC} \left(\frac{120VAC_{cap}}{120VAC_{req}} \right) \\ H_{28VDC} \left(\frac{28VDC_{cap}}{28VDC_{req}} \right) \\ H_{270VDC} \left(\frac{270VDC_{cap}}{270VDC_{req}} \right) \end{array} \right\} \quad (51)$$

For complex architectures, capability allocations change which hazard or hazards become dominant in this Min/Max optimization. The objective function is characterized by flat regions or shelves in which only give way following coordinated variations in the design variables. When implementing gradient based optimization these shelves present false optimum values ($\nabla H(\{\bar{\alpha}\}) = 0$). Furthermore, the optimal allocation of failure requires the coordinated variation of allocation variables. With a large number of design variables, stochastic optimization routines do not guarantee the identification of the optimum.

Due to the assumption discussed previously, that the probability of failure for a

unit is constant with magnitude of failure, only the optimal allocation of failure for the total loss of unit capability must be obtained. However, with this complex shelved objective function it is necessary for the initial conditions to remain sufficiently close to the optimal allocation. When the initial values of the design variables are sufficiently close to the optimum, gradient based optimization is able to obtain the minimum available hazard.

The optimal setting for the design variables was achieved by discretizing the magnitude of the failure (0% to 100%) and optimizing allocation in sequence. The setting of the design variables for optimal allocation ($\{\bar{\alpha}\}$) for the failure magnitude are then used as the initial conditions for optimization at the next failure magnitude. Allowing only small variations in the objective function in this manners, ensures that the initial conditions are sufficiently close to the new optimum, thus avoiding shelves and enabling the use of gradient based optimization in search for the minimum hazard. This idea illustrated in figure 83.

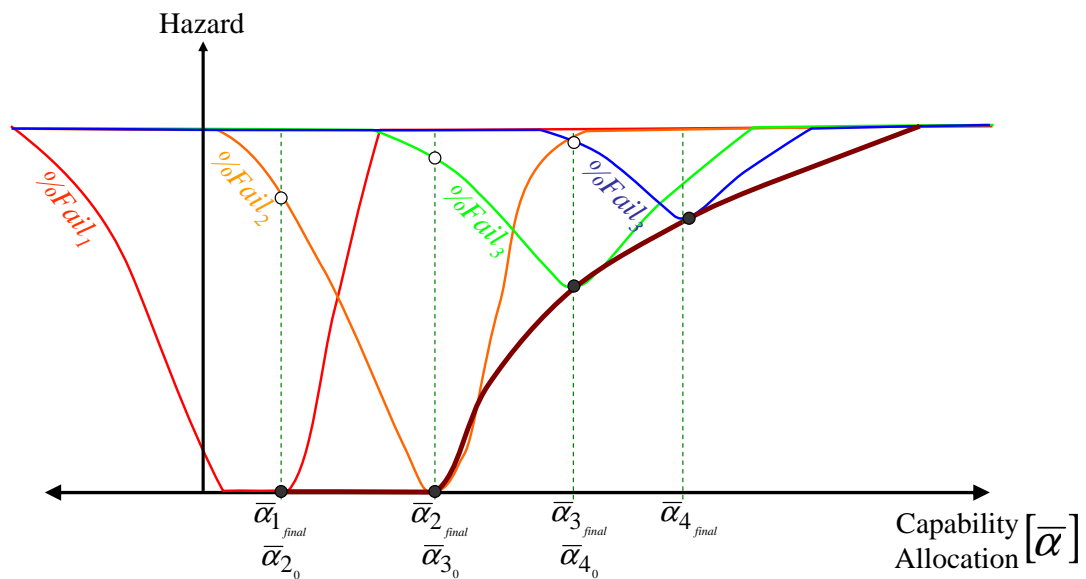
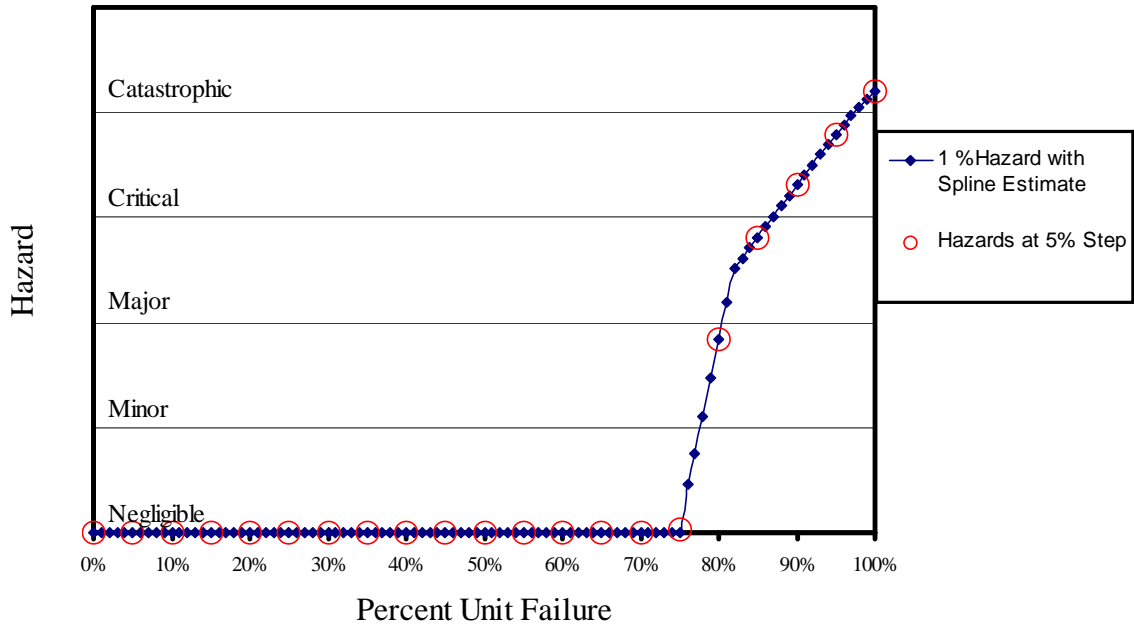


Figure 83: Ensuring Validity of Gradient Based Optimization Small Augmentations of the Objective Function

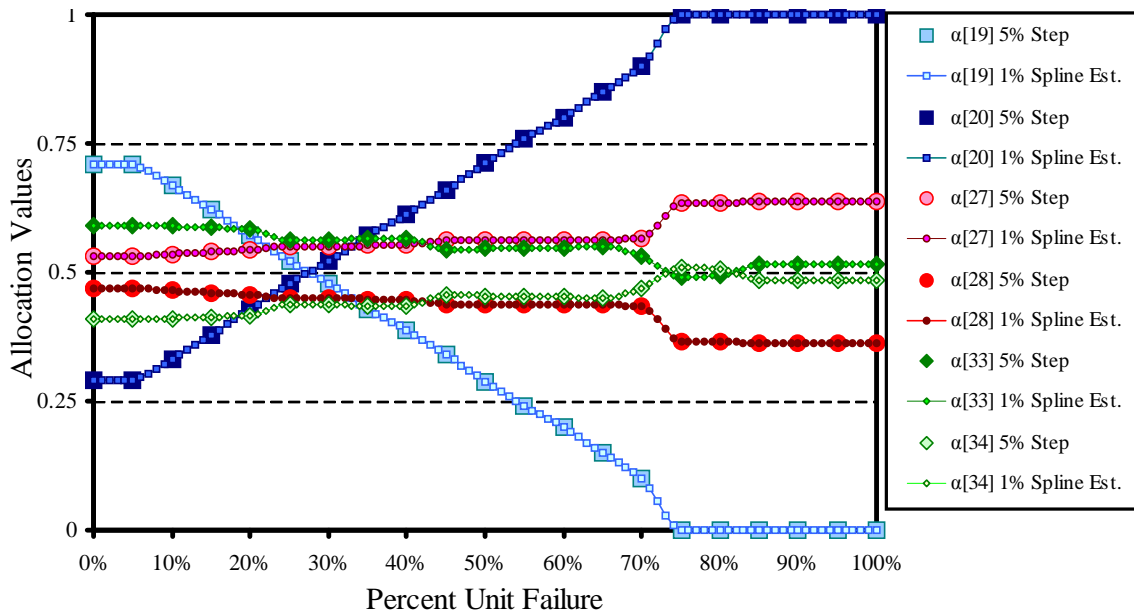
The colored lines in this image represent proportional unit failures. As the failure state changes, the relationship between the allocation variables and the hazard incurred changes. This is illustrated with the shifting of the objective function as the magnitude of the function loss changes. The black dots represent the minimum hazard incurred for each failure state. Fine discretization of the failure percentage ensures that the initial conditions (e.g. $\bar{\alpha}_{20} = \bar{\alpha}_{1_{final}}$) for each subsequent optimization is poised to ensure the validity gradient based optimization. These initial conditions are illustrated by the white dots. The failure/hazard relationship can then be fit to approximate the hazard for interstitial failure values.

The results of this optimization procedures are traces relating magnitude of failure both to magnitude of hazard and to the optimal setting of the design variables. These trace aids in the evaluation of the load shedding optimization. A stepsize of 5% was initially used for identifying the magnitude of the hazard. The initial failure percentage of 0% should naturally yield no hazards. Optimal allocation for failure of increasing magnitude were then determine (5%, 10%, ...). Values of the allocation variables for these evaluations are stored.

The primary indication as to whether the optimization was appropriately performed is the slope of the loss verses hazard relationship. Hazard monotonically increases with magnitude of failure. Following the identification of optimal load allocation for a 100% failure, the failure space is further discretized with a stepsize of 1%. Allocations variables are fit with a hermetic cubic approximation in terms of the magnitude of failure. Beginning and 100% failure and proceeding downward (99%, 98%, 99% ...) the hazard for each magnitude of failure is evaluated by applying that allocation ($\{\bar{\alpha}\}$) indicated by the hermetic cubic approximation. If the value of this hazard does not decrease with decreasing failure magnitude the optimization is performed again. This process is illustrated in figures 84a and b for the ‘more-electric’ aircraft architecture concept.



(a) Hazard Incurred with Combined APU and Power Converter Failure



(b) Significant Allocation Variables with Combined APU and PCU Failure

Figure 84: Means for Determining Optimum Failure Allocation for Unit Failures

The hazards indicated by the red circles in figure 84a are generated by the initial 5% failure samplings. These samplings generate the alpha cubic spline approximation in figure 84b. There are a total of 52 allocation variables for this architecture. Figure 84b illustrates the 6 most significant of these variables for this unit failure. The allocation variable fits shown in figure 84b are used to generate the loss/hazard relationship indicated in blue in figure 84a.

Appendices G and H include the computational process for achieving this optimization.

6.8 Hypothesis Testing Overview

Two hypothesis were introduced in the previous chapter regarding the need for higher fidelity in the application of requirements during exploratory design of conceptual architectures. Both hypothesis focus on the need to characterize the off-nominal aspects of architecture operations and the need to systematically characterize reliability requirements in context.

Conceptual safety and reliability tools place constraints on the physical system in terms of functional hazards. In order to apply load shedding optimization in a continuous fashion both the physical and operational domains must be characterized.

In the physical domain, alternative concept architecture were defined for the vehicle systems of a medium range business jet. Two concept architecture models were defined: a conventional architecture and a ‘more-electric’ architecture. The functional relationships between the systems was defined and transfer functions were outlined which characterize the capability of units within these architectures.

In the operational domain, function/hazard relationships were defined for each of the architecture functions at multiple operating conditions. These functions act as constraints on the functional performance of the architecture and as the objective function for load shedding optimization. All but one of these functions were defined

heuristically following three basic assumptions. The first set of hazard characterizations assume that maximum hazards begin to occur with any reduction in functional capability. The second set of function/hazard relationship assume that hazard is directly proportional to the percent loss of functionality. The third set applied heuristics regarding the criticality of various levels of load and their associated criticality. The function to propel was characterized considering the physics of the failure. Loss of thrust was characterized in terms of its impact of the required takeoff distance and its impact on available range during cruise.

Load shedding optimization was performed for both concept architectures in terms of the three function/hazard relationships. Optimal failure allocation was assessed for failure states which are statistically significant to the fulfillment of system functions. 1120 failure conditions were considered for the conventional architecture and 665 for the “more-electric.”

CHAPTER VII

ANALYSIS RESULTS

The results obtained from evaluating the effect of load shedding optimization is presented at multiple levels of abstraction. Results are presented illustrating the overall system level reliability, the risk associated with each system function, and the criticality of individual components. System evaluations are achieved by four means: Continuous Hazard Probability Evaluation, Functional Risk Assessment, Hazard Covariance Assessment, and Component Importance Evaluation. All of these metrics are used to compare the application of requirements towards both architecture concepts and assess the error associated with hazard characterization assumptions.

For complex systems catastrophic hazards ($H_S \geq 0.8$) are naturally less likely to occur than minor hazards. Additionally, more significant hazards must be bounded by more stringent probability constraints. The probability of failure is therefore expressed in terms of the magnitude of the incurred system level hazard ($F_s(H_S)$). This tool was illustrated in chapter five when considering system level implementation of load shedding optimization. The system level failure probability (F_s) is evaluated with respect to magnitude of hazard and continuous reliability constraints.

The overall and undesirable risk is determined for each independent functional failure. Two risk assessment metrics are introduced which characterize the system: overall system failure risk (R_{SF_O}) and undesirable system failure risk (R_{SF_U}). The probability of incurring certain hazards is determined with respect to each functionality lost. For this study, system level hazard (H_S) is determined by independently evaluating the impact of the loss of each system function ($H_S = \max[H_{F1}, H_{F2}, \dots]$).

The risk associated with the provision of system level functions differs between architecture concepts. Assimilating assignments of risk between concepts supports the claim that architecture specific load shedding strategies should be considered during requirement definition and early concept development. The relationship between the probability of functional failure ($F_{Fi}(H_{Fi})$) and the functional hazard constraints are compared for concept architectures.

The load shedding ability of each concept is also illustrated by considering the covariance of the independent functional hazards. A system with perfect load shedding capability exhibits a covariance of 1 between all functional hazards. The magnitude of the system level failure is reduced by distributing the failure between the systems functions according functional hazards. Concepts lacking the ability to do so will have correspondingly low hazard covariance. The covariance matrix and $H_{Fi} \times H_{Fj}$ multivariate plots are compared for the architecture concepts.

The last level of comparison looks at the importance of individual components within the concept architectures. Birnbaum's and component criticality importance are evaluated for each unit. These metrics are expressed in terms of magnitude of hazard incurred ($I_k^C(t) \Rightarrow I_k^C(t_{max}, H_S)$) to identify which components will most effect the reduction of risk. Additionally, another criticality metric is introduced which calculates criticality in terms of unit capability. This metric, 'component capability importance' (I_k^{CC}), provides an additional design perspective towards sizing a complex architecture.

These metrics are evaluated for both concept architecture in terms of all of the function/hazard relationships. Comparisons between these architectures in terms of system level and functional risk and component importance provide verification of the hypothesis.

7.1 Hazard Probability and Performance Risk

The initial measure employed to evaluate the architecture concepts is the risk associated with the provision of functions. As discussed in chapter five, system failure risk (R_{SF}) is calculated as the product of system failure probability (F) and the operational consequences of the failure.

$$\text{Risk} = \text{Probability} \times \text{Consequence}$$

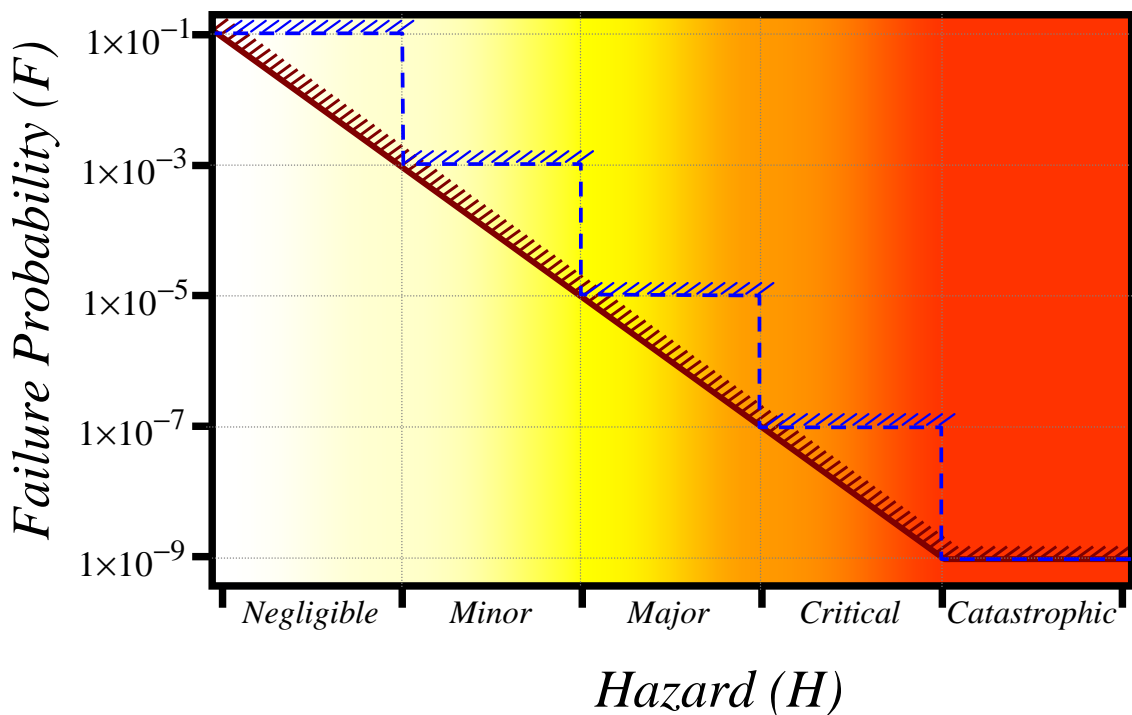


Figure 85: Hazard Probability Constraint

All consequences of the failure (economic, social, environmental, etc.) are distilled into a fixed probability constraint. Functional hazard assessment and preliminary system safety analysis define the severity of failures in terms of probability limits. More severe consequences are limited by lower failure probability limits. Traditional hazard constraints are applied in discrete stages. This takes the form of the dashed blue constraint in this figure 85. The hazard probability constraint used for this study is

illustrated by the red constraint in the figure. This constraint interpolates logarithmically between the discrete hazard constraints. The most stringent constraints act on catastrophic hazards (1×10^{-9}). The hazard level is expressed on a $[0,1]$ scale. Under this scale $0 \leq H_S \leq 0.2$ gives negligible hazards and $0.8 \leq H_S \leq 1$ gives catastrophic hazards.

$$R_{SF}(H_S) = \frac{F(H_S)}{F_{Lim}(H_S)} \quad (52)$$

The severity of consequences are reflected by the inverse of the failure probability constraint value ($F_{Lim}(H_S)$). Therefore, system failure risk (R_{SF}) is calculated by the ratio of system failure probability (F_S) to failure probability constraint (F_{Lim}), as given in equation 52. Both the system failure probability and the probability constraint vary with the magnitude of system level hazard incurred (H_S). The failure limit used for this study and illustrated in figure 85 is given by: $F_{Lim}(H_S) = \max [10^{-9}, 1 \times 10^{-(10 \cdot H_S + 1)}]$.

Two metrics are used to evaluate the cumulative risk associated with a given architecture. The first is the overall system failure risk (R_{SFo}). This metric is determined by considering the integral of the risk in terms of magnitude of system hazard as is given by equation 53. Feasible architecture design requires a cumulative overall risk values less than 1.

$$R_{SFo} = \int_{H_S=0}^{H_S=1} \frac{F(h)}{\max [10^{-9}, 1 \times 10^{-(10 \cdot h + 1)}]} dh \quad (53)$$

The second metric only considers undesirable risks. When the probability of failure exceeds the probability constraint design augmentation is required. Therefore, a single metric for undesirable design risk is obtained by equation 54.

$$R_{SFu} = \int_{H_S=0}^{H_S=1} -1 + \max \left[1, \frac{F(h)}{\max [10^{-9}, 1 \times 10^{-(10 \cdot h + 1)}]} \right] dh \quad (54)$$

The total amount of undesirable risk due to system failure metric (R_{SF_U}) is obtained by integrating risk deficiencies in terms of hazard. For regions where failure probability constraints are not violated the value of the integral yields zero undesirable risk. When constraints are violated the system risk integral is relative to the ratio of the failure probability to the constraint. This is made clear with analysis of the risk associated with the conventional architecture in table 36.

The architecture performance risk assessment is presented for each function/hazard relationship: takeoff, cruise, and linear and discrete assumptions. The first results column in this table gives the failure probability obtained with each load shedding optimization case. The second results column gives the risk associated with this performance. The third column gives the integral risk metrics.

From this table it becomes clear which mission segment introduces the most risk for the conventional architecture. The takeoff and cruise segments introduce total undesirable risks (R_{SF_U}) of 3.54 and 1.22 respectively. While it may be tempting at this point to eliminate the evaluation of load shedding for the cruise segment, additional information must be considered. While the risk is lower for this segment, one must consider which function loss is driving these hazards. This will be addressed in the next section.

These two metrics represent the effectiveness of an architecture in meeting continuous reliability constraints. Feasible architecture designs require a cumulative undesirable risk metric (R_{SF_U}) equal to zero. The preferred value for the cumulative overall risk metric (R_{SF_O}) is 1. The hazard probability relationship for an architecture with this R_{SF_O} equal to 1 and a R_{SF_U} equal to 0 would lie directly on the hazard probability constraint. Such an architecture would meet the reliability requirements and eliminate all overdesign for reliability.

Also notable from the charts in this tables is the fact that the total risk associated with an architecture (third and fourth row of table 36) is not always dominated by

Table 36: Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Func./Haz.	Hazard Probability ($F(H_S)$)	System Failure Risk ($R_{SF}(H_S)$)	Total Risk
Takeoff			$R_{SF_U} \cong 3.54$ $R_{SF_O} \cong 4.11$
Cruise			$R_{SF_U} \cong 1.22$ $R_{SF_O} \cong 1.75$
Linear Approx.			$R_{SF_U} \cong 4.05$ $R_{SF_O} \cong 4.60$
Step Approx.			$R_{SF_U} \cong 3.06 \times 10^4$ $R_{SF_O} \cong 3.06 \times 10^4$

the highest hazard considerations. Consider the system failure risk for takeoff; more risk is associated with minor and major hazards than for critical and catastrophic hazards for the conventional architecture. For this mission segment, non-catastrophic reliability constraints are more design critical for the current form of the conventional architecture. The risk measures for the function/hazard approximations both overestimate this risk. Allocating and evaluating load shedding using the linear approximation yields an undesirable risk equals 4.05. The step approximation dramatically overestimates the risk. This is due to the fact that very small deviations in functional performance is assumed to yield large hazard consequences. These comparisons illustrate the necessity to accurately express the function/hazard relationships. An overestimation of total risk leads to the oversizing of the architecture.

Risk analysis was repeated for the ‘more-electric’ architecture. The results are presented in table 37. Results are again presented for each function/hazard relationship used during load shedding optimization. Failure probability and risk are plotted in terms of hazard magnitude and the total risk metrics are given.

Similar to the conventional architecture the step approximation greatly overpredicts the total risk associated with this architecture for the same reasons discussed previously. In contrast, however, the takeoff and cruise segments yield fairly comparable risk values for the ‘more-electric’ architecture concept. It is also notable that the linear approximation underpredicts the risk associated with this architecture. Information provided by the linear approximation alone would lead to an architecture design which may not guarantee fulfillment of reliability requirements. This same approximation applied on the conventional architecture would lead to system overdesign. Approximations of the function/hazard relationships have dissimilar impact of system sizing for dissimilar architectures. The unique sources of this system risk is discussed in the next section in terms of independent functional hazards.

Table 37: Hazard Probability Assessment for the 'All-Electric' Vehicle Systems Architecture

Func./Haz.	Hazard Probability ($F(H_S)$)	System Failure Risk ($R_{SF}(H_S)$)	Total Risk
Takeoff			$R_{SF_U} \cong 2.86$ $R_{SF_O} \cong 3.28$
Cruise			$R_{SF_U} \cong 2.46$ $R_{SF_O} \cong 2.89$
Linear Approx.			$R_{SF_U} \cong 1.05$ $R_{SF_O} \cong 1.51$
Step Approx.			$R_{SF_U} \cong 1.51 \times 10^4$ $R_{SF_O} \cong 1.51 \times 10^4$

7.1.1 Function Specific Hazard Probability

The conventional and ‘more-electric’ architecture exhibit unique sources for system risk. The system level performance risk presented in the previous section is generated differently for dissimilar architecture concepts. Overall system level hazard is calculated as the maximum of the independent hazards associated with each system function ($H_S = \max [H_{F1}, H_{F2}, \dots]$). Each function presents its own associated risk. Differences in the criticality of the system level functions for each architecture concepts indicate disparate motives which drive design decisions.

In order to understand the drivers for system level reliability, a risk analysis is performed for each independent functional hazard. This analysis takes a similar form to the analysis performed on the overall hazard in the previous section. The functional sources of risks associated with the conventional architecture were compared for takeoff and cruise. Additionally, the results of the linear function/hazard relationship for the ‘more-electric’ architecture are compared with takeoff results.

Independent functional risk for the conventional architecture takeoff are given in table 38. The green and blue curve represent the hazard probabilities derived from the takeoff and cruise segment load shedding optimizations respectively. All functions, save the provision of 120VAC power, exhibit failure probabilities that exceed constraints. The loss of thrust, 28VDC power, and pneumatic air flow also contribute to undesirable risk. However, functional failure which introduces the most performance risk for the conventional architecture is the provision of hydraulic power.

The significant functional failures vary with mission segment due to variations in the function/hazard relationships for the vehicle systems architectures. Additionally, the relative significance of each functional failure varies with the magnitude of the hazard. Figure 86 gives the risk associated with each individual functional failure for the conventional architecture at takeoff and at cruise. Overall risk values over 1 indicate a breach of the reliability constraints.

Table 38: Takeoff and Cruise Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
Pneumatic <i>Takeoff</i> : $\begin{bmatrix} R_{FFU} \cong 0.37 \\ R_{FFO} \cong 0.75 \end{bmatrix}$ <i>Cruise</i> : $\begin{bmatrix} R_{FFU} = 0.21 \\ R_{FFO} \cong 0.61 \end{bmatrix}$		Elec. 120VAC <i>Takeoff</i> : $\begin{bmatrix} R_{FFU} = 0 \\ R_{FFO} \cong 0.01 \end{bmatrix}$ <i>Cruise</i> : $\begin{bmatrix} R_{FFU} = 0 \\ R_{FFO} \cong 0.01 \end{bmatrix}$	
Elec. 28VDC <i>Takeoff</i> : $\begin{bmatrix} R_{FFU} \cong 0.25 \\ R_{FFO} \cong 0.64 \end{bmatrix}$ <i>Cruise</i> : $\begin{bmatrix} R_{FFU} = 0.16 \\ R_{FFO} \cong 0.54 \end{bmatrix}$		Hydraulic <i>Takeoff</i> : $\begin{bmatrix} R_{FFU} \cong 3.07 \\ R_{FFO} \cong 3.59 \end{bmatrix}$ <i>Cruise</i> : $\begin{bmatrix} R_{FFU} = 0.57 \\ R_{FFO} \cong 0.92 \end{bmatrix}$	
Thrust <i>Takeoff</i> : $\begin{bmatrix} R_{FFU} \cong 0.18 \\ R_{FFO} \cong 0.48 \end{bmatrix}$ <i>Cruise</i> : $\begin{bmatrix} R_{FFU} = 0.42 \\ R_{FFO} \cong 0.72 \end{bmatrix}$			

Red Line: Hazard Probability Constraint
Green Line: Hazard Probability at Takeoff
Blue Line: Hazard Probability at Cruise

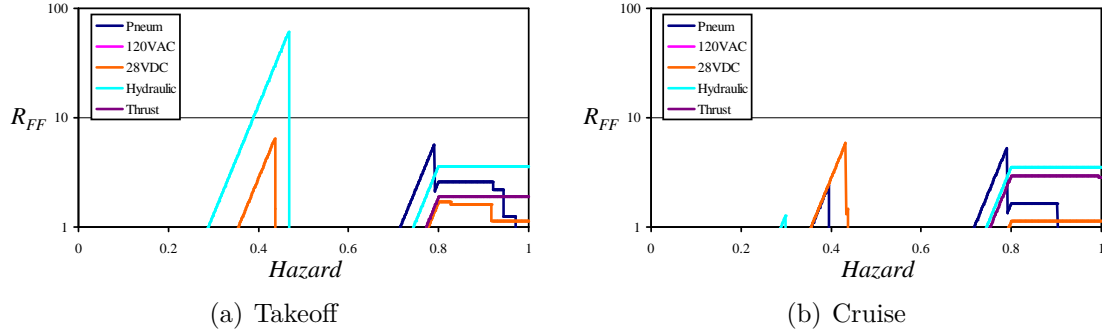


Figure 86: Comparisons of Risks Introduced by Functional Failures for the Conventional Architecture

As illustrated with these graphs, the provision of hydraulic fluid introduces the largest risk during the takeoff mission segment for minor ($0.2 \leq H_S < 0.4$) and major hazards ($0.4 \leq H_S < 0.6$). The risk associated with failures of larger magnitude is dominated by pneumatic and hydraulic hazards for both the cruise and takeoff mission segments. In contrast to takeoff, the risk associated with mid-range hazards is no longer dominated by the hydraulic system. With reductions in the criticality of thrust, the capability and reliability of shaft power at the AGB is transferred from the fuel pump to the hydraulic pump. Reductions in capability of the fuel system, engine, and AGB results in a lower impact on the provision of hydraulic power. Subsequent sections will discuss the unit level aspect of this failure state.

Takeoff functional risks for the ‘more-electric’ architecture are given in table 39. The risk for the takeoff objective function is given in green and the risk for the linear approximate objective function is given in blue.

The reduction in perceived risk obtained by assuming a linear relationship between function loss as hazard results from inaccuracies in defining the hazard associated with loss of thrust. The linear hazard approximation yields an underprediction of thrust risk for hazards of catastrophic and critical significance and overpredictions of thrust risk for hazards of major significance. The hazard probabilities for the other functions follow similar trends with minor deviations. Both risk associated with both

Table 39: Take-off and Linear Approx. Functional Hazard Probability Assessment for the ‘All-Electric’ Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
Pneumatic <i>Takeoff :</i> $\begin{bmatrix} R_{FFU} = 0 \\ R_{FFO} \cong 0.00 \end{bmatrix}$ <i>Lin.Approx. :</i> $\begin{bmatrix} R_{FFU} = 0 \\ R_{FFO} \cong 0.00 \end{bmatrix}$		Elec. 270VDC <i>Takeoff :</i> $\begin{bmatrix} R_{FFU} = 0 \\ R_{FFO} \cong 0.23 \end{bmatrix}$ <i>Lin.Approx. :</i> $\begin{bmatrix} R_{FFU} \cong 0.46 \\ R_{FFO} \cong 0.76 \end{bmatrix}$	
Elec. 28VDC <i>Takeoff :</i> $\begin{bmatrix} R_{FFU} \cong 0.56 \\ R_{FFO} \cong 0.91 \end{bmatrix}$ <i>Lin.Approx. :</i> $\begin{bmatrix} R_{FFU} \cong 0.85 \\ R_{FFO} \cong 1.17 \end{bmatrix}$		Thrust <i>Takeoff :</i> $\begin{bmatrix} R_{FFU} \cong 2.45 \\ R_{FFO} \cong 2.82 \end{bmatrix}$ <i>Lin.Approx. :</i> $\begin{bmatrix} R_{FFU} \cong 0.20 \\ R_{FFO} \cong 0.33 \end{bmatrix}$	

of the electrical functions slightly overpredict the risk for hazards of catastrophic significance. This is illustrated in with the functional failure graphs in figure 87.

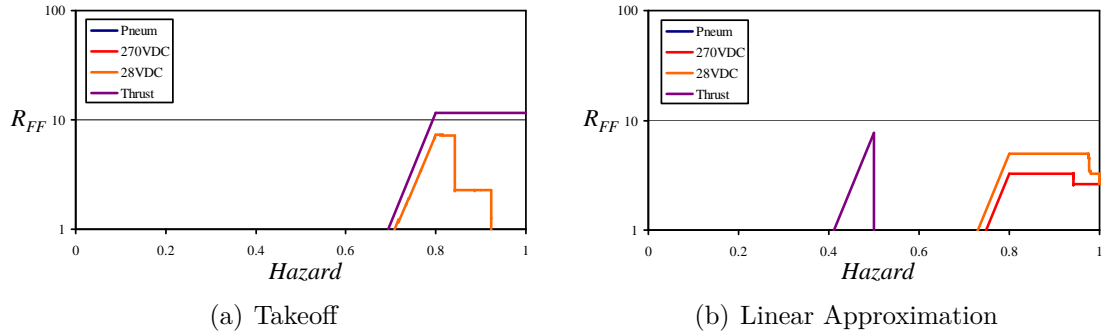


Figure 87: Comparison of Risks Introduced by Functional Failures for the ‘All-Electric’ Architecture

The linear approximation more accurately predicts the design issues associated with off-nominal performance better than the step hazard approximations. However, the application of inaccurate hazard estimates opens designers to potential problems. Assuming step hazards will lead to systems which are overdesigned but linear assumptions may lead to systems which are underdesigned. Leveraging the effects of load shedding on off-nominal requirements requires accurate identification of the function/hazard relationships.

Evident from continuous hazard probability analysis is the fact that unique architectures respond differently to failure. Critical functions, overall performance risk, and sensitivity to assumptions are emergent attributes of the architecture. With the two examples considered here, the single heuristic used to size the architectures presented in table 23 from the previous chapter is insufficient to capture all off-nominal requirements.

Additional insights into the implications of load shedding optimization can be obtained by considering all the hazard probabilities for the other functional hazard relationships. The risk attributes for all of the function/hazard relationships for both architectures are given in appendices I and J.

7.2 Hazard Correlation

Analysis performed in the previous section indicate that the ‘more-electric’ architecture, as sized according to the similar heuristic, does exhibit less performance risk for this embodiment of the ‘more-electric’ vehicle systems architecture than the conventional architecture. This result must not be overstated. It is only valid for the current embodiment of each architecture and does not indicate greater performance attributes. Weight, cost, and other metrics besides risk must also be considered. However, this advantageous risk performance occurs due to the ability of the ‘more-electric’ architecture to distribute failures among the system level functions. By so doing a general reduction in the severity of failure is achieved.

The metric used to characterize an architectures ability to shed loads is the sample correlation matrix of the functional hazards. Each unit level failure state for which load shedding optimization was performed represents an independent observation of system failure. Each case yields a vector, $h_F \in R^{p \times 1}$, indicating the level of hazard realized by each system function (p is the number of system level functions). The statistical relationship between system level functional hazards can be given by the correlation matrix. For a given number of independent samples (n), the Pearson product-moment correlation matrix for system hazards is given by equation 55. In this equation $h_{i,j}$ is the j -th sample result for the i -th function hazard. The i -th function failure sample mean, \bar{h}_i , is given by $\bar{h}_i = \frac{1}{n} \sum_{m=1}^n h_{i,m}$.

$$\rho[i, j] = \frac{\sum_{k=1}^n (h_{i,k} - \bar{h}_i) (h_{j,k} - \bar{h}_j)}{\sqrt{\sum_{k=1}^n (h_{i,k} - \bar{h}_i)^2 \sum_{k=1}^n (h_{j,k} - \bar{h}_j)^2}}, \forall (i, j) = [1, p] \quad (55)$$

The correlation matrix of the system level hazards expresses the ability of an architecture to distribute failure between the system functions. The min / max optimization means that the ideal system hazard level occurs when all hazards are equal.

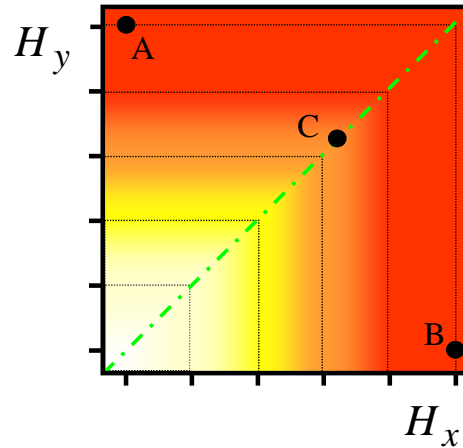


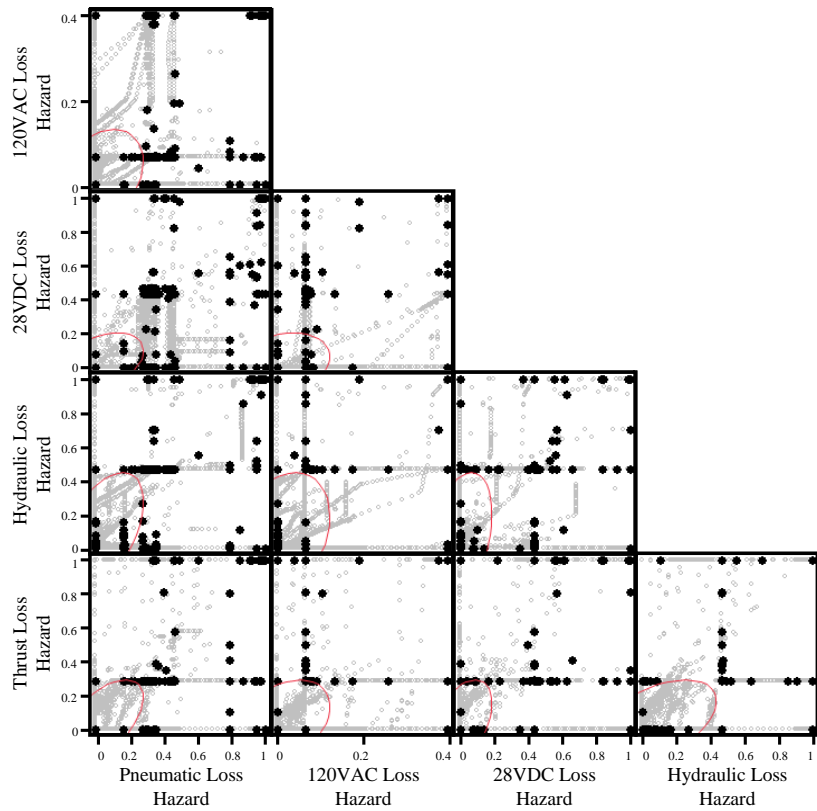
Figure 88: Correlation Between the Magnitude of System Level Functional Hazards

This is illustrated in figure 88. Each axis represents the magnitude of independent system level function hazards. Assume that flight control is provided exclusively by electrical actuation and utility actuation is provided exclusively by hydraulic actuation. The failure of either function yields catastrophic failures. For such an architecture, point *A* represents the consequences of electrical distribution failure. Point *B* represents hydraulic system failure. An architecture which applies segregated redundant actuation (hydraulic and electric) for these functions yields hazards of point *C* for either distribution system failure.

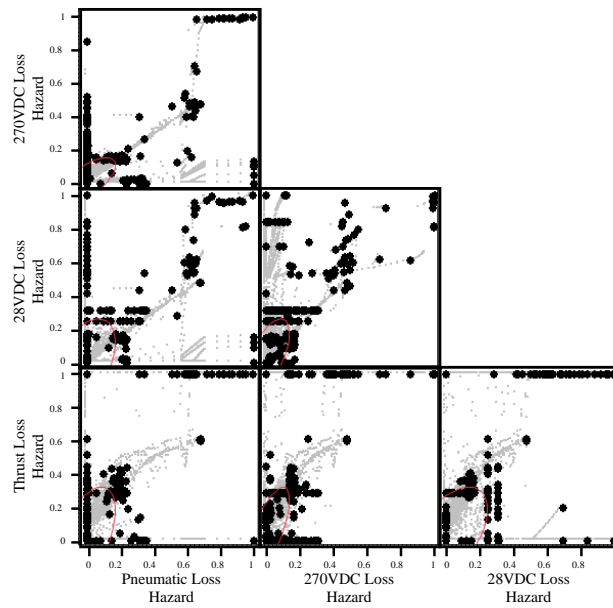
A perfectly shedding architecture would have a correlation matrix of ones. While this is infeasible for real architecture concepts, large positive correlation values indicate a greater ability to distribute load failures. The Euclidean Norm ($\|\rho\|_2$) of the correlation matrix can be used as a single metric characterization of the shedding flexibility of the architecture. The norm is limited on $1 \leq \|\rho\|_2 \leq N$, where N is the number of functions provided by the system. Larger values of the norm of the correlation matrix indicate higher flexibility to shed loads.

A multivariate plot for functional hazards for the conventional and ‘more-electric’ architectures optimized for the takeoff segment requirements is given in figure 89.

1120 failure combinations were evaluated for the conventional architecture and 665



(a) Conventional Architecture



(b) 'All-Electric' Architecture

Figure 89: Comparison of Functional Hazards with Load Shedding Optimization

for the ‘more-electric’. The disparity in the number of statistically significant failure cases is due to a reduced number of units for the ‘more-electric’ concept and the reliabilities of all of these units. The black markers in these two figures indicate 100% unit loss for each failure case. The gray markers corresponds to proportional failures for each failure case (0%, 1%, 2%, \dots , 100%). The axis of these plots represent the hazard associated with the loss of each function individual. Load shedding optimization balances the failure effect among 5 architecture functions for the conventional concept (provide pneumatic, 120VAC, 28VDC, hydraulic fluid, and thrust). The ‘more-electric’ concept requires optimization of the effects among 4 functions (provide pneumatic, 270VDC, 28VDC, and thrust).

Visual inspection of the hazard multivariates illustrates the effectiveness of load shedding optimization. As is expected, neither architecture balance the functional effects of failures perfectly. However, the multivariate of the ‘more-electric’ architecture displays clustering along the diagonal. Correlation information of the functional hazards are given in table 40. The hazard correlation matrices are given as well at the relative magnitude of the matrix norm. The indices of the correlation matrices correspond to loss of architecture functions. For the conventional architecture the indices, [1, 5], are in the order [Pneumatic Air Loss, 120VAC Loss, 28VDC Loss, Hydraulic Flow Loss, and Thrust Loss]. For the ‘more-electric’ architecture the indices, [1, 4], are in the order [Pneumatic Air Loss, 270VDC Loss, 28VDC Loss, and Thrust Loss]. The number of functions (N) for the conventional and ‘more-electric’ architectures are 4 and 3 respectively.

Higher correlations between functional hazards are seen for the ‘more-electric’ architecture. This indicates greater flexibility in the provision of load shedding. Hence, with larger magnitude correlation values, the ‘more-electric’ architecture concepts is more apt at load shedding.

