



SYSTEM MANAGEMENT RECOMMENDED PRACTICE

TAHB009™

REV. A

Issued 2013-05
Revised 2019-05

Superseding TAHB0009

(R) Reliability Program Handbook

RATIONALE

With the cancellation in 1998 of MIL-STD-785B, the government has not provided a suitable reliability standard that includes reliability management practices and reliability design and testing Activities that its customers want developers to propose. To restore and enhance the ability of government contracting authorities to contract for reliability, GEIASTD0009 was developed by incorporating and aligning with best practices, without prescriptively defining the reliability tasks or Methods to be performed. This orientation made developers equal partners in deciding which reliability Methods are applicable and resulted in the release of GEIASTD0009 on November 13, 2008, and its subsequent adoption for voluntary use by the Department of Defense on August 20, 2009.

NOTE: ANSI/GEIA-STD-0009 has become GEIASTD0009. Therefore, all further references will reflect this change. On November 13, the government has not provided a suitable reliability standard that includes reliability management practices and reliability design and testing Activities that its customers want developers to propose.

FOREWORD

This Reliability Handbook, TAHB0009, is the companion implementation guide for GEIASTD0009 and provides comprehensive “how to” guidance to industry and government for the four Objectives of GEIASTD0009, which are:

- Understand customer/user requirements and constraints
- Design and redesign for reliability
- Produce reliable systems/products
- Monitor and assess user reliability

The second edition of TAHB0009 is substantially expanded and renewed on such topics as:

- Software Reliability
- Reliability Program
- FMEA

Besides support to GEIASTD0009 standard, the Handbook can be seen as a stand-alone e-publication that provides comprehensive and modern methodology for reliability practitioners.

SAE Technical Standards Board Rules provide that: “This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user.”

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2019 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: customerService@sae.org
<http://www.sae.org>

SAE WEB ADDRESS:

Full document details: SAE TAHB0009A

SAE values your input. To provide feedback
on this Technical Report, please visit
<http://standards.sae.org/TAHB0009A>

Documents
Document Sharing Hub

ACKNOWLEDGMENTS (SECOND EDITION)

This Handbook could not have been developed without the skills and contributions of a team of subject matter experts from industry, the Department of Defense, research institutes, and other government agencies.

TABLE OF CONTENTS

1.	Scope	18
1.1	Scope	18
1.2	Handbook Approach	21
1.3	Definitions	23
1.4	Handbook Activities.....	23
1.5	Handbook Methods	26
2.	ACTIVITIES.....	27
2.1	Engineering Process	27
2.1.1	Purpose	27
2.1.2	Benefits, Enablers, and Constraints.....	32
2.1.3	Timing.....	33
2.1.4	Application Guidelines.....	34
2.1.5	Applicable Methods/Submethods	38
2.2	System/Product-Level User and Environmental Life-Cycle Loads	40
2.2.1	Purpose	40
2.2.2	Benefits, Enablers, and Constraints.....	42
2.2.3	Timing.....	43
2.2.4	Application Guidelines.....	43
2.2.5	Applicable Methods/Submethods	44
2.3	Life-Cycle Loads on Assemblies, Subassemblies, Components.....	45
2.3.1	Purpose	45
2.3.2	Benefits, Enablers, and Constraints.....	48
2.3.3	Timing.....	49
2.3.4	Application Guidelines.....	50
2.3.5	Applicable Methods/Submethods	50
2.4	Closed-Loop Failure-Mode Mitigation Process	51
2.4.1	Purpose	51
2.4.2	Benefits, Enablers, and Constraints.....	56
2.4.3	Timing.....	56
2.4.4	Application Guidelines.....	56
2.4.5	Applicable Methods/Submethods	58
2.5	Identification of Failure Modes and Mechanisms.....	59
2.5.1	Purpose	59
2.5.2	Benefits, Enablers, and Constraints.....	62
2.5.3	Timing.....	62
2.5.4	Application Guideline	63
2.5.5	Applicable Methods/Submethods	64
2.6	Conceptual Reliability Model.....	65
2.6.1	Purpose	65
2.6.2	Constraints	67
2.6.3	Timing.....	68
2.6.4	Application Guidelines.....	68
2.6.5	Applicable Methods/Submethods	68
2.7	System/Product Reliability Model	