Table 40: Functional Hazard Correlations for Takeoff Operation

	ρ	$\frac{\ \rho\ _2 - 1}{N - 1}$
Conventional	$\begin{bmatrix} 1 & 0.337 & 0.422 & 0.541 & 0.606 \\ 0.337 & 1 & 0.243 & 0.291 & 0.393 \\ 0.422 & 0.243 & 1 & 0.334 & 0.462 \\ 0.541 & 0.291 & 0.334 & 1 & 0.523 \\ 0.606 & 0.393 & 0.462 & 0.523 & 1 \end{bmatrix}$	0.565
'All-Electric'	$\begin{bmatrix} 1 & 0.677 & 0.398 & 0.498 \\ 0.677 & 1 & 0.641 & 0.748 \\ 0.398 & 0.641 & 1 & 0.538 \\ 0.498 & 0.748 & 0.538 & 1 \end{bmatrix}$	0.883

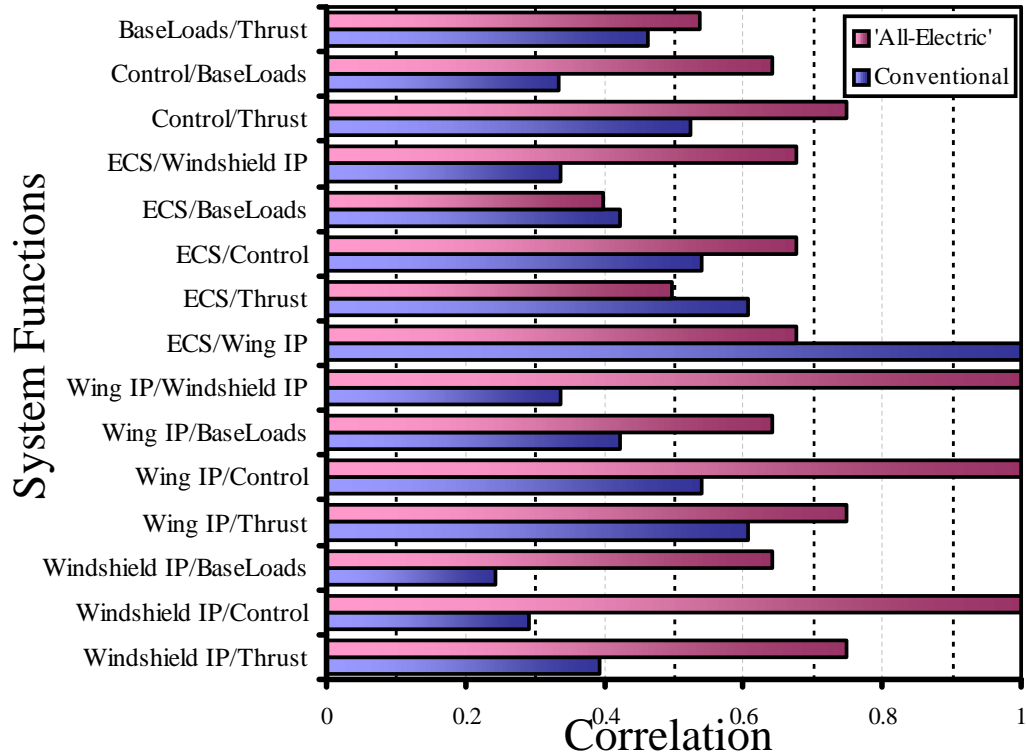


Figure 90: Correlation Between System Functions for Both the Conventional and 'All-Electric' Architectures

Extending these evaluations to the platform level functions supported by the architecture, failure correlations of all system functions are depicted in figure 90. In this chart, the vertical axis lists all combinations of system level functions. The bar charts indicate the magnitude of the correlation between system level functional failures. System functions provided by the same architecture function exhibit correlation values of 1. For example, the all electric architecture provides wing ice protection (Wing IP) and control actuation (Control) with the same power type (270VDC power). Assuming the ability to optimally allocate power external to the architecture, a loss in 270VDC power can be distributed to either function.

As is clear in this chart, the ‘more-electric’ architecture exhibits a greater ability than the conventional architecture to proportionally allocate failures between almost all platform level functions. The conventional architecture only exhibits higher correlation in the failure of environmental control and thrust, and between environment control and ice protection. This is logical due to the fact that engine bleed air is used as the air source for environment control and wing ice protection in conventional architectures.

Similar trends are evident for the other functional/hazard relationship objective functions. This data is given in appendices K and L. For both mission segments and the linear objective function approximation, the ‘more-electric’ architecture exhibits higher hazard correlation.

This measure does not in itself justify the selection of one architecture over another. Sizing and mission analysis must be performed to determine efficient fulfillment of performance requirements. This analysis, however, does give insight into the effect that architecture structure and composition has on the efficient fulfillment of reliability requirements.

7.3 Unit Level Importance

Component importance values identify the driving unit level design considerations which are used to augment system requirements. These metrics act in architecture optimization to determine what further variations must be made to remedy design infeasibility or reduce overdesign. Comparison of these metrics for the two concept architectures highlight the need to understand off-nominal operations and apply accurate objective functions to optimal load shedding.

It has been illustrated in the preceding sections that architecture design must consider an individual architectures ability to optimally allocate failure. The design importance of a function depends on the architecture. In this section, the relative emphasis placed on architecture units is explored.

Evaluating off-nominal requirements in terms of the magnitude of capability lost requires the augmentation of traditional component importance metrics. Unit failures must be evaluated on the spectrum of magnitude of loss. Comparing unit importance and hazard probability in terms of magnitude of loss help identify which components are most critical to the architecture performance and where focus should be placed in architecture refinement and redesign.

7.3.1 Reliability Based Unit Importance

Traditional component importance measures attempt to determine which unit reliability most greatly effect performance risk. This is done by identifying the sensitivity of the system level reliability to the reliability of individual units. The units whose reliabilities effect the system level reliability the greatest are deemed more important.

The first class of metrics describing component importance express this value in terms of a differential change in reliability. Birnbaum's importance measure describes the relative growth of system reliability(R_S) in terms of increases in the probability of some unit k failure (R_k). In so doing this metric assigns component importance in

terms of a partial derivative of system failure probability in terms of unit reliability (equation 56). As seen in this equation, the reliability derivative can also be expressed in terms of failure probability (F_S, F_k).

$$I_k^B(t) = \frac{\partial R_S(t)}{\partial R_k(t)} = \frac{\partial F_S(t)}{\partial F_k(t)} \quad (56)$$

Birnbaum's Importance metrics does not consider the magnitude of the reliability change with respect to the systems baseline reliability. This is remedied by 'Component Criticality Importance'. This metric corrects scales Birnbaum's importance by the ratio of unit unreliability (F_k) to system unreliability (F_S) as seen in equation 57.

$$I_k^C(t) = \frac{\partial R_S(t)}{\partial R_k(t)} \frac{F_k}{F_S} = I_k^B \frac{F_k}{F_S} \quad (57)$$

Both the Birnbaum's importance and 'component criticality importance' metrics are easily calculated by simple augmentation of the failure probability equation. All calculations made for this study assume that probability of failure is evaluated at $t = t_{max}$ for each unit as prescribed in table 35. Hereby, all importance metrics were calculated independent of time.

Both of these importance metrics assign importance in terms of unit reliability while assuming fixed unit capability. Performance risk, however, is not solely a function of failure probability. The magnitude of the hazard incurred with unit loss must also be considered. Considering failure probabilities in an analog fashion requires component criticality to be expressed in terms of failure magnitude. Therefore, much like system risk assessment discussed in the previous section, unit importance values must also be expressed in a cumulative fashion.

Cumulative importance of each component is obtained by integrating the importance in terms of the magnitude of the hazard incurred, as given in equation 58. For importance values which do not vary with the magnitude of hazard, the hazard integral yields the same result as the original importance equation. The empty

boxes in this expression indicate that cumulative importance can be calculated for all importance metric types.

$$\mathcal{I}_k^\square = \int_{H=0}^{H=1} I_k^\square(h) dh \quad (58)$$

Two different sets of bounds are applied to this integration. Overall component importance is determined by integrating on the bounds as indicated in equation 58 ($H = [0, 1]$). The second set of bounds considers only regions of the hazard continuum where probability constraints are breached. These regions exhibit undesirable system risk ($R_{SF} > 1$).

Figure 91 illustrates the bounds applied for the calculation of cumulative undesirable risk. The bottom plot illustrates overall system probability of failure (F_S) and the probability constraint (F_{Lim}) in terms of the magnitude of hazard compared for the takeoff requirements. The top plot gives the both the Birnbaum and “component criticality” importance of the APU in terms of the hazard magnitude. As indicated by the gray dashed lines, the bounds of the integral may be limited to regions where reliability requirements are not met.

An additional limitation to these traditional importance metrics is the inadequate capture of system risk. The basis for this importance is assigned directly to the reliability of the system. There is no consideration of the required reliability due to limitations on adverse effects. The loss of a given unit can be directly associated with the occurrence of consequences with associated hazard levels. These hazard levels are limited by different reliability constraints. Units with the same reliability based importance as calculated by the method above may differ in importance on the basis of risk. Risk importance is obtained by scaling importance values by risk $\left(\frac{F_S(H)}{F_{Lim}(H)} \right)$. This is by equation 59.

$${}^R I_k^\square(H) = \left[\frac{F_S(H)}{F_{Lim}(H)} \right] I_k^\square \quad (59)$$

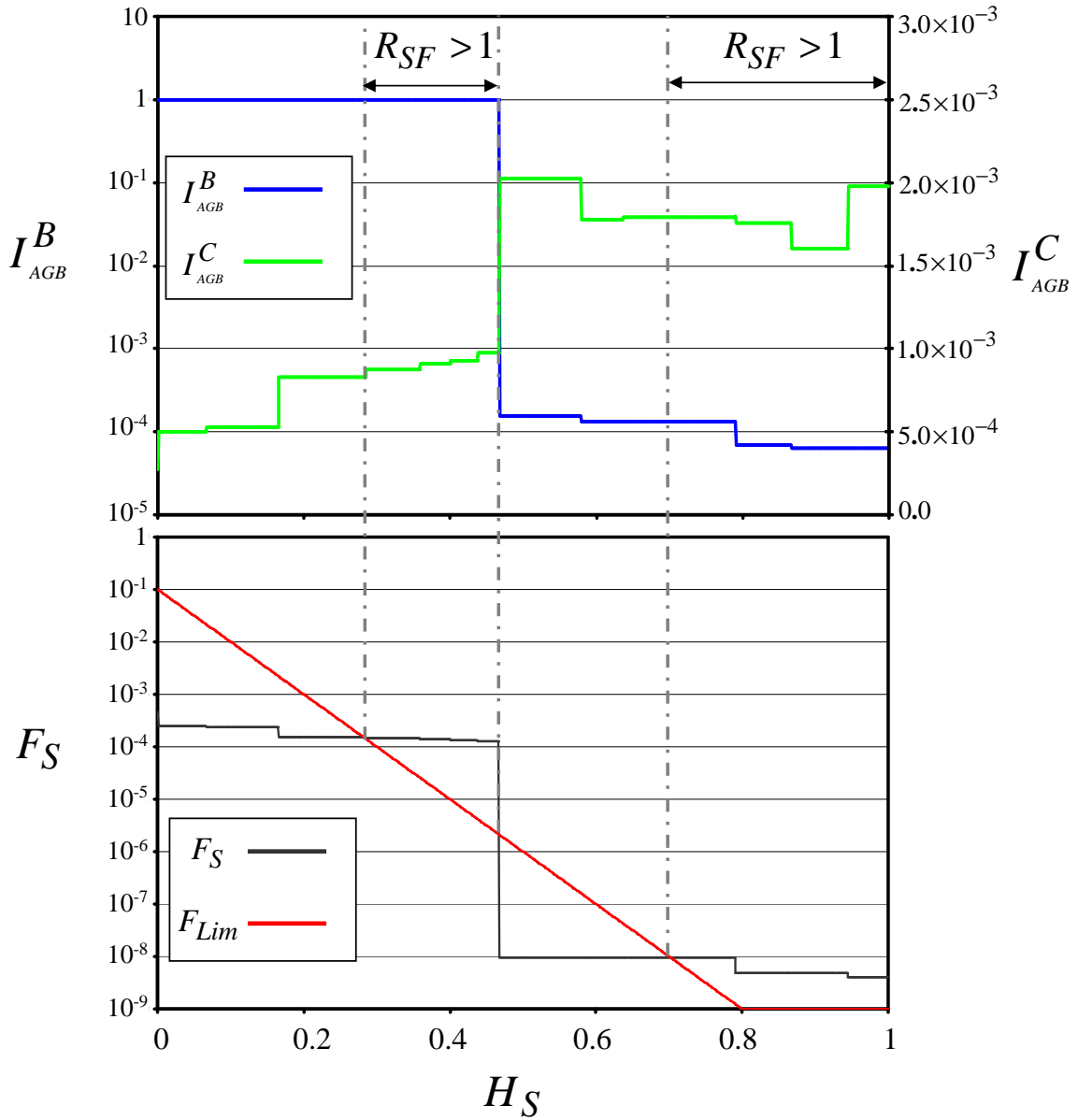


Figure 91: Bounds on the Integration Towards Cumulative Risk Importance Identification for the Accessory Gear Box in the Conventional Architecture for Takeoff Functional Hazards

Risk importance following Birnbaum's and "component criticality" importance are given by equations 60 and 61 respectively.

$$R I_k^B (H) = \left[\frac{F_S (H)}{F_{Lim} (H)} \right] \frac{\partial F_S (H)}{\partial F_k (H)} \quad (60)$$

$$R I_k^C (H) = \left[\frac{F_k (H)}{F_{Lim} (H)} \right] \frac{\partial F_S (t)}{\partial F_k (H)} \quad (61)$$

Figure 92 illustrates the effect of scaling the importance values by risk ($\frac{F_S}{F_{Lim}}$). This plot applies risk scaling to both the Birnbaum and "component criticality" importance values given in figure 91.

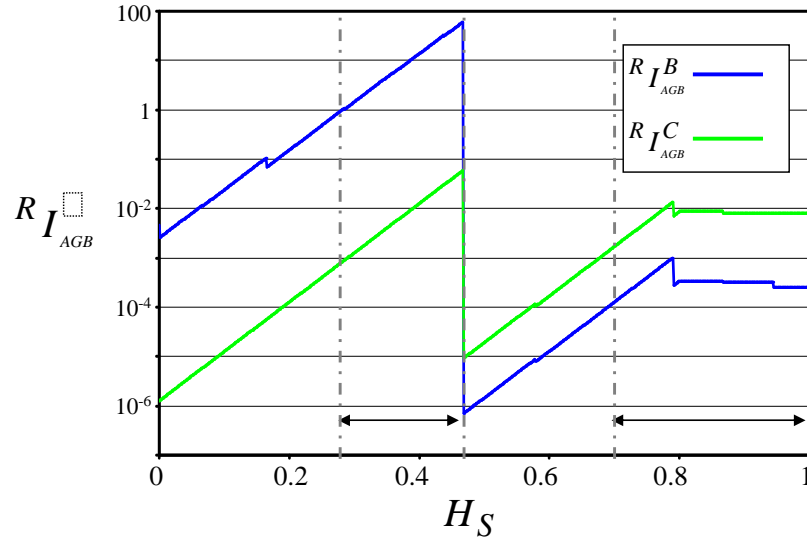


Figure 92: Risk Importance of the Accessory Gear Box in the Conventional Architecture for Takeoff Functional Hazards

Both importance values exhibit a similar trend. Considering equations 60 and 61; Birnbaum's risk based importance is requires scaling by system level risk and "component criticality" risk based importance is equivalent to Birnbaum's importance scaled by component failure risk. When system failure probability exceeds the probability of unit failure, Birnbaum's importance is larger. Conversely, when unit failure probability exceeds that of system failure probability, "component criticality importance"

is larger. The integral of both risk importance metrics will be integrated in terms of hazard to yield a cumulative unit level risk importance metrics.

All normalized results for Birnbaum and ‘component criticality’ importance are given in appendix M.

Tables 41 and 42 list the ten units whose risk based cumulative component criticality importance (${}^R\mathcal{I}_k^C$) drive design considerations for each architecture. These results are obtained using the reliability values given in table 35, in the previous chapter.

Table 41: Units of Highest Importance for the Conventional Architecture

Rank	Takeoff	Cruise	Linear Approximation
1	Fuel Systems	Fuel Systems	Fuel Systems
2	Fuel Pumps	Fuel Pumps	Fuel Pumps
3	Hydraulic Pumps	Hydraulic Pumps	Hydraulic Pumps
4	Engines	Fan Ducts	Engines
5	Fan Ducts	Engines	Hydraulic Systems
6	Precoolers	DC Generators	Precoolers
7	Hydraulic Systems	Precooler	Fan Ducts
8	DC Generators	DC Busses	DC Generators
9	DC Busses	Pneumatic Systems	DC Busses
10	AC Bus	AC Bus	AC Bus

Table 42: Units of Highest Importance for the ‘All-Electric’ Architecture

Rank	Takeoff	Cruise	Linear Approx.
1	Fuel Pumps	Fuel Pumps	Fuel Pumps
2	PCU’s	Low Speed 270V Gen’s	Low Speed 270V Gen’s
3	Low Speed 270V Gen’s	PCU’s	High Speed 270V Gen’s
4	Fuel Systems	Fuel Systems	Engines
5	Engines	High Speed 270V Gen’s	Fuel Systems
6	APU Fuel Pump	Engines	270V Busses
7	Ram Compressors	APU Fuel Pump	PCU’s
8	Ram Duct - ECS	Ram Compressors	AGB’s
9	High Speed 270V Gens	Ram Ducts	28V Busses
10	Ram Duct	28V Gen.	Ram Compressors

The component importance indicates how the individual components relate to the functional risk discussed in the previous chapter. Some of the results obtained

through this analysis can be inferred from unit reliability, functional risk, and design expertise. However, risk based cumulative component criticality importance gives a systematic metric which highlights where design changes (in terms of reliability) must be made to avoid overdesign.

From these results, the provision of fuel to the engines is of the highest relative importance for both architectures. For the conventional architecture, the fuel systems and fuel pumps exhibit the highest cumulative risk importance. For the ‘more-electric’ architecture, the fuel pumps hold the highest importance with the fuel systems ranked fourth and fifth. The largest effect on system risk can be achieved by augmenting the reliability of the fuel pumps on both architectures. This result is not surprising. With fuel as the sole source of energy in the system, the provision of fuel is correlated to the provision of all architecture level functions.

The engine sits at fourth and fifth in terms of relative importance for the conventional architecture, and fifth and sixth for the ‘more-electric’. While the engine plays a central role in both architectures, a larger initial reliability value for this unit (see table 35) places the engine lower on the list of importance.

Naturally, the provision of electrical power is of much higher importance for the ‘more-electric’ architecture. Electrical devices don’t appear in table 41 until rank 6 for cruise. The conventional architecture places emphasis on the provision of hydraulic flow and airflow towards independent support of control and ECS functions. However, the ‘more-electric’ architecture ranks DC to DC power converter units (PCU) and 270VDC generators as high as 2. This architecture places electrical devices into a more central role. Electrical power is used for all system level functions in addition to supporting the ram air compression and fuel distribution.

The results in this study highlight the discrepancies in design focus which occur when approximating the relationship between functional loss and hazard. The unit

of highest importance vary with changes in the load shedding optimization objective function. The linear function/hazard approximation performs admirably for the conventional architecture. The top ten unit criticality values obtained under this approximation coincide with those obtained from the takeoff and cruise cases. However, significant variation to unit importance occurs by using this approximation for the ‘more-electric’ architecture concept.

The first significant difference is the drop in importance of the DC to DC Power converter under the linear approximation. While ranked second and 3 in importance for the takeoff and cruise segments respectively, the PCU drops to rank 7. Application of this approximation would place less emphasis on the need for reliable power conversion.

Also notable with the linear function/hazard approximation for the ‘more-electric’ concept is the introduction of different units on the importance listings. Neither the higher fidelity takeoff or cruise objective functions place large importance on 270VDC distribution of the engine AGB’s. However, this lower fidelity objective function places 270VDC Busses at rank 6 and engine AGB’s at rank 8. Limited to results from the linear approximation, undue design emphasis would be placed on units which, in reality, play a less significant role in providing adequate reliability.

7.3.2 Capability Based Unit Importance

A third importance metric must be introduced when considering variation in risk in terms of magnitude of the component capability. Importance must be assigned to components in terms of the magnitude of the capability they provide.

Birnbaum’s and ‘component criticality’ importance address the impact of unit level reliability on system level risk. As discussed in the previous chapters, risk may also be mitigated by varying unit capabilities. Therefore, a new metric is introduced, ‘Component Capability Risk Importance,’ which assesses which components have the

greatest ability to affect changes to the analog hazard probability relationship at the system level. This importance calculation is given by equation 62. The variable C_k represents the functional capability of unit k .

$${}^R I_k^{CC}(H) = \frac{C_k}{F_{Lim}(H)} \frac{\partial F_S(H)}{\partial C_k} = C_k \frac{\partial}{\partial C_k} \left[\frac{F_S(H)}{F_{Lim}(H)} \right] \quad (62)$$

‘Component capability importance’ is the partial derivative of function or system hazard probability in terms of the percent change in component capability. Dividing this hazard value by the maximum allowable probability of failure for the given hazard value expresses this importance value in terms of a risk partial derivative.

The total cumulative component capability risk importance is obtained by integrating this risk value in terms of probability as illustrated in equation 63. Results for this study are obtained by setting the bounds of the integration for regions of undesirable risk as was discussed in the previous section.

$${}^R \mathcal{J}_k^{CC} = C_k \frac{\partial}{\partial C_k} \left[\int_H \frac{F_S(h)}{F_{Lim}(h)} dh \right] \quad (63)$$

Applying backward finite difference approximation to the differential yields equation 64.

$${}^R \mathcal{J}_k^{CC} = \int_H \frac{C_{k_0}}{\Delta C_k} \left[\frac{F_S(h; C_k = C_{k_0} + \Delta C_k) - F_S(h; C_k = C_{k_0})}{F_{Lim}(h)} \right] dh \quad (64)$$

Reliability based importance values are greater than zero. Increases in component failure probability increase the probability of failure. However, capability based importance values are negative. One would expect that increases in component capability would yield lower overall risk. Portions of the hazard vs. probability curve would be expected to shift to the left and this translation would, in effect, reduce the undesirable risk.

Additional risk is introduced to the system with reductions of component capability is illustrated in figure 93. This figure considers the importance of the AGB. A 10%

reduction in AGB capability was imposed while holding the α capability values fixed. The red line is the imposed probability constraint. The section of the graph shaded in blue represents the original system risk. The green shaded region represents the additional risk introduced in the system with 10% reduction in the capability of one accessory gear boxes.

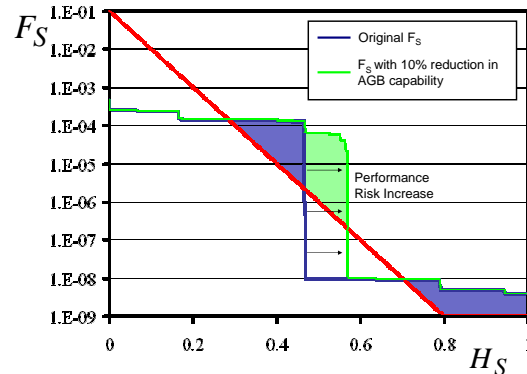


Figure 93: Shift in System Hazard Probability with 10% Reduction in Peak Steady State AGB Capability for Takeoff Requirements

As is apparent in this figure, reductions in unit level capability shift the hazard probability curve to the right. Higher severity loss occur with a higher probability. The unit with reduced capability can not accommodate for the failure at the same magnitude.

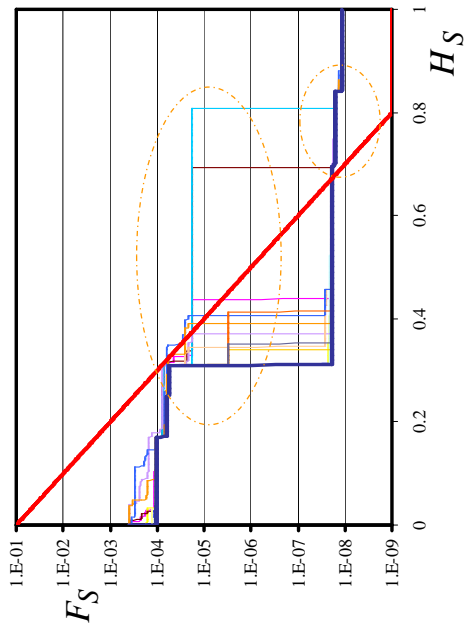
Defining the variation in system reliability in terms of unit capability introduces challenges not encountered with importance calculations. The importance factors introduced in the previous section can be obtained from closed form differentiation of the reliability equations. However, derivatives in terms of unit capability require the identification of the optimal allocation of unit failure with respect to the augmented system. Each differential change in the composition of the physical architecture may introduce variations in the load shedding optimization. Significant computational resources would be necessary to accurately identify these importance values in a timely fashion.

Approximations to these importance derivatives are made here by applying the existing failure allocation splines (α) and representing the partial derivatives and applying backward finite difference derivative approximations. However, the the results of this differentiation depends on the the step size used. The nature of finite difference derivative approximations desire small differentials. Additionally, the use of small differentials also ensure that the (α) approximations hold. However, large enough backward difference value are desired to capture increases in performance risk. This issue is illustrated in figure 94.

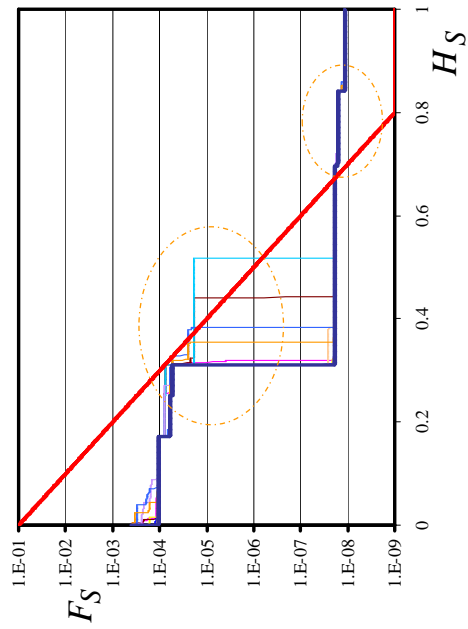
Figures 94 a through d represent the hazard probabilities for the ‘more-electric’ architecture during takeoff. The dark blue line represents the hazard probability for the baseline architecture. The other lines represent the hazard probabilities which are calculated using differential for all statistically significant unit failures of the ‘more-electric’ architecture at takeoff. These charts are meant to be illustrative of the differential increases in risk only. Numeric capability importance values are given later. Offsets in hazard probabilities are determined for different differentials in AGB capability. The backwards differentials used are 10%, 5%, 1%, and 0.01% changes in overall unit capabilities.

The shape of the hazard probability curve impacts the calculation of cumulative undesirable risk importance. This is illustrated in figures 94 a and b. The component capability importance value calculated with a large differential values are dominated by variation in hazard severity for failures which were originally of minor importance. When considering variations in undesirable risk only for the ‘more-electric’ hazard probability curve at takeoff, small differentials ($< 1\%$) do not consider variations in the originally minor hazards. These importance values are dominated by variations hazard magnitude of higher severity.

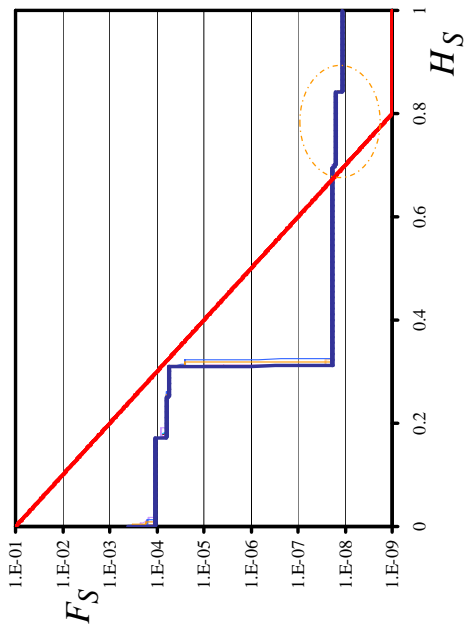
A compromise is necessary between the accuracy of the prescribed load shedding optimization for the failure state and the capture of significant hazard differences when



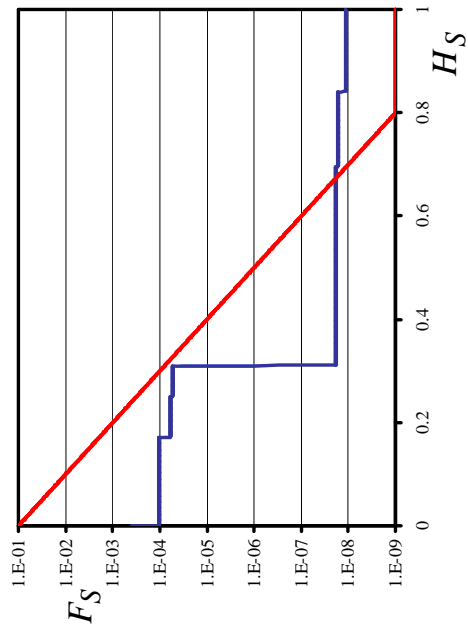
(a) -10% Capability Differential



(b) -5% Capability Differential



(c) -1% Capability Differential



(d) -0.1% Capability Differential

Figure 94: Cumulative Component Capability Risk Importance with Varying Backward Finite Difference Derivative Differentials

only considering variation in undesirable risk. Large differentials capture a larger ranges of risk variations but are subject to inaccurate failure allocation. Conversely, for this architecture, a differential value of 0.01 ensures sufficient closeness to the optimal failure allocation settings (α) but gives all undesirable risk importance values equal to 0.

Other issues encountered in the identification of component importance is the fact that statistical significance can not be used for eliminating the number of importance cases. Combinations of component will naturally yield higher importance values than single components. The benefits of increasing one components capability may not yield desired risk results without subsequent changes to components which provide for that components requirements. Increases in component capability criticality require targeted variations in component capabilities. For the purposes of this study, the focus is placed on improvements obtained by increasing the capability importance of individual units.

What further complicates the identification of component capability importance is the nature of system level continuous reliability assessment. The capability improvement or degradation of one unit does not in itself realize decreases in risk. Variations in system reliability result from decreasing the hazard associated with the failure of other system units. Capability performance, therefore, depends on the magnitude of capability provided by redundant systems. Each differential system augmentation requires the re-evaluation of all statistically significant failure cases.

Tables 43 and 44 list the most important units in terms of cumulative component capability risk importance for the conventional and 'more-electric architectures'. This list is generated by averaging the cumulative importance values from all four differential values (10%, 5%, 1%, and 0.1%). The importance values for each symmetric unit is calculated as the average importance for all symmetric units.

All cumulative component capability importance data for the conventional and

Table 43: Units of Highest Capability Importance for the Conventional Architecture

Rank	Takeoff	Cruise
1	Hydraulic Pumps	DC Busses
2	Hydraulic System	DC Gen's
3	AGB's	Ram Duct
4	DC Busses	Ram Heat Exchanger
5	DC Gen's	APU Bleed
6	Ram Heat Exchanger	Pneumatic System
7	APU Bleed	Engines Thrust
8	Engine Thrust	Hydraulic Pumps
9	Ram Duct	Fuel Systems
10	Fuel Systems	Hydraulic Systems

'more-electric' architectures is given in appendix N. This data includes both architectures, mission segments (takeoff and cruise), and four magnitudes of differential values.

Table 44: Units of Highest Capability Importance for the 'All-Electric' Architecture

Rank	Takeoff	Cruise
1	Engine Thrust	Engine Thrust
2	Low Speed 270VDC Gen's	PCU's
3	PCU's	Low Speed 270VDC Gen's
4	270VDC Busses	High Speed 270VDC Gen's
5	High Speed 270VDC Gen's	270VDC Busses
6	Ram Duct	Ram Duct
7	Fuel Systems	28VDC Bus
8	28VDC Busses	Ram Compressors
9	Ram Compressors	Pneumatic System
10	Pneumatic Systems	–

Compare these results with the results obtained using the reliability based cumulative 'component criticality importance' (tables 41 and 42). Analysis of cumulative 'component capability importance' (tables 43 and 44) places emphasis on a different set of technologies in terms of their performance risk. For the conventional architecture fuel systems held the highest importance on the basis of vertical impact on risk in terms of probability. In terms of horizontal impact on risk, fuel systems are de-emphasized for 'component capability importance'. The APU bleed system, engine

accessory gear boxes, and DC electrical systems receive higher importance values. Hydraulic systems remain highly important following both analysis.

The provision of fuel is also not of highest importance for the ‘more-electric’ architecture in terms of component capability. Higher import is placed on engine thrust capability.

These results provide insight into the architecture augmentations which can take place to optimize the architecture while avoiding undesirable risk. While fuel has a large impact on risk in terms of reliability, sufficient capability is already provided. Reductions in capability cost very little in terms of risk. It may be advantageous to decrease potential oversizing of the fuel systems and improve its reliability.

The inferences from these results should also not be overstated. Derivatives used for ‘component capability importance’ are estimated using the backward finite difference method. Therefore, the derivative is considering reductions in available performance by removal of unit capability. While these results may be accurate, they do not adequately reflect the ability to improve system performance.

Each unit plays a role within the context of the system. While reductions in unit capability may reduce system performance, increases in unit capability do not necessarily infer similar improvements. Reducing the capability of the AGB will decrease the amount of shaft power available for customer loads and engine auxiliaries. In consequence, the system may exhibit higher performance risk. However, increasing the AGB capability does not guarantee performance improvement. The system level performance improvement must consider the capability of the auxiliary devices. While higher shaft power may be available, higher generator capability must also be made available to yield system level improvements. While identification of degradation is straight forward, the systematic identification of the combined improvements necessary to yield reductions in performance risk is a matter for ancillary research opportunities.

CHAPTER VIII

RESULTS SUMMARY

The ability to ensure accurate allocation of requirements is critical during vehicle systems architecture exploratory design. Fair comparisons between architecture concepts demands that the application of requirements does not bias architecture trades. Each architecture concept yields unique sets of requirements which emerge due to complex unit level behavioral attributes. As such, systems architecture must capture off-nominal operational requirements in the context of each specific architecture concept.

The objective was states as follows, “Provide systematic risk and reliability based means for the identification of off-nominal operational requirements which can be rapidly implemented during concept architecture trades.” It was asserted that continuous function hazard assessment and systematic load shedding optimization provided for this capability. Quantitative evidence to this effect was gathered by implementing an analog extension to system safety analysis. This required the development of several new safety and reliability metrics.

The case studies performed in the previous chapter illustrates the benefits of accurate load shedding optimization. It also introduces a number of tools and metrics which enable a more rigorous and systematic exploration and assessment of off-nominal performance.

Case study results provide evidence towards the justification of the hypothesis. Experiments were executed which compared changes in design conclusions arising through variations in the system of interest and in the form of the function/hazard

relationship. It was made evident in this chapter that off-nominal system requirements interact with architecture in unique ways. Additionally, it was illustrated that inaccurate design emphasis is generated through inaccurate representations of functional hazards.

8.1 Hypothesis 1 Validation

Hypothesis 1: *Optimizing load shedding strategies yields more accurate predictions of unit level requirements than heuristically defined performance degradation during the exploratory design of revolutionary vehicle systems architectures.*

Applying load shedding optimization and performing analog system safety assessment provide information not available when sizing systems with predefined heuristics. Comparing the results obtained from off-nominal performance analysis of two distinct architecture concept provides validation for this hypothesis. Although the architectures were sized following the same heuristics, the performance risk associated with each architecture was shown to be unique. Quantitative results are illustrated in tables 36 and 37.

The application of the engine out sizing heuristic is insufficient to guarantee the fulfillment of risk requirements. While both architectures exhibit undesirable risk (R_{SFV}), the magnitude of this risk varies between concepts. For takeoff and cruise, the conventional architecture has an undesirable risk magnitude of 3.54 and 1.16. The cumulative undesirable risks for the ‘more-electric’ architecture are 2.44 and 2.47. The hazard severity levels which introduces these risks vary between architecture concepts. While the risk associated with the ‘more-electric’ concept is dominated by catastrophic losses, the probability of major and minor failures introduce a large amount of undesirable risk for the conventional architecture. This illustrates the unique way in which hazard characterizations relate to architecture concepts

The sources of this performance risk vary due to differences in the architecture

concept. Each unique architecture places different emphasis on function and unit design. This is evidenced by considering the hazard probability relationships. The fulfillment of catastrophic requirements does not always pose the highest performance risk. The magnitude of risk associated with system functions varies in terms of the magnitude of the hazard incurred.

Each unique architecture concept allocates risk to the provision of functions differently. The hydraulic and pneumatic requirements drive the magnitude of undesirable risk for the conventional architecture during takeoff. Providing 28VDC power, hydraulic fluid flow, and pneumatic air flow dominate performance risk for the conventional architecture during cruise. Different functions dominate the risk attributes of the ‘more-electric’ architecture. The provision of thrust introduces the most risk during takeoff and cruise for the ‘more-electric’ concept.

The smaller amount of risk associated with the ‘more-electric’ architecture compared to the conventional architecture is due in part to this architecture’s ability to distribute failures among the system functionalities. A higher correlation between functional hazards indicates this ability.

The definition of sizing critical requirements must take off-nominal operations into account. Applying load shedding optimization and assessing off-nominal performance as illustrated in this chapter provides increased justification for further architecture design. Accurate sizing warrants a systematic method for capturing off-nominal operational requirements. The metrics used to compare the off-design performance for these architecture were developed towards this purpose.

8.2 Hypothesis 2 Validation

Hypothesis 2: *Assumptions regarding the relationship between function loss and hazard severity employed during traditional Functional Hazard Assessment bias architecture design and lead to inaccurate estimation of unit level requirements.*

Testing the second hypothesis required the identification of issues which arise when approximating the function/hazard relationship. Therefore, load shedding optimization was performed under two different operating conditions and two function/hazard approximations (linear and step hazard characterizations). Optimal load shedding was performed and hazard probability was calculated for both architectures with respect to all of these hazard objective functions.

Obvious limitations were encountered when performing load shedding optimization with the step function/hazard relationships. This pseudo-step relationship between loss and hazard attempts to replicate the amount of information made available during traditional functional hazard assessment. Applying this assumption to conceptual design would dramatically overdesign the architecture.

Due to the dramatic overprediction of risk which occurs by applying this pseudo-step hazard characterization applying a linear relationship between loss and hazard more aptly illustrates the impact of applying inaccurate hazard assumptions. A linear relationship between loss percentage and hazard also yielded undesirable results. This assumption overpredicts the risk associated with the conventional architecture and underpredicts the risk associated with the ‘more-electric’ architecture. Applying this assumption does not guarantee adequate capture of off-nominal operational requirements.

General assumptions regarding the function/hazard relationship also create a false sense of importance for designers. The higher fidelity objective function indicates that the risk associated with thrust requirements dominate all other functions for the ‘more-electric’ architecture. However, the linear hazard approximation sees higher risk associated with the provision of 28VDC electrical power and pneumatic air flow.

It was also observed that component importance values are sensitive to the fidelity of the function/hazard relationship. By varying the functional sources of performance

risk, component importance values change. Therefore, inaccuracies in the hazard objective functions can misplace design emphasis in terms of unit requirements. This was observed by considering the ranking of the units in term of their importance values. Applying the linear approximation for the ‘more-electric’ architecture assigns greater importance to some units than is assigned with the higher fidelity function/hazard relationships.

CHAPTER IX

CONCLUDING REMARKS

The challenges arising from the implementation and integration of electrical technologies in the aircraft subsystem architecture is comparable to the revolution necessitated at the advent of the turbojet era. Potential order of magnitude changes in power demand on military and commercial platforms challenges the historically adopted methods for aircraft subsystem definition. Additionally, with current advances in system-level technologies and the outsourcing of technology development, architecture innovation and integration have become driving differentiators between competing aircraft concepts.

Revolutionary aircraft systems architectures promise benefits over incremental improvements achieved through technology insertion and system adaptation or evolution. However, changes to the fundamental architecture of aircraft subsystems introduce unique challenges in the definition and allocation of sizing critical unit and platform level requirements. As discussed in the second chapter, the paradigm of aircraft vehicle systems architecture design is changing due to the complexity introduced by increased electrical power demands and propulsion efficiency.

As changes are made to the complex vehicle systems architectures, additional effort must be applied in the identification and management of emergent requirements. Generally accepted rules of thumb concerning the relationship between aircraft capabilities and system attributes and performance may not be legitimately applied.

The overarching objective for this thesis is the development of tools and techniques which systemically identify these emergent requirements during concept architecture validation. The tools and methods developed here are intended to be implemented

early in the exploratory design process. Therefore, modeling tools must be flexible to potential architecture alternatives. Additionally, results must be quantifiable and provide insight towards architecture requirement definition.

This broad goal encompasses many architecture requirements and was refined to a manageable level. Time, operation, and safety/reliability dependence are three behavioral sources of architecture complexity. These three dimensions of behavioral complexity lead to emergent off-nominal requirements. The traditional heuristic nature of defining sizing critical load-shedding strategies and operating modes could potentially under- or over-predict unit level requirements.

Sizing critical performance requirements are infrequently derived from normal operating conditions but rather emerge from responses to system failures or off-nominal operating states. During the early stages of conceptual architecting, responses to exceptional courses of events are often defined anecdotally and heuristically. However, optimal implementation of revolutionary concepts require architecture specific load shedding strategies in response to system failures. Fair comparisons between architecture concepts must involve the identification of off-nominal performance requirements unique to each individual concept.

The objective was refined to developing a method for identifying optimal deployment of a systems capabilities during these degraded system and operational states. This method is necessary to evaluate the actual benefits achieved by adopting a revolutionary architecture concept.

Two hypotheses were posed in this thesis which consider the impact of implementing load shedding optimization during exploratory design. The first hypothesis expresses the needed for identifying architecture specific load shedding strategies for accurate prediction of unit level requirements. This in turn would ensure fair comparison. Without implementing such a method, system architects deploy requirements in a manner which biases solutions towards the status quo. Therefore, this work begins

to enable more accurate evaluation of non-traditional architecture concepts early in the exploratory design phase.

The second hypothesis considers the effect of inaccuracy in the defined relationship between functional fulfillment and hazard. Traditional Functional Hazard Assessment and other system safety analysis tools make fundamental assumptions regarding failure states. Expressing the function/hazard relationship in a continuous fashion enables accurate estimation of the impact of unit failures.

The case studies performed in this thesis illustrate the impact of optimal load shedding during the assignment of system level requirements to the unit level. Load shedding strategies were shown to be architecture specific. Additionally, the accuracy to which this load shedding optimization is performed was shown to greatly impact design conclusions.

These advantages come at a some cost. Structuring the architecture models, modeling unit capability transfer functions, and executing load shedding optimization for all statistically significant failure case pose difficulties for implementation of SONOMA during architecture expository design. With increased architecture size or decreases in component reliability, the number of statistically significant failure scenarios greatly increases. Load shedding optimization must then be performed for each failure case. Depending on the number of allocation variables and the computational cost for unit transfer function the time and resources available during conceptual design complete performance of analog SSA may be infeasible.

The primary objective of this thesis was the development of tools and techniques which systematically identify architecture specific emergent requirements for architecture validation. While work is still necessary for implementing these methods in the system optimization and design process, the methods and frameworks implemented here provide a structured and flexible means for the elicitation of architecture specific

requirements during hazard probability analysis. An extension of system reliability evaluation tools was required to address the operational consequences of partial function loss.

9.1 Significant Contributions

The first significant contribution from this thesis is the systematic structuring of load shedding optimization to be implemented during exploratory design. Traditional architecture sizing apply heuristic relationships regarding the unit level requirements and the impact of unit loss on system functionality. In contrast, the approach taken here directly identifies the most advantageous flow of capability between system units to minimize operational hazards. This analysis was based on the functional dependencies between these units.

The optimization process is given by equation 15 from chapter five and the algorithm used is given in appendices G and H.

$$\begin{array}{l|l}
 \text{Min:} & \text{Operational Hazard} = H(\mathbf{X}_\infty) \\
 \left[\begin{array}{c} \alpha_{x_1, y_1} \\ \alpha_{x_2, y_2} \\ \alpha_{x_3, y_3} \\ \vdots \end{array} \right] & s.t.: \quad \sum_{j=1, i \neq j}^n \alpha_{i,j} = 1, \quad \forall i \in \mathbf{C} \\
 & \quad \quad \quad \alpha_{i,j} \geq 0, \quad \forall i, j
 \end{array}$$

Where: $\mathbf{X}_{i+1} = f([\mathbf{A}] \times \min(\mathbf{X}_i, \mathbf{K}_i), \mathbf{Op})$

In order to take advantage of the results obtained by load shedding optimization, or optimal failure allocation, both hazard assessment and system safety analysis are required to be developed as continuous functions.

$$\text{Hazard}(t) = h[X, \tau, Op(t)] \tag{65}$$

The second significant contribution presented in this thesis is the extension of traditional functional hazard analysis and system safety analysis to consider the magnitude of unit and function loss when assessing an architecture. System level hazards

are determined as functions of system capabilities (X), failure duration (τ), and the operating conditions (Op) as was illustrated with equation 9.

Function/hazard relationships can be defined heuristically, be derived from certification and flight safety requirements, or be determined by system level performance analysis. Replacing discrete hazard constraints on predefined unit failures with continuous hazard loss functions requires reliability to be assessed in a continuous fashion. This is achieved by identifying all statistically significant failure states and evaluating the probability and hazard level associated with each failure as is discussed in appendix D.

The last contributions provided by this work are the tools and metrics used to evaluate and compare the off-nominal functional performance of complex architectures. The metrics introduced in this thesis are outlined in table 45.

Table 45: Continuous Off-Nominal Architecture Performance Metrics

Symbol	Name
$\frac{F_S(H)}{F_{Lim}(H)}$	Continuous System Risk
R_{SF_O}	Cumulative Overall Risk
R_{SF_U}	Cumulative Undesirable Risk
$[\rho], \ \rho\ _2$	Functional Hazard Correlation
$\frac{F_S(H)}{F_{Lim}(H)} \frac{\partial F_S(H)}{\partial F_k(H)}$	Risk Scaled Birnbaum's Importance
$\frac{F_k(H)}{F_{Lim}(H)} \frac{\partial F_S(H)}{\partial F_k(H)}$	Risk Scaled 'Component Criticality Importance'
$\frac{C_k}{F_{Lim}(H)} \frac{\partial F_S(H)}{\partial C_k}$	Component Capability Importance
${}^R\mathcal{I}_k^\square = \int_H {}^R I_k^\square(h) dh$	Cumulative Risk Importance

The first tool used to compare off-nominal performance is the comparison of continuous hazard probability. This tool indicates which functions introduce the highest performance risk in terms of the failure probability constraints. Additionally, this tool indicates what magnitude of hazard encounters the highest risk. The cumulative overall and undesirable risk (R_{SF_O} and R_{SF_U}) are used to quantify the total risk

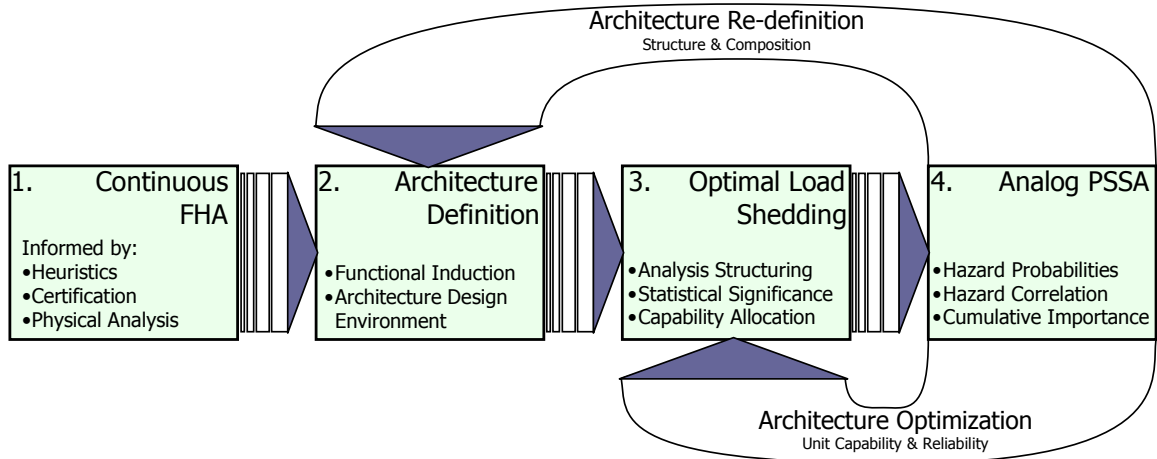


Figure 95: Process Used for Integrating Emergent Operational Requirements During Architecture Design, **SONOMA**

associated with off-nominal performance.

An architecture’s ability to distribute failures among its functions is measured by the correlation of functional hazards. Architectures which exhibit larger values of functional hazard correlation provide greater flexibility in terms of load shedding. Correlation values of 1 indicate an ability to ideally distribute failures between functions. The Euclidean Norm of the correlation matrix provides a single value metric to compare between architecture concepts.

The last set of metrics introduced to identify off-nominal architecture requirements are the cumulative risk based importance values. The traditional importance values are given as partial differentials of system failure probability in terms of unit failure probability. The new cumulative risk importance metrics are generated by integrating the product of the traditional importance value and system risk in terms of hazard. Additional importance metrics are also introduced which consider the partial differential of system risk in terms of the differential changes in unit capability.

The combined contribution of all of these tools is a process illustrated in figures 51 and 95. The SONOMA process is used to identify the off-nominal performance of an architecture and make recommendations for future architecture refinement. It

identifies over- and under- designed units and identifies the most stringent functional requirements. This analysis considers unique features of the architecture concept and allows for the tailoring of requirements in this context.

Systematizing the process for identifying off-nominal performance supports the objective of this thesis. The unit level requirements are emergent and architecture specific. In order to justify architecture selection, system sizing and performance analysis must take these considerations into account. This in turn supports the ability to more quickly explore the vehicle systems design space with greater confidence.

9.2 Ancillary Research Opportunities

The work presented here introduced multiple potential future research opportunities. These opportunities were introduced in context within this document but are outlined here for convenience.

As was discussed in the methods chapter, the impact of a failure depends on both the magnitude and duration of a given failure. The test cases executed for this thesis only considered reductions of unit capabilities of indefinite duration. Further effort is required to capture the effect of failure duration on system hazards. Additionally, this work also did not consider undesirable increases in unit and system capability. Extension of this analysis towards these ends provides opportunities for further architecting research. It was shown in this work that assuming a pseudo-step loss/hazard relationship greatly overpredicts system risk for both architectures. Additionally, it was shown that the linear assumption may over or underpredict risk depending on the structure and composition of the system. If approximations of the loss/hazard relationship are required additional research is necessary to be able to identify the appropriate structure of this approximation for the comparison of complex systems.

A second extension to this work would be the reconciliation of the potentially complex nature of system units. Characterizing the hazard probability space in this

thesis was accomplished by assuming a constant relationships between unit failure magnitude and failure probability. However, each unit can in its own right be considered a complex system with internal redundancies. Therefore, the failure probability of complex unit exhibits a tiered structure in terms of capability loss. As discussed in the methods chapter, this presents challenges in determining the probability of given magnitudes of system failures. Allowing units to exhibit continuous or multi-tiered failure probabilities would required a finer sampling of the failure space and a means for estimating the probability of failures of a given hazard magnitude for combined unit failures.

This thesis comments on how off-nominal performance considerations would potentially impact further design refinement. However, closing the design loop in terms of architecture attribute optimization was not developed in full. A system level cost or utility function for an aircraft architecture must consider the impact of unit design capability (*Cap*), unit reliability (Weibull parameters α and β), and maintenance scheduling (*MTTR*) on overall platform level architecture efficiency and performance. These decisions are informed by the metrics defined in this thesis and constrained by allowable system risk.

$$\begin{array}{c|c}
 \text{Min:} & \text{Cost} = f(\mathbf{Cap}, \eta, \beta, \mathbf{MTTR}) \\
 \hline
 \begin{array}{c} \mathbf{Cap} \\ \eta \\ \beta \\ \mathbf{MTTR} \end{array} & \begin{array}{l} s.t.: \\ y_i - H_{Lim}(x_i) \leq 0 \end{array} \\
 \hline
 \end{array}$$

Where: $x_i = f_{x_i}(\mathbf{Cap})$ and $y_i = f_{y_i}(\eta, \beta, \mathbf{MTTR})$

Closing the design loop requires efficient evaluation of optimal load shedding. This introduces additional ancillary research opportunities. Further improvements towards systematic implementation of off-nominal requirements may require the development of optimization methods tailored to expedite the identification of optimal capability allocation. Identifying off-nominal operational requirements may also be accelerate

by developing a means for recognizing trends in unit and system failure relationships. These trends may relate to the system structure and composition, or system relationships which are not based on functional dependencies. At the same time, improvements may be achieved through determining how frequently load shedding optimization must play a role in exploratory design.

The final recognized ancillary research opportunity is the extension of the functional relationships between system units. The work presented in this thesis assigned each allocation variable, α_i , to the fulfillment of a single functional capability. However, it was discussed that each functional capability must be decomposed into different characteristics (e.g. the function to provide airflow is expressed in terms of mass flow rate, pressure, and temperature). Under failure conditions, some units, like the environment control system, may be able to reduce the impact of failure by augmenting the functional capability characteristics. For the ECS system, the amount of mass flow may be increased if the air temperature is allowed to increase or decrease. The hazard associated with higher or lower cabin inflow temperatures is weighed in relation to the hazard associated with reductions in mass flow. In this case the trade is not between functional capabilities, but how a single functional capability is provided.

APPENDIX A

SCENARIO BASED STRATEGIC PLANNING AND HUMAN-COMPUTER INTERACTION

Strategic planning is primarily interested in scenarios as tools to assist in forecasting and contingency planning. Managers utilize scenarios to capture a spectrum of possible situations which must could be encountered. Kahn describes these scenarios as “future history [159].” Here scenario based design is used for structured imagination intended to avoid underpredicting and overpredicting the requirements during the decision making process. This is illustrated in figure 96. Schoenmaker illustrates strategic planning by the incredulity with which the idea of air strikes on naval ships was handle in the early 1900’s and by Royal Dutch/Shell’s preparations for the oil crisis in the 1970’s [260].

The goal of scenarios in strategic planning is to determine a course of action during “what-if” situations [113]. While this typically occurs at an organization level, methods for determining similar considerations at the system and technology will be discussed with off-nominal sizing cases identification.

Human-Computer Interaction (HCI) places the user at the center of the design focal point. While not discussed formally as dedicated processes until the mid 80’s [113], scenario based design techniques play an important role in HCI system illustration, design/redesign, and evaluation [38]. Examples of development in HCI are direct manipulation of graphical objects, the mouse, windows, text editing, hypertext, and gesture recognition [216]. Such studies require an understanding of human factors in relation to a system under specific conditions. Kuutti writes:

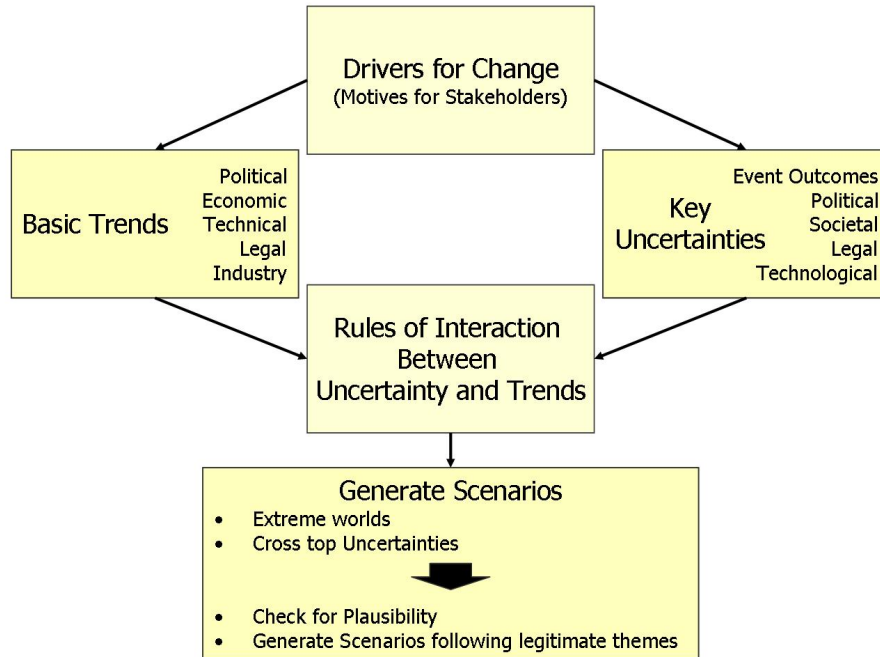


Figure 96: Schoemaker’s Process for Scenario Development in Strategic Planning [260]

“It is necessary to delineate the system and describe it by the services it is giving to users, but because the system will get its meaning from the situation in which it will be user, it is also necessary to describe the context as well [181].”

Illustrative scenario based design processes are creative in nature. HCI uses scenario techniques to describe the use and usability of future computer systems. Similarly to strategic planning, HCI uses scenarios to envisage future means in which human’s interact with a computer and provides rationale for the pursuit of specific technologies or design strategies.

The second use for scenarios, design/redesign, takes a detailed approach in determining the specific interface tools, hardware, and software are necessary to interact with external “human processors [39].” Functional specification are derived following scenario descriptions [38]. Some research goes to the extent of modeling the user as an

external processor that receives information from the computer, determines proper action, and execute pursuit appropriate results [39]. This aids in the definition of functional specifications what happens when users take specific action.

In regard to HCI evaluation, the aerospace community benefits from relative standardization of aircraft controls. Much research and development towards designing and analyzing pilot and operator control interfaces in terms of the workload required, controllability, and other human factors. Since the late 60's and early 70's standard techniques like the Cooper-Harper and University of Stockholm rating scales have provided means towards evaluation of pilot workload. Workload is a term in the aerospace community referring to the portion of the total capacity of the pilot which is necessary to perform a task [23]. These task based evaluations of operator interfaces are common in platform valuation.

APPENDIX B

SCENARIO BASED REQUIREMENTS ENGINEERING TOOLS

Inquiry-Based Cycle Model (IBCM): Potts, Takahashi, and Anton's inquiry-based cycle model (IBCM) [234] for requirements analysis consists primarily on managing relationships between hypertext descriptions of requirements. Focusing on the elicitation of requirements from stakeholders with no clear customer authority, the IBCM method consists of three phases as illustrated in figure 97: documentation, discussion, and evolution.

Scenarios play a role during the requirements documentation process through text, tables, and diagrams [113]. These scenarios are described as “end-to-end transactions” between the system and its environment [234].

During requirements discussion, scenarios facilitates discussion. Potts writes:

“Answering the what-if question by analyzing specific scenarios gives stakeholders insight into general requirements and helps in the refinement process[234].”

Detrimental to the application of IBCM to the identification of architecture emergent requirements is the high level of abstraction taken. This tool is intended to be used during the requirements phase of development and necessitates a low degree of formality. It is also based on the assumptions made by the stakeholder before concept definition takes place. “Progress becomes impossible unless an assumption or decision is made [234].” Each assumption must be validated to ensure applicability to the specific architecture. It is a process based method characterized by a long iteration

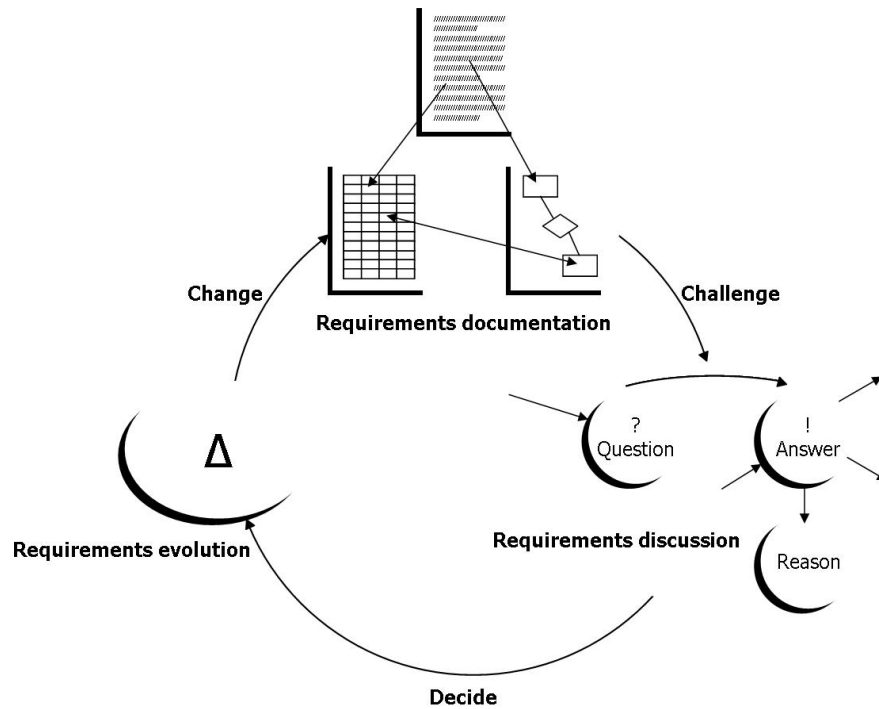


Figure 97: Inquiry-Based Cycle Model for Requirements Analysis [234]

cycle in a meeting based format. Potts estimates that defining 16 scenarios would take approximately 500 to 1000 man hours [234].

Questions Options Criteria (QOC): Questions, Options, & Criteria (QOC) is another semi-formal use-case requirements engineering method. It attempts to mirror typical decision making processes which are applied by designers. While QOC is not in itself a scenario based design techniques, it is used to define and refine operational requirements. Questions are used to uncover design issues, options represent means to provide solutions to issues discovered during questioning, and criteria are arguments supporting or opposing given options [195]. A QOC diagram is shown in figure 98. In this image solid lines and boxes represent positive assessments and dashed lines and boxes are negative assessments.

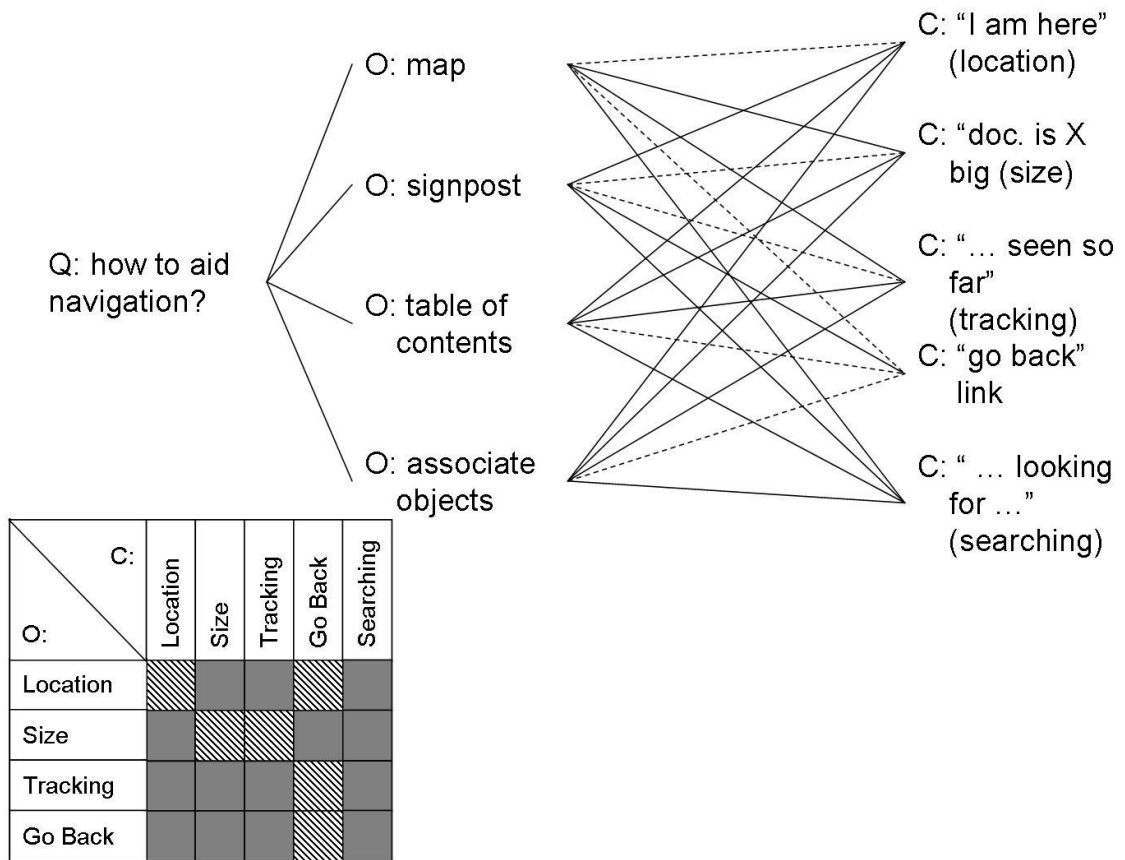


Figure 98: QOC Diagram Showing Different Navigation Properties [195]

This process is essentially provide means for the generation of qualitative evaluation matrices of potential solutions to evaluation criteria. As expressed by Mack, QOC “provide[s] a scheme for making design decisions explicit, and analyzing them in relation to user needs, and possible tradeoffs among potentially conflicting design implications[194].”

Integrating this method with scenario based design tools presents questions regarding the accomplishment of a requirement or task. The option is a system which provides fulfillment to the requirements by means of a specific method or tool. The criteria can be direct evaluation of the solution or may be a specific scenario in which the solution will be used. Thus, scenarios enter into the process as a question (how to fulfill a task), options (solution includes a method) and criteria (method can be used using specific solution). Maclean and McKerlie write:

“When tasks are viewed as Criteria, our approach relies on the designer to provide the argumentation to justify the extent to which the task under consideration is satisfied by the possible Options identified [195].”

QOC is essentially an evaluation tool which is qualitative in nature. Specific tasks must be independently defined and constructed to act as questions, options, criteria. Thus, this tool would be useful in evaluating particular architecture solutions for a series of tasks. However, it would need to be augmented to address emergent operating scenario identification.

Claims Analysis (CA): Like QOC, Claims Analysis (CA) analyzes the relationship between the system in light of user needs and options, and forces detailed and complete descriptions of design decisions. A claim is “the set of hypothesized causal relations pertaining to a given feature within a given scenario [255].” Claims represent the assumptions made by the designers regarding the benefit or detriment induced by specific system features. This requires designers and requirement engineers to

systematically address the logic behind specific trades and expand on the existing scenarios. Rosson and Carroll write:

“Analyzing a feature-consequence relation in a scenario encourages the designer to engage in what-if scenario reasoning, envisioning slight variants of the scenario that may not have been expanded in a narrative but that help to complete the analysis of a feature’s consequences [255].”

Additionally, CA assists designers to identify connections between scenarios. Implementing specific solutions during different scenarios may yield adverse or advantageous claims, necessitating decisions as to value of the solution.

This process assists in formulating evaluations of the operations and design space. Again, it does not directly address the formulating of scenarios but manages the qualitative assessment of the specific operational and physical solutions with regard to its claimed benefit.

Formal Scenario Analysis (FSA): Hsia et. al. introduced a formal approach to scenario analysis in 1994 [139]. In contrast to the other methods introduced with requirements development, FSA is a formal process of defining and developing scenarios. The scenarios correspond to interactions specific users have with the system. This process is visualized in figure 99.

Scenarios are generated considering the views of specific users of the system. Hsia et. al. use the example of a private branch exchange (PBX). In this environment the user views are those from specific “callers” or “callees”. Each user group generates a number of scenarios called a user view. These scenarios represent sequences of potential actions the user can take in relation to the system.

The first tool scenario structuring tool introduced with FSA is a scenario tree. In a scenario tree the nodes represent states and arrows represent events. Each node has one “parent” node but may have multiple “children” nodes. As specific actions

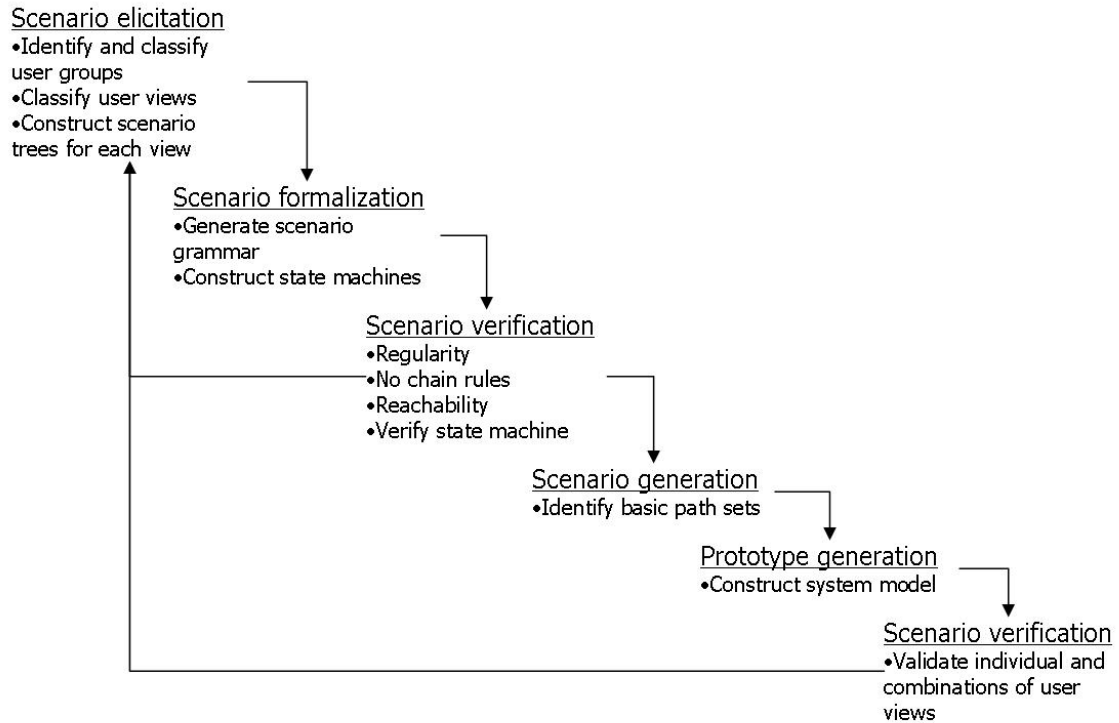


Figure 99: Process for Formal Scenario Analysis [139]

are taken the scenario procedures from parent to child throughout the tree. For FSA the terminating branches of the tree end in the same state as the initial state. Thus the tree represents legitimate sequences of states and actions that may occur linking the initial state to some final state. Each route throughout the tree presents distinct requirements on the attributes of the system. FSA translates the tree into a formal textual description of the tree.

The formal textual description is used to translate the scenario tree into the second scenario structuring tool introduced with FSA: deterministic finite-state Machine. A deterministic finite-state Machine, like the scenario tree, represents states with nodes and transitions with arrows. However, these are displayed in a graph as opposed to a tree with the initial and final states embodied in the same state. The state Machine is deterministic because each event results in a specific state. It is finite because the number of states is confined to those expressed by the user views. The tools used for

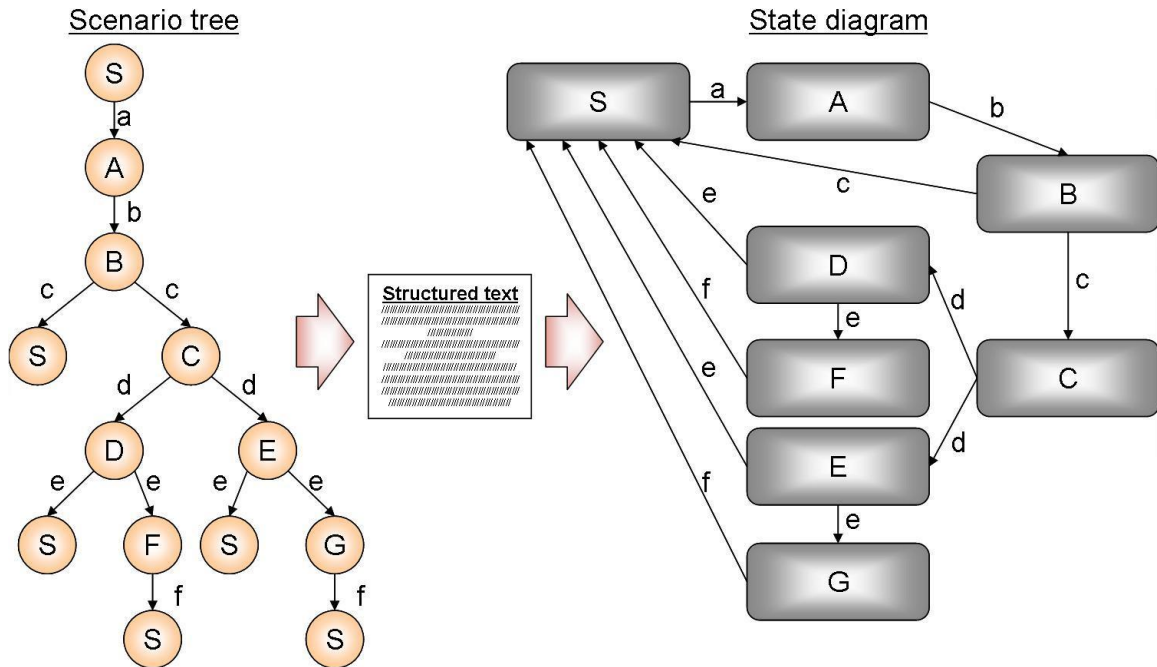


Figure 100: Tools for Formal Scenario Analysis [139]

scenario identification are displayed in figure 100.

FSA tools provide guidance towards the identification of sizing scenarios which drive the design of the system. Each path through the tree or state model represents a scenario scenario which could present new requirements to the system. While all states can be identified for a simple state diagram, complex systems interactions require means for identifying significant scenarios or simplifying the tree in order to be able to explore the system.

Task Analysis and Modeling (TA/TM): A task is more than a simple action, but a “purposeful activity [153]” intended to achieve a specific goal. Task analysis and modeling (TA/TM) approaches emerged from the HCI field [152] and, like use-case modeling, focus on the “context of usage [153].” Task modeling has driven the development of methods including and primarily GOMS (Goals, Operators, methods, and selection rules) [39, 149] as well as the formalization of a user knowledge through task knowledge structures (TKS) [152]. Johnson writes:

“In developing the technology of computer systems it is often necessary to focus upon properties of the technology. However, in developing systems that are intended to be used by people in the varied contexts of their work, private, social, and leisure activities, the focus of design must be on the suitability of the designed artifact to support and complement human activity [153].”

Many techniques for task definition take a very tightly focused view in order to understand details which are necessary for HCI definition. However, TKS does not address the command level to interaction design. TKS extends the GOMS approach to human computer interface design by exploring and leveraging task-knowledge. It is intended towards a higher level view by focusing on what Johnson terms “work tasks [153].” The basic motivation behind a task knowledge structuring is to understand the structured or unstructured way in which people do their work and characterizing these plans and procedures to drive design requirements.

TKS describes a task as encompassing goals, subgoals, procedures, objects, and actions. These are generated from observing the way work is currently done, formalizing these task descriptions and task models and generalizing these models. Goals are structured through decomposing high to lower level goals and defining subgoal relationships. Tools addressing these categories include textual descriptions, lists, and object diagrams for goal decomposition.

Johnson evokes an example for X-ray system design in generating the TKS seen in figure 101. As evident with this example, this tool is semi-formal. Categories of information are delineated and structured models are used for goal relationships. However, additional modeling would be required to generate executable representations of the embodied scenarios.

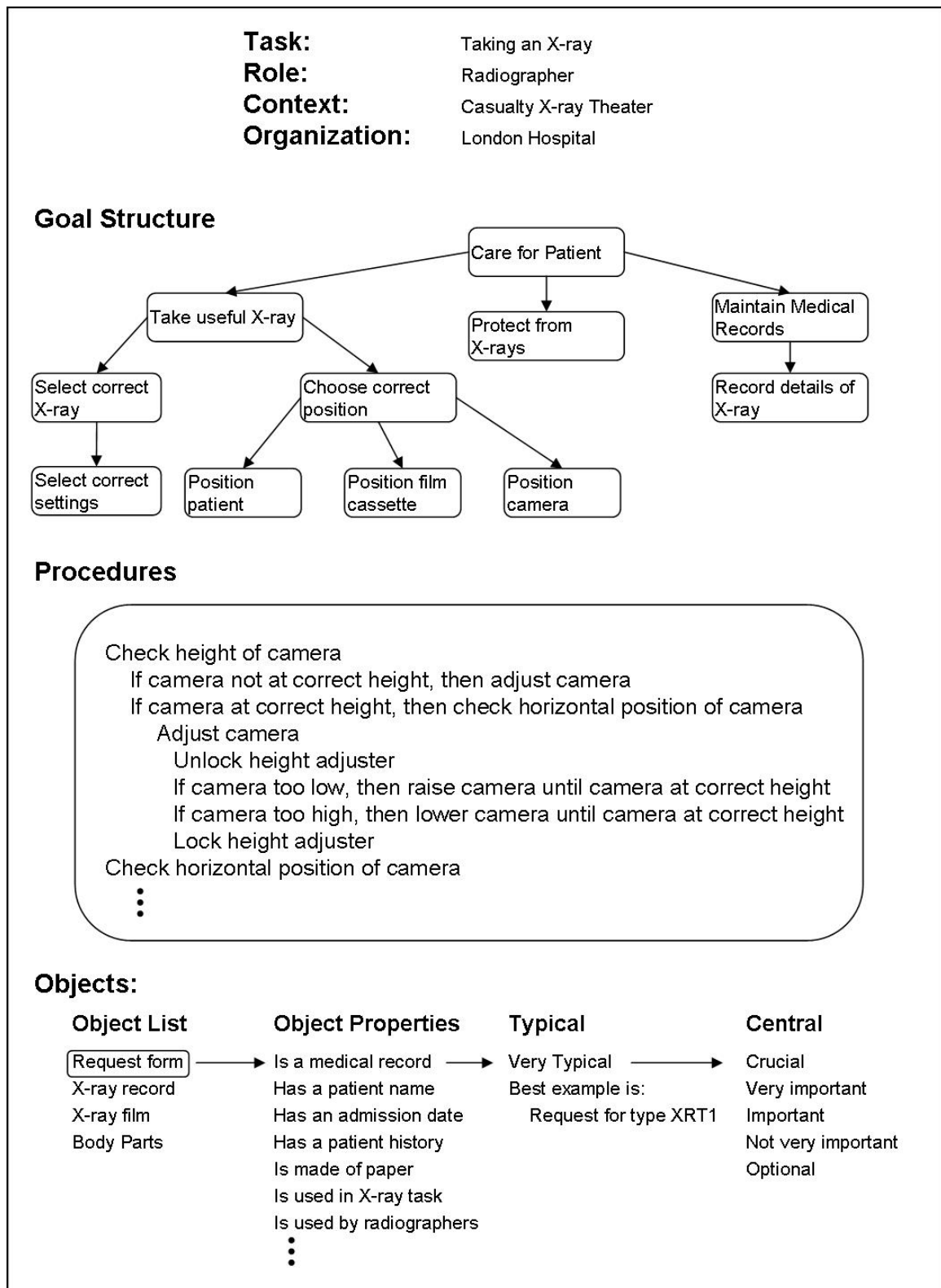


Figure 101: Task Knowledge Structure for "Taking and X-ray" Johnson [153]

The primary focus for this method is also the understanding of common sequences of actions in order to delineate requirements. For aircraft design, standardized methods exist to provide the framework for operational requirements identification in the form of a mission. The content for this tool and its methods are not ideally aligned with the need to identify emergent requirements from vehicle systems.

APPENDIX C

SCENARIO BASED OBJECT-ORIENTED ANALYSIS/DESIGN TOOLS

Responsibility-Driven Approach: This approach to scenario based design focuses on informally characterizing specific objects, relationships, and responsibilities. Wirfs-Brock et. al. breaks this method into two phases: the exploratory phase and the analysis phase [303]. During the exploratory phase object and conceptual entity classes are defined in terms of attributes and external interfaces. These classes are grouped and textually described. General class responsibilities and relationships are assigned to classes with the use of Class-Responsibility-Collaboration Cards (CRC's).

Once object classes, responsibilities, and collaborations are identified the analysis phase begins. Hierarchical relationships between classes are built and shared class responsibilities are explored. With these classes defined and collaborations mapped, potential subsystems are tacitly defined when complex collaboration is necessary. Finally, the responsibilities and relationships between subsystems are more specifically defined in terms of conceptual operations.

This process for object identification and specification relies heavily on informal methods for identifying classes, objects, and relationships. Scenarios play a role during the initial phases of explorations. Here informal descriptions of scenarios are used to identify specific 'nouns.' These nouns become the framework for classes, which are formalized into systems. Object graphs and hierarchies, textual descriptions (CRC's), Venn diagrams, and other tools are recommended (but not prescribed) in order to generate information in developing a class and system specification document [303].

The responsibility-driven approach described here is a traditional, tacit knowledge based process for software architecture definition. It takes an up front conceptual design perspective. However, its informal methods for generating systems decompositions drive towards the specification and development of a single hierarchically structured systems architecture. Scenarios play an initial role in initializing the generation of systems and requirements, however there is no formal means for specified for forming and deploying these scenarios. Additionally, there is no formal means for capturing additional operational requirements which are sensitive to physical implementation.

Use-Cases Diagrams: Similar to the scenarios which comprise the user view with FSA, Jacobson's [146] use-cases model ways in which the system can be used. They provide an important view on the requirements by assisting the designer in determining functional requirements and systems processes, and structuring requirement for an object model [296]. Use-case models are not intended to model the internals of the system. The use-case approach focuses on external interactions between the system under design and its external systems or users. However, a use-case is not a scenario. A use-case expresses all the possible paths of events, but a scenario describes part of the possible paths. [113]. In this sense a use-case can be seen as FSA user view. Jacobson writes

“Scenarios normally mean use-case instances ... use-cases are treated more formally, and described in a model of their own, as well as in interactions between objects in different object models. Scenarios are normally described as interactions between objects only [146].”

Two basic conceptual elements are necessary for use-case modeling: actors and use-cases. Figure 102 shows a simple use-case model of a ATM system. The actors which interface with the system are the bank customer, the bank system, and the

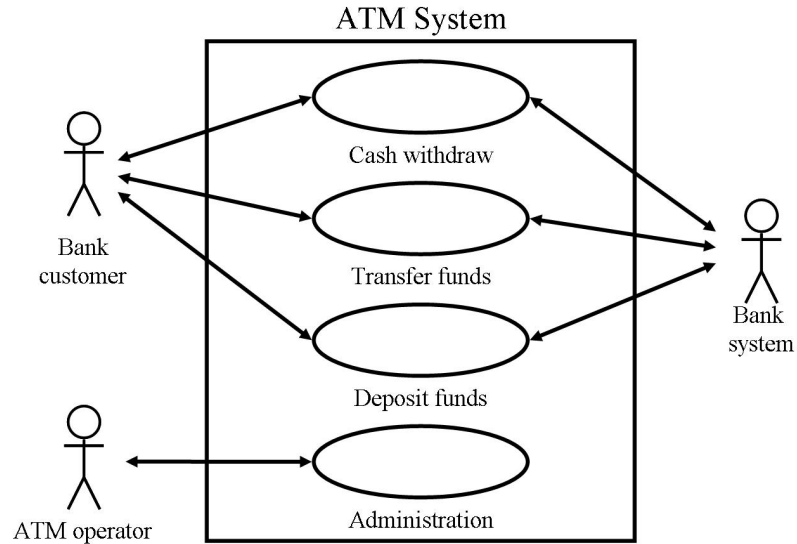


Figure 102: Notional use-case Model of ATM System [146]

ATM operator. Their relationships with the ATM fall into four distinct use-cases as depicted.

Relations between use-cases are captured. Use-cases at high levels of abstraction may require use-cases defined at lower levels. This is termed a “use” relationship. Additionally, the performance of one use-case may depend upon the other use-cases being performed. These are termed “extends” relationships. Extends help to capture “optional parts of use-cases, complex and alternative courses, subsequences that are executed only in certain cases, and the insertion of several different use-cases into another use-case [146].”

In the case of a commercial or military aircraft at the level of platform conceptual design, the actors can be generalized. From an external view of the system, platform level services provided remain the same regardless of the architecture implementation. The diagrams are typically very simple and are used primarily as communication tools between systems engineering and stakeholders [296].

The use-case model falls short of managing some temporal and physical aspects of scenario based design. Use-cases focus on interaction, not process. The use-case

focuses primarily on the services that a system provides. Qualitative aspects like “response times, weight, or size” are seen as “supportive” in nature [296]. Concurrency, conflicts and object modeling are not addressed with use-case modeling.

State Transition Diagrams: The framework for state Machine came about to manage issues arising from design and analysis of reactive systems. While a transformational system received inputs, performs transformations, and produces outputs, a reactive system accepts stimuli from its environment and is required to “maintain a certain ongoing relationship [120].” Difficulty arises in understanding and decomposing the behavior of the a reactive system. Both behavioral specification and implementation (design) are necessary for design and construction or a reactive systems [120]. Based on Mealy and Moore definitions of finite state automata, state charts were initially introduced as a visual language and methodology for formally specifying the behavioral space [119].

IEEE standard glossary of software engineering terminology define a state as “a condition or mode of existence that a system, component, or simulation may be in [274].” State Machines or state transition diagrams express the state of a system with a node and transitions between states as arrows between nodes. Transitions induce changes in state as a result of some activity or event introduced from external actors or environment, or internal system objects. While implementation or structure models remain reactive, statecharts are transformational. Objects exist in states, operations cause a transition between states [248].

Harel illustrates statecharts which were precursors to the state transition diagram with a simple digital watch as displayed in figure 103. Each state represents the current display on the watch and events triggered by pushing buttons a through d. Additionally alarm states are toggled at different times (P1: alarm 1 enabled at T1, P2: alarms 2 enabled at time T2, P: alarm 1 and 2 enabled at T1=T2).

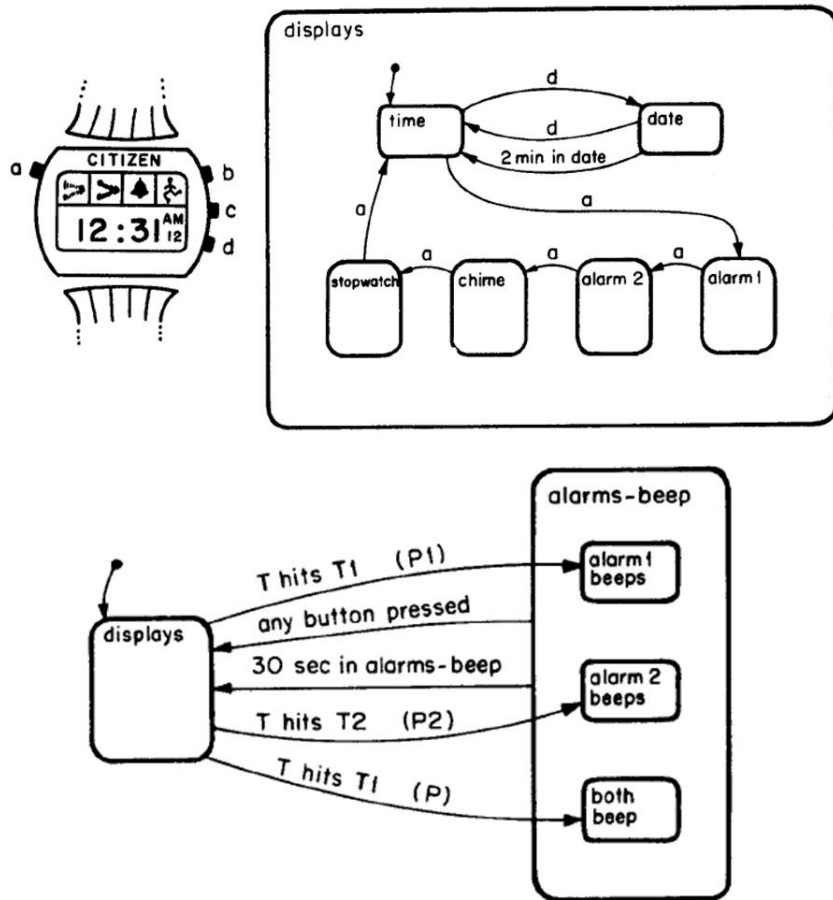


Figure 103: Harel's Watch State Chart Illustrations [119]

One difficulty in the definition of activity diagrams is the need to maintain a behavioral perspective. Even with the simple watch example transitions and states were defined following some predefinition regarding the implementation space. With highly flexible architecture trades, the physical definition is highly variable. Thus, the transitions and states must be so defined in order to be independent of the design variables. At the platform level, a state representation of the mission profile may enhance the ability to more closely interrelate the operation/mission requirements and the operational implications of adopting specific systems.

Activity Diagrams: Like state and transition diagrams, activity diagrams are “behavioral in nature [296]”: meaning that they describe processes not structural. However, while state diagrams use nodes to represent system states, activity diagrams use nodes to represent sequences of actions. Information, objects, or controls relate the various actions making up an activity. Actions can occur concurrently or serially, and logic can dictate the relationships between actions.

Considering literature from Pahl et. al. [229] and Suh [282] a function is defined as the objective physical performance of a given object [12]. A function can be described as an actions with qualifications. To enumerate a function, something must be done to a given extent. Thus, in a general sense a function is fundamentally characterized by an action. Activity diagrams are similar to functional flow block diagrams (FFBD) in the information their composition and structure [75].

As discussed in the third chapter, functions play critical role in formulating the requirements definition and physical embodiment of the system. Functions or actions provide the means by which requirements are allocated and communicated to the embodied elements of the system. an important role in allocating requirements to the unit level.

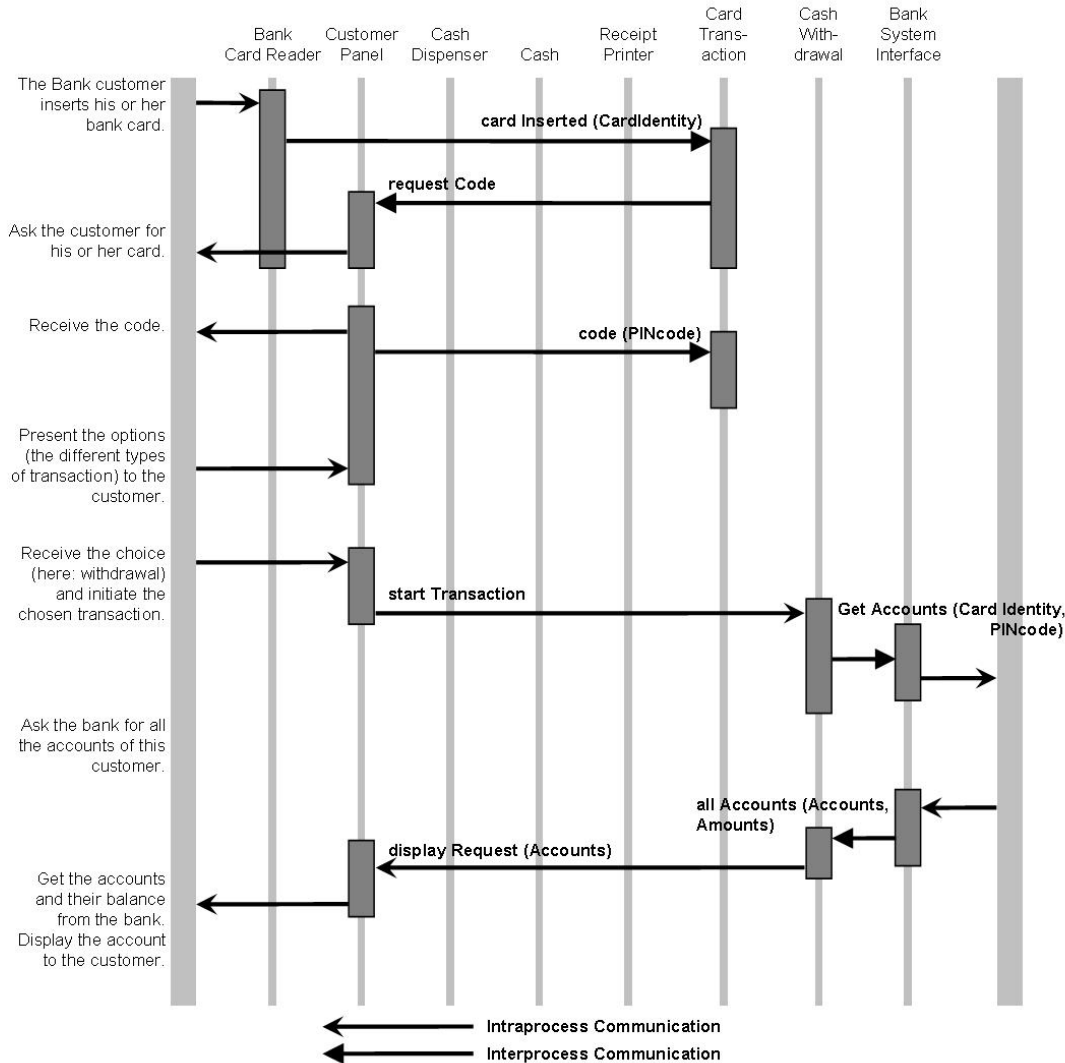


Figure 104: Interaction Diagram for ATM Cash Withdrawal Operation [146]

Interaction Diagrams: Working in conjunction with use-case diagrams in providing use-case design, interaction diagrams are object models which focus on internal interactions between system objects and external interactions between the system and use-case actors. Serial and parallel operations performed by systems objects represent sequences of events which must be accomplished in the fulfillment of a particular use-case. Jacobson continues his ATM example with the interaction diagram seen in figure 104.

The objects are listed across the top of the of figure 104 are system objects with the

left and right columns representing external actors. Events are represented by arrows between the columns. On the left hand side of the interaction diagram, interactions between the system and external actors are listed.

For every use case, an interaction diagram shows how the participating objects interact. Thus, for a complex architecture defined by complex operations many interaction diagrams would be necessary to describe all potential sizing scenarios. Using a functional induction based approach to system composition presents additional challenges in the implementation of interaction diagrams during conceptual architecting. With variable system objects characterizing concept architecture trades, potential variations in architecture would require a redefinition of the interaction diagram for each use case. Adequate flexibility would require augmentation to interaction diagram methods to allow for the identification of emergent operation mode requirements.

This approach begins, however, does begin to explore internal relationship in the system. Interactions between systems in the interaction diagram effect the usability of the system in performing the denoted operation. Timing and sequencing are also introduced with the interaction diagram. For concept level architecture some time dependence is of import when defining requirements. However, the level to which sequences of distinct interactions begins to complicate requirements derivation.

APPENDIX D

ALGORITHM FOR DETERMINING STATISTICAL SIGNIFICANCE OF UNIT FAILURES

The Matlab® code, “./StatisticalSignificance.m”, given below determines which failure states are statistically significant ([*combins*] matrix). It also finds which failure combination preclude the consideration of other failure states ([*covers*] matrix). The third output, [*AllProbs*], lists the failure probabilities of all units corresponding to their *IO* index. Lastly, *combfails* capture all the maximum number of concurrent failures required to give statistically significant failures.

The [*combins*] output is a $n \times m$ matrix. Each row represents a single statistically significant failure state. Each column in the row lists the IO indices which are affected during this failure.

The [*covers*] variable is also an $n \times p$ matrix. Each row, i , in the [*covers*] matrix characterizes the failure case in [*combins*] of the same row index, i . The columns in this matrix indicate which other rows in [*combins*] preclude the need for considering this the failure case in row i . Consider the scenario when the case at index i is the combined failure of unit 1 and unit 2. If case at index j is the failure of unit 1, then case j covers case i [$P_i \cup P_j = ((P_A \cap P_B) \cup P_A) = P_A = P_j$]. The i 'th row of the [*covers*] matrix is given as $covers[i, :] = [j \dots]$. In this scenario, if j is already considered in the union calculations, the probability of i need not be addressed.

The inputs to this significance function include the an array of strings which are the labels for system IO. This matrix is of same length as the X vector discussed in the methods chapter and includes names of each functional relationship. Each IO label is formatted as (*unitname*)-(*functionalcapabilityname*)-(*directionof flow*). The

direction of flow is given by *ds* or *us* indicating downstream and upstream capability relationships respectively.

The other input, *[unitvaratts]*, gives all attributes values for the units. The first column of this string array gives the name of the unit attribute. This is formatted as *unitname_functionalcapabilityname_attributename*. The second column of this array includes the value of this attribute. If the capability attribute name includes probability information (*F*) and the namespace matches the IO, this value is recorded and linked to the IO index.

./StatisticalSignificance.m

```

1 function [combins , covers , AllProbs , combfails]= StatisticalSignificance(IO, unitvaratts)
2 %% This function determines all statistically significant failure combinations (combins) and
   which combinations preclude the considerations of others for probability calculations (covers)
   %%
3 A=length(IO);
4 B=size(unitvaratts);
5 %% Determine all unit failure probabilities in architecture %%
6 for i=1:A(1) % Look at all IO Variables
7     L=length(outputname);
8     if strcmp(outputname(L-1:L), 'ds') % Identify downstream cap IO
9         for j=1:B(1) % Look for failure prob info
10            unitattributes = regexp(unitvaratts(1, j), '-', 'split'); % Parse unit att variable name
11            C=size(unitattributes);
12            if strcmp(unitattributes(C(3)), 'Rel') % Check if unit attribute name
13                outputnamecheck=strcat(C(1) , '-' , C(2) , '_ds'); % Recase output variable name
14                if strcmp(outputname, outputnamecheck)
15                    AllProbs(i)=str2double(unitvaratts(2, j)); % Index Failure Probability
16                    if AllProbs(i) > 0
17                        failnodes(numfails) = i; % List all unit failures
18                    end
19                end
20            end
21        end
22    end
23 end
24 %% Construct upper bound of failure probability (P(k)) for failure combinations assuming all units
   exhibit max probability of failure %%
25 maxprob=max(AllProbs); % Determine max fail prob
26 for i = 1:length(failnodes)
27     combs=nchoosek(length(failnodes), i);
28     if i>1
29         Pk(i)=Pk(i-1) + combs(i)*(maxprob^i);
30     else
31         Pk(i)=combs(i)*(maxprob^i);
32     end
33 end
34 %% Limit number of combinations allowed by error (error must kept less than 10^-11) %%

```



```

35 combcount = 0;
36 for i = 1:length(failnodes)
37     error=Pk(i) - Pk(length(failnodes)); % Calc i comb fail prob error
38     if theval>10^(-11) % Determine necessary i limit
39         combfails = i; % Number of req combined fail
40         tempcombins = nchoosek(failnodes ,i);
41         for j=1:combs(i)
42             for k = 1:i
43                 combins1(j+combcount,k)= tempcombins(j,k); % List init stat sig failures
44             end
45         end
46         combcount = combcount + combs(i); % Count init stat sig
47     else
48         break
49     end
50 end
51 %% Selected significant failures based on failure case probability %%
52 x=0;
53 combcount = 0;
54 D=size(combins);
55 for i=1:D(1) % Look at all combinations
56     probs = 1; % Calculate fail prob
57     for j = 1:combfails
58         if combins1(i,j) ~=0
59             probs = probs * AllProbs(combins1(i,j) );
60         end
61     end
62     if probs > 10^(-14) % Check fail case prob
63         x=x+1;
64         for k = 1:combfails
65             combins2(x,k) = combins1(i,k); % List stat sig fail final
66         end
67         combcount = combcount+1; % Count final stat sig fail
68     end
69 end
70 %% Identify which probability covers %%
71
72 for i=1:combcount % Look at all fail combs
73     currentcount = 0;
74     for k=1:combfails
75         if thefails(i, k)~=0
76             currentcount=currentcount+1; % # of combined failures
77         end
78     end
79     theindex = 1;
80     for j = 1:(i-1)
81         lastcount = 0;
82         for k = 1:combfails
83             if thefails(j,k) ~= 0
84                 lastcount=lastcount + 1; % # of combined failures
85             end
86         end
87         if currentcount > lastcount % 1st covers check
88             thenums = 0;
89             for k = 1:lastcount

```

```

90         for m = 1:currentcount
91             if thefails(j, k) == thefails(i, m)           % 2nd covers check
92                 thenums = thenums + 1;
93             end
94         end
95     end
96     if thenums == lastcount
97         covers(i, theindex)=j;           % Failure i covered by j
98         theindex=theindex + 1;
99     end
100 end
101 end
102 end

```

All of the “./StatisticalSignificance.m” routine are used to find the continuous hazard probability relationship.

The outputs of ./FindHazardProbRelationship.m function characterize this relationship between hazard and probability. The variable [failstates] is a $1 \times m$ vector listing all of the discrete hazard values at which a step change in probability occurs. The probability is given in the Probs vector of the same length as [failstates]. The output [theequations] is a $m \times n \times p$ matrix representing the closed form probability equation. For each state (n), the first column of the sub-matrix represents a sign value (-1 or +1), the remaining columns include the indices of each unit indices. The probability is determined by replacing the index value with the unit failure probability, taking the product of all values within a single row, and summing all of the products.

$$P_F = P_1 + P_2 \cdot P_3 - P_1 \cdot P_2 \cdot P_3$$

Using this notation the equation above is given by the theequations matrix here:

$$\begin{bmatrix} +1 & 1 & 0 & 0 \\ +1 & 2 & 3 & 0 \\ -1 & 1 & 2 & 3 \end{bmatrix}$$

This function receives five inputs as discussed previously. The first input [combins] lists all statistically significant failure combinations. Each row of this matrix contains unit

value indices representing which units are failure for this case. The magnitude of the hazard incurred and the failure probability are given in the $[FinHazard]$ and the $[Allprobs]$ vectors. The $[covers]$ variable indicates which failure combination in $[combins]$ remove the necessity to take the union with other rows in formulating $[theequation]$ (e.g. P_1 covers $P_1 \cap P_2$). Lastly, the variable $[combfails]$ indicates the minimum number of columns required in $[theequation]$ to give statistically significant probability calculations.

./FindHazardProbRelationship.m

```

1 function [failstates , Probs , theequations]=FindHazardProbRelationship( combins , covers , FinHazard ,
    Allprobs , combfails)
2 %% This function calculates the hazard probabilities in terms of discrete hazard steps %%
3 failstates=unique( FinHazard ); % List unique hazard states
4 Probs=zeros( length( failstates ) , 1 ); % Initialize Probs
5 theequations=zeros( length( failstates ) , 10000 , 2+ combfails ^ 2 ); % Initialize the equation
6 allprobs=horzcat( Allprobs ( 1 , : ) , 1 ); % Allprobs: 1 in last col
7 A=size( FinHazard ' ); % Find size of FinHazard
8 B=size( covers ); % Find size of the covers
9 used=zeros( 0 , 1 ); % Temp array to check covers
10
11
12 for i=1:length( failstates ) % Consider failure magnitudes
13     used=zeros( 0 , 1 );
14     r=1;
15     for j=1:A( 1 ) % Consider each failure state
16         if FinHazard( j ) >= failstates( i ) % Check failure magnitudes
17             yes=1;
18             for k=1:B( 2 )
19                 if sum( used==covers( j , k ) ) && covers( j , k ) ~ = 0 % Check covers
20                     yes=0;
21                     break
22                 end
23             end
24             if yes==1 % List used cases
25                 used( r ) = j ;
26             end
27         end
28     end
29     % Execute function which formats the union of combined failures
30     [sumofprods , thesigns]=groupmultiplications( used , combins , combfails );
31     check=sum( sumofprods ~ = 0 , 2 ) <= combfails ; % Limits to stat sig unions
32     sumofprods( ~ any( check , 2 ) , : ) = [ ] ;
33     thesigns( ~ any( check , 2 ) , : ) = [ ] ;
34     C=size( sumofprods ); % Determine union eq length
35     theequations( i , 1 : C( 1 ) , 2 : 1+ combfails ^ 2 ) = sumofprods ; % Write theequations output
36     theequations( i , 1 : C( 1 ) , 1 ) = thesigns( : , 1 ); % Write signs to theequations
37     theequations( i , 1 : C( 1 ) , 2+ combfails ^ 2 ) = - 0.1 ; % Mark the end of the matrix
38     probindices=sumofprods+( length( allprobs ) ) *( sumofprods==0 ); % Format sum of prods matrix
39     TheProbs=allprobs( probindices( : , : ) ); % Replace indices with probs
40     TheProbs2=prod( TheProbs , 2 ); % Calculate probs for state i
41     Probs( i ) = sum( TheProbs2 );

```

```

42 end
43
44
45
46 function [sumprods, thesign]=groupmultiplications(used,combins,combfails)
47 %% This formats the unions of all combined failure intersections %%
48
49 allactive=combins(used,:); % ID all failure states
50 sign=1; % Initialize sign function
51 thesign=zeros(0,1);
52 sumprods=zeros(0,combfails*combfails); % Init prob function matrix
53 for i=1:combfails
54     touse=sum(allactive~=0,2)<(combfails+2-i); % Checks stat sig
55     if sum(touse)>0
56         theused=(used)';
57         theused(~any(touse,2),:)=[];
58         if length(theused)>i || i==1
59             thecomb=nchoosek(theused(:,:),i); % Find all fail state combos
60             S=size(thecomb);
61             X=zeros(S(1),0);
62             for j=1:combfails % Formulate the equation
63                 if j<=i
64                     clear F
65                     F(:,:)=combins(thecomb(:,j),:);
66                     X=horzcat(X,F);
67                 else
68                     X=horzcat(X,zeros(S(1),combfails));
69                 end
70             end
71             X=sort(X,2,'descend');
72             Y=horzcat(diff(X,1,2),ones(S(1),1));
73             X=sort(X.*(Y~=0),2,'descend');
74             sumprods=vertcat(sumprods,X);
75             signs=sign*ones(S(1),1);
76             thesign=vertcat(thesign,signs);
77         end
78     end
79     sign=-sign; % Flip sign for next combo #
80 end

```

Outputs from the “./FindhazardProbRelationship.m” code is further manipulated by the routine below.

./FormatContinuousHazProb.m

```

1
2 for i=1:length(failstates)
3     if i>1
4         if Totalfailstates(2*(i-1))>=failstates(i)
5             Totalfailstates(2*(i-1)+1)=Totalfailstates(2*(i-1))+eps;
6         else
7             Totalfailstates(2*(i-1)+1)=failstates(i);
8         end
9     else

```

```
10     Totalfailstates (2*(i-1)+1)=failstates (i);
11     end
12     Totalfailstates (2*(i-1)+2)=Totalfailstates (2*(i-1)+1)+eps;
13     Totalfailprobs (2*(i-1)+1)=failprobs (i);
14     if i<length (failstates)
15         Totalfailprobs (2*(i-1)+2)=failprobs (i+1);
16     else
17         Totalfailprobs (2*(i-1)+2)=0;
18     end
19 end
20 HazProbs=interp1 (Totalfailstates ,Totalfailprobs ,0:0.001:1 , 'nearest');
```

APPENDIX E

ANALYTICAL HAZARD FUNCTION PROPAGATION

There are three ways in which requirements can be allocated to systems. A relationship which involves one element on the demand side and one element on the supply side is termed 'simple.' Multiple demand side element placing requirements on one supply side element is termed a 'combination' relationship. The requirements are combined from the load demands of multiple requirements sources. Multiple supply side elements fulfilling requirements generated from one demand side element is termed an 'allocation' relationship. Here a single requirement source may be allocated to a number of potential suppliers. When multiple demand side elements place requirements on multiple supply side elements the relationship consists of a 'combination' followed by an 'allocation.' These relationships are outlined in table 46. The notation here is source centric; meaning that the functional notation intends to determine the requirements and reliability of one of the source elements. Functional requirements flow from demand element to source element. Cap_N is the capability or capacity of source element N , U_N and A_N denote the functional requirements from unit and allocation elements respectively.

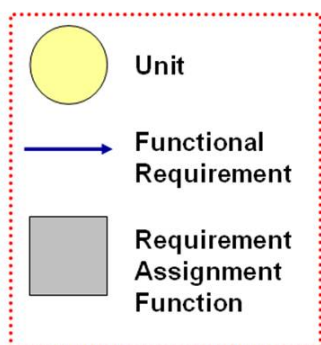
The equations in table 46 are read as follows. The simple relationship in this table indicates the functional and criticality requirements placed on unit 2 from unit 1 given the capacity of unit 2. The functional notation for an allocation relationship determines the requirements on unit 1, given the allocated requirements on functional group 1, the capacity of unit 1, and all other units within the functional group. The combination relationship indicates the functional and reliability requirements on the elements upstream of the combination given the requirements from all demand side elements and the capacity of the upstream element.

Describing requirements assigning relationships following this convention for the sake of system modeling translates well to functional induction. Each relationship is designated

Table 46: Convention for Unit Requirements Relationships Relationship Types

Type	Diagram	Notation
Simple		$\left\langle \frac{U_1}{U_2} \right\rangle$
Allocation		$\left\langle \frac{U_1}{U_2, \dots, U_n} \right\rangle$
Combination		(U_1, U_2, \dots, U_n)

By convention, arrows point upstream with the flow of functional requirements and opposite the flow of energy, material, or information.



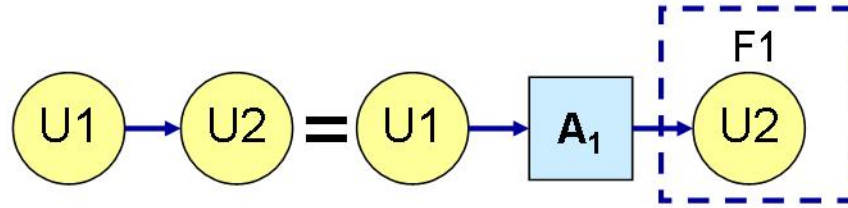


Figure 105: Simple Relationship

by a functional intra-relationship and ‘allocations’ are used to describe requirements placed on a given number of potential sources each of which has can provide the desired function. Elements which can provide spatial or complete fulfillment of the same function belong to a ‘functional group.’

These relationships, driven by functional induction form the framework for analysis in this thesis. Maintaining these relationships with the information provided by the upstream and downstream elements facilitates the flow of behavioral hazard derived safety and reliability requirements throughout the system and the necessary relationships for architecture safety analysis.

The criticality associated with the fulfillment of a given function at the unit level relates directly to criticality at the platform level. ‘Simple,’ ‘allocation,’ and ‘combination’ relationships augment are means by which criticality is defined for the upstream elements and reliability is defined towards the downstream functional requirements. Each of these relationships augment the criticality and reliability depending on the units involved in the relationship. In addition to the flow of reliability requirements and attributes through these relationship elements, each of the units must designate the criticality requirements associated with their own induced requirements as a function of the criticality of the loads that they are supporting. Just as reliability is sensitive to both unit reliability and the reliability of supporting the unit’s induced functions, as the load an element supports becomes more critical, the induced requirements demanded by that element must also become more critical.

E.1 Simple Relationship

Reliability Relationship The reliability of a downstream unit is a function of its own reliability and the reliability of the unit supporting its induced functions. Assuming that the unit capability is directly contingent on the induced functions, this reliability can be expressed by multiplication. The magnitude of the induced function requirements on unit 2 (Req_2) from figure 105 is a function of the magnitude of the functional requirement on unit 1 (Req_1). Defining the ‘system’ as unit 1 and 2 shown in figure 105 and using $f(Req_1)$ to represent this relationship the reliability of unit 1 is given by:

$$P_{system}(Req_1) = P_1(Req_1) \cdot P_2(f(Req_1)) \quad (66)$$

Criticality Requirement Relationship When the criticality requirement of the downstream element is known, this requirement/hazard relationship can be propagated upstream. Expanding the relationship shown in table 46, the ‘simple’ relationship defining the hazard relationship for unit 2 (U_{2crit}) to the hazard relationship of unit 1 (U_{1crit}) is given by equation 67.

$$U_{2crit}(\%loss_{Req_2}) = U_{1crit} \left(\frac{\langle \frac{U_1}{U_2} \rangle \cdot Cap_{U2}}{\max(f(Req_1))} f^{-1}(\%loss_{Req_2}) + \left(1 - \frac{Cap_{U2}}{\max(f(Req_1))} \right) \right) \quad (67)$$

With increasing capacity of unit 2, the percentage loss at which hazards begin to be introduced becomes larger. However, at 100 % function loss the hazard remains the same. This hazard relationship is also scaled by the relationship between function and induced function given through unit 1, and the level of dependence of unit 1 on the induced function. When failures in the induced function do not directly correlate to failures of in the downstream unit the dependence of unit 1 on its own induced function must be defined and included as a scaling factor in equation 67.

While the hazard related to failures of individual elements is given by this criticality

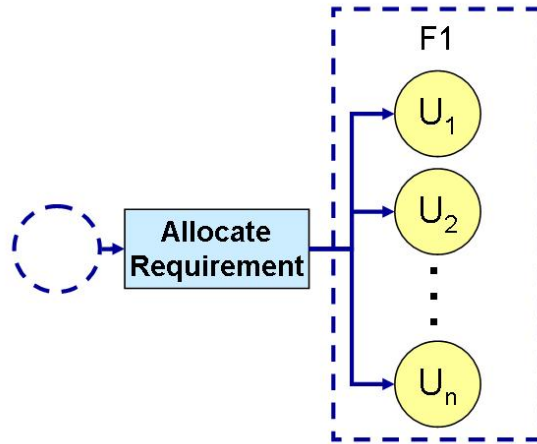


Figure 106: Allocation Relationship

relationships, the actual reliability which constrains the upstream unit must take the reliability of additional upstream and downstream capability. This holds for each of the unit types.

E.2 Allocation Relationship

With complex graphs, subsequent upstream relationships may necessitate that information be made available from all downstream functional dependencies. These relationships are affected by the complexity of the system graph.

Criticality Requirement Relationship Propagating criticality through an ‘allocation’ relationship is more complex than for a ‘simple’ relationship. Indeed, a ‘simple’ relationship can be considered a unique form of an ‘allocation,’ where there exists only one element in the functional group to which hazards must be allocated. The ‘allocation’ block is considered an element in the system for this analysis with no physical attributes whose capabilities are defined by the upstream functional group, and whose requirements and criticality are defined by the downstream unit. Assigning criticality to units within a function group from a downstream allocation element (as pictured in figure 106) is given in equation 68.

$$\left\langle \frac{U_1}{U_2, \dots, U_n} \right\rangle$$

$$U_{1crit} (\%loss_{Req1}) = A_{crit} \left((\%loss_{Req1} - \%offset) \frac{Cap_{U1}}{max(Req_A)} \right) \quad (68)$$

$$\%offset = \frac{\left(\left(\sum_{i=1}^n Cap_{U_i} \right) - max(Req_A) \right)}{Cap_{U1}}$$

Comparing equation 68 for an allocation relationship and equation 67 for a simple relationship, a simple relationship is one in which requirements are allocated to only one upstream element. For the 'allocation' relationship, the capability of other upstream units must also be taken into account. Depending on the capacity of the other units within the group, the criticality of each individual unit changes. For example, if one unit is responsible for individually supporting the entire load, its criticality will be much higher than if multiple units are available. With increasing capacity of the redundant units, the criticality of a complete capability loss of one of the units within the group is greatly reduced. This can be seen as a shifting of the criticality relationship for the allocation element using

The allocation element is an representation of the entire functional group subsequent downstream units. An 'allocation' element has no intrinsic physical properties which alter the reliability or capability requirements of the system. Induced requirements and criticality attributes are inherited from downstream and capability and reliability attributes are inherited from the functional group. If the functional group is induced, subsequent downstream elements perceive the upstream group as an allocation element.

Reliability Relationship Determining the reliability of the allocation element is generated using the parallel formatting of unit combinations as introduced in Method 2. These relationships were discussed in section *Proportional Function Failure*.

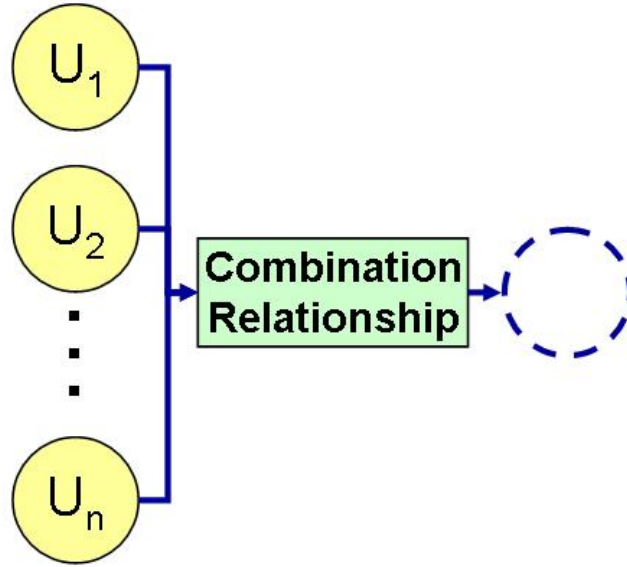


Figure 107: Combination Relationship

E.2.0.1 Combination Relationship

Criticality Requirement Relationship The ‘combination’ relationship is the most complex of the three relationship types. In assigning criticality, the multiple downstream elements each contribute the hazard associated upstream ‘combination’ unit loss. Similar to the ‘allocation’ unit, ‘combinations’ have no physical attributes. Capability and reliability attributes are inherited from the bounding upstream unit and requirements and criticality are inherited from the combined downstream units. In this situation, where multiple requirements are placed on the same unit, the criticality of the combination unit (C) is calculated by equation 69.

$$(U_{1,4}, U_{2,4}, \dots, U_{n,4})$$

$$\%loss_C(C_{crit}) = 1 - \frac{1}{Cap_C} \sum_{i=1}^n \max(Req_i) (1 - \%loss_{Req_i}(U_{icrit})) \quad (69)$$

$$C_{crit}(\%loss_C) = \%loss_C^{-1}(C_{crit})$$

For convenience sake, while the other relationships which express the criticality in terms

of functional requirement loss, ‘combination’ relationships express the loss in terms of criticality. This relationship is then inverted to generate criticality in terms of failure.

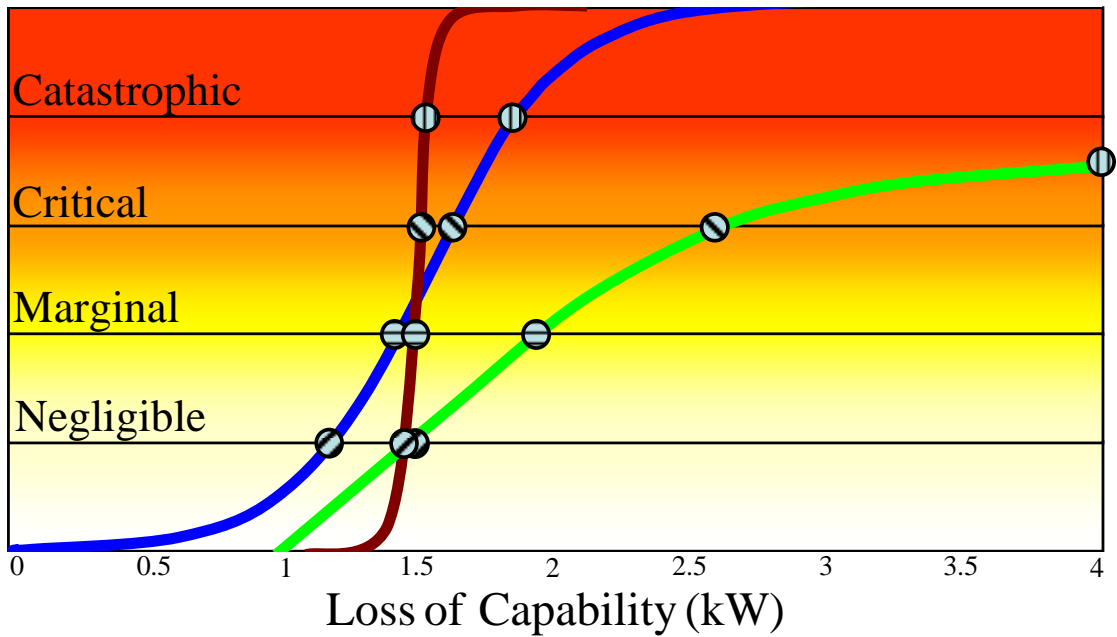
Figure 108 illustrates the hazard relationship for a ‘combination’ element in terms of three downstream units with displayed criticality curves. These three units demand 2, 3, and 4 units of some notional functional requirement from a single entity. Thus, the total capacity demanded from the upstream combination element is 9 units. Through equation 69, the hazard associated with these combined elements was determined.

As is evident in figure 108 (a), in order for a marginal hazard to occur, unit 1 has to be failed by approximately 1.45, unit 2 must be fail 1.4, and unit 3 must fail by 1.9. If the criticality of these unit failures are independent and trades are made to minimize hazard, then the criticality element must lose 4.75 out of a 9 units of capability. As can be seen in figure 108 (b), this is indeed the case.

Reliability Relationship Load shedding optimization strategies are managed through combination relationships. With one element supporting multiple loads, the loss of this element requires represents a degradation in one or multiple downstream elements. Deciding which of these elements lose functional support necessitates optimization. The percent function loss of downstream elements is determined through the optimization process shown in equation 70. The hazard is minimized by varying which downstream load is no longer supported. This optimization is constrained by the remaining capacity of the combination element element. The probability of an induced function loss on an element downstream from a combination relationship is determined thusly.

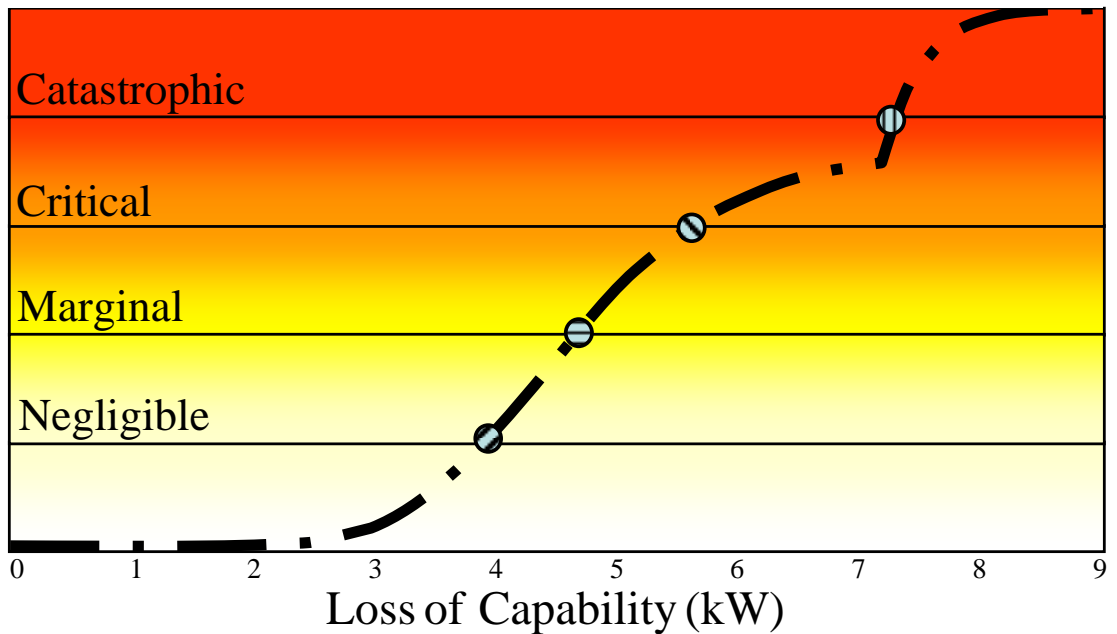
$$\begin{array}{c|c}
 \text{Min:} & \text{Hazard} = H_{op}(\mathbf{F}) \\
 \hline
 \mathbf{F} = \begin{pmatrix} fail\%_{unit1} \\ fail\%_{unit2} \\ fail\%_{unit3} \\ \vdots \end{pmatrix} & \text{s.t.:} \begin{pmatrix} Req_{unit1} & 0 & 0 & \dots \\ 0 & Req_{unit2} & 0 & \dots \\ 0 & 0 & Req_{unit3} & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 - fail\%_{unit1} \\ 1 - fail\%_{unit2} \\ 1 - fail\%_{unit3} \\ \vdots \end{pmatrix} \leq (1 - fail\%_C) Cap_C
 \end{array}
 \tag{70}$$

Criticality of Downstream Units



(a) Downstream Hazard

Criticality of Upstream Unit



(b) Combined Hazard

Figure 108: 'Combination' Hazard Relationship for Three Notional Downstream Units

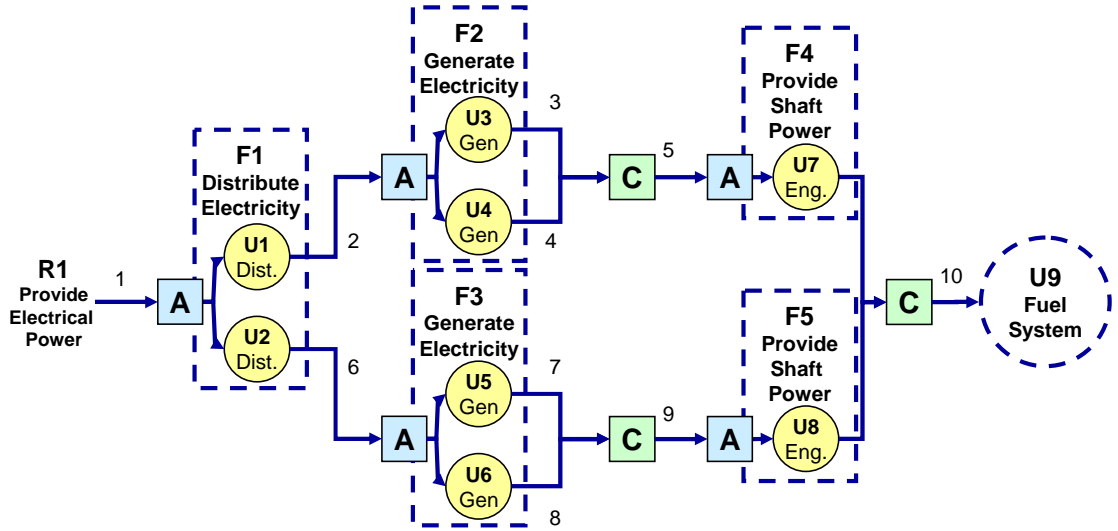


Figure 109: Combination-Allocation Relationship for Notional System Providing Electrical Power

E.3 Complex Allocation-Combination Relationships

Consider the notional example displayed in figure 109. The hazard associated with the upstream Unit 9 (Fuel System) must be expressed as the combination of multiple downstream elements all supporting a similar allocation element. With total loss of U9, R1 (provide electrical power) cannot be fulfilled. Therefore, the U9 failure/hazard curve cannot be calculated directly as a function of the adjacent unit criticality. Structural information must propagate upstream all the way from the boundary requirement.

Requirements and criticality communicated through each of the edges in this directed graph must carry information regarding requirement origin and augmentation. Edge tags for the figure above are displayed in table 47. In this table, the allocation relationship is indicated by triangular brackets: e.g. $\langle \frac{U_i}{U_1, U_2, \dots} \rangle$. Combinations are displayed with comma separated and parenthesized elements or allocations. Edges which stem from units in an allocation relationship are tagged by the proportion of the downstream requirement (in this case R1) provided by the unit. In order to fully characterize the sources of criticality for upstream units, criticality elements sum the requirements being received from downstream.

For allocation-combination graphs efficiency information must be taken into account while considering optimal load shedding. Assuming paths are shed in order of efficiency

Table 47: Information Communicated with Graph Edges from Figure 109

Edge	Requirement
1	R_1
2	$\frac{1}{\eta_1} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle$
3	$\frac{1}{\eta_1 \eta_3} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U3}{U3,U4} \right\rangle$
4	$\frac{1}{\eta_1 \eta_4} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U4}{U3,U4} \right\rangle$
5	$\frac{1}{\eta_1} R_1 \left\langle \frac{U1}{U1,U2} \right\rangle \left \left(\frac{1}{\eta_3} \left\langle \frac{U3}{U3,U4} \right\rangle , \frac{1}{\eta_4} \left\langle \frac{U4}{U3,U4} \right\rangle \right) \right.$
6	$\frac{1}{\eta_2} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle$
7	$\frac{1}{\eta_2 \eta_5} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U5}{U5,U6} \right\rangle$
8	$\frac{1}{\eta_2 \eta_6} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U6}{U5,U6} \right\rangle$
9	$\frac{1}{\eta_2} R_1 \left\langle \frac{U2}{U1,U2} \right\rangle \left \left(\frac{1}{\eta_5} \left\langle \frac{U5}{U5,U6} \right\rangle , \frac{1}{\eta_6} \left\langle \frac{U6}{U5,U6} \right\rangle \right) \right.$
10	$R_1 \left \left(\frac{1}{\eta_1 \eta_3 \eta_7} \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U3}{U3,U4} \right\rangle , \frac{1}{\eta_1 \eta_4 \eta_7} \left\langle \frac{U1}{U1,U2} \right\rangle \left\langle \frac{U4}{U3,U4} \right\rangle , \right. \right.$ $\left. \frac{1}{\eta_2 \eta_5 \eta_8} \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U5}{U5,U6} \right\rangle , \frac{1}{\eta_2 \eta_6 \eta_8} \left\langle \frac{U2}{U1,U2} \right\rangle \left\langle \frac{U6}{U5,U6} \right\rangle \right)$

(least efficient to most efficient) the slope of the function/hazard relationship will sequentially increase as the shed parallel paths increase in efficiency. Graph tags, therefore, include information regarding the efficiency of the paths. The parenthesized groupings of elements seen in table 47 indicate that the associated criticality curve (R_1 in the case of edge 10) must be reformed with regards to the capability and efficiencies of the parallel unit paths.

Looking at combination elements in this example, the criticalities of engines U7 and U8 are derived through an efficiency scaled simple relationship with the buses U1 and U2 respectively. Additionally, the criticality of the fuel system (U9) receiving edge 10 can be expressed as an efficiency adjusted simple relationship with the original boundary requirement to provide power R1. With total loss at U9 the requirement, R1, cannot be fulfilled.

Decomposing and propagating unit criticality in this fashion imposes reliability constraints which limit the capacity and reliability of each unit depending on its specific functional dependencies. These reliability constraints are defined with respect to architecture specific load shedding strategies generated by hazard minimization for every combination relationship which consider the support of the ultimate downstream functionality.

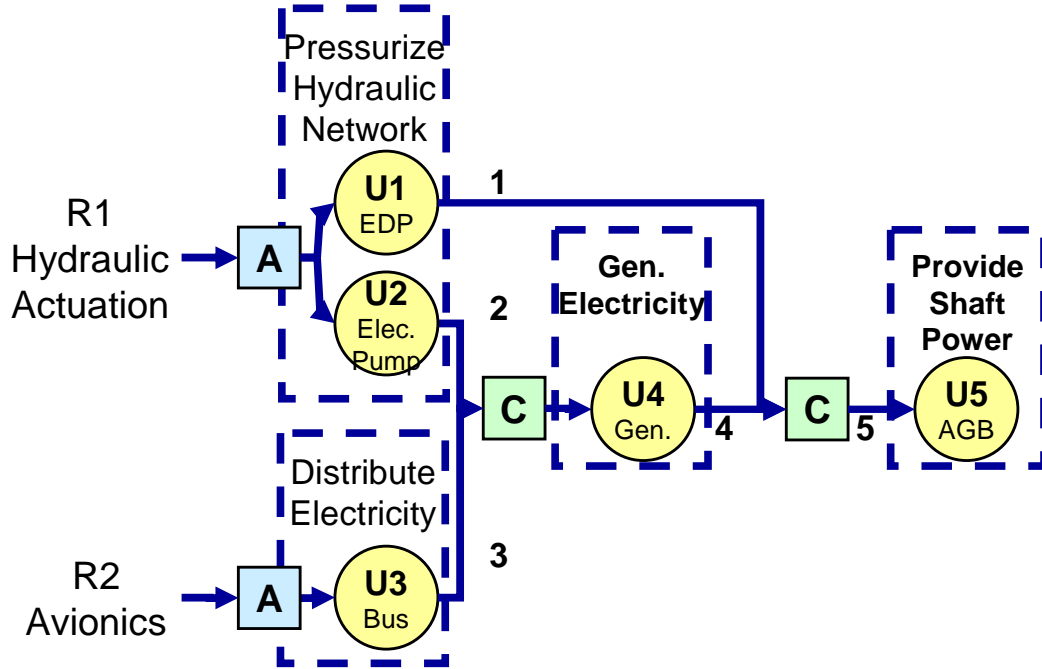
E.3.1 Staggered Combinations and Allocations

Load shedding optimization is further complicated when multiple boundary functions, combinations, and allocations interact simultaneously. Two staggered relationships are displayed in figure 110. In the staggered combination situation (figure 110a), U5 supports both requirements R1 and R2. However, multiple combinations are imposed. The staggered allocation relationship (figure 110b) presents an issue of combining portions of a downstream requirement which can be fulfilled by multiple sources following multiple allocations.

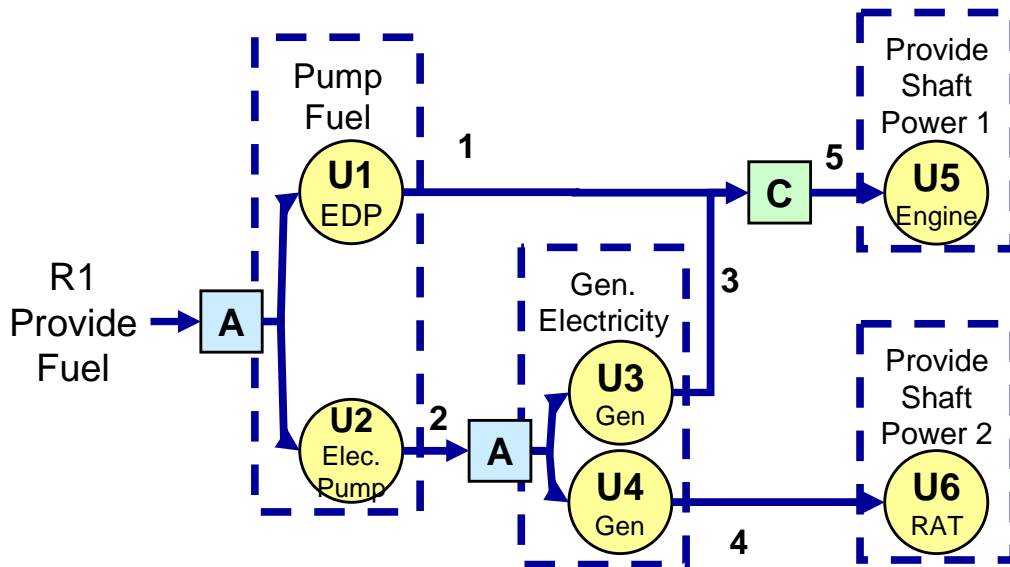
Applying the notation introduced in the previous section assists in propagating requirements. This notation and decomposition is applied here for the staggered combination graph. For illustrations sake linear function/hazard relationships for the boundary requirements are assumed. This assumption is not a requirement to apply this criticality propagation but is employed to simplify the visualization of the effect of allocation and combination relationships. Unit efficiencies are also assumed constant for this example. The criticality relationships for each of the graph edges are displayed in figure 111. The horizontal axis of these graphs represents the magnitude of capability loss of the upstream element connected by the edge. The vertical axis represents the normalized criticality (catastrophic hazard =1, no effect=0). Associated allocation-combination notation and calculated graph notations are given in table 48.

Assuming a linear relationship between function and hazard for the boundary requirements yields figure 111a and b. The loss of ability to support requirement 1 or 2 (R1, R2) yields catastrophic consequences. Edges 1 and 2 come from the allocation element upstream of R1. As shown in figure 111 c and d, loss of functionality of each redundant unit yields no hazardous effect until a threshold has been crossed. This threshold is defined by the overall capacity of the functional group. Additionally, total failure of one of the units does not mean loss of functional capability. The max hazard incurred by each independent unit failure corresponds to the capacity of the element with regard to the total functional requirements.

Edge 3 maintains a linear relationship with a catastrophic failure for 100% loss of the

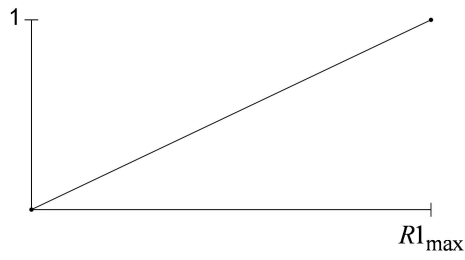


(a) Staggered Combinations

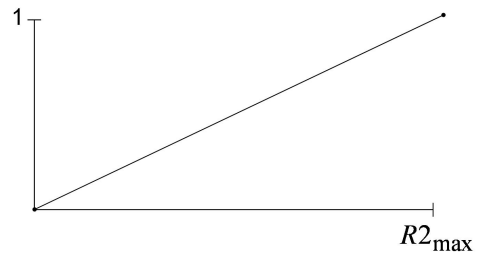


(b) Staggered Allocations

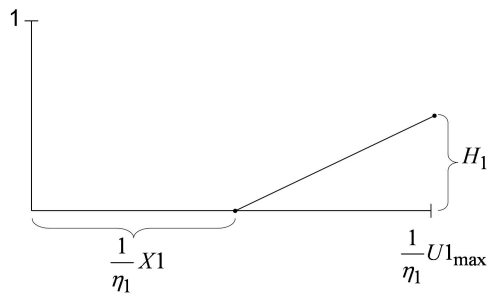
Figure 110: Requirements Propagation with Complex Allocations and Combinations



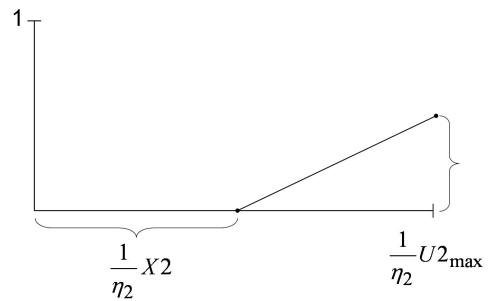
(a) Edge R1



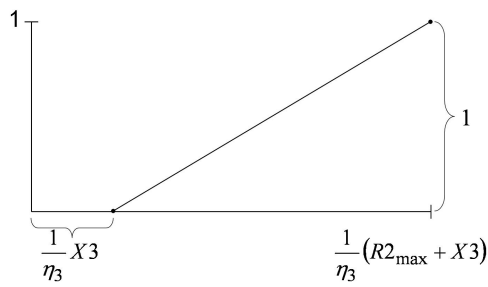
(b) Edge R2



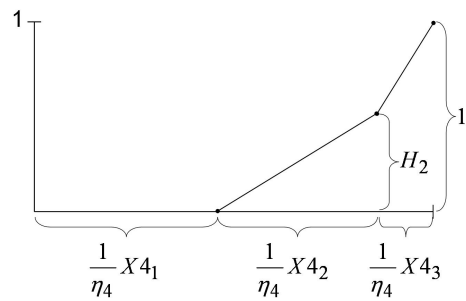
(c) Edge 1



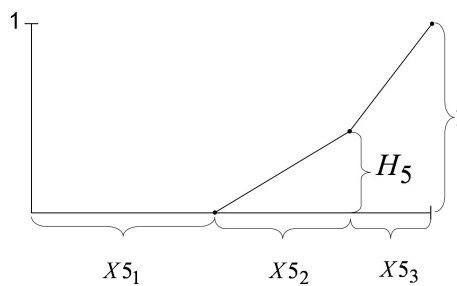
(d) Edge 2



(e) Edge 3



(f) Edge 4



(g) Edge 5

Figure 111: Function/Hazard Relationships for Edges of the Staggered Combination Graph Depicted in Figure 110a.

Table 48: Propagation of Function/Hazard Relationship for the Edges in Figure 110a.

Equations	
111c.	$\text{Notation : } \frac{1}{\eta_1} R_1 \left\langle \frac{U_1}{U_1, U_2} \right\rangle$ $X_1 = U_{1_{max}} + U_{2_{max}} - R_{1_{max}}$ $H_1 = H_{R_1}(U_{1_{max}})$
111d.	$\text{Notation : } \frac{1}{\eta_2} R_1 \left\langle \frac{U_2}{U_1, U_2} \right\rangle$ $X_2 = U_{1_{max}} + U_{2_{max}} - R_{1_{max}}$ $H_2 = H_{R_1}(U_{2_{max}})$
111e.	$\text{Notation : } \frac{1}{\eta_3} R_1$ $X_3 = U_{3_{max}} - R_{2_{max}}$
111f.	$\text{Notation : } \frac{1}{\eta_4} \left(\frac{1}{\eta_2} R_1 \left\langle \frac{U_2}{U_1, U_2} \right\rangle, \frac{1}{\eta_3} R_2 \right)$ $X_{4_1} = U_{4_{max}} - \frac{1}{\eta_2} (U_{2_{max}} - X_2) - \frac{1}{\eta_3} (U_{3_{max}} - X_3)$ $X_{4_2} = \frac{1}{\eta_2} U_{2_{max}} - \frac{1}{\eta_2} X_2$ $X_{4_3} = \frac{1}{\eta_3} R_{3_{max}} - \left[R_3(H_2) - \frac{1}{\eta_3} X_3 \right]$
111g.	$\text{Notation : } \frac{1}{\eta_4} \left(\frac{1}{\eta_1} R_1 \left\langle \frac{U_1}{U_1, U_2} \right\rangle, \frac{1}{\eta_2} R_1 \left\langle \frac{U_2}{U_1, U_2} \right\rangle, \frac{1}{\eta_3} R_2 \right)$ $X_{5_1} = \max \left(\frac{1}{\eta_1}, \frac{1}{\eta_2 \eta_3} \right) X_1 + \frac{1}{\eta_3 \eta_4} X_3$ $X_{5_2} = \left\{ \begin{array}{l} \frac{1}{\eta_1} \leq \frac{1}{\eta_2 \eta_4} : \frac{1}{\eta_1} U_{1_{max}} - \frac{1}{\eta_1} X_1 + R_3(H_1) \\ o.w. : \frac{1}{\eta_2 \eta_4} U_{2_{max}} - \frac{1}{\eta_2 \eta_4} X_1 + R_3(H_2) \end{array} \right\}$ $X_{5_3} = \left\{ \begin{array}{l} \frac{1}{\eta_1} \leq \frac{1}{\eta_2 \eta_4} : \frac{1}{\eta_2 \eta_4} U_{2_{max}} - \frac{1}{\eta_2 \eta_4} X_2 + [R_3(H_1 + H_2) - R_3(H_1)] \\ o.w. : \frac{1}{\eta_1} U_{1_{max}} - \frac{1}{\eta_1} X_1 + [R_3(H_1 + H_2) - R_3(H_2)] \end{array} \right\}$ $H_5 = \left\{ \begin{array}{l} \frac{1}{\eta_1} \leq \frac{1}{\eta_2 \eta_4} : H_1 \\ o.w. : H_2 \end{array} \right\}$

First column in reference to the graph displayed in figure 111

upstream unit. However, this criticality is offset by the overrating of U3 and scaled by U3 efficiency.

Calculating the criticality of requirements communicated through edge 4 begins to address optimal load shedding. No hazard is seen with failures of units upstream of U4 until all overrated capability has been lost from U2, U3, and U4. The first linear increase in hazard occurs with simultaneous failure through U2 and U3 until the max hazard for U2 loss has been seen. The steeper linear section occurs once U2 has lost all functional support and R1 has lost all possible capability through U4 failure. Therefore, this second section represents loss to R1.

Edge 5 has 4 linear sections. The first is a constant offset which includes the overrating associated with the path R2-U3-U4 and the maximum available overrating from R1-U1 or R1-U2-U4. The second section includes load shedding for the least efficient path from U1 to U5 and the path from U2 to U5. Once load has been shed from the least efficient path, the third section represents proportional losses through the more efficient path.

Characterizing the system in terms of a directed graph through functional induction relationships between elements allows criticality relationships to be propagated throughout a complex system through unit interdependencies. Supplying information regarding downstream graphical relationships to the upstream load providers allows complicated relationships to be reduced in terms of their impact on the ultimate provision of some capability demand expressed at the platform level. Propagating this information throughout the system is necessary in order to optimize load shedding for each combination relationship.

While calculations for this example do not extend into the time domain, these graphs can represent the projection of the hazard curve for a given failure duration (τ).

Additionally, with more complex unit requirement propagation (i.e. a requirement criticality coming out of a unit has a nonlinear relationship with incoming requirement criticality) downstream *%loss* must be expressed as a function of upstream *%loss*. Therefore, to fully characterize this continuous relationship future work will explore the use of surrogate models in defining the efficiencies as a function of magnitude of requirements and other environment conditions.

E.4 Analytical Formulation Limitations

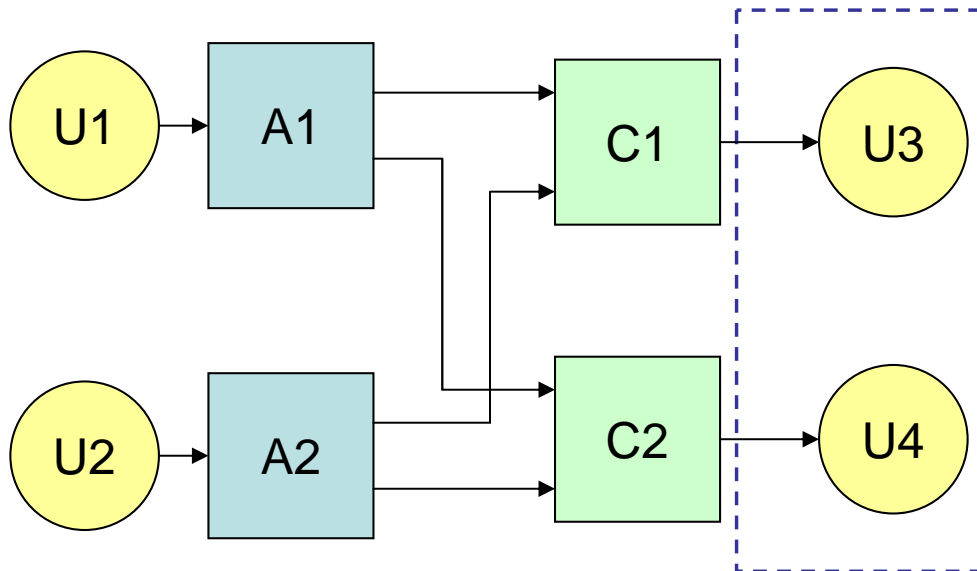
Certain limitations exist in applying this analytical process to the allocation of criticality throughout a system. As is evident in the analysis presented in tables 111 and 48, even relatively small systems mathematic formulations become very complex. As the system size and interconnectivity increases analytical formulations become inordinately heavy. Linear gains are also applied to represent the relationships between upstream capability available and downstream capability for each component of the system.

Additionally, certain system features necessitate numeric evaluation. These include systems dedicated to multiple system boundary functions which are allocated to multiple upstream combinations. When the total requirement is entirely allocated to the source the graph can be simplified as indicated in the figure 112 a. Because the combination elements $C1$ and $C2$ completely fulfill the requirements from allocation elements $A1$ and $A2$, the allocations/combinations relationships can be reposed as a combination/allocation relationship. This is illustrated in figure 112 b.

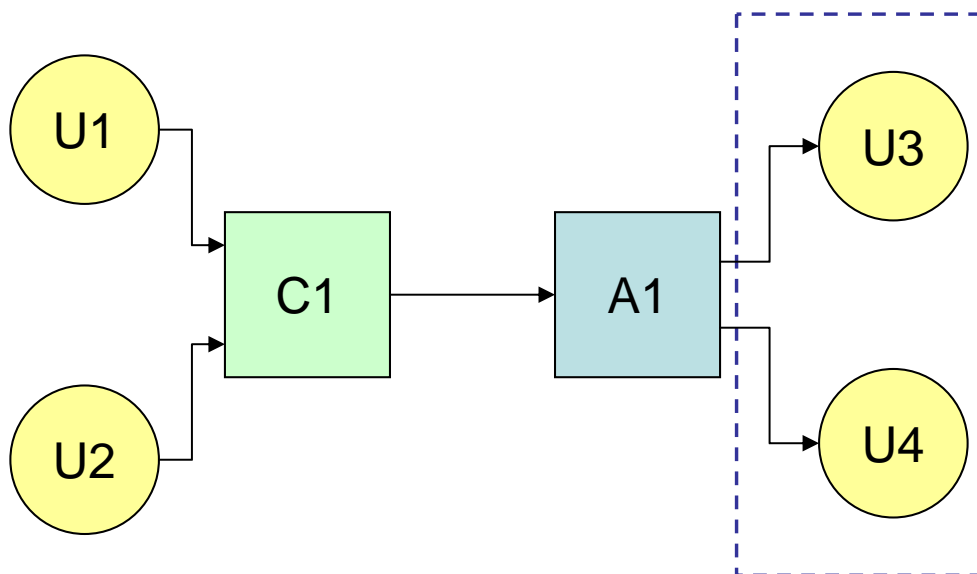
Table 49: Information Communicated with Graph Edges from Figure 112

Edge	Requirement	Simplified Graph Requirements
1	$\frac{1}{\eta_1} R_1$	
2	$\frac{1}{\eta_2} R_2$	
3	$\frac{1}{\eta_1} R_1 \left\langle \frac{C_{1,1}}{C_{1,1}, C_{2,1}} \right\rangle$	
4	$\frac{1}{\eta_1} R_1 \left\langle \frac{C_{2,1}}{C_{1,1}, C_{2,1}} \right\rangle$	
5	$\frac{1}{\eta_2} R_2 \left\langle \frac{C_{1,2}}{C_{1,1}, C_{1,2}} \right\rangle$	
6	$\frac{1}{\eta_2} R_2 \left\langle \frac{C_{2,2}}{C_{2,1}, C_{2,2}} \right\rangle$	
10	$\left(\frac{1}{\eta_1} R_1 \left\langle \frac{C_{1,1}}{C_{1,1}, C_{2,1}} \right\rangle, \frac{1}{\eta_2} R_2 \left\langle \frac{C_{1,2}}{C_{1,1}, C_{1,2}} \right\rangle \right)$	$\left(\frac{1}{\eta_1} R_1, \frac{1}{\eta_2} R_2 \right) \left\langle \frac{U_3}{U_3, U_4} \right\rangle$
11	$\left(\frac{1}{\eta_1} R_1 \left\langle \frac{C_{2,1}}{C_{1,1}, C_{2,1}} \right\rangle, \frac{1}{\eta_2} R_2 \left\langle \frac{C_{2,2}}{C_{2,1}, C_{2,2}} \right\rangle \right)$	$\left(\frac{1}{\eta_1} R_1, \frac{1}{\eta_2} R_2 \right) \left\langle \frac{U_4}{U_3, U_4} \right\rangle$

When combination elements are not entirely dedicated to the partial fulfillment of downstream requirements, allocation variables must be applied. Consider the system in figure 113. The analytical formulation in this circumstance cannot be reduced completely and numerical optimization must be performed in order to determine the optimal allocation of component capability ($\alpha_{i,j}$).



(a) Simplification of Allocation-Combination Relationship



(b) Combination-Allocation Relationship

Figure 112: Grouped Allocation-Combination Relationship

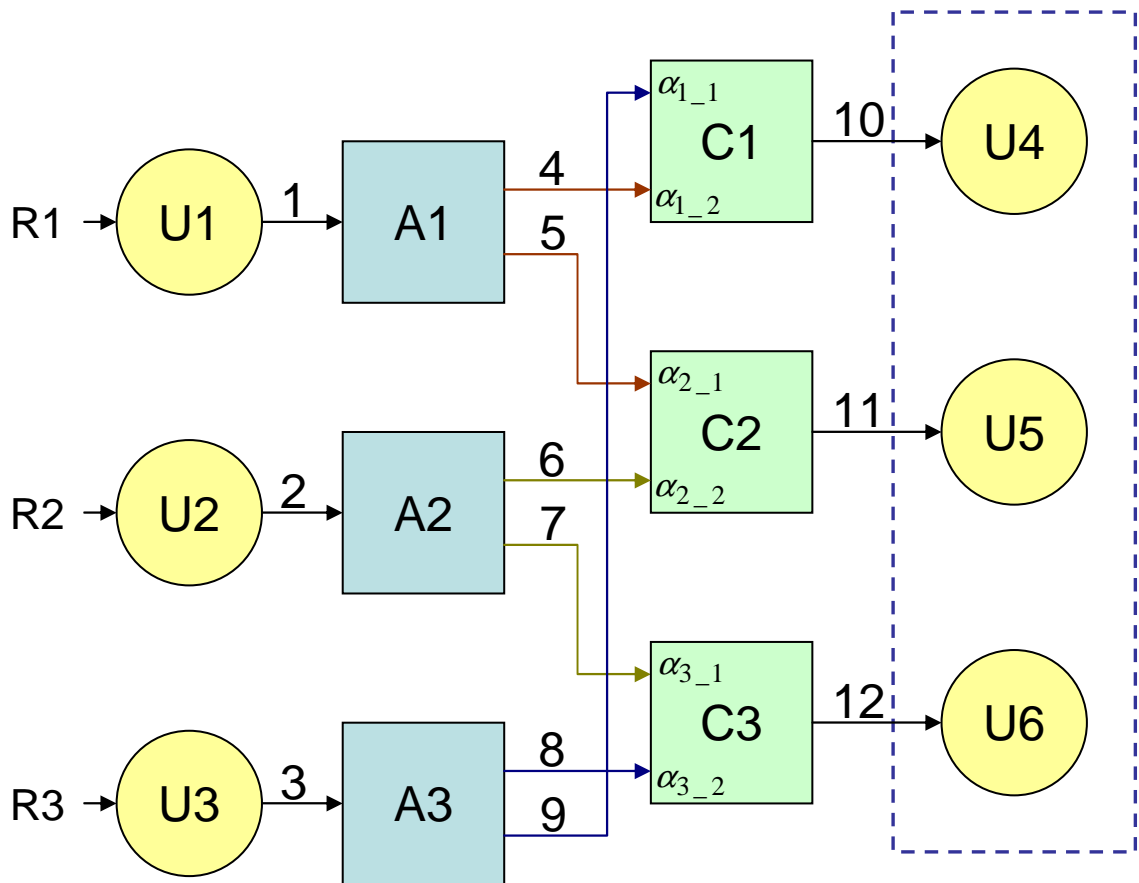


Figure 113: Irreducible Allocation-Combination Relationship

Table 50: Information Communicated with Graph Edges from Figure 113

Edge	Requirement	Simplified Graph Requirement
1	$\frac{1}{\eta_1} R_1$	
2	$\frac{1}{\eta_2} R_2$	
3	$\frac{1}{\eta_3} R_3$	
4	$\frac{1}{\eta_1} R_1 \left\langle \frac{C_{1,2}}{C_{1,2}, C_{2,1}} \right\rangle$	$\frac{1}{\eta_1} R_1 \left\langle \frac{\alpha_{1,2} U_4}{\alpha_{1,2} U_4, \alpha_{2,1} U_5} \right\rangle$
5	$\frac{1}{\eta_1} R_1 \left\langle \frac{C_{2,1}}{C_{1,2}, C_{2,1}} \right\rangle$	$\frac{1}{\eta_1} R_1 \left\langle \frac{\alpha_{2,1} U_5}{\alpha_{1,2} U_4, \alpha_{2,1} U_5} \right\rangle$
6	$\frac{1}{\eta_2} R_2 \left\langle \frac{C_{2,2}}{C_{2,2}, C_{3,1}} \right\rangle$	$\frac{1}{\eta_2} R_2 \left\langle \frac{\alpha_{2,2} U_5}{\alpha_{2,2} U_5, \alpha_{3,1} U_6} \right\rangle$
7	$\frac{1}{\eta_2} R_2 \left\langle \frac{C_{3,1}}{C_{2,2}, C_{3,1}} \right\rangle$	$\frac{1}{\eta_2} R_2 \left\langle \frac{\alpha_{3,1} U_6}{\alpha_{2,2} U_5, \alpha_{3,1} U_6} \right\rangle$
8	$\frac{1}{\eta_3} R_3 \left\langle \frac{C_{3,2}}{C_{3,2}, C_{1,1}} \right\rangle$	$\frac{1}{\eta_3} R_3 \left\langle \frac{\alpha_{3,2} U_6}{\alpha_{3,2} U_6, \alpha_{1,1} U_4} \right\rangle$
9	$\frac{1}{\eta_3} R_3 \left\langle \frac{C_{1,1}}{C_{3,2}, C_{1,1}} \right\rangle$	$\frac{1}{\eta_3} R_3 \left\langle \frac{\alpha_{1,1} U_4}{\alpha_{3,2} U_6, \alpha_{1,1} U_4} \right\rangle$
10	$\left(\frac{1}{\eta_3} R_3 \left\langle \frac{C_{1,1}}{C_{3,2}, C_{1,1}} \right\rangle, \frac{1}{\eta_1} R_1 \left\langle \frac{C_{1,2}}{C_{1,2}, C_{2,1}} \right\rangle \right)$	$\left(\frac{1}{\eta_3} R_3 \left\langle \frac{\alpha_{1,1} U_4}{\alpha_{3,2} U_6, \alpha_{1,1} U_4} \right\rangle, \frac{1}{\eta_1} R_1 \left\langle \frac{\alpha_{1,2} U_4}{\alpha_{1,2} U_4, \alpha_{2,1} U_5} \right\rangle \right)$
11	$\left(\frac{1}{\eta_1} R_1 \left\langle \frac{C_{2,1}}{C_{1,2}, C_{2,1}} \right\rangle, \frac{1}{\eta_2} R_2 \left\langle \frac{C_{2,2}}{C_{2,2}, C_{3,1}} \right\rangle \right)$	$\left(\frac{1}{\eta_1} R_1 \left\langle \frac{\alpha_{2,1} U_5}{\alpha_{1,2} U_4, \alpha_{2,1} U_5} \right\rangle, \frac{1}{\eta_2} R_2 \left\langle \frac{\alpha_{2,2} U_5}{\alpha_{2,2} U_5, \alpha_{3,1} U_6} \right\rangle \right)$
12	$\left(\frac{1}{\eta_2} R_2 \left\langle \frac{C_{3,1}}{C_{2,2}, C_{3,1}} \right\rangle, \frac{1}{\eta_3} R_3 \left\langle \frac{C_{3,2}}{C_{3,2}, C_{1,1}} \right\rangle \right)$	$\left(\frac{1}{\eta_2} R_2 \left\langle \frac{\alpha_{3,1} U_6}{\alpha_{2,2} U_5, \alpha_{3,1} U_6} \right\rangle, \frac{1}{\eta_3} R_3 \left\langle \frac{\alpha_{3,2} U_6}{\alpha_{3,2} U_6, \alpha_{1,1} U_4} \right\rangle \right)$

$$\sum_{j=1}^2 \alpha_{i,j} = 1, \quad i = 1 : 3$$

Considering the complex nature of aircraft subsystems and the desired variability in architecture concept during exploratory design, an analytical approach is insufficient in itself for identifying and allocating off-nominal requirements. Determining ideal allocation of capabilities during off-nominal operations requires numeric analysis of the complex architecture.

Another shortcoming to this analytical approach is that it does not assign criticality to component groups. Fail-safe requirements dictate that no single point failure will result in a catastrophic consequence. The reliability requirements for a single system or component are not solely a function of loss incurred by its own loss, but also the combined loss when multiple failures occur simultaneously. The emergent nature of these requirements requires the criticality of groupings of components to be ascertained.

APPENDIX F

ADJACENCY MATRICES FOR VEHICLE SYSTEMS ARCHITECTURES

The adjacency matrices are sparsely populated. All values in the adjacency matrix are zero except for the indices listed in the following tables.

F.1 Conventional Architecture

Table 51 lists all matrix indices which are set by the allocation vector (α) for the conventional architecture. Table 52 lists all matrix indices which are equal to 1 for the conventional architecture.

Table 51: Conventional Architecture Adjacency Matrix Indices given by Allocation Variables

$A[24,26]=\alpha_{24,26}$	$A[96,29]=\alpha_{96,29}$	$A[114,32]=\alpha_{114,32}$
$A[81,26]=\alpha_{81,26}$	$A[99,29]=\alpha_{99,29}$	$A[115,32]=\alpha_{115,32}$
$A[85,28]=\alpha_{85,28}$	$A[102,29]=\alpha_{102,29}$	$A[116,37]=\alpha_{116,37}$
$A[88,28]=\alpha_{88,28}$	$A[104,29]=\alpha_{104,29}$	$A[117,37]=\alpha_{117,37}$
$A[91,28]=\alpha_{91,28}$	$A[107,30]=\alpha_{107,30}$	$A[120,63]=\alpha_{120,63}$
$A[93,28]=\alpha_{93,28}$	$A[110,30]=\alpha_{110,30}$	$A[121,63]=\alpha_{121,63}$

The α values in table 51 are augmented by the optimizer to identify optimal failure allocation for each fail case. Not all α values act through the adjacency matrix. Additional values are assigned directly to units which provide for multiple functionalities.

Table 52: Conventional Architecture Adjacency Matrix Indices Equal to One

A[65,1]	A[82,2]	A[124,3]	A[3,11]	A[18,18]	A[132,27]
A[73,1]	A[86,2]	A[126,3]	A[11,11]	A[61,18]	A[113,31]
A[122,1]	A[89,2]	A[1,9]	A[5,13]	A[22,22]	A[130,33]
A[66,2]	A[97,2]	A[9,9]	A[13,13]	A[62,22]	A[116,35]
A[74,2]	A[100,2]	A[2,10]	A[128,14]	A[25,25]	A[117,36]
	A[108,2]	A[10,10]		A[63,25]	
A[15,39]	A[28,45]	A[20,50]	A[118,55]	A[120,61]	A[42,69]
A[39,39]	A[45,45]	A[50,50]	A[119,56]	A[121,62]	A[69,69]
A[16,41]	A[134,46]	A[21,52]	A[23,58]	A[38,67]	A[44,70]
A[41,41]	A[19,48]	A[52,52]	A[58,58]	A[67,67]	A[70,70]
A[17,43]	A[48,48]	A[29,54]	A[30,60]	A[40,68]	A[46,71]
A[43,43]		A[54,54]	A[60,60]	A[68,68]	A[71,71]
A[47,75]	A[53,78]	A[59,84]	A[55,92]	A[36,101]	A[37,109]
A[75,75]	A[78,78]	A[84,84]	A[92,92]	A[101,101]	A[109,109]
A[49,76]	A[46,79]	A[34,87]	A[64,95]	A[56,103]	A[80,112]
A[76,76]	A[79,79]	A[87,87]	A[95,95]	A[103,103]	A[112,112]
A[51,77]	A[57,83]	A[35,90]	A[34,98]	A[72,106]	A[94,113]
A[77,77]	A[83,83]	A[90,90]	A[98,98]	A[106,106]	A[105,114]
A[111,115]	A[32,127]	A[7,133]	A[14,139]	A[27,145]	
A[26,123]	A[127,127]	A[133,133]	A[139,139]	A[145,145]	
A[123,123]	A[4,129]	A[8,135]	A[14,141]	A[33,147]	
A[31,125]	A[129,129]	A[135,135]	A[141,141]	A[147,147]	
A[125,125]	A[6,131]	A[12,137]	A[27,143]	A[33,149]	
	A[131,131]	A[137,137]	A[143,143]	A[149,149]	

F.2 ‘All-Electric’ Architecture

Table 53 lists all matrix indices which are set by the allocation vector (α) for the ‘more-electric’ architecture. Table 54 lists all matrix indices which are equal to 1 for the ‘more-electric’ architecture.

Table 53: ‘All-Electric’ Architecture Adjacency Matrix Indices given by Allocation Variables

$A[64,11]=\alpha_{64,11}$	$A[64,12]=\alpha_{64,12}$	$A[72,15]=\alpha_{72,15}$
$A[65,11]=\alpha_{65,11}$	$A[65,12]=\alpha_{65,12}$	$A[75,15]=\alpha_{75,15}$
$A[66,11]=\alpha_{66,11}$	$A[66,12]=\alpha_{66,12}$	$A[78,26]=\alpha_{78,26}$
$A[67,11]=\alpha_{67,11}$	$A[67,12]=\alpha_{67,12}$	$A[81,26]=\alpha_{81,26}$
$A[68,11]=\alpha_{68,11}$	$A[68,12]=\alpha_{68,12}$	$A[84,27]=\alpha_{84,27}$
$A[69,11]=\alpha_{69,11}$	$A[69,12]=\alpha_{69,12}$	$A[85,27]=\alpha_{85,27}$
$A[70,11]=\alpha_{70,11}$	$A[70,12]=\alpha_{70,12}$	$A[86,27]=\alpha_{86,27}$
$A[71,11]=\alpha_{71,11}$	$A[71,12]=\alpha_{71,12}$	
$A[84,28]=\alpha_{84,28}$	$A[87,31]=\alpha_{87,31}$	$A[89,35]=\alpha_{89,35}$
$A[85,28]=\alpha_{85,28}$	$A[88,31]=\alpha_{88,31}$	$A[90,35]=\alpha_{90,35}$
$A[86,28]=\alpha_{86,28}$	$A[87,32]=\alpha_{87,32}$	$A[89,36]=\alpha_{89,36}$
$A[87,29]=\alpha_{87,29}$	$A[88,32]=\alpha_{88,32}$	$A[90,36]=\alpha_{90,36}$
$A[88,29]=\alpha_{88,29}$	$A[87,33]=\alpha_{87,33}$	$A[91,37]=\alpha_{91,37}$
$A[87,30]=\alpha_{87,30}$	$A[88,33]=\alpha_{88,33}$	$A[92,37]=\alpha_{92,37}$
$A[88,30]=\alpha_{88,30}$	$A[89,34]=\alpha_{89,34}$	$A[91,38]=\alpha_{91,38}$
	$A[90,34]=\alpha_{90,34}$	$A[92,38]=\alpha_{92,38}$

Do to the more integrated nature of the electric architecture, more than double the number of α values are required for load shedding optimization. Sixteen of these allocation variables assign capability from the 270VDC Busses ($A[-,11]$ and $A[-,12]$).

Table 54: ‘All-Electric’ Architecture Adjacency Matrix Indices Equal to One

A[53,1]	A[18,2]	A[60,2]	A[103,3]	A[3,10]	A[22,22]
A[59,1]	A[21,2]	A[79,2]	A[105,3]	A[10,10]	A[29,22]
A[93,1]	A[24,2]	A[82,2]	A[1,8]	A[107,13]	A[25,25]
A[95,1]	A[44,2]	A[97,2]	A[8,8]	A[111,14]	A[30,25]
	A[50,2]	A[100,2]	A[2,9]	A[19,19]	A[26,40]
	A[54,2]		A[9,9]	A[39,19]	A[40,40]
A[20,42]	A[23,48]	A[43,56]	A[49,62]	A[101,66]	A[37,74]
A[42,42]	A[48,48]	A[56,56]	A[62,62]	A[73,67]	A[74,74]
A[32,45]	A[33,51]	A[46,57]	A[46,63]	A[76,68]	A[38,77]
A[45,45]	A[51,51]	A[57,57]	A[63,63]	A[128,69]	A[77,77]
A[113,46]	A[41,55]	A[47,61]	A[109,64]	A[131,70]	A[31,80]
	A[55,55]	A[61,61]	A[98,65]	A[134,71]	A[80,80]
A[34,83]	A[115,87]	A[15,94]	A[36,102]	A[4,108]	A[7,114]
A[83,83]	A[117,88]	A[94,94]	A[102,102]	A[108,108]	A[114,114]
A[127,84]	A[119,89]	A[16,96]	A[27,104]	A[5,110]	A[11,116]
A[130,85]	A[121,90]	A[96,96]	A[104,104]	A[110,110]	A[116,116]
A[133,86]	A[123,91]	A[35,99]	A[28,106]	A[6,112]	A[12,118]
	A[125,92]	A[99,99]	A[106,106]	A[112,112]	A[118,118]
A[13,120]	A[14,124]	A[52,129]	A[17,135]		
A[120,120]	A[124,124]	A[129,129]	A[135,135]		
A[13,122]	A[14,126]	A[58,132]			
A[122,122]	A[126,126]	A[132,132]			

APPENDIX G

OPTIMIZATION ROUTINE FOR CONVENTIONAL ARCHITECTURE

The routine entitled *./FindMinHazards.m* determines the optimal allocation of capability which minimizes the operational hazards associated with the failure of the units indicated by the $\{cindex\}$ array. Four outputs are generated by this routine. All optimal failure information is given in 1 % increments for magnitude of failure from 0% failed to 100% failed.

[*AllCaps*] - This 2 dimensional, $n \times 101$ matrix lists all n unit and system input and output capabilities for level of failure.

[*Hazard*] - This matrix gives the magnitude of the system level hazard incurred from 0 to 100% failure in increments of 1%.

[*alphavals*] - This 2 dimensional, $p \times 101$ matrix gives the values of the capability allocation variables for all magnitude of failure.

[*initalphas*] - This vector gives the initial setting for the α variables which yield 0 hazard. This information is used as the starting point for subsequent optimizations.

Seven input variables are used to generate the hazard information: the adjacency matrix ($[A]$), initial capability ($[C]$), external unit capability limits ($\{Clims\}$), the failure indices ($\{cindex\}$), the initial allocation variable values ($\{allalphas\}$), the adjacency matrix indices for these allocation variables ($[matrixalphainds]$), and the mission segment being considered (*misseg*).

The adjacency matrix is constructed with the adjacency matrix, $[A]$, the allocation variables, $[allalphas]$, and the locations where these allocation variables act, $[matrixalphainds]$. $[A]$ is a square matrix which maps the flow of capability between system units. When multiple users receive capability from one unit in the system the allocation variable determine

how capability is proportionally assigned to the users.

The initial capability matrix $[C]$ and any external limitation on unit capabilities ($\{Clims\}$). The capability matrix carries all necessary information that is required to characterize the functional relationship between two units. Shaft power capability is given $C(,1) = power$ and $C(,2) = speed$. Pneumatic airflow is given by $C(,1) = \dot{m}$, $C(,2) = Pressure$, and $C(,3) = Temperature$. Thrust is the most complicated capability variable. Engine thrust capability requires is characterized by $C(,1) = Thrust$, $C(,2) = \%Failure$, $C(,3) = FuelFlow$, $C(,4) = EngineBleedHP$, $C(,5) = EngineBleedLP$, $C(,6) = EngineBleedFan$, $C(,7) = EngineHPShaftLoad$, and $C(,8) = EngineLPShaftLoad$. With two engines providing thrust the overall thrust capability is characterized by these variables for both engines.

The $\{cindex\}$ vector is used to limit the capability of the listed units. The indices in this vector correspond the specific row values in the $[Clims]$ matrix. As failures are imposed the capability limit value is scaled by the loss.

./FindMinHazards.m

```

1 function [AllCaps , Hazard , alphavals , initalphas]=FindMinHazards(A,C,Clims , cindex , allalphas ,
   matrixalphainds , misseg)
2 %% This function determines load shedding optimization (LSO) for the Conventional Architecture.
3 thestep=5; % Set step size for LSO
4 matrixalphainds=transpose(matrixalphainds); % Format alpha val indices
5
6 options=optimset('Tolfun',1e-3); % Optimization settings
7 options=optimset(options,'TolX',1e-3);
8 options=optimset(options,'MaxIter',10000);
9 initialalphavals(1,:)=allalphas;
10 exitflag=zeros(1,101);
11
12 as=length(allalphas); % Initialize output vars
13 alphavals=ones(101,as(1));
14 Hazard=zeros(1,101);
15
16 %% Perform initial optimizations
17 checkhazval=0;
18 s=0;
19 for x=0:thestep:100
20     for f=1:length(cindex)
21         Climscindex(f)=(1-x/100)*C(cindex(f),1); % Impose % failure
22     end
23     check=GethazardConv(A,C,Clims,initialalphavals(s,:),...
24         matrixalphainds,misseg); % Check initial hazard
25     if check==0 || checkhazval==1 % Check need to find optimal

```

```

26     alphavals(x+1,:)=initialalphavals(s,:);
27     Hazard(x+1)=0;
28     else
29         % Use gradient based fminsearch to find optimum
30         [alphavals(x+1,:), Hazard(x+1), exitflag(x+1)]=fminsearch(@(allalphas) GethazardConv(A,C,
           Clims, allalphas, matrixalphahinds, misseg), initialalphavals(s,:), options);
31     end
32     checkhazval = Hazard(x+1);
33     s=s+1;
34     capability(s)=(1-x/100)*C(cindex(1),1); % Store fail state
35     initialalphavals(s,:)=alphavals(x+1,:); % Store allocation variables
36     if x==0
37         initalphas=alphavals(x+1,:); % Store initial optimal
38     end
39 end
40
41 %% Fit pchip spline to alpha vals
42 allcaps=C(cindex(1),1):-C(cindex(1),1)/100:0;
43 for j=1:as(1)
44     alphavals(:,j)=pchip(capability, initialalphavals(:,j), allcaps);
45 end
46
47 %% Estimate hazards with alpha spline
48 for x=1:101
49     for f=1:length(cindex)
50         Clims(cindex(f))=(1-(x-1)/100)*C(cindex(f),1);
51     end
52     Hazard(x)=GethazardConv(A,C, Clims, alphavals(x,:), matrixalphahinds, misseg);
53 end
54
55 %% Check hazards and fill in with local optimization on smaller intervals
56 s=0;
57 yes=0;
58 for i=100:-1:1 % Check from 100% downward
59     if min(Hazard((i+1):101))<Hazard(i) && i~=1 % Check if monotonic
60         yes=yes+1;
61     else
62         if yes~=0
63             for new=1:(yes/3):yes+1 % Run 4 optimizations
64                 ind=i+yes+1-new;
65                 for f=1:length(cindex)
66                     Clims(cindex(f))=(1-(ind-1)/100)*C(cindex(f),1);
67                 end
68                 capability(s+1)=(1-(ind-1)/100)*C(cindex(1),1);
69                 [initialalphavals(s+1,:), Haz(s+1), exitflag(s+1)]=fminsearch(@(allalphas)
           GethazardConv(A,C, Clims, allalphas, matrixalphahinds, misseg), alphavals(round(ind
           +1),:), options);
70                 s=s+1;
71             end
72             for new=1:yes+1 % Resample with spline fit
73                 ind=i+yes+1-new;
74                 cap=(1-(ind-1)/100)*C(cindex(1),1);
75                 for f=1:length(cindex)
76                     Clims(cindex(f))=(1-(ind-1)/100)*C(cindex(f),1);
77             end

```



```

78         for j=1:sum(as)
79             alphavals(ind,j)=pchip(capability,initialalphavals(:,j),cap);
80         end
81         Hazard(ind)=GethazardConv(A,C,Clims,alphavals(ind,:),matrixalphainds,misseg);
82     end
83     yes=0;
84 end
85 end
86 end
87
88 %% Check hazards on 1% intervals
89 for i=100:-1:1
90     if min(Hazard((i+1):101))<Hazard(i) % Check if monotonic
91         for f=1:length(cindex) % Optimize all errors
92             Clims(cindex(f))=(1-(i-1)/100)*C(cindex(f),1);
93         end
94         [alphavals(i,:), Hazard(i), exitflag(i)]=fminsearch(@(allalphas) GethazardConv(A,C,Clims,
95             allalphas,matrixalphainds,misseg),alphavals(i+1,:),options);
96     end
97 Hazard=transpose(Hazard);
98
99 %% Find all capabilities with optimal alpha allocations
100 AllClims=Clims;
101 for i=1:101
102     for f=1:length(cindex)
103         AllClims(cindex(f))=(1-(i-1)/100)*C(cindex(f),1);
104     end
105     X=FindBFCaps(A,C,AllClims,alphavals(i,:),matrixalphainds);
106     AllCaps(:,i)=X(:,1);
107 end
108
109 %% Find proportional alpha values
110 thesum=zeros(101,length(matrixalphainds));
111 for i=1:length(matrixalphainds)
112     for j=1:length(matrixalphainds)
113         if matrixalphainds(j,2)==matrixalphainds(i,2)
114             thesum(:,i)=thesum(:,i)+abs(alphavals(:,j));
115         end
116     end
117 end
118 alphavals(:,1:length(matrixalphainds))=abs(alphavals(:,1:length(matrixalphainds)))./thesum;

```

The optimal allocation of capability is achieved by implementing the gradient based “*fminsearch*” embedded Matlab® routine. The optimization method is crucial to determining off-nominal performance attributes. More efficient and accurate optimizers could be identified and implemented for this process. However, the application of this optimizer was sufficient to address the hypothesis for this research. Exploration of more ideal optimization processes is a matter for ancillary research opportunities.

Optimal failure allocation is achieved by augmentation of the values in the *allalphas* matrix and determining its effect on the system as a whole. The function “./GethazardConv.m” is used to determine the system capability. This portion of the Matlab® code is autowritten from the structure and composition of the architecture as defined by the Architecture Design Environment (ADEN) as discussed in the methods chapter.

Hazard is calculated by the “*hazardfunction*” function call which consists of table lookups. These table lookups reflect the function/hazard relationship discussed in the methods chapter. All boundary function capability values (*Capsout*) not equal to -1 in this function call are active in hazard identification. This hazard lookup must also consider the mission segment in which the evaluation must take place (*misseg*).

The system capability itself is determined by the function “*FindBFCaps*”. This code is also autogenerated from the Architecture Design Environment. System attributes are read from the global Matlab workspace as defined by the user from system sizing and mission analysis. Following the formatting of input variables this function determines system capabilities by the the following equation:

$$\mathbf{X}_{i+1} = f([\mathbf{A}] \times \min(\mathbf{X}_i, \mathbf{K}_i), \mathbf{Op}) \quad (71)$$

The first column of the $[C]$ matrix is given by $\{X\}$. This value is determined by repetitive execution of the unit capability transfer functions, application of capability limits, and multiplication with the adjacency matrix. Other capability info is also transferred. Once the capability is converged the level of hazard associated with the available capability is determined.

./GethazardConv.m

```

1 function Hazard=GethazardConv(A,C,Clims , allalphas , matrixalphainds , misseg)
2     Capsout=FindBFCaps(A,C,Clims , allalphas , matrixalphainds);           % Get system capabilities
3     BFCaps=ones(8,22);                                                       % All inactive caps -1
4     BFCaps(2,:)=Capsout(5,:);                                               % Hot Pneumatic Capability
5     BFCaps(4,:)=Capsout(4,:);                                               % 28VDC Capability
6     BFCaps(6,:)=Capsout(6,:);                                               % 120VAC Capability
7     BFCaps(7,:)=Capsout(7,:);                                               % Hydraulic Capability
8     BFCaps(8,:)=Capsout(8,:);                                               % Thrust Capability
9     Hazard=hazardfunction(BFCaps, misseg);                                   % Get hazard value
10

```

```

11 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
12 function Capsout=FindBFCaps(A,C,Clims , allalphas , matrixalphainds)
13 %% This function calculates system capabilities
14 %Global unit attributes values set externally by designer in the ADEN
15 global AC120VLoads_AC120VReq_Cap_design
16 global PreCooler_1_HotPn_Cap_design
17 global PreCooler_2_HotPn_Cap_design
18 global RamHX_HotPn_Cap_design
19 global HPBleed_1_HPPn_Cap_design
20 global Zone_Length_ft_6_6_out
21 global Zone_Length_ft_6_5_out
22 global Zone_Length_ft_6_3_out
23 global Zone_Length_ft_5_5_out
24 global Zone_Length_ft_5_3_out
25 global Zone_Length_ft_3_3_out
26 global LPBleed_1_LPPn_Cap_design
27 global FanDuct_1_FanAir_Cap_design
28 global HPAGB_1_HPShaft_Cap_design
29 global HPBleed_2_HPPn_Cap_design
30 global LPBleed_2_LPPn_Cap_design
31 global FanDuct_2_FanAir_Cap_design
32 global HPAGB_2_HPShaft_Cap_design
33 global HPBleed_3_HPPn_Cap_design
34 global HPAGB_3_HPShaft_Cap_design
35 global Engine_1_HPPn_Cap_design
36 global Engine_1_LPPn_Cap_design
37 global Engine_1_FanAir_Cap_design
38 global Engine_1_HPShaft_Cap_design
39 global Engine_1_LPShaft_Cap_design
40 global Engine_1_Thrust_Cap_design
41 global Integration_Altitude_ft_out
42 global Integration_Mach_out
43 global Engine_2_HPPn_Cap_design
44 global Engine_2_LPPn_Cap_design
45 global Engine_2_FanAir_Cap_design
46 global Engine_2_HPShaft_Cap_design
47 global Engine_2_LPShaft_Cap_design
48 global Engine_2_Thrust_Cap_design
49 global APU_HPPn_Cap_design
50 global APU_HPShaft_Cap_design
51 global HSACGen_1_AC120V_Cap_design
52 global HSDC28VGen_1_DC28V_Cap_design
53 global Pump_1_Hyd_Cap_design
54 global FuelPump_1_FuelPress_Cap_design
55 global HSACGen_2_AC120V_Cap_design
56 global HSDC28VGen_2_DC28V_Cap_design
57 global Pump_2_Hyd_Cap_design
58 global FuelPump_2_FuelPress_Cap_design
59 global HSDC28VGen_3_DC28V_Cap_design
60 global FuelPump_3_FuelPress_Cap_design
61 global RamDuct_RamAir_Cap_design
62 global FuelSys_1_Fuel_Cap_design
63 global FuelSys_2_Fuel_Cap_design
64 global DC28VLoads_DC28VReq_Cap_design
65 global HotPnLoads_HotPnReq_Cap_design

```

```

66 global HydLoads_HydReq_Cap_design
67 global ThrustLoads_ThrustReq_Cap_design
68 global AC120VBus_AC120V_Cap_design
69 global Zone_Length_ft_6_2_out
70 global Zone_Length_ft_5_2_out
71 global Zone_Length_ft_2_2_out
72 global DC28VBus_1_DC28V_Cap_design
73 global DC28VBus_2_DC28V_Cap_design
74 global HydSys_1_Hyd_Cap_design
75 global HydSys_2_Hyd_Cap_design
76 global HotPnSys_1_HotPn_Cap_design
77 global HotPnSys_2_HotPn_Cap_design
78
79 % Initialize capability info
80 Cl=zeros(length(C),22);
81 thesize=size(matrixalphainds);
82 alphalength=size(allalphas);
83 matrixalpha=abs(allalphas(1:thesize(1)));
84 %Write allocation variable (allalphas) values to Adjacency matrix
85 for i=1:thesize(1)
86     thealphas=abs(transpose(allalphas(1:thesize(1)))));
87     thesum=sum((squeeze(matrixalphainds(:,2))=squeeze(matrixalphainds(i,2)).*thealphas);
88     matrixalpha(i)=matrixalpha(i)/thesum;
89     A(matrixalphainds(i,1),matrixalphainds(i,2))=matrixalpha(i);
90 end
91 alpha=allalphas(thesize+1:alphalength(2));
92 %Initialize the capability matrix
93 C(:,1)=min(Clims(:),C(:,1));
94 for i=1:2*length(C)
95     C(:,1)=A*C(:,1);
96     C(:,2)=A*C(:,2)./(sum(A,2));
97     C(:,3)=A*C(:,3)./(sum(A,2));
98 end
99 x=1;
100 k=1;
101 while x>0.000001 && k<3*length(C)
102     D(:,k)=C(:,1);
103     %Run All Unit Transfer Functions
104     [C(13,1)]=DS.AC120VLoads_Caps(C(12,1),AC120VLoads.AC120VReq_Cap_design);
105     [C(18,1:3)]=DS.PreCooler_Caps(C(15,1:3),C(16,1:3),C(17,1:3),PreCooler_1_HotPn_Cap_design);
106     [C(22,1:3)]=DS.PreCooler_Caps(C(19,1:3),C(20,1:3),C(21,1:3),PreCooler_2_HotPn_Cap_design);
107     [C(25,1:3)]=DS.RamHX_Caps(C(23,1:3),zeros(1,21),C(24,1:3),RamHX_HotPn_Cap_design);
108     [C(39,1:3)]=DS.HPBleed_Caps(C(38,1:3),HPBleed_1_HPPn_Cap_design,Zone_Length_ft_6_6_out+
        Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
        Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
109     [C(41,1:3)]=DS.LPBleed_Caps(C(40,1:3),LPBleed_1_LPPn_Cap_design,Zone_Length_ft_6_6_out+
        Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
        Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
110     [C(43,1:3)]=DS.FanDuct_Caps(C(42,1:3),FanDuct_1_FanAir_Cap_design,Zone_Length_ft_6_6_out+
        Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
        Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
111     [C(45,1:2)]=DS.HPAGB_Caps(C(44,1:2),HPAGB_1_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
        Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
        Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

```

112 [C(48,1:3)]=DS_HPbleed_Caps(C(47,1:3),HPBleed_2_HPPn_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

113 [C(50,1:3)]=DS_LPbleed_Caps(C(49,1:3),LPBleed_2_LPPn_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

114 [C(52,1:3)]=DS_FanDuct_Caps(C(51,1:3),FanDuct_2_FanAir_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

115 [C(54,1:2)]=DS_HPAGB_Caps(C(53,1:2),HPAGB_2_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

116 [C(58,1:3)]=DS_HPbleed_Caps(C(57,1:3),HPBleed_3_HPPn_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

117 [C(60,1:2)]=DS_HPAGB_Caps(C(59,1:2),HPAGB_3_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

118 [C(67,1:3),C(68,1:3),C(69,1:3),C(70,1:2),OneTempOut5,C(71,1:14)]=DS_Engine_Caps(C(65,1:3),
C(66,1),C(64,1),Engine_1_HPPn_Cap_design,Engine_1_LPPn_Cap_design,
Engine_1_FanAir_Cap_design,Engine_1_HPShaft_Cap_design,Engine_1_LPShaft_Cap_design,
Engine_1_Thrust_Cap_design,Integration_Altitude_ft_out,Integration_Mach_out,alpha(1),
alpha(2),alpha(3),alpha(4),0,alpha(5));

119 C(71,2)=max(eps,1-Clims(71)/7000);

120 [C(75,1:3),C(76,1:3),C(77,1:3),C(78,1:2),OneTempOut5,C(79,1:14)]=DS_Engine_Caps(C(73,1:3),
C(74,1),C(72,1),Engine_2_HPPn_Cap_design,Engine_2_LPPn_Cap_design,
Engine_2_FanAir_Cap_design,Engine_2_HPShaft_Cap_design,Engine_2_LPShaft_Cap_design,
Engine_2_Thrust_Cap_design,Integration_Altitude_ft_out,Integration_Mach_out,alpha(6),
alpha(7),alpha(8),alpha(9),0,alpha(10));

121 C(79,2)=max(eps,1-Clims(79)/7000);

122 [C(83,1:3),C(84,1:2)]=DS_APU_Caps(C(81,1:3),C(82,1),C(80,1),APU_HPPn_Cap_design,
APU_HPShaft_Cap_design,alpha(11),alpha(12));

123 [C(87,1)]=DS_HSACGen_Caps(C(85,1:2),C(86,1),HSACGen_1_AC120V_Cap_design);

124 [C(90,1)]=DS_HSDC28VGen_Caps(C(88,1:2),C(89,1),HSDC28VGen_1_DC28V_Cap_design);

125 [C(92,1)]=DS_Pump_Caps(C(91,1:2),Pump_1_Hyd_Cap_design);

126 [C(95,1)]=DS_FuelPump_Caps(C(94,1),C(93,1:2),FuelPump_1_FuelPress_Cap_design);

127 [C(98,1)]=DS_HSACGen_Caps(C(96,1:2),C(97,1),HSACGen_2_AC120V_Cap_design);

128 [C(101,1)]=DS_HSDC28VGen_Caps(C(99,1:2),C(100,1),HSDC28VGen_2_DC28V_Cap_design);

129 [C(103,1)]=DS_Pump_Caps(C(102,1:2),Pump_2_Hyd_Cap_design);

130 [C(106,1)]=DS_FuelPump_Caps(C(105,1),C(104,1:2),FuelPump_2_FuelPress_Cap_design);

131 [C(109,1)]=DS_HSDC28VGen_Caps(C(107,1:2),C(108,1),HSDC28VGen_3_DC28V_Cap_design);

132 [C(112,1)]=DS_FuelPump_Caps(C(111,1),C(110,1:2),FuelPump_3_FuelPress_Cap_design);

133 [C(123,1:3)]=DS_RamDuct_Caps(C(122,1:3),RamDuct_RamAir_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

134 [C(125,1)]=DS_FuelSys_Caps(C(124,1),FuelSys_1_Fuel_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

135 [C(127,1)]=DS_FuelSys_Caps(C(126,1),FuelSys_2_Fuel_Cap_design,Zone_Length_ft_6_6_out+
Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);

136 [C(129,1)]=DS_DC28VLoads_Caps(C(128,1),DC28VLoads_DC28VReq_Cap_design);

137 [C(131,1:3)]=DS_HotPnLoads_Caps(C(130,1:3),HotPnLoads_HotPnReq_Cap_design);

138 [C(133,1)]=DS_HydLoads_Caps(C(132,1),HydLoads_HydReq_Cap_design);

139 [C(135,1:14)]=DS_ThrustLoads_Caps(C(134,1:14),ThrustLoads_ThrustReq_Cap_design);

```

140 [C(137,1)]=DS.AC120VBus.Caps(C(136,1),AC120VBus.AC120V_Cap_design,Zone_Length_ft_6_6_out+
      Zone_Length_ft_6_5_out+Zone_Length_ft_6_2_out+Zone_Length_ft_5_5_out+
      Zone_Length_ft_5_2_out+Zone_Length_ft_2_2_out);
141 [C(139,1)]=DS.DC28VBus.Caps(C(138,1),DC28VBus_1.DC28V_Cap_design,Zone_Length_ft_6_6_out+
      Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
      Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
142 [C(141,1)]=DS.DC28VBus.Caps(C(140,1),DC28VBus_2.DC28V_Cap_design,Zone_Length_ft_6_6_out+
      Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
      Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
143 [C(143,1)]=DS.HydSys.Caps(C(142,1),HydSys_1.Hyd_Cap_design,Zone_Length_ft_6_6_out+
      Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
      Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
144 [C(145,1)]=DS.HydSys.Caps(C(144,1),HydSys_2.Hyd_Cap_design,Zone_Length_ft_6_6_out+
      Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_5_5_out+
      Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
145 [C(147,1:3)]=DS.HotPnSys.Caps(C(146,1:3),HotPnSys_1.HotPn_Cap_design,
      Zone_Length_ft_6_6_out+Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+
      Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
146 [C(149,1:3)]=DS.HotPnSys.Caps(C(148,1:3),HotPnSys_2.HotPn_Cap_design,
      Zone_Length_ft_6_6_out+Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+
      Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_3_3_out);
147 %Impose Capability Limits
148 C(:,1)=min(Clims,C(:,1));
149 %Special management of thrust capability
150 C1(8,2)=max(eps,1-Clims(8)/7000);
151 C1(71,2)=max(eps,1-Clims(71)/7000);
152 C1(79,2)=max(eps,1-Clims(79)/7000);
153 C1(134,2)=max(eps,1-Clims(134)/7000);
154 C1(135,2)=max(eps,1-Clims(135)/7000);
155 %Format capability vector
156 C1(:,1)=A*C(:,1);
157 C1(:,2)=(A*(C(:,2).*C(:,1)))/(C1(:,1)+eps);
158 C1(:,3)=(A*(C(:,3).*C(:,1)))/(C1(:,1)+eps);
159 %Special management of thrust capability
160 C1(8,:)=C(135,:);
161 X1 = nonzeros(A(46,:)'.*C(:,2));
162 X2 = nonzeros(A(46,:)'.*C(:,3));
163 X3 = nonzeros(A(46,:)'.*C(:,4));
164 X4 = nonzeros(A(46,:)'.*C(:,5));
165 X5 = nonzeros(A(46,:)'.*C(:,6));
166 X6 = nonzeros(A(46,:)'.*C(:,7));
167 X7 = nonzeros(A(46,:)'.*C(:,8));
168 for r=1:length(X1)
169     C1(46,1+r) = X1(r);
170 end
171 for r=1:length(X2)
172     C1(46,1+1*2+r) = X2(r);
173 end
174 for r=1:length(X3)
175     C1(46,1+2*2+r) = X3(r);
176 end
177 for r=1:length(X4)
178     C1(46,1+3*2+r) = X4(r);
179 end
180 for r=1:length(X5)

```

```

181         C1(46,1+4*2+r) = X5(r);
182     end
183     for r=1:length(X6)
184         C1(46,1+5*2+r) = X6(r);
185     end
186     for r=1:length(X6)
187         C1(46,1+6*2+r) = X7(r);
188     end
189     C1(71,:) = C(71,:);
190     C1(79,:) = C(79,:);
191     C1(134,:) = C(46,:);
192     C1(135,:) = C(135,:);
193     %Evaluate difference in capability
194     x = sum(abs(C1(:,1) - C(:,1)));
195     %Update capabilities
196     C = C1;
197     k = k + 1;
198     D(:,k) = C(:,1);
199     %Iterate
200 end;
201 Capsout = C;

```

APPENDIX H

FUNCTION CALL FOR OPTIMIZATION OF 'ALL-ELECTRIC' ARCHITECTURE

The function call used to calculate the system capability for the 'more-electric' architecture concept is given below. This code was autogenerated by the Architecture Design Environment. Its structure is similar to the code generate for the conventional architecture and is discussed in the previous appendix.

./GethazardAE.m

```
1 function Hazard=GethazardAE(A,C,Clims , allalphas , matrixalphainds , misseg)
2     Capsout=FindBFCaps(A,C,Clims , allalphas , matrixalphainds);           % Get system capabilities
3     BFCaps=ones(8,22);                                                       % All inactive caps -1
4     BFCaps(3,:)=Capsout(5,:);                                               % Cool Pneumatic Capability
5     BFCaps(4,:)=Capsout(4,:);                                               % 28VDC Capability
6     BFCaps(5,:)=Capsout(6,:);                                               % 270VDC Capability
7     BFCaps(8,:)=Capsout(7,:);                                               % Thrust Capability
8     Hazard=hazardfunction(BFCaps, misseg);                                   % Get Hazard Value
9
10 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
11
12 function Capsout=FindBFCaps(A,C,Clims , allalphas , matrixalphainds)
13 %% This function calculates system capabilities
14 %Global unit attributes values set externally by designer in the ADEN
15 global APU_HPPn_Cap_design
16 global APU_HPShaft_Cap_design
17 global HSDC270VGen_1_DC270V_Cap_design
18 global HSDC270VGen_2_DC270V_Cap_design
19 global HPAGB_3_HPShaft_Cap_design
20 global Zone_Length_ft_6_6_out
21 global Zone_Length_ft_6_3_out
22 global Zone_Length_ft_6_2_out
23 global Zone_Length_ft_3_3_out
24 global Zone_Length_ft_3_2_out
25 global Zone_Length_ft_2_2_out
26 global HPAGB_1_HPShaft_Cap_design
27 global Zone_Length_ft_6_5_out
28 global Zone_Length_ft_5_5_out
29 global Zone_Length_ft_5_2_out
30 global LSDC270VGen_1_DC270V_Cap_design
31 global HPAGB_2_HPShaft_Cap_design
32 global LSDC270VGen_2_DC270V_Cap_design
33 global Engine_1_HPPn_Cap_design
```



```

34 global Engine_1_LPPn_Cap_design
35 global Engine_1_FanAir_Cap_design
36 global Engine_1_HPShaft_Cap_design
37 global Engine_1_LPShaft_Cap_design
38 global Engine_1_Thrust_Cap_design
39 global Integration_Altitude_ft_out
40 global Integration_Mach_out
41 global Engine_2_HPPn_Cap_design
42 global Engine_2_LPPn_Cap_design
43 global Engine_2_FanAir_Cap_design
44 global Engine_2_HPShaft_Cap_design
45 global Engine_2_LPShaft_Cap_design
46 global Engine_2_Thrust_Cap_design
47 global RamCom270V_1_CoolPn_Cap_design
48 global RamCom270V_2_CoolPn_Cap_design
49 global HSDC270VGen_3_DC270V_Cap_design
50 global HSDC28VGen_DC28V_Cap_design
51 global RamDuct_1_RamAir_Cap_design
52 global RamDuct_2_RamAir_Cap_design
53 global PCU270to28V_1_DC28V_Cap_design
54 global PCU270to28V_2_DC28V_Cap_design
55 global FuelSys_1_Fuel_Cap_design
56 global Zone_Length_ft_5_3_out
57 global FuelSys_2_Fuel_Cap_design
58 global DC28VLoads_DC28VReq_Cap_design
59 global DC270VLoads_DC270VReq_Cap_design
60 global PnLoads_PnReq_Cap_design
61 global ThrustLoads_ThrustReq_Cap_design
62 global DC270VBus_1_DC270V_Cap_design
63 global DC270VBus_2_DC270V_Cap_design
64 global DC28VBus_1_DC28V_Cap_design
65 global DC28VBus_2_DC28V_Cap_design
66 global CoolPnSys_1_CoolPn_Cap_design
67 global CoolPnSys_2_CoolPn_Cap_design
68 global DCFuelPump_1_FuelPress_Cap_design
69 global DCFuelPump_2_FuelPress_Cap_design
70 global DCFuelPump_3_FuelPress_Cap_design
71
72 % Initialize capability info
73 Cl=zeros(length(C),22);
74 thesize=size(matrixalphainds);
75 alphalength=size(allalphas);
76 matrixalpha=abs(allalphas(1:thesize(1)));
77 %Write allocation variable (allalphas) values to Adjacency matrix
78 for i=1:thesize(1)
79     thealphas=abs(transpose(allalphas(1:thesize(1))));
80     thesum=sum((squeeze(matrixalphainds(:,2))=squeeze(matrixalphainds(i,2)).*thetalphas);
81     matrixalpha(i)=matrixalpha(i)/thesum;
82     A(matrixalphainds(i,1),matrixalphainds(i,2))=matrixalpha(i);
83 end
84 alpha=allalphas(thesize+1:alphalength(2));
85 %Initialize the capability matrix
86 C(:,1)=min(Clims(:),C(:,1));
87 for i=1:2*length(C)
88     C(:,1)=A*C(:,1);

```

```

89     C(:,2)=A*C(:,2)./(sum(A,2));
90     C(:,3)=A*C(:,3)./(sum(A,2));
91     end
92     x=1;
93     k=1;
94     while x>0.000001 && k<3*length(C)
95         D(:,k)=C(:,1);
96         %Run All Unit Transfer Functions
97         [OneTempOut1,C(19,1:2)]=DS_APU_Caps(C(16,1:3),C(18,1),C(17,1),APU_HPPn_Cap_design ,
          APU_HPShaft_Cap_design,0,0);
98         [C(22,1)]=DS_HSDC270VGen_Caps(C(20,1:2),C(21,1),HSDC270VGen_1_DC270V_Cap_design);
99         [C(25,1)]=DS_HSDC270VGen_Caps(C(23,1:2),C(24,1),HSDC270VGen_2_DC270V_Cap_design);
100        [C(40,1:2)]=DS_HPAGB_Caps(C(39,1:2),HPAGB_3_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+Zone_Length_ft_3_3_out+
          Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
101        [C(42,1:2)]=DS_HPAGB_Caps(C(41,1:2),HPAGB_1_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_5_out+Zone_Length_ft_6_2_out+Zone_Length_ft_5_5_out+
          Zone_Length_ft_5_2_out+Zone_Length_ft_2_2_out);
102        [C(45,1)]=DS_LSDC270VGen_Caps(C(43,1:2),C(44,1),LSDC270VGen_1_DC270V_Cap_design);
103        [C(48,1:2)]=DS_HPAGB_Caps(C(47,1:2),HPAGB_2_HPShaft_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_2_out+Zone_Length_ft_2_2_out);
104        [C(51,1)]=DS_LSDC270VGen_Caps(C(49,1:2),C(50,1),LSDC270VGen_2_DC270V_Cap_design);
105        [OneTempOut1,OneTempOut2,OneTempOut3,C(55,1:2),C(56,1:2),C(57,1:14)]=DS_Engine_Caps(C
          (53,1:3),C(54,1),C(52,1),Engine_1_HPPn_Cap_design,Engine_1_LPPn_Cap_design,
          Engine_1_FanAir_Cap_design,Engine_1_HPShaft_Cap_design,Engine_1_LPShaft_Cap_design,
          Engine_1_Thrust_Cap_design,Integration_Altitude_ft_out,Integration_Mach_out,0,0,0,
          alpha(1),alpha(2),alpha(3));
106        C(57,2)=max(eps,1-Clims(57)/7000);
107        [OneTempOut1,OneTempOut2,OneTempOut3,C(61,1:2),C(62,1:2),C(63,1:14)]=DS_Engine_Caps(C
          (59,1:3),C(60,1),C(58,1),Engine_2_HPPn_Cap_design,Engine_2_LPPn_Cap_design,
          Engine_2_FanAir_Cap_design,Engine_2_HPShaft_Cap_design,Engine_2_LPShaft_Cap_design,
          Engine_2_Thrust_Cap_design,Integration_Altitude_ft_out,Integration_Mach_out,0,0,0,
          alpha(4),alpha(5),alpha(6));
108        C(63,2)=max(eps,1-Clims(63)/7000);
109        [C(74,1:3)]=DS_RamCom270V_Caps(C(73,1),C(72,1:3),RamCom270V_1_CoolPn_Cap_design);
110        [C(77,1:3)]=DS_RamCom270V_Caps(C(76,1),C(75,1:3),RamCom270V_2_CoolPn_Cap_design);
111        [C(80,1)]=DS_HSDC270VGen_Caps(C(78,1:2),C(79,1),HSDC270VGen_3_DC270V_Cap_design);
112        [C(83,1)]=DS_HSDC28VGen_Caps(C(81,1:2),C(82,1),HSDC28VGen_DC28V_Cap_design);
113        [C(94,1:3)]=DS_RamDuct_Caps(C(93,1:3),RamDuct_1_RamAir_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_2_out+Zone_Length_ft_2_2_out);
114        [C(96,1:3)]=DS_RamDuct_Caps(C(95,1:3),RamDuct_2_RamAir_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+Zone_Length_ft_3_3_out+
          Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
115        [C(99,1)]=DS_PCU270to28V_Caps(C(98,1),C(97,1),PCU270to28V_1_DC28V_Cap_design);
116        [C(102,1)]=DS_PCU270to28V_Caps(C(101,1),C(100,1),PCU270to28V_2_DC28V_Cap_design);
117        [C(104,1)]=DS_FuelSys_Caps(C(103,1),FuelSys_1_Fuel_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+
          Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_5_2_out+
          Zone_Length_ft_3_3_out+Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
118        [C(106,1)]=DS_FuelSys_Caps(C(105,1),FuelSys_2_Fuel_Cap_design,Zone_Length_ft_6_6_out+
          Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+
          Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_5_2_out+
          Zone_Length_ft_3_3_out+Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
119        [C(108,1)]=DS_DC28VLoads_Caps(C(107,1),DC28VLoads_DC28VReq_Cap_design);
120        [C(110,1)]=DS_DC270VLoads_Caps(C(109,1),DC270VLoads_DC270VReq_Cap_design);

```

```

121 [C(112,1:3)]=DS.PnLoads_Caps(zeros(1,21),C(111,1:3),PnLoads.PnReq_Cap_design);
122 [C(114,1:14)]=DS.ThrustLoads_Caps(C(113,1:14),ThrustLoads.ThrustReq_Cap_design);
123 [C(116,1)]=DS.DC270VBus_Caps(C(115,1),DC270VBus_1.DC270V_Cap_design,Zone_Length_ft_6_6_out
    +Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+
    Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_5_2_out+
    Zone_Length_ft_3_3_out+Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
124 [C(118,1)]=DS.DC270VBus_Caps(C(117,1),DC270VBus_2.DC270V_Cap_design,Zone_Length_ft_6_6_out
    +Zone_Length_ft_6_5_out+Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+
    Zone_Length_ft_5_5_out+Zone_Length_ft_5_3_out+Zone_Length_ft_5_2_out+
    Zone_Length_ft_3_3_out+Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
125 [C(120,1)]=DS.DC28VBus_Caps(C(119,1),DC28VBus_1.DC28V_Cap_design,Zone_Length_ft_6_6_out+
    Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+Zone_Length_ft_3_3_out+
    Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
126 [C(122,1)]=DS.DC28VBus_Caps(C(121,1),DC28VBus_2.DC28V_Cap_design,Zone_Length_ft_6_6_out+
    Zone_Length_ft_6_3_out+Zone_Length_ft_6_2_out+Zone_Length_ft_3_3_out+
    Zone_Length_ft_3_2_out+Zone_Length_ft_2_2_out);
127 [C(124,1:3)]=DS.CoolPnSys_Caps(C(123,1:3),CoolPnSys_1.CoolPn_Cap_design,
    Zone_Length_ft_6_6_out+Zone_Length_ft_6_2_out+Zone_Length_ft_2_2_out);
128 [C(126,1:3)]=DS.CoolPnSys_Caps(C(125,1:3),CoolPnSys_2.CoolPn_Cap_design,
    Zone_Length_ft_6_6_out+Zone_Length_ft_6_2_out+Zone_Length_ft_2_2_out);
129 [C(129,1)]=DS.DCFuelPump_Caps(C(127,1),C(128,1),DCFuelPump_1.FuelPress_Cap_design);
130 [C(132,1)]=DS.DCFuelPump_Caps(C(130,1),C(131,1),DCFuelPump_2.FuelPress_Cap_design);
131 [C(135,1)]=DS.DCFuelPump_Caps(C(133,1),C(134,1),DCFuelPump_3.FuelPress_Cap_design);
132 %Impose Capability Limits
133 C(:,1)=min(Clims,C(:,1));
134 %Special Management of thrust capability
135 C1(7,2)=max(eps,1-Clims(7)/7000);
136 C1(57,2)=max(eps,1-Clims(57)/7000);
137 C1(63,2)=max(eps,1-Clims(63)/7000);
138 C1(113,2)=max(eps,1-Clims(113)/7000);
139 C1(114,2)=max(eps,1-Clims(114)/7000);
140 %Format capability vector
141 C1(:,1)=A*C(:,1);
142 C1(:,2)=(A*(C(:,2).*C(:,1)))/(C1(:,1)+eps);
143 C1(:,3)=(A*(C(:,3).*C(:,1)))/(C1(:,1)+eps);
144 %Special management of thrust capability
145 C1(7,:)=C(114,:);
146 X1 = nonzeros(A(46,:)'.*C(:,2));
147 X2 = nonzeros(A(46,:)'.*C(:,3));
148 X3 = nonzeros(A(46,:)'.*C(:,4));
149 X4 = nonzeros(A(46,:)'.*C(:,5));
150 X5 = nonzeros(A(46,:)'.*C(:,6));
151 X6 = nonzeros(A(46,:)'.*C(:,7));
152 X7 = nonzeros(A(46,:)'.*C(:,8));
153 for r=1:length(X1)
154     C1(46,1+r) = X1(r);
155 end
156 for r=1:length(X2)
157     C1(46,1+1*2+r) = X2(r);
158 end
159 for r=1:length(X3)
160     C1(46,1+2*2+r) = X3(r);
161 end
162 for r=1:length(X4)
163     C1(46,1+3*2+r) = X4(r);

```

```

164     end
165     for r=1:length(X5)
166         C1(46,1+4*2+r) = X5(r);
167     end
168     for r=1:length(X6)
169         C1(46,1+5*2+r) = X6(r);
170     end
171     for r=1:length(X6)
172         C1(46,1+6*2+r) = X7(r);
173     end
174     C1(57,:) = C(57,:);
175     C1(63,:) = C(63,:);
176     C1(113,:) = C(46,:);
177     C1(114,:) = C(114,:);
178     %Evaluate difference in capability
179     x=sum(abs(C1(:,1)-C(:,1)));
180     %Update capabilities
181     C=C1;
182     k=k+1;
183     D(:,k)=C(:,1);
184     %Iterate
185 end;
186 Capsout=C;

```

APPENDIX I

HAZARD PROBABILITY FOR ALL APPLIED FUNCTIONAL HAZARDS FOR THE CONVENTIONAL ARCHITECTURE

Table 55: Take-off Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} \cong 0.37$ $R_{FFO} \cong 0.75$</p>		<p><i>Elec.120V AC</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.01$</p>	
<p><i>Elec.28V DC</i> $R_{FFU} \cong 0.25$ $R_{FFO} \cong 0.65$</p>		<p><i>Hydraulic</i> $R_{FFU} \cong 3.07$ $R_{FFO} \cong 3.59$</p>	
<p><i>Thrust</i> $R_{FFU} \cong 0.18$ $R_{FFO} \cong 0.48$</p>		<p><i>Total</i> $R_{sFFU} \cong 3.54$ $R_{sFFO} \cong 4.11$</p>	

Table 56: Cruise Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} \cong 0.21$ $R_{FFO} \cong 0.61$</p>		<p><i>Elec.120V AC</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.01$</p>	
<p><i>Elec.28V DC</i> $R_{FFU} \cong 0.16$ $R_{FFO} \cong 0.54$</p>		<p><i>Hydraulic</i> $R_{FFU} \cong 0.57$ $R_{FFO} \cong 0.92$</p>	
<p><i>Thrust</i> $R_{FFU} \cong 0.42$ $R_{FFO} \cong 0.72$</p>		<p><i>Total</i> $R_{sFFU} \cong 1.22$ $R_{sFFO} \cong 1.75$</p>	

Table 57: Linear Approximation Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} \cong 0.33$ $R_{FFO} \cong 0.63$</p>		<p><i>Elec.120V AC</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.01$</p>	
<p><i>Elec.28V DC</i> $R_{FFU} \cong 0.04$ $R_{FFO} \cong 0.29$</p>		<p><i>Hydraulic</i> $R_{FFU} \cong 3.50$ $R_{FFO} \cong 4.03$</p>	
<p><i>Thrust</i> $R_{FFU} \cong 0.20$ $R_{FFO} \cong 0.33$</p>		<p><i>Total</i> $R_{sFFU} \cong 4.05$ $R_{sFFO} \cong 4.60$</p>	

Table 58: Step Approximation Functional Hazard Probability Assessment for the Conventional Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} \cong 1.63 \times 10^4$ $R_{FFO} \cong 1.63 \times 10^4$</p>		<p><i>Elec.120V AC</i> $R_{FFU} = 0.04$ $R_{FFO} \cong 0.14$</p>	
<p><i>Elec.28VDC</i> $R_{FFU} \cong 1.72 \times 10^4$ $R_{FFO} \cong 1.72 \times 10^4$</p>		<p><i>Hydraulic</i> $R_{FFU} \cong 2.33 \times 10^4$ $R_{FFO} \cong 2.33 \times 10^4$</p>	
<p><i>Thrust</i> $R_{FFU} \cong 1.34 \times 10^3$ $R_{FFO} \cong 1.34 \times 10^3$</p>		<p><i>Total</i> $R_{sFFU} \cong 3.06 \times 10^4$ $R_{sFO} \cong 3.06 \times 10^4$</p>	

APPENDIX J

HAZARD PROBABILITY FOR ALL APPLIED FUNCTIONAL HAZARDS FOR THE 'ALL-ELECTRIC' ARCHITECTURE

Table 59: Take-off Functional Hazard Probability Assessment for the 'All-Electric' Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.00$</p>		<p><i>Elec.270VDC</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.23$</p>	
<p><i>Elec.28VDC</i> $R_{FFU} \cong 0.56$ $R_{FFO} \cong 0.91$</p>		<p><i>Thrust</i> $R_{FFU} \cong 2.45$ $R_{FFO} \cong 2.82$</p>	
<p><i>Total</i> $R_{FFU} \cong 2.86$ $R_{FFO} \cong 3.28$</p>			

Table 60: Cruise Functional Hazard Probability Assessment for the 'All-Electric' Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.00$</p>		<p><i>Elec.270VDC</i> $R_{FFU} = 0.10$ $R_{FFO} \cong 0.36$</p>	
<p><i>Elec.28VDC</i> $R_{FFU} \cong 0.57$ $R_{FFO} \cong 0.97$</p>		<p><i>Thrust</i> $R_{FFU} \cong 1.98$ $R_{FFO} \cong 2.33$</p>	
<p><i>Total</i> $R_{FFU} \cong 2.47$ $R_{FFO} \cong 2.89$</p>			

Table 61: Linear Approximation Functional Hazard Probability Assessment for the 'All-Electric' Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} = 0$ $R_{FFO} \cong 0.00$</p>		<p><i>Elec.270VDC</i> $R_{FFU} = 0.46$ $R_{FFO} \cong 0.76$</p>	
<p><i>Elec.28VDC</i> $R_{FFU} \cong 0.85$ $R_{FFO} \cong 1.17$</p>		<p><i>Thrust</i> $R_{FFU} \cong 0.20$ $R_{FFO} \cong 0.33$</p>	
<p><i>Total</i> $R_{FFU} \cong 1.05$ $R_{FFO} \cong 1.51$</p>			

Table 62: Step Approximation Functional Hazard Probability Assessment for the 'All-Electric' Vehicle Systems Architecture

Function	Hazard Probability ($F(H_F)$)	Function	Hazard Probability ($F(H_F)$)
<p><i>Pneumatic</i> $R_{FFU} \cong 102$ $R_{FFO} \cong 102$</p>		<p><i>Elec.270VDC</i> $R_{FFU} \cong 103$ $R_{FFO} \cong 104$</p>	
<p><i>Elec.28VDC</i> $R_{FFU} \cong 1.37 \times 10^4$ $R_{FFO} \cong 1.37 \times 10^4$</p>		<p><i>Thrust</i> $R_{FFU} \cong 1.34 \times 10^3$ $R_{FFO} \cong 1.34 \times 10^3$</p>	
<p><i>Total</i> $R_{FFU} \cong 1.51 \times 10^4$ $R_{FFO} \cong 1.51 \times 10^4$</p>			

APPENDIX K

FUNCTIONAL HAZARD CORRELATION FOR THE CONVENTIONAL ARCHITECTURE

The hazard correlation matrix is a measure of the ability of an architecture to disperse failures between the system functions. Architectures that exhibit higher correlation between the loss of system functionality have a greater ability to shed loads. For the conventional architecture the indices, 1 through 5, are in the order [Pneumatic Air Loss, 120VAC Loss, 28VDC Loss, Hydraulic Flow Loss, and Thrust Loss]. The correlations between the loss of these functions for 1120 unit failure combination cases are given in table 63. The number of functions provided by the system is given by N and is equal to 4.

Table 63: Conventional Functional Hazard Correlations

	Correlation Matrix (ρ)					$\frac{\ \rho\ _2 - 1}{N - 1}$
Takeoff	1	0.337	0.422	0.541	0.606	0.565
	0.337	1	0.243	0.291	0.393	
	0.422	0.243	1	0.334	0.462	
	0.541	0.291	0.334	1	0.523	
	0.606	0.393	0.462	0.523	1	
Cruise	1	0.331	0.392	0.521	0.267	0.425
	0.331	1	0.247	0.306	0.206	
	0.392	0.247	1	0.353	0.216	
	0.521	0.306	0.353	1	0.272	
	0.267	0.206	0.216	0.272	1	
Linear	1	0.369	0.374	0.518	-0.022	0.344
	0.369	1	0.199	0.302	-0.035	
	0.374	0.199	1	0.256	-0.018	
	0.518	0.302	0.256	1	-0.018	
	-0.0216	-0.035	-0.018	-0.018	1	
Step	1	0.360	0.335	0.316	-0.053	0.302
	0.360	1	0.316	0.225	-0.079	
	0.335	0.316	1	0.216	-0.047	
	0.316	0.225	0.216	1	-0.064	
	-0.053	-0.079	-0.047	-0.064	1	

APPENDIX L

FUNCTIONAL HAZARD CORRELATION FOR THE 'ALL-ELECTRIC' ARCHITECTURE

For the 'more-electric' architecture the indices, 1 through 4, are in the order [Pneumatic Air Loss, 270VDC Loss, 28VDC Loss, and Thrust Loss]. Load shedding optimization was performed for 665 unit failure combinations. Table 64 gives the correlation between the loss of functions for all system level functions of the 'more-electric' architecture. The number of functions provided by the system is given by N and is equal to 3.

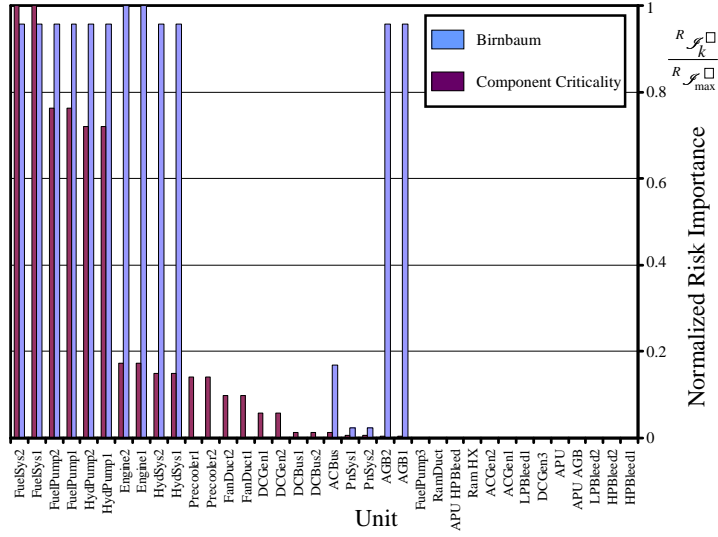
Table 64: 'All-Electric' Functional Hazard Correlations

	Correlation Matrix (ρ)	$\frac{\ \rho\ _2 - 1}{N - 1}$
Takeoff	$\begin{bmatrix} 1 & 0.677 & 0.398 & 0.498 \\ 0.677 & 1 & 0.641 & 0.748 \\ 0.398 & 0.641 & 1 & 0.538 \\ 0.498 & 0.748 & 0.538 & 1 \end{bmatrix}$	0.883
Cruise	$\begin{bmatrix} 1 & 0.776 & 0.646 & 0.644 \\ 0.776 & 1 & 0.750 & 0.614 \\ 0.646 & 0.750 & 1 & 0.520 \\ 0.644 & 0.614 & 0.520 & 1 \end{bmatrix}$	0.992
Linear	$\begin{bmatrix} 1 & 0.910 & 0.859 & -0.059 \\ 0.910 & 1 & 0.912 & 0.090 \\ 0.859 & 0.912 & 1 & 0.100 \\ -0.059 & 0.090 & 0.100 & 1 \end{bmatrix}$	0.896
Step	$\begin{bmatrix} 1 & 0.615 & 0.489 & -0.067 \\ 0.615 & 1 & 0.623 & 0.375 \\ 0.489 & 0.623 & 1 & 0.224 \\ -0.067 & 0.375 & 0.224 & 1 \end{bmatrix}$	0.619

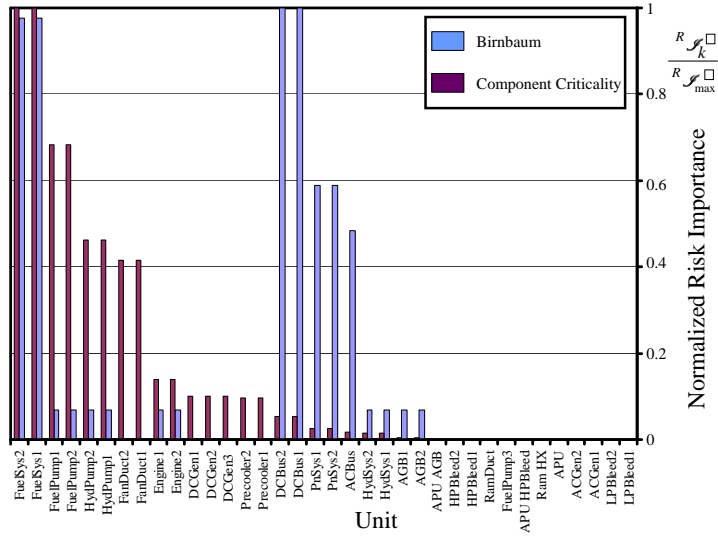
APPENDIX M

CUMULATIVE COMPONENT CRITICALITY IMPORTANCE FOR THE CONVENTIONAL AND 'ALL-ELECTRIC' ARCHITECTURES

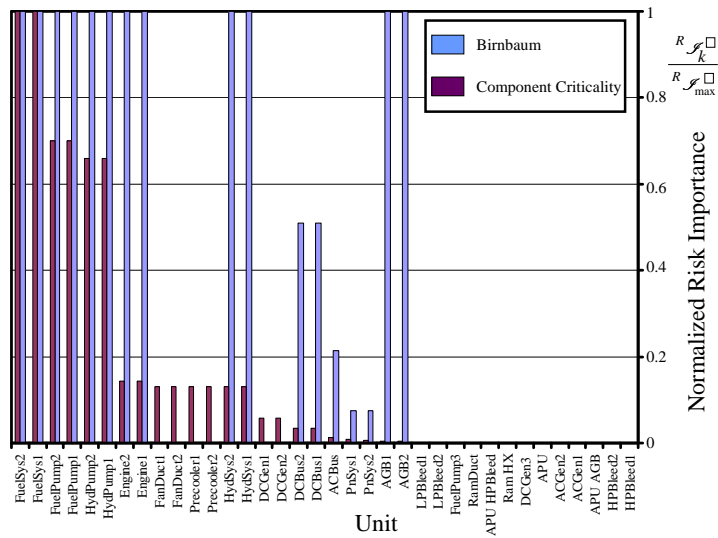
Figures 114 and 115 cumulative component risk importance values normalized by the maximum cumulative risk importance value ($\frac{R \mathcal{J}_k^{\square}}{R \mathcal{J}_{\max}^{\square}}$). Figure 114 gives the values for the conventional architecture and figure 115 gives values for the 'more-electric' architecture. Cumulative risk values are obtained on all ranges of undesirable risks. Each independent architecture places emphasis on each unit differently depending on the risk associated with the provision of function. The units that exhibit the highest importance become the design focus when for design augmentation.



(c) Linear

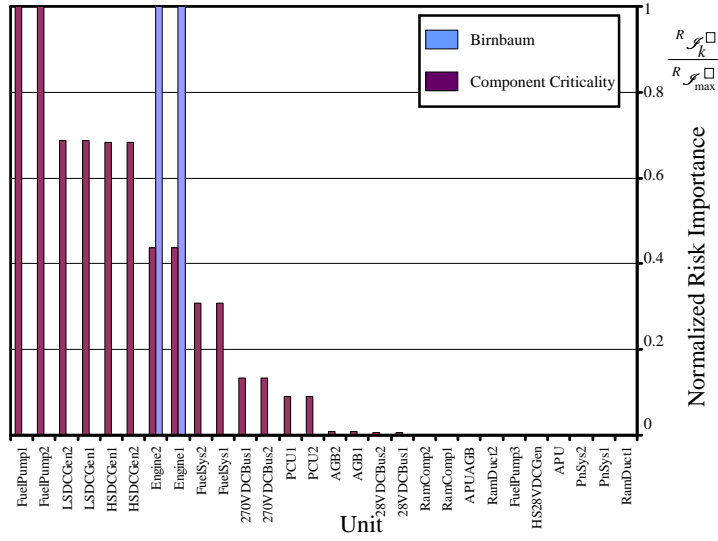


(b) Cruise

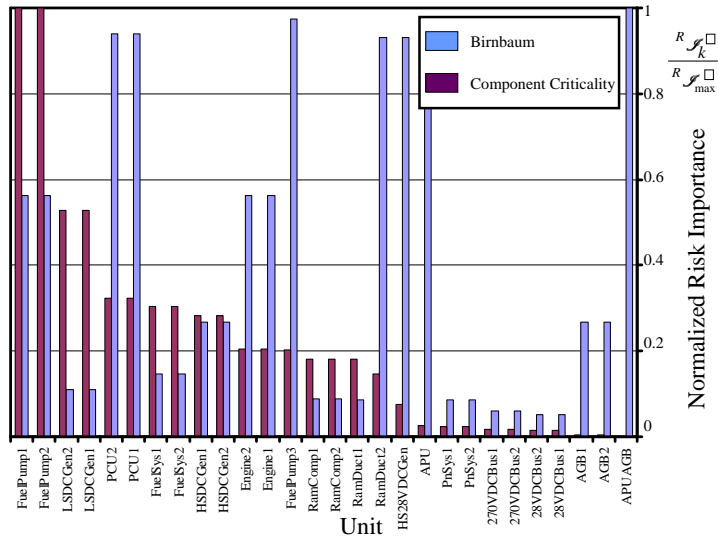


(a) Takeoff

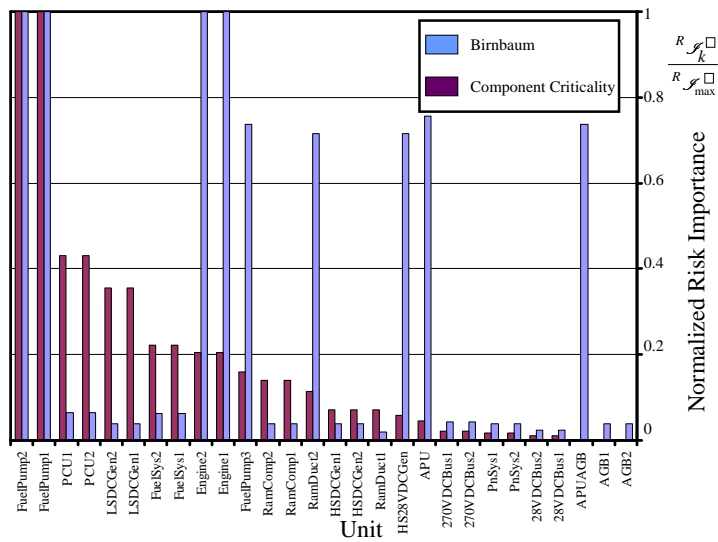
Figure 114: Normalized Cumulative Risk for Conventional Architecture Units



(c) Linear



(b) Cruise



(a) Takeoff

Figure 115: Normalized Cumulative Risk for 'All-Electric' Architecture Units

APPENDIX N

CUMULATIVE COMPONENT CAPABILITY IMPORTANCE FOR THE CONVENTIONAL AND 'ALL-ELECTRIC' ARCHITECTURES

Figures 116, 117, 118, and 119 display the cumulative component capability risk importance for both the conventional and 'more-electric' architectures. These metrics consider how decreases in unit capability impact the overall performance risk of the architecture concepts. Risk is integrated in terms of magnitude of hazard. Undesirable risk importance only integrates on ranges which breach hazard probability constraints. The bounds on the integration for overall risk extend for the whole range of hazard characterization.

Capability risk importance values were obtained using the backward finite difference method. Failure allocation was fixed for these calculations. Importance values obtained using large differentials are subject to inaccuracies which stem from inappropriate load shedding. Additionally, undesirable risk importance values may be subject to limitations in applicability when no constraint is breached.

The information conveyed by these importance values gives insight into which units contribute most to the performance risk of the system. Augmentation of unit capabilities of systems with the highest importance values will lead to larger variations in overall and undesirable risk. Additionally, this analysis highlights situations where oversizing has occurred. The capability of units which are characterized by little to no importance can be reduced with no adverse effect on performance risk.

Figures 120 and 121 summarize all risk values. The cumulative importance values displayed in these figures were obtained by averaging the importance from each differential. For symmetric units the importance values were also averaged. This data was used to generate the tables seen in the results chapter.

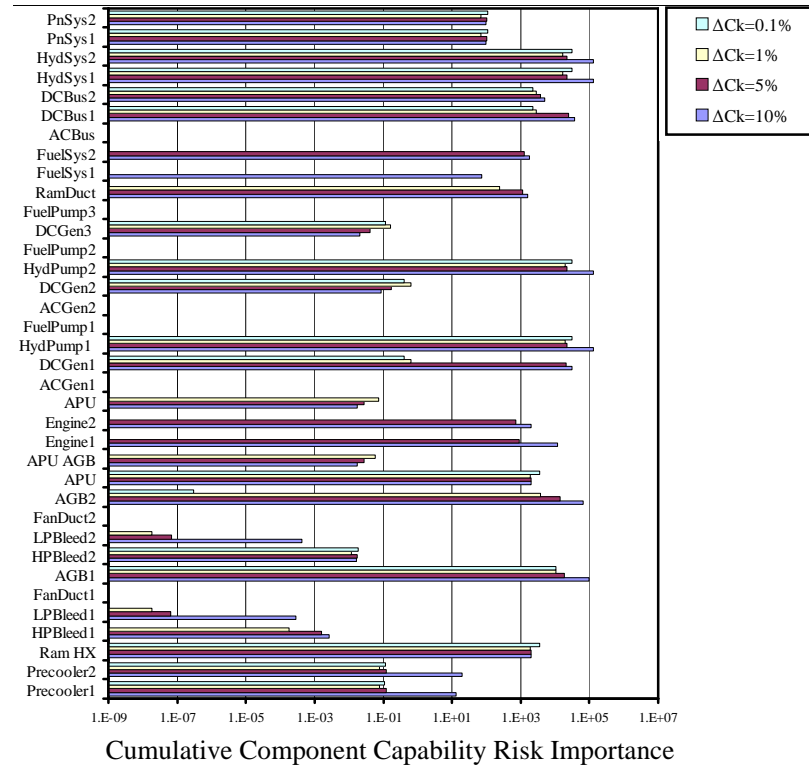
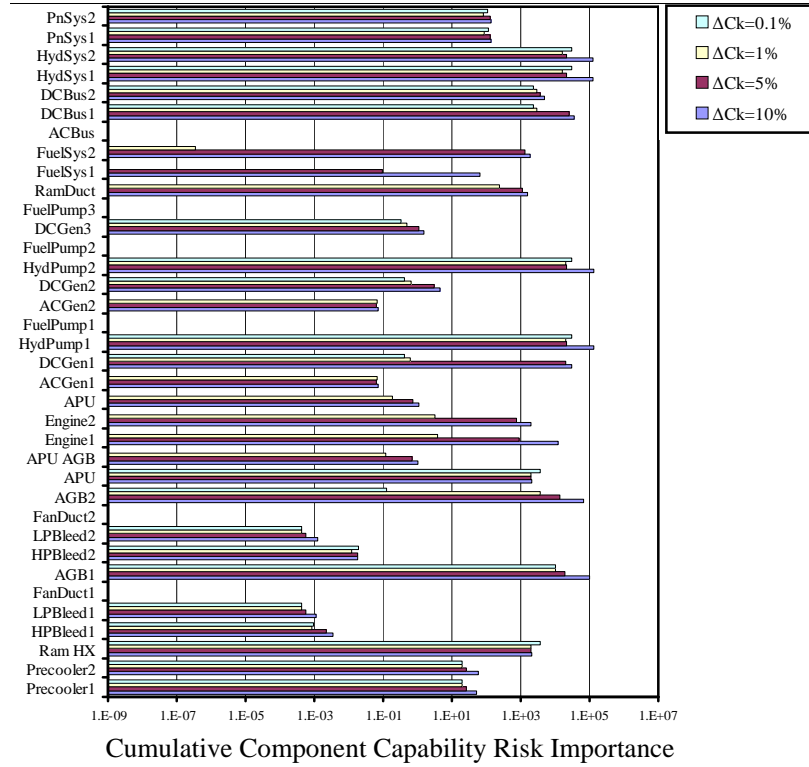


Figure 116: Cumulative Component Capability Importance Values for Conventional Architecture at Takeoff

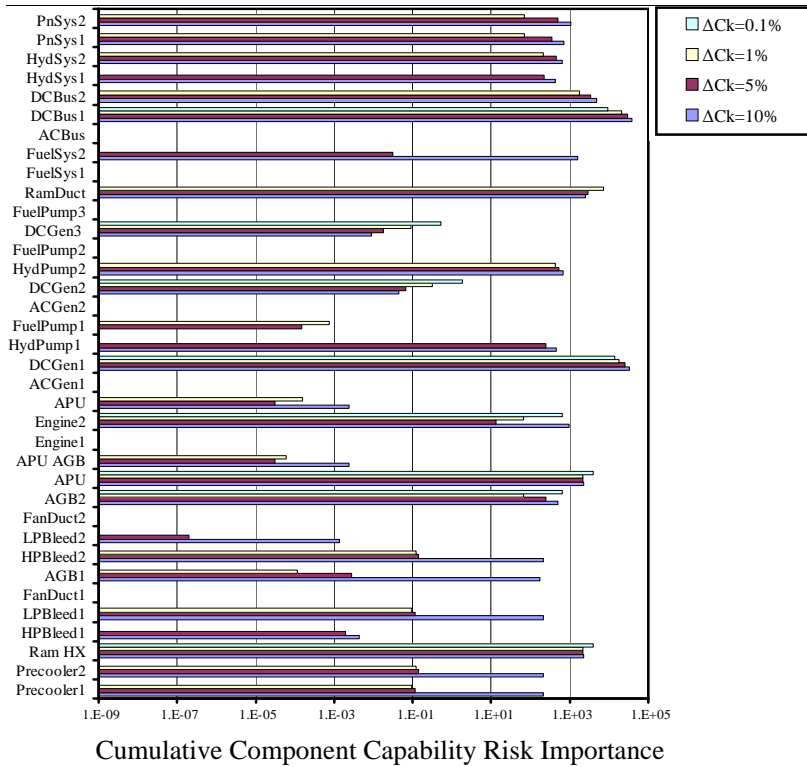
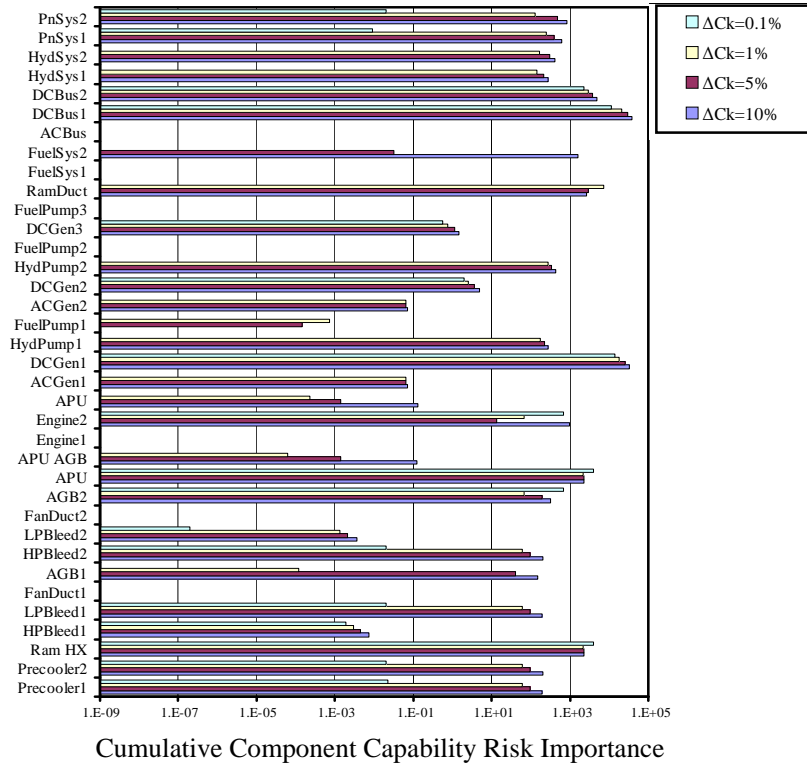
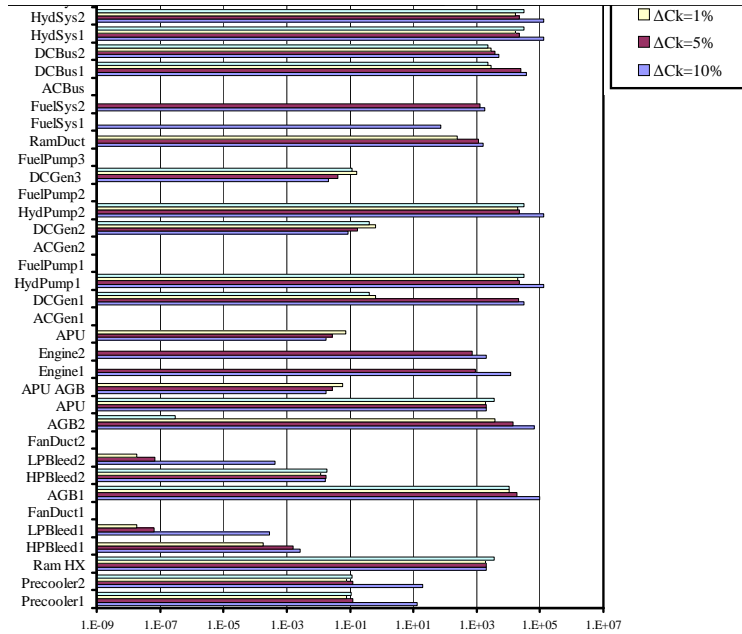
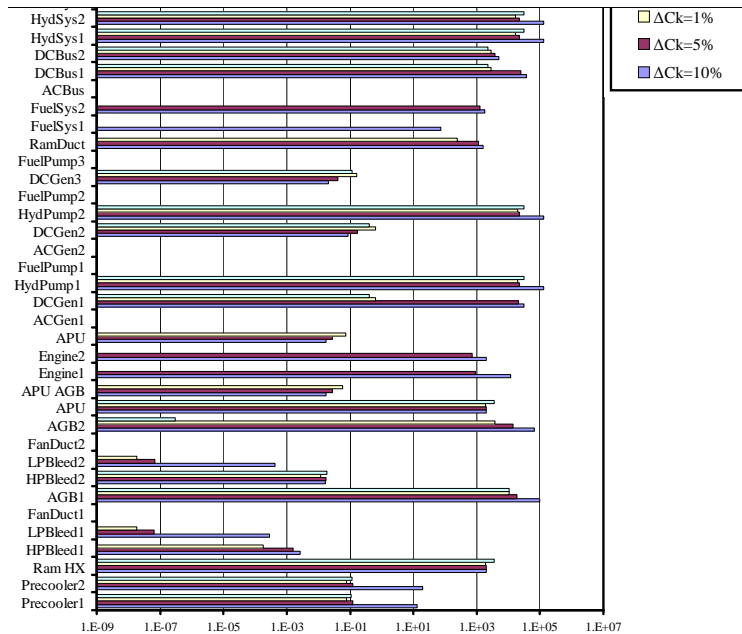


Figure 117: Cumulative Component Capability Importance Values for Conventional Architecture at Cruise



(b) Overall Risk Importance



(a) Undesirable Risk Importance

Figure 118: Cumulative Component Capability Importance Values for 'All-Electric' Architecture at Takeoff

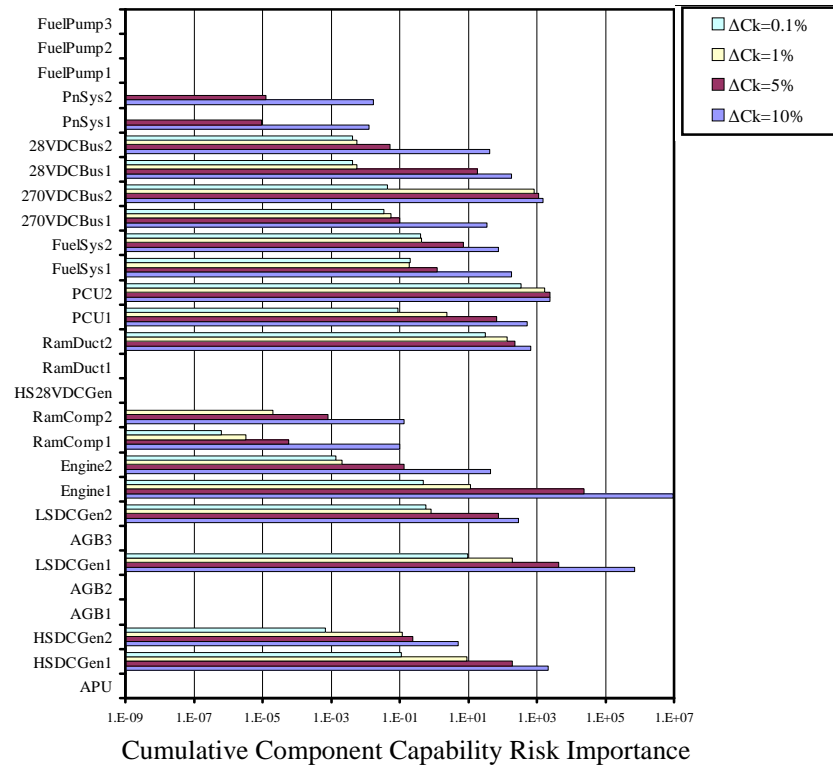
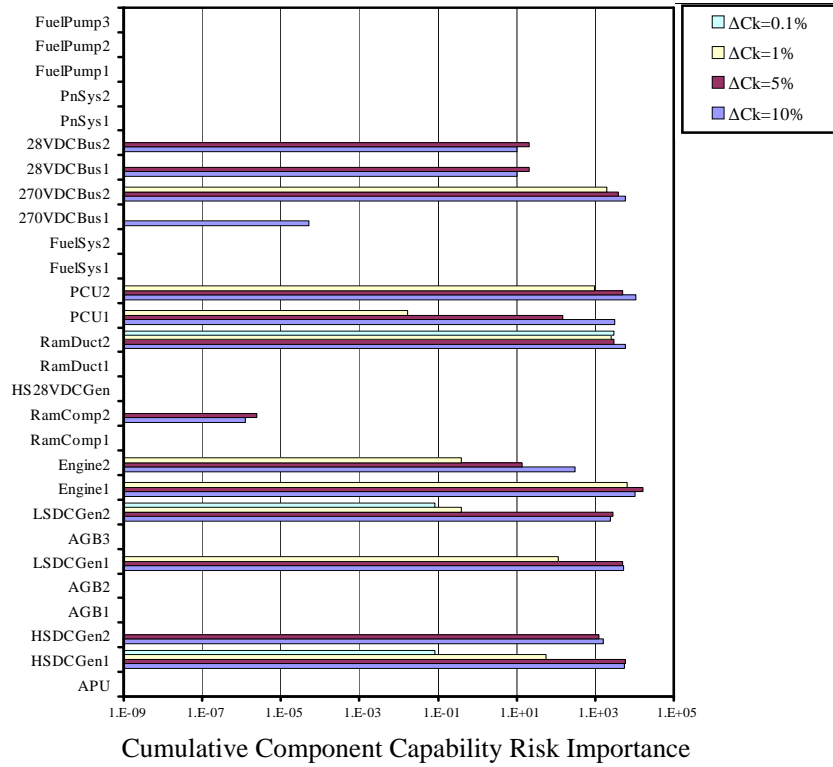


Figure 119: Cumulative Component Capability Importance Values for 'All-Electric' Architecture at Cruise

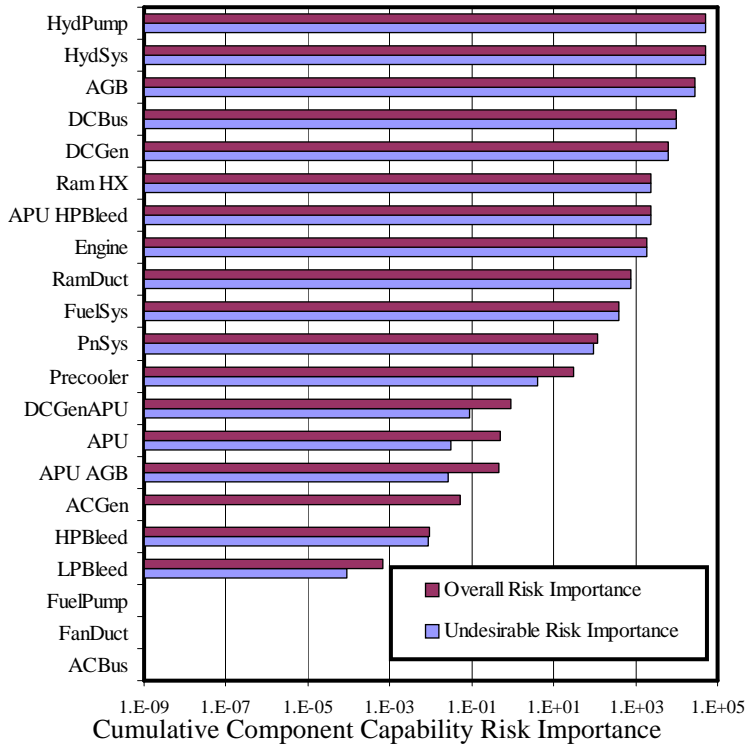
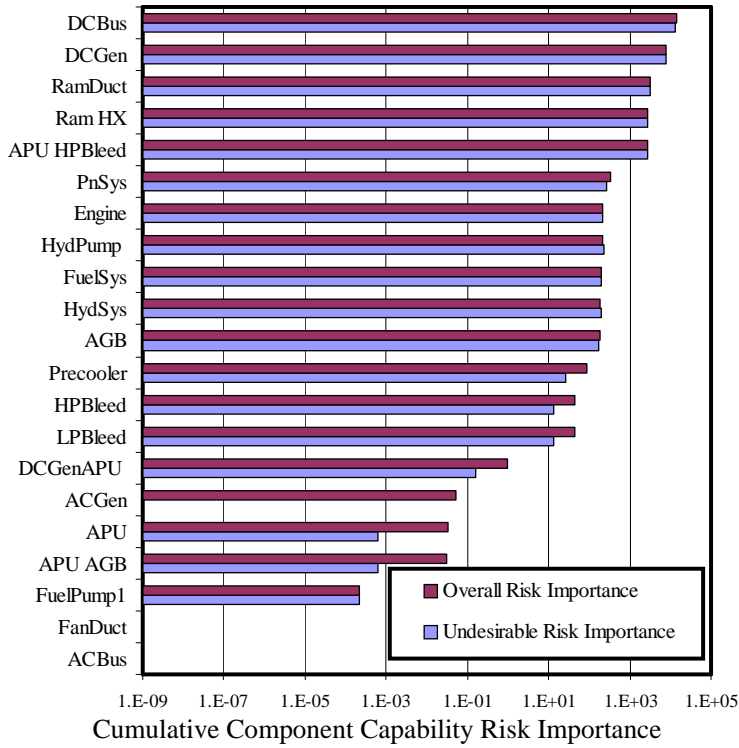
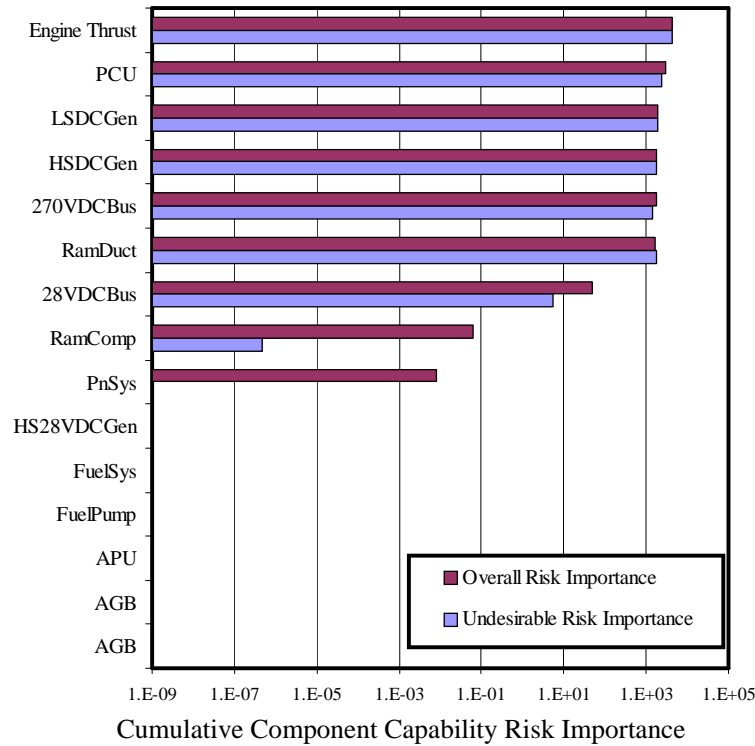
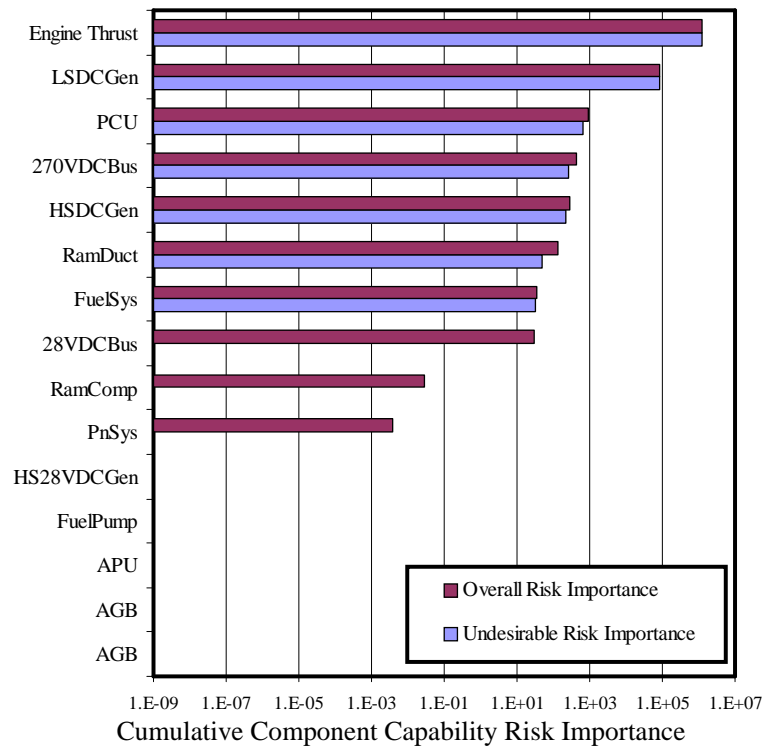


Figure 120: Averaged Cumulative Component Capability Importance Values for the Conventional Architecture



(b) Cruise



(a) Takeoff

Figure 121: Averaged Cumulative Component Capability Risk Importance Values for the 'All-Electric' Architecture

REFERENCES

- [1] "Standard Aircraft Characteristics: Navy Model AV-8B Harrier II Aircraft." Naval Air Systems Command, October 1986.
- [2] "The 'More Electric' Architecture Revolution," *Military Technology*, vol. 29, Issue 10, pp. 60–64, 2005.
- [3] "Products & Markets: Electronic Power Controllers & electrical systems." <http://www.hispano-suiza-sa.com>, 2010.
- [4] ACHERMANN, D., *Modelling, Simulation and Optimization of Maintenance Strategies under Consideration of Logistic Processes*. PhD thesis, Swiss Federal Institute of Technology Zurich, 2008.
- [5] AIR TRANSPORTATION ASSOCIATION OF AMERICA, "ATA Specification 100: Manufacturers' Technical Data," 1999.
- [6] ALLEN, K. and CARLSON-SKALAK, S., "Defining product architecture during conceptual design," in *ASME Design Engineering Technical Conferences, DETC1998/DTM*, vol. 5650, 1998.
- [7] ALLENBY, K. and KELLY, T., "Deriving safety requirements using scenarios," *Rolls-Royce PLC-Report-PNR*, 2001.
- [8] ANDERSON, J., *Aircraft performance and design*. McGraw-Hill, 1999.
- [9] ANDERSON, J. and DURNEY, B., "Using scenarios in deficiency-driven requirements engineering," in *Proceedings of IEEE International Symposium on Requirements Engineering*, pp. 134–141, 1993.
- [10] ANDREWS, J. D. and MOSS, T. R., *Reliability and Risk Assessment*. Longman Scientific and Technical, 1993.
- [11] ARMSTRONG, M., "Function Based Architecture Design Space Definition and Exploration," in *26th International Congress of the Aeronautical Sciences*, no. ICAS 2008-1.9.3, September 2008.
- [12] ARMSTRONG, M., "A process for function based architecture definition and modeling," Master's thesis, Georgia Institute of Technology, 2008.
- [13] ARTHUR, W., "The structure of invention," *Research Policy*, vol. 36, no. 2, pp. 274–287, 2007.
- [14] AUDSLEY, N., BURNS, A., RICHARDSON, M., TINDELL, K., and WELLINGS, A., "Applying new scheduling theory to static priority pre-emptive scheduling," *Software Engineering Journal*, 1993.

- [15] AVERY, C., BURROW, S., and MELLOR, P., “Electrical Generation and Distribution for the More Electric Aircraft,” *University of Bristol, UK, UPEC*, 2007.
- [16] BALDWIN, T. and LEWIS, S., “Distribution load flow methods for shipboard power systems,” *IEEE Transactions on Industry Applications*, vol. 40, no. 5, pp. 1183–1190, 2004.
- [17] BENFORD, J., SCHAMILOGLU, E. D. L., and SWEGLE, J. A., *High power microwaves*. CRC Press, 2007.
- [18] BIAN, X., MA, Q., and ZHOU, Y., “A Multi-Agent Approach to the More Electric Aircraft Power System Reconfiguration,” in *International Conference on Mechatronics and Automation, 2007.*, pp. 978–982, 2007.
- [19] BILTGEN, P., ENDER, T., and MAVRIS, D., “Development of a collaborative capability-based tradeoff environment for complex system architectures,” in *44th AIAA Aerospace Sciences Meeting and Exhibit*, no. AIAA-2006-0728, 2006.
- [20] BIROLINI, A., *Reliability engineering: theory and practice*. Springer Verlag, 2007.
- [21] BLOCH, H. P. and GEITNER, F. K., *Practical Machinery Management for Process Plants, Volume 2: Machinery Failure Analysis and Troubleshooting, 2nd Edition*. Gulf Publishing Company, 1994.
- [22] BOCK, C., “SysML and UML 2 support for activity modeling,” *Systems Engineering-New York*, vol. 9, no. 2, p. 160, 2006.
- [23] BOFF, K., KAUFMAN, L., THOMAS, J., and G., A. H., *Handbook of Perception and Human Performance. Volume 2. Cognitive Processes and Performance*. John Wiley & Sons, 1994.
- [24] BOND, A. and RICCI, R., “Cooperation in aircraft design,” *Research in Engineering Design*, vol. 4, no. 2, pp. 115–130, 1992.
- [25] BONNEAU, V., “Tailored Electrical Power Systems.” <http://www.geaviationsystems.com/Products-/Electrical-Power/>, June 2008.
- [26] BORER, N. and MAVRIS, D., “Formulation of a multi-mission sizing methodology for competing configurations,” in *42nd Aerospace Sciences Meeting and Exhibit.*, no. AIAA-2004-0535, 2004.
- [27] BORISSOVA, A., FAIRWEATHER, M., and GOLTZ, G., “An option generation and selection methodology for process equipment selection,” *Research in Engineering Design*, vol. 17, no. 1, pp. 13–26, 2006.
- [28] BOTTEN, S., WHITLEY, C., and KING, A., “Flight Control Actuation Technology for Next-Generation All-Electric Aircraft,” *Technology Review*, vol. 23, no. 6, 2000.
- [29] BREYFOGLE, F., *Implementing Six Sigma: smarter solutions using statistical methods*. Productivity Press, 2003.
- [30] BRICENO, S. and MAVRIS, D., “Implementation of a physics-based decision-making framework for evaluation of the multidisciplinary aircraft uncertainty,” *SAE transactions*, vol. 112, no. 1, pp. 651–661, 2003.

- [31] BROWNING, T., "Applying the design structure matrix to system decomposition and integration problems: a review and new directions," *IEEE Transactions on Engineering management*, vol. 48, no. 3, pp. 292–306, 2001.
- [32] BROWNING, T., "Process integration using the design structure matrix," *Systems Engineering*, vol. 5, no. 3, pp. 180–193, 2002.
- [33] BRUGGINK, G. M., "The First Two Minutes," *Flight Safety Foundation: Flight Safety Digest*, May, 1989.
- [34] BRYANT, C. R., STONE, R. B., MCADAMS, D. A., KURTOGLU, T., and CAMPBELL, M. I., "Concept generation from the functional basis of design," in *Proceedings of International Conference on Engineering Design*, vol. ICED05, 2005.
- [35] BUHR, R., "Use case maps as architecture entities for complex systems," *IEEE Transactions on Software Engineering*, vol. 24, pp. 1131–1155, 1998.
- [36] BURRIS, T. and HASHEM, P., "Hamilton Sundstrand adds first Italian supplier for Pratt & Whitney F135 engine , British firm to provide inlet and exhaust monitoring" <http://www.hamiltonsundstrand.com>, July 2002.
- [37] BURRIS, T. K., SUTTON, J. K., and GREGG, M., "AFRL-VA-WP-TP-2003-342: Military Utility of HEL Fighter," tech. rep., Directed Energy Professional Society, 2003.
- [38] CAMPBELL, R., "Will the real scenario please stand up?," *ACM SIGCHI Bulletin*, vol. 24, no. 2, pp. 6–8, 1992.
- [39] CARD, S., MORAN, T., and NEWELL, A., *The psychology of human-computer interaction*. CRC, 1983.
- [40] CARROLL, J., *Scenario-based design*, vol. 2. 1997.
- [41] CASTAGNE, S., CURRAN, R., ROTHWELL, A., PRICE, M., BENARD, E., and RAGHUNATHAN, S., "A generic tool for cost estimating in aircraft design," *Research in Engineering Design*, vol. 18, no. 4, pp. 149–162, 2008.
- [42] CASTI, J., "On system complexity: Identification, measurement and management," *Complexity, Language and Life: Mathematical Approaches*, vol. 16, pp. 146–173, 1986.
- [43] CHO, S. and EPPINGER, S., "Product development process modeling using advanced simulation," in *Proc. ASME Design Engineering Technical Conference DETC01*, pp. 1–10.
- [44] CLOYD, J. S., "Status of the United States Air Force's More Electric Aircraft Initiative," *IEEE Aerospace and Electronics Systems Magazine*, vol. 13, pp. 17–22, 1998.
- [45] COLBY, R. and FLORA, D., "Measured efficiency of high efficiency and standard induction motors," in *Conference Record of the 1990 IEEE Industry Applications Society Annual Meeting*, pp. 18–23, IEEE, 1990.
- [46] COLEBROOK, C., "Turbulent flow in pipes, with particular reference to the transition region between the smooth and rough pipe laws," *Journal of the Institution of Civil Engineers*, vol. 11, pp. 133–156, 1938-39.

- [47] COMMITTEE ON ADVANCED ENGINEERING ENVIRONMENTS, AERONAUTICS AND SPACE ENGINEERING BOARD, COMMISSION ON ENGINEERING AND TECHNICAL SYSTEM, NATIONAL RESEARCH COUNCIL, NATIONAL ACADEMY OF ENGINEERING, *Design in the new millennium: advanced engineering environments: Phase 2*. National Academies Press, 2000.
- [48] COMMITTEE ON AIR QUALITY IN PASSENGER CABINS OF COMMERCIAL AIRCRAFT, *The Airliner Cabin Environment and the Health of Passengers and Crew*. National Academy Press, Washington, D.C., 2002.
- [49] COMONATION, P., GHOLSTON, S., HYATT, L., and SIMMONS, B., “Benefits of modeling and simulation in implementing a shared component build strategy,” *Systems Engineering*, vol. 6, no. 2, pp. 63–75, 2003.
- [50] COULOM, D., “Hamilton Sundstrand signs agreement with All Nippon Airways for 787 maintenance support.” <http://www.hamiltonsundstrand.com>, Nov 2008.
- [51] COULOM, D. and CARROLL, C., “Hamilton Sundstrand Congratulates Boeing on 787 First Flight; Achieves Several Technical ‘Firsts’.” <http://www.hamiltonsundstrand.com>, December 2009.
- [52] COZON, G. and SPOUGE, J., “OATA Safety Assessment: Functional Hazard Assessment (En-Route),” tech. rep., European Organisation for the Safety of Air Navigation, 2007.
- [53] CRAWLEY, E., DE WECK, O., EPPINGER, S., MAGEE, C., MOSES, J., SEERING, W., SCHINDALL, J., WALLACE, D., and WHITNEY, D., “The influence of architecture in engineering systems,” *Engineering Systems Monograph*, vol. 2006, 2004.
- [54] CRAWLEY, F., PRESTON, M., and TYLER, B., *HAZOP: guide to best practice: guidelines to best practice for the process and chemical industries*. Inst of Chemical Engineers, 2000.
- [55] CRISTIAN, F., *Understanding fault-tolerant distributed systems*. ACM New York, NY, USA, 1991.
- [56] CRONIN, M., “All-electric vs conventional aircraft- The production/operational aspects,” *Journal of Aircraft*, vol. 20, pp. 481–487, 1983.
- [57] CROWLEY, T., CORRIE, T., DIAMOND, D., FUNK, S., HANSEN, W., STENHOFF, A., and SWIFT, D., “Transforming The Way DOD Looks At Energy,” 2007.
- [58] CRUTCHFIELD, J., “The calculi of emergence,” *Physica D*, vol. 75, pp. 11–54, 1994.
- [59] CSERMELY, P., *Weak links: Stabilizers of complex systems from proteins to social networks*. Springer Verlag, 2006.
- [60] DAHMANN, J.S., F. R. and WEATHERLY, R., “DoD high level architecture,” in *Proceedings of the 1997 Winter Simulation Conference*, 1997.
- [61] DALTON, J., “Commercial Airplane Processes for Safety Assessment.” Presentation: Boeing Commercial Airplanes, February 28th - Mar 1st 2006.

- [62] DALY, K., "Some generalizations of state-space-averaged modelling in continuous mode," *International Journal of Electronics*, vol. 60, no. 2, pp. 191–198, 1986.
- [63] DANILOVIC, M. and BROWNING, T., "Managing complex product development projects with design structure matrices and domain mapping matrices," *International Journal of Project Management*, vol. 25, no. 3, pp. 300–314, 2007.
- [64] DANO, B., BRIAND, H., and BARBIER, F., "A use case driven requirements engineering process," *Requirements Engineering*, vol. 2, no. 2, pp. 79–91, 1997.
- [65] DAWKINS, S., KELLY, T., MCDERMID, J., MURDOCH, J., and PUMFREY, D., "Issues in the conduct of PSSA," in *Proceedings of the 17th International System Safety Conference*, vol. 122, 1999.
- [66] DE NEUFVILLE, R., DE WECK, O., FREY, D., HASTINGS, D., LARSON, R., SIMCHILEVI, D., OYE, K., WEIGEL, A., and WELSCH, R., "Uncertainty management for engineering systems planning and design," in *Engineering Systems Symposium, MIT, Cambridge, MA*, 2004.
- [67] DE TENORIO, C., ARMSTRONG, M., and MAVRIS, D., "Architecture subsystem sizing and coordinated optimization methods," in *47th AIAA Aerospace Sciences Meeting*, 2009.
- [68] DE TENORIO, C., "Methodology for aircraft systems architecture sizing," in *26th International Congress of the Aeronautical Sciences*, 2008.
- [69] DE TENORIO, C., *Methods for collaborative conceptual design of aircraft power architectures*. PhD thesis, Georgia Institute of Technology, 2011.
- [70] DENSON, W., *Nonelectronic parts reliability data*. Reliability Analysis Center, 1991.
- [71] DEPARTMENT OF ENERGY, *Root Cause Analysis Guidance Document*. US Department of Energy: Washington, 1992.
- [72] DEPARTMENT OF DEFENSE, "MIL-STD-882D: Standard Practice for System Safety," February 2000.
- [73] DEPARTMENT OF DEFENSE, "MIL-STD-704F Aircraft Electric Power Characteristics," March 2004.
- [74] DEPARTMENT OF DEFENSE, "DoD Architecture Framework Version 1.5," April 2007.
- [75] DEPARTMENT OF DEFENSE SYSTEMS MANAGEMENT COLLEGE, "Systems engineering fundamentals." Defense Acquisition University Press, Fort Belvoir, VA, January 2001.
- [76] DIETER, G., *Engineering design: a materials and processing approach*. McGraw-Hill Science/Engineering/Math, 2000.
- [77] DORAN, T., "IEEE 1220: for practical systems engineering," *Computer*, vol. 39, no. 5, pp. 92–94, 2006.
- [78] DORNHEIM, M. A., "Boeing 787 Technology: Massive 787 Electrical System Pressurizes Cabin," *Aviation Week and Space Technology*, 2005.

- [79] DORST, K. and VERMAAS, P., "John Gero's Function-Behaviour-Structure model of designing: a critical analysis," *Research in Engineering Design*, vol. 16, no. 1, pp. 17–26, 2005.
- [80] DOUGLASS, P. and EVANGELIST, C., "Safety-critical systems design," *Electronic Engineering*, vol. 70, no. 862, pp. 45–6, 1998.
- [81] DUGAN, J., "Automated analysis of phased-mission reliability," *IEEE Transactions on Reliability*, vol. 40, no. 1, pp. 45–52, 1991.
- [82] ECKERT, C., CLARKSON, P., and ZANKER, W., "Change and customisation in complex engineering domains," *Research in Engineering Design*, vol. 15, no. 1, pp. 1–21, 2004.
- [83] EDELMAN, G., "Interview with Gerald M. Edelman: part II.," *BioEssays: News and Reviews in Molecular, Cellular and Developmental Biology*, vol. 26, no. 3, p. 326, 2004.
- [84] EISNER, H., "RCASSE: Rapid computer-aided systems of systems engineering," in *Proceedings of the 3rd International Symposium of the National Council of System Engineering*, pp. 267–273, 1993.
- [85] EKSTRAND, C. and PANDET, M., "New Etops Regulations," *Aero*, vol. 22, pp. 3–11, 2003.
- [86] EMADI, A., EHSANI, M., and MILLER, J., *Vehicular electric power systems: land, sea, air, and space vehicles*. CRC, 2004.
- [87] EMADI, K. and EHSANI, M., "Aircraft power systems: technology, state of the art, and future trends," *IEEE Aerospace and Electronic Systems Magazine*, vol. 15, no. 1, pp. 28–32, 2000.
- [88] ENSIGN, T., "Performance and Weight Impact of Electric Environmental Control System and More Electric Engine on Citation CJ2," in *45th AIAA Aerospace Sciences Meeting and Exhibit*, 2007.
- [89] ERICKSON, T., "Notes on design practice: Stories and prototypes as catalysts for communication," in *Scenario-based design*, p. 58, John Wiley & Sons, Inc., 1995.
- [90] ERICSON, C., *Hazard analysis techniques for system safety*. John Wiley and Sons, 2005.
- [91] FALEIRO, L., "Beyond the more electric aircraft," *Aerospace America*, vol. 43, no. 9, pp. 35–40, 2005.
- [92] FALEIRO, L., ROUTEX, J., DODDS, G., DOUCET, B., and AUBRIL, J., eds., *Technologies for Energy Optimized Aircraft Equipment Systems: Technical Summary*, Power Optimized Aircraft Project Consortium, June 2006.
- [93] FALEIRO, L., "Power Optimized Aircraft to Change Industry Mindset," *Interavia Business and Technology*, 2002.

- [94] FALIERO, L., "Power Optimised Aircraft," tech. rep., Technologies for Energy Optimized Aircraft Equipment Systems, 2006.
- [95] FEDERAL AVIATION ADMINISTRATION, "Advisory Circular 25.1309-1A," June 21 1988.
- [96] FEDERAL AVIATION ADMINISTRATION, "FAA System Safety Handbook," December 30 2000.
- [97] FEDERAL AVIATION ADMINISTRATION, "AC 120-91: Airport Obstacle Analysis," May 5 2006.
- [98] FEDERAL AVIATION ADMINISTRATION, "Advisory Circular: Aircraft Ice Protection," August 16 2006.
- [99] FEDERAL AVIATION ADMINISTRATION, "FAR 121: Operating Requirements: Domestic, Flag, and Supplemental Operations," February 2007.
- [100] FEDERAL AVIATION ADMINISTRATION, "AC-120-42B: Extended Operations (ETOPS and Polar Operations)," June 13 2008.
- [101] FEDERAL AVIATION ADMINISTRATION, "Take-off minimums and (obstacle) departure procedures," July 26 2011.
- [102] FÉLIX, M., "A Copper Bird for Aircraft Equipment Systems Integration and Electrical Network Characterization," in *45th AIAA Aerospace Sciences Meeting and Exhibit*, 2007.
- [103] FENELON, P., MCDERMID, J., NICOLSON, M., and PUMFREY, D., "Towards integrated safety analysis and design," *ACM SIGAPP Applied Computing Review*, vol. 2, no. 1, pp. 21–32, 1994.
- [104] FLAKE, G., "Review of the Computational Beauty of Nature," *AI Magazine*, vol. 21, no. 2, 2000.
- [105] FORSBERG, K., MOOZ, H., and COTTERMAN, H., *Visualizing project management: models and frameworks for mastering complex systems*. Wiley, 2005.
- [106] FREEH, J., LIANG, A., BERTON, J., and WICKENHEISER, T., "Electrical Systems Analysis at NASA Glenn Research Center: Status and Prospects," *Applied Vehicle Technology Panel of the NATO Research and Technology Agency, Brussels, Belgium*, 2003.
- [107] FUNTOWICZ, S. and RAVETZ, J., "Emergent complex systems," *Futures*, vol. 26, no. 6, pp. 568–582, 1994.
- [108] GAILLARD, C., *An Analysis of the Impact of Modularization and Standardization of Vehicles Electronics Architecture on the Automotive Industry*. PhD thesis, MIT, 2005.
- [109] GAVEL, H., "Aircraft fuel system synthesis aided by interactive morphology and optimization," in *45th AIAA Aerospace Sciences Meeting and Exhibit*, 2007.
- [110] GERWIN, D. and BARROWMAN, N., "An evaluation of research on integrated product development," *Management Science*, vol. 48, no. 7, pp. 938–953, 2002.

- [111] GLINZ, M., “An integrated formal model of scenarios based on statecharts,” *Lecture Notes in Computer Science*, vol. 989, pp. 254–271, 1995.
- [112] GLOVER, F., KELLY, J., and LAGUNA, M., “New advances and applications of combining simulation and optimization,” in *Proceedings of the 28th Conference on Winter simulation*, pp. 144–152, IEEE Computer Society Washington, DC, 1996.
- [113] GO, K. and CARROLL, J., “The blind men and the elephant: Views of scenario-based system design,” *interactions*, vol. 11, no. 6, pp. 44–53, 2004.
- [114] GOLICH, V., “From competition to collaboration: the challenge of commercial-class aircraft manufacturing,” *International Organization*, vol. 46, no. 4, pp. 899–934, 1992.
- [115] GRAHAM, I. and GREEN, I., *Military Technology*. Evans Brothers, Limited, 2008.
- [116] GRENIER, D. and LOUIS, J., “Modeling for control of non-sinewave permanent-magnet synchronous drives by extending Park’s transformation,” *Mathematics and Computers in Simulation*, vol. 38, no. 4-6, p. 452, 1995.
- [117] HAMMER, J., CALIGARIS, G., and LLOBET, M., “Safety Assessment Methodology for ADS-B Surveillance Applications,” in *7th USA/Europe Air Traffic Management Research and Development Seminar*, 2007.
- [118] HANDLEY, H. and LEVIS, A., “Organizational architectures and mission requirements: A model to determine congruence,” *Systems Engineering*, vol. 6, no. 3, pp. 184–194, 2003.
- [119] HAREL, D., “Statecharts: A visual formalism for complex systems,” *Science of computer programming*, vol. 8, no. 3, pp. 231–274, 1987.
- [120] HAREL, D. and PNEULI, A., “On the development of reactive systems,” *Weizmann Institute of Science, Dept. of Computer Science*, 1985.
- [121] HARRIGAN, F., “Integrating theories of boundary choice: a case from the global aircraft industry,” in *The International Conference on Coordination and Cooperation across Organizational Boundaries*, 2006.
- [122] HARTIGAN, J., *Clustering algorithms*. Wiley, New York, 1975.
- [123] HARWELL, R., ASLAKSEN, E., HOOKS, I., MENGOT, R., and PTACK, K., “What is a requirement,” in *Proceedings of the Third International Symposium of the NCOSE*, vol. 2, 1993.
- [124] HASHEMIAN, M., *Design for adaptability*. PhD thesis, Universtiy of Saskatchewan, 2005.
- [125] HASKINS, C., “Systems engineering handbook: A guide for system life cycle processes and activities, version 2a.” International Council on Systems Engineering, June 2004.
- [126] HASKINS, C., *INCOSE Systems Engineering Handbook*, vol. 3. 2007.
- [127] HAYS, D., *Requirements analysis: from business views to architecture*. Prentice Hall, 2003.

- [128] HECHT, J., "Solid-state high-energy laser weapons," *Optics and Photonics News*, vol. 14, no. 1, pp. 42–47, 2003.
- [129] HEIMBOLD, R., CRONIN, M., and HOWISON, W., "Study of the Application of Advanced Electrical/Electronic Technologies to Conventional Aircraft," tech. rep., NASA/JSC/Lockheed, 1979.
- [130] HENDERSON, R. and CLARK, K., "Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms," *Administrative science quarterly*, vol. 35, no. 1, 1990.
- [131] HICKIE, D., "Knowledge and competitiveness in the aerospace industry: The cases of toulouse, seattle and north-west England," *European Planning Studies*, vol. 14, no. 5, pp. 697–716, 2006.
- [132] HIRTZ, J., STONE, R., MCADAMS, D., SZYKMAN, S., and WOOD, K., "A functional basis for engineering design: reconciling and evolving previous efforts," *Research in engineering Design*, vol. 13, no. 2, pp. 65–82, 2001.
- [133] HOBAN, F. and HOFFMAN, E., "NASA Systems Engineering Handbook," *NASA SP-610S*, 1995.
- [134] HOBDAY, M., DAVIES, A., and PRENCIPE, A., "Systems integration: a core capability of the modern corporation," *Industrial and Corporate Change*, vol. 14, no. 6, p. 1109, 2005.
- [135] HOLBROOK III, H., "A scenario-based methodology for conducting requirements elicitation," *ACM SIGSOFT Software Engineering Notes*, vol. 15, no. 1, pp. 95–104, 1990.
- [136] HOOPER, J. and HSIA, P., "Scenario-based prototyping for requirements identification," *Software Engineering Notes*, vol. 7(5), pp. 88–93, 1982.
- [137] HOWSE, M., "All-electric aircraft," *Power Engineer*, vol. 17, p. 35, 2003.
- [138] HOYLAND, A. and RAUSAND, M., *System reliability theory: models and statistical methods*. Wiley-Interscience, 1994.
- [139] HSIA, P., SAMUEL, J., GAO, J., KUNG, D., TOYOSHIMA, Y., and CHEN, C., "Formal approach to scenario analysis," *IEEE Software*, vol. 11, no. 2, pp. 33–41, 1994.
- [140] HSU, C., CHEN, C., and CHEN, J., "The load-shedding scheme design for an integrated steelmaking cogeneration facility," *IEEE Transactions on Industry Applications*, vol. 33, no. 3, pp. 586–592, 1997.
- [141] HUANG, S., LUO, J., LEONARDI, F., and LIPO, T., "A general approach to sizing and power density equations for comparison of electrical machines," *Industry Applications, IEEE Transactions on*, vol. 34, no. 1, pp. 92–97, 1998.
- [142] HUGHES, T., *Networks of power: electrification in Western society, 1880-1930*. Johns Hopkins Univ Pr, 1993.
- [143] HUNDAL, M., "A systematic method for developing function structures, solutions and concept variants," *Mechanism and Machine theory*, vol. 25, no. 3, pp. 243–256, 1990.

- [144] IGLESIA, E., "Design, synthesis, and use of cobalt-based Fischer-Tropsch synthesis catalysts," *Applied Catalysis A, General*, vol. 161, no. 1-2, pp. 59–78, 1997.
- [145] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, "Systems engineering: System life cycle processes," 2002.
- [146] JACOBSON, I., "The use-case construct in object-oriented software engineering," *Scenario-based design: envisioning work and technology in system development*, pp. 309–336, 1995.
- [147] JACOBSON, I., *Object-Oriented Software Engineering: A Use Case Driven Approach*. Addison-Wesley Longman Publishing Co., Inc. Essex, England, 1992.
- [148] JARDINE, A., ANDERSON, P., and MANN, D., "Application of the weibull proportional hazards model to aircraft and marine engine failure data," *Quality and reliability engineering international*, vol. 3, no. 2, pp. 77–82, 1987.
- [149] JOHN, B. and KIERAS, D., "The GOMS family of user interface analysis techniques: Comparison and contrast," *ACM Transactions on Computer-Human Interaction (TOCHI)*, vol. 3, no. 4, pp. 320–351, 1996.
- [150] JOHNSON, C. L., "Control Boosters: Design Problems and Their Solution on the Lockheed Constellation," *Flight*, pp. 195–198, 1946.
- [151] JOHNSON, H. and JOHNSON, P., "Task Knowledge Structures: Psychological basis and integration into system design," *Cognitive Ergonomics: Contributions from Experimental Psychology*, vol. 78, pp. 3–26, 1992.
- [152] JOHNSON, P., JOHNSON, H., WADDINGTON, R., and SHOULS, A., "Task-related knowledge structures: analysis, modelling and application," in *Proceedings of the Fourth Conference of the British Computer Society on People and computers IV*, pp. 35–62, Citeseer, 1988.
- [153] JOHNSON, P., JOHNSON, H., and WILSON, S., "Rapid Prototyping of User Interfaces Driven by Task Models," *Scenario-based design: envisioning work and technology in system development*, pp. 209–246, 1995.
- [154] JOMIER, T., "More Open Electric Technologies: Technical Report," tech. rep., European Commission within the Sixth Framework Programme, 2006.
- [155] JONES, R., "The more electric aircraft: Assessing the benefits," *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, vol. 216, no. 5, pp. 259–269, 2002.
- [156] JOYNER, C. and MCGINNIS, P., "The application of itaps for evaluation of propulsion and power at the system level," in *40th AIAA/ASME/SAE/ASEE Joint Propulsion Conference and Exhibit*, no. AIAA 2004-3849, 2004.
- [157] JUNG, J., LIU, C., TANIMOTO, S., and VITTAL, V., "Adaptation in load shedding under vulnerable operating conditions," *IEEE Transactions on Power Systems*, vol. 17, no. 4, pp. 1199–1205, 2002.

- [158] JURJENS, J., “Developing safety-critical systems with UML,” *Lecture notes in computer science*, pp. 360–372, 2003.
- [159] KAHN, H., *Thinking about the Unthinkable*. Avon, 1968.
- [160] KAHNEMAN, D., SLOVIC, P., and TVERSKY, A., *Judgment under uncertainty: Heuristics and biases*. Cambridge Univ Pr, 1982.
- [161] KAINDL, H., HUBER, S., KARACAN, O., KONDO, I., SCHREINER, H., and SUSS, H., “ooSEM: a process model for object-oriented development in an industrial environment,” in *Conference on Object Oriented Programming Systems Languages and Applications*, 2000.
- [162] KARAT, J., “Scenario in the design of a speech recognition system,” *Scenario-based design: envisioning work and technology in system development*, pp. 109–133, 1995.
- [163] KECECIOGLU, D., *Reliability engineering handbook, volume 1/2*. DEStech Publications, Inc, 2002.
- [164] KELLY, T., *Arguing safety-a systematic approach to managing safety cases*. PhD thesis, University of York Department of Computer Science, 1999.
- [165] KIM, J., KIM, J., PARK, S., and SUGUMARAN, V., “A multi-view approach for requirements analysis using goal and scenario,” *Industrial Management and Data Systems*, vol. 104, pp. 702–711, 2004.
- [166] KIRBY, M. R., *A Method for Technology Identification, Evaluation, and Selection in Conceptual and Preliminary Aircraft Design*. PhD thesis, Georgia Institute of Technology, 2001.
- [167] KIRBY, M. and MAVRIS, D., “An approach for the intelligent assessment of future technology portfolios,” in *40th AIAA Aerospace Sciences Meeting*, Georgia Institute of Technology, 2002.
- [168] KLETZ, T., *HAZOP and HAZAN: identifying and assessing process industry hazards*. Taylor & Francis, 1999.
- [169] KOCH, P., ALLEN, J., MISTREE, F., and MAVRIS, D., “The problem of size in robust design,” *Advances in Design Automation*, pp. 253–258, 1997.
- [170] KOCH, T. and MURER, S., “Service architecture integrates mainframes in a CORBA environment,” in *Enterprise Distributed Object Computing Conference, 1999 Proceedings. Third International*, pp. 194–203, 1999.
- [171] KOGUT, B., SHAN, W., and WALKER, G., “The make-or-cooperate decision in the context of an industry network,” *Networks and organizations: Structure, form and action*, pp. 348–365, 1992.
- [172] KOSKIMIES, K., SYSTA, T., TUOMI, J., and MANNISTO, T., “Automated support for modeling OO software,” *IEEE software*, vol. 15, no. 1, pp. 87–94, 1998.
- [173] KRAUSE, P., WASYNCZUK, O., and SUDHOFF, S., *Analysis of electric machinery and drive systems*. IEEE press, 2002.

- [174] KREIN, P., BENTSMAN, J., BASS, R., and LESIEUTRE, B., "On the use of Averaging for the Analysis of Power Electronics Systems," in *IEEE Transactions on Power Electronics*, vol. 5, pp. 182–190, 1990.
- [175] KRISHNAN, V. and ULRICH, K. T., "Product Development Decisions: A Review of the Literature," *Management Science*, vol. 47, pp. 1–21, 2001.
- [176] KRITZINGER, D., *Aircraft system safety: military and civil aeronautical applications*. CRC, 2006.
- [177] KRITZINGER, D. and GOLDSMITH, S., "Aircraft System Safety: An Introduction to Tools and Techniques." www.aircraftsystemsafety.com, April 20 2010.
- [178] KUHN, M., GRIFFO, A., WANG, J., and BALS, J., "A components library for simulation and analysis of aircraft electrical power systems using Modelica," in *13th European Conference on Power Electronics and Applications*, pp. 1–10, 2009.
- [179] KUHN, M., OTTER, M., RAULIN, L., DLR, G., and FRANCE, A., "A multi level approach for aircraft electrical systems design," in *Sixth International Modelica Conference*, vol. 1, pp. 95–101, 2008.
- [180] KURAKAWA, K., "A scenario-driven conceptual design information model and its formation," *Research in Engineering Design*, vol. 15, no. 2, pp. 122–137, 2004.
- [181] KUUTTI, K., "Work processes: Scenarios as a preliminary vocabulary," *Scenario-based design: envisioning work and technology in system development*, pp. 19–36, 1995.
- [182] KYNG, M., "Creating contexts for design," *Scenario-based design: envisioning work and technology in system development*, pp. 85–107, 1995.
- [183] LAWRENCE, P. and THORNTON, D., *Deep stall: The turbulent story of Boeing commercial airplanes*. Ashgate Pub Co, 2005.
- [184] LAZONICK, W. and PRENCIPE, A., "Dynamic capabilities and sustained innovation: strategic control and financial commitment at Rolls-Royce plc," *Industrial and Corporate Change*, vol. 14, no. 3, p. 501, 2005.
- [185] LEACH, L., "Critical chain project management improves project performance," *Project Management Journal*, vol. 30, pp. 39–51, 1999.
- [186] LELIEVRE, T., LAPIE, J., BEAULIEU, R., and RATTIER, R., "Afi rvsm programme: Functional hazard assessment," tech. rep., ALTRAN Technologies, December 2005.
- [187] LEVI, S. and AGRAWALA, A., *Fault tolerant system design*. McGraw-Hill Companies, 1994.
- [188] LIN, J., FOX, M., and BILGIC, T., "A requirement ontology for engineering design," *Concurrent Engineering*, vol. 4, no. 3, p. 279, 1996.
- [189] LISCOUËT-HANKE, S., PUFE, S., and MARE', J., "A simulation framework for aircraft power management," vol. 222, pp. 749–756, Prof Eng Publishing, 2008.

- [190] LISCOUËT-HANKE, S., *A Model-Based Methodology for Integrated Preliminary Sizing and Analysis of Aircraft Power System Architectures*. PhD thesis, Université de Toulouse, 2008.
- [191] LOMBARDO, D., *Aircraft Systems*. McGraw-Hill Professional, 1998.
- [192] LÖSCH, U., DUGDALE, J., and DEMAZEAU, Y., "Requirements for Supporting Individual Human Creativity in the Design Domain," *International Conference on Entertainment Computing*, pp. 210–215, 2009.
- [193] LUMSDAINE, E. and LUMSDAINE, M., *Creative problem solving: Thinking skills for a changing world*. McGraw-Hill, 1995.
- [194] MACK, R., "Discussion: scenarios as engines of design," p. 386, 1995.
- [195] MACLEAN, A. and MCKERLIE, D., "Design space analysis and use-representations," *Scenario-based design: envisioning work and technology in system development*, pp. 183–207, 1995.
- [196] MACPHERSON, A. and VANCHAN, V., "The Outsourcing of Industrial Design Services by Large US Manufacturing Companies," *International Regional Science Review*, vol. 2009, pp. 1–28, 2009.
- [197] MAGUIRE, R., *Safety cases and safety reports: meaning, motivation and management*. Ashgate Pub Co, 2006.
- [198] MAIER, M., "Architecting principles for systems-of-systems," *Systems Engineering*, vol. 1, no. 4, pp. 267–284, 1998.
- [199] MAKOWSKI, L., "This is Hamilton Sundstrand." <http://ieee.rackoneup.net>, July 2007.
- [200] MATSON, R., *Aircraft Electrical Engineering*. McGraw-Hill Book Company, York, PA, 1943.
- [201] MATTINGLY, J., HEISER, W., and PRATT, D., *Aircraft engine design*. American Institute of Aeronautics and Astronautics, 2002.
- [202] MATTINGLY, J. and VON OHAIN, H., *Elements of propulsion: gas turbines and rockets*. American Institute of Aeronautics and Astronautics, 2006.
- [203] MAVRIS, D., DE TENORIO, C., and ARMSTRONG, M., "Methodology for Aircraft System Architecture Definition," in *46 th AIAA Aerospace Sciences Meeting and Exhibit*, 2008.
- [204] MAVRIS, D., PHAN, L., and GARCIA, E., "Formulation and Implementation of an Aircraft System Subsystem Interrelationship Model for Technology Evaluation," in *25th International Congress of the Aeronautical Sciences*, vol. 21, pp. 35–36, 2006.
- [205] MCLOUGHLIN, A., "More Electric-Ready for take off?," *13th European Conference Power Electronics and Applications*, 2009.
- [206] MEADOWS, D. and ROBINSON, J., "The electronic oracle: computer models and social decisions," *System Dynamics Review*, vol. 18, no. 2, pp. 271–308, 2002.

- [207] MICHELENA, N. and PAPALAMBROS, P., “Optimal model-based decomposition of powertrain system design,” *Journal of Mechanical Design*, vol. 117, pp. 499–505, 1995.
- [208] MIDDLEBROOK, R. and ČUK, S., “A general unified approach to modelling switching-converter power stages,” *International Journal of Electronics*, vol. 42, no. 6, pp. 521–550, 1977.
- [209] MITCHAM, A. and GRUM, N., “An integrated LP shaft generator for the more electric aircraft,” in *IEE Colloquium on All Electric Aircraft (Digest No. 1998/260)*, p. 8, 1998.
- [210] MOIR, I. and SEABRIDGE, A., *Design and development of aircraft systems: an introduction*. Wiley-Blackwell, 2004.
- [211] MOIR, I. and SEABRIDGE, A., *Aircraft systems: Mechanical, Electrical, and Avionics Subsystems Integration*. American Institute of Aeronautics and Astronautics, Inc., 2008.
- [212] MOMOH, J. and DIOUF, O., “Optimal reconfiguration of the navy ship power system using agents,” in *2005/2006 IEEE PES Transmission and Distribution Conference and Exhibition*, pp. 562–567, 2005.
- [213] MORRIS, J. and KOOPMAN, P., “Representing design tradeoffs in safety-critical systems,” *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 4, p. 5, 2005.
- [214] MUKKAMALA, R. and RAMESH, R., “A process model for engineering of complex systems architectures with complex subsystem architecture reuse in mind,” in *The 24th Digital Avionics Systems Conference*, vol. 2, 2005.
- [215] MURDOCH, J., “Safety assessment of system architectures,” in *International Council on Systems Engineering Tenth Annual International Symposium on A Decade of Progress... A New Century of Opportunity*, 2000.
- [216] MYERS, B., HOLLAN, J., CRUZ, I., BRYSON, S., BULTERMAN, D., CATARCI, T., CITRIN, W., GLINERT, E., GRUDIN, J., and IOANNIDIS, Y., “Strategic Directions in Human Computer Interaction,” *ACM Computing Surveys*, vol. 28, no. 4, pp. 794–809, 1996.
- [217] NAIRUS, J., “Air Force Research Laboratory’s INVENT Program: 88ABW-2009-2770.” INVENT to Pace Webinar, July 2009.
- [218] NALEBUFF, B., “Bundling: GE-Honeywell (2001),” *The Antitrust Revolution, 4th Edition*, Oxford University Press, vol. 16, 2003.
- [219] NAM, T., SOBAN, D., and MAVRIS, D., “Power Based Sizing Method for Aircraft Consuming Unconventional Energy,” in *43rd AIAA Aerospace Sciences Meeting and Exhibit*, p. 2005, 2005.
- [220] NARDI, B., “The use of scenarios in design,” *ACM SIGCHI Bulletin*, vol. 24, no. 4, pp. 13–14, 1992.

- [221] NASA OFFICE OF SAFETY AND MISSION ASSURANCE, “NASA Procedures and Guidelines: Risk Management Procedures and Guidelines NPG 8000.4,” November 2002.
- [222] NEUFELD, D. and CHUNG, J., “Development of Aircraft Conceptual Design Optimization Software,” in *International Conference on Computational Science and its Applications*, pp. 313–317, 2007.
- [223] NEWHOUSE, J., *The sporty game*. Knopf, 1982.
- [224] NICOLAI, L., *Fundamentals of aircraft design*. University of Dayton, School of Engineering, 1975.
- [225] NIELSEN, J., *Scenarios in discount usability engineering*. John Wiley & Sons, Inc. New York, NY, USA, 1995.
- [226] NUSEIBEH, B. and EASTERBROOK, S., “Requirements engineering: a roadmap,” in *Proceedings of the Conference on the Future of Software Engineering*, pp. 35–46, ACM New York, NY, USA, 2000.
- [227] OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION TECHNOLOGY AND LOGISTICS, “Unmanned Systems Safety Guide for DoD Acquisition,” June 2007.
- [228] OLVANDER, J., LUNDEN, B., and GAVEL, H., “A computerized optimization framework for the morphological matrix applied to aircraft conceptual design,” *Computer-Aided Design*, vol. 41, no. 3, pp. 187–196, 2009.
- [229] PAHL, G., BEITZ, W., WALLACE, K., BLESSING, L., and BAUERT, F., *Engineering design: A systematic approach*. Springer Verlag, 1996.
- [230] PARKER, G. and ANDERSON JR, E., “From buyer to integrator: the transformation of the supply-chain manager in the vertically disintegrating firm,” *Production and Operations Management*, vol. 11, no. 1, pp. 75–91, 2002.
- [231] PAUL, S., “Functional Hazard Assessment and Very Preliminary System Safety Assessment Report,” tech. rep., Thales ATM: 6th FP Project FP6 -503192, 2006.
- [232] PELLEGRINI, L., GANDOLFI, R., DA SILVA, G., and DE OLIVEIRA JR, S., “Exergy Analysis as a Tool for Decision Making in Aircraft Systems Design,” in *45th AIAA Aerospace Sciences Meeting and Exhibit, Reno, USA*, Citeseer, 2007.
- [233] PHAN, L., MAVRIS, D., CHARRIER, J.-J., THALIN, P., and GARCIA, E., “Parametric Modeling of an Electrical Test Rig for Power Optimized Aircraft Architectures,” in *26th International Congress of the Aeronautical Sciences*, 2008.
- [234] POTTS, C., A. T. K. and ANTON, A. I., “Inquiry-based requirements analysis,” *IEEE Software*, vol. 11(2), pp. 21–32, 1994.
- [235] PRITCHARD, D. and MACPHERSON, A., “Outsourcing US commercial aircraft technology and innovation: implications for the industry’s long term design and build capability,” *Canada-United States Trade Center, Occasional Paper*, July 2004.

- [236] PRITCHARD, D. and MACPHERSON, A., “Boeing’s Diffusion of Commercial Aircraft Design and Manufacturing Technology to Japan: Surrendering the US Aircraft Industry for Foreign Financial Support,” *Canada-United States Trade Center, Occasional Paper*, March 2005.
- [237] PRITCHARD, D. and MACPHERSON, A., “Strategic destruction of the North American and European commercial aircraft industry,” *Airframer: The Journal of Aircraft Manufacturing*, vol. 17, pp. 1–8, 2007.
- [238] PRNEWswire, “Hamilton Sundstrand Nearing Completion of Delivery of Systems for Boeing 787 Dreamliner.” Press Release, June 18, 2007.
- [239] PRZEMIENIECKI, J., *Critical technologies for national defense*. American Institute of Aeronautics and Astronautics, 1991.
- [240] QUET, A., “Revision of rules for etops and lrops: Extented twin-engined and long range three - and four - engined operations,” *FAST: Flight Airworthiness Support Technology*, vol. 32, pp. 17–24, 2003.
- [241] RAKSCH, C., VAN MAANEN, R., REHAGE, D., THIELECKE, F., and CARL, U., “Performance degradation analysis of fault-tolerant aircraft systems,” in *First CEAS European Air and Space Conference*, September 2007.
- [242] RAUSAND, M. and HØYLAND, A., *System reliability theory: models, statistical methods, and applications*. Wiley-IEEE, 2004.
- [243] RAUSAND, M. and HØYLAND, A., *System Reliability Theory: Models, Statistical Methods, and Applications (Second Edition)*. Wiley, 2004.
- [244] RAYMER, D., *Aircraft design: a conceptual approach*. American Institute of Aeronautics and Astronautics, 2006.
- [245] RECHTIN, E., “The art of systems architecting,” *IEEE Spectrum*, vol. 29, no. 10, pp. 66–69, 1992.
- [246] REGNELL, B., KIMBLER, K., and WESSLEN, A., “Improving the use case driven approach to requirements engineering,” in *Proceedings of Second International Symposium on Requirements Engineering*, pp. 40–47, 1995.
- [247] REHAGE, D., CARL, U., MERKEL, M., and VAHL, A., “The effects on reliability of integration of aircraft systems based on integrated modular avionics,” *Lecture notes in computer science*, pp. 224–238, 2004.
- [248] ROBERTSON, S., “Generating object-oriented design representations via scenario queries,” p. 308, 1995.
- [249] ROGERS, E., ZOOK, K., and GOWDA, S., “Requirements Development for the NASA Advanced Engineering Environment (AEE),” in *42nd AIAA Aerospace Sciences Meeting and Exhibit*, 2004.
- [250] ROGERS, J., SALAS, A., and WESTON, R., “A Web-based monitoring system for multidisciplinary design projects,” in *7th AIAA/USAF/NASA/ISSMO Symposium on Multidisciplinary Analysis and Optimization*, pp. 35–43, 1998.

- [251] ROLLAND, C., BEN ACHOUR, C., CAUVET, C., RALYTÉ, J., SUTCLIFFE, A., MAIDEN, N., JARKE, M., HAUMER, P., POHL, K., DUBOIS, E., and OTHERS, “A proposal for a scenario classification framework,” *Requirements Engineering*, vol. 3, no. 1, pp. 23–47, 1998.
- [252] ROONEY, J. and HEUVEL, L., “Root cause analysis for beginners,” *Quality progress*, vol. 37, no. 7, pp. 45–56, 2004.
- [253] ROSKAM, J., *Airplane design Part V: Component Weight Estimation*. DARcorporation, 2003.
- [254] ROSS, P., *Taguchi techniques for quality engineering: loss function, orthogonal experiments, parameter and tolerance design*. McGraw-Hill Professional, 1995.
- [255] ROSSON, M. and CARROLL, J., “Narrowing the specification-implementation gap in scenario-based design,” *Scenario-based design: envisioning work and technology in system development*, pp. 247–78, 1995.
- [256] ROTMANS, J., KEMP, R., and VAN ASSELT, M., “More evolution than revolution: transition management in public policy,” *Foresight-The journal of future studies, strategic thinking and policy*, vol. 3, no. 1, pp. 15–31, 2001.
- [257] RUSSELL, N., TER HOFSTEDÉ, A., VAN DER AALST, W., and MULYAR, N., “Work-flow control-flow patterns: A revised view,” *BPM Center Report BPM-06-22*, pp. 06–22, 2006.
- [258] SAGE, A. and LYNCH, C., “Systems integration and architecting: An overview of principles, practices, and perspectives,” *Systems Engineering*, vol. 1, no. 3, pp. 176–227, 1998.
- [259] SANGIOVANNI-VINCENTELLI, A., CARLONI, L., DE BERNARDINIS, F., and SGROI, M., “Benefits and challenges for platform-based design,” in *Proceedings of the 41st annual conference on Design automation*, pp. 409–414, ACM New York, 2004.
- [260] SCHOEMAKER, P., “Scenario planning: a tool for strategic thinking,” *Sloan Management Review*, vol. 36, pp. 25–25, 1995.
- [261] SCHÖN, D.A., *Educating the reflective practitioner*. Jossey-Bass San Francisco, 1987.
- [262] SCHONNING, A., “An integrated design and optimization environment for industrial large scaled systems,” *Research in Engineering Design*, vol. 16, p. 86–95, 2005.
- [263] SCHUT, E., “Development and Implementation of Knowledge-Based Design Process Primitives,” in *26th International Congress of the Aeronautical Sciences*, 2008.
- [264] SECUNDE, R., MACOSKO, R., and REPAS, D., “Integrated engine-generator concept for aircraft electric secondary power: Design and characteristics of integrated engine-generator system for installation on aircraft turbojet and turbofan engines,” tech. rep., NASA Lewis Research Center, 1972.
- [265] SHANNON, C., “XXII. Programming a computer for playing chess,” *Philosophical Magazine (Series 7)*, vol. 41, no. 314, pp. 256–275, 1950.

- [266] SHARMAN, D. and YASSINE, A., "Characterizing complex product architectures," *Systems Engineering*, vol. 7, no. 1, pp. 35–60, 2004.
- [267] SHENHAR, A., "A new systems engineering taxonomy," in *Proceedings of the 4th International Symposium of the National Council on System Engineering*, vol. 2, pp. 261–276, 1994.
- [268] SHENHAR, A., "A new conceptual framework for modern project management," *Management of technology IV*, 1994.
- [269] SIMPLEMAN, L., MCMAHON, P., BAHNMAIER, B., EVANS, K., and LLOYD, J., "Risk Management Guide for DoD Acquisition." Department of Defense, August 2006.
- [270] SMITH, D., *Reliability, maintainability and risk: practical methods for engineers*. Butterworth-Heinemann, 2005.
- [271] SOCCI, V. P., "System Design Considerations for Vehicle-based Mobile Electric Power Applications," in *Power Electronic Technology 2005/Session PET06*, 2005.
- [272] SOCIETY OF AUTOMOTIVE ENGINEERS, "ARP 4754: Certification Considerations for Highly-Integrated or Complex Aircraft Systems," November 1996.
- [273] SOCIETY OF AUTOMOTIVE ENGINEERS, "ARP 4761: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," December 1996.
- [274] SOFTWARE ENGINEERING STANDARDS COMMITTEE, "IEEE Std 610.12-1990,IE EE Standard Glossary of Software Engineering Terminology," 1990.
- [275] SOFTWARE ENGINEERING STANDARDS COMMITTEE, "IEEE Guide for Developing System Requirements Specifications (IEEE std 1233)," 1998.
- [276] SOFTWARE ENGINEERING STANDARDS COMMITTEE, "IEEE Standard for Functional Modeling Language Syntax and Semantics for IDEF0," 1998.
- [277] SRIVASTAVA, S. and BUTLER-PURRY, K., "A pre-hit probabilistic reconfiguration methodology for shipboard power systems," in *Proc. IEEE Electric Ship Technologies Symposium, Philadelphia, PA*, pp. 25–27, 2005.
- [278] STAMATELATOS, M., APOSTOLAKIS, G., DEZFULI, H., EVERLINE, C., GUARRO, S., MOIENI, P., MOSLEH, A., PAULOS, T., and YOUNGBLOOD, R., "Probabilistic risk assessment procedures guide for NASA managers and practitioners," *NASA Office of Safety and Mission Assurance*, 2002.
- [279] STERMAN, J., "All models are wrong: reflections on becoming a systems scientist," *System Dynamics Review*, vol. 18, no. 4, pp. 501–531, 2002.
- [280] STONE, C. and HOLTERY, C., "The JWST integrated modeling environment," in *2004 IEEE Aerospace Conference, 2004. Proceedings*, vol. 6, 2004.
- [281] STROHMAYER, A., "Improving Aircraft Design Robustness with Scenario Methods," *Acta Polytechnica-Czech Technical University in Prague*, vol. 41, no. 4/5, pp. 68–73, 2001.

- [282] SUH, N., *The principles of design*. Oxford University Press, USA, 1990.
- [283] TAGGE, G., IRISH, L., and BAILEY, A., “Systems Study for an Integrated Digital/-Electric Aircraft (IDEA). NASA CR 3840,” tech. rep., Boeing Commercial Airplane Company, 1985.
- [284] TALBOT, J. and JAKEMAN, M., *Security risk management body of knowledge*. Wiley, 2009.
- [285] TORENBEEK, E., *Synthesis of Subsonic Airplane Design*. Delft University Press, 1976.
- [286] TZENG, Y., CHEN, C., HSU, C., CHEN, J., and CHANG, W., “Design of load shedding scheme for a cogeneration facility: a case study,” *International Journal of Electrical Power and Energy Systems*, vol. 18, no. 7, pp. 431–436, 1996.
- [287] ULLMAN, D., *The mechanical design process*. McGraw-Hill Science/Engineering/Math, 2002.
- [288] ULRICH, K. and EPPINGER, S., *Product Design and Development, 3rd edition*. McGraw-Hill Inc, New York, NY, 2004.
- [289] UPTON, E., *An Intelligent, Robust Approach to Volumetric Aircraft Sizing*. PhD thesis, Georgia Institute of Technology, 2007.
- [290] VANCHAN, V. and MACPHERSON, A., “The Recent Growth Performance of US Firms in the Industrial Design Sector: An Exploratory Study,” *Industry & Innovation*, vol. 15, no. 1, pp. 1–17, 2008.
- [291] VINCENTELLI, A. and COHN, J., “Platform-based design,” *IEEE Design e Test*, vol. 18, no. 6, pp. 23–33, 2001.
- [292] WAGENHALS, L., HAIDER, S., and LEVIS, A., “Synthesizing executable models of object oriented architectures,” pp. 85–93, 2002.
- [293] WAGENHALS, L., SHIN, I., KIM, D., and LEVIS, A., “C4ISR architectures: II. A structured analysis approach for architecture design,” *Systems Engineering*, vol. 3, no. 4, pp. 248–287, 2000.
- [294] WAGNER, M. and NORRIS, G., *Boeing 787 Dreamliner*. Zenith Press, 2009.
- [295] WEIDENHAUPT, K., POHL, K., JARKE, M., HAUMER, P., and AACHEN, T., “Scenarios in system development: Current practice,” *IEEE software*, vol. 15, no. 2, pp. 34–45, 1998.
- [296] WEILKIENS, T., *Systems engineering with SysML/UML: modeling, analysis, design*. Morgan Kaufmann, 2007.
- [297] WEIMER, J., “Electrical power technology for the more electric aircraft,” in *12th AIAA/IEEE Digital Avionics Systems Conference*, pp. 445–450, 1993.
- [298] WHITE, S. and EDWARDS, M., “A requirements taxonomy for specifying complex systems,” in *First IEEE International Conference on Engineering of Complex Computer Systems*, pp. 373–376, 1995.

- [299] WHITNEY, D., DONG, Q., JUDSON, J., and MASCOLI, G., “Introducing knowledge-based engineering into an interconnected product development process,” *MIT Center for Innovation in Product Development, White Paper*, vol. 27, 1999.
- [300] WILKINSON, P. and KELLY, T., “Functional hazard analysis for highly integrated aerospace systems,” in *Colloquium Digest-IEE*, pp. 1400–1439, 1998.
- [301] WILLIAMSON, J., “Largest Mergers and Acquisitions by Corporations in 2007,” *Federal Publications*, p. 490, 2008.
- [302] WILSON, S. and JOHNSON, P., “Empowering users in a task-based approach to design,” in *Proceedings of the 1st conference on Designing interactive systems: processes, practices, methods, & techniques*, pp. 25–31, 1995.
- [303] WIRFS-BROCK, R., WILKERSON, B., and WIENER, L., *Designing Object-Oriented Software*. Prentice Hall Inc., New Jersey, 1990.
- [304] WRIGHT, P., “What’s in a scenario?,” *ACM SIGCHI Bulletin*, vol. 24, no. 4, p. 12, 1992.
- [305] XU, Q., ONG, S., and NEE, A., “Function-based design synthesis approach to design reuse,” *Research in engineering design*, vol. 17, no. 1, pp. 27–44, 2006.
- [306] YEN, I.-L., PAUL, R., and MORI, K., “Toward integrated methods for high-assurance systems,” *Computer*, vol. 31, no. 4, p. 34, 1998.
- [307] YOUNG, R., *Effective requirements practices*. Addison-Wesley Longman Publishing Co., Boston, 2001.
- [308] ZARETSKY, E. V. and HENDRICKS, R. C., “Weibull-based design methodology for rotating aircraft engine structures,” tech. rep., NASA Glenn Research Center, 2002.
- [309] ZHU, H. and JIN, L., “Scenario analysis in an automated tool for requirements engineering,” *Requirements Engineering*, vol. 5, no. 1, pp. 2–22, 2000.
- [310] ZWICKY, F., “The morphological method of analysis and construction,” *Courant Anniversary Volume*, New York Wiley-Interscience, 1948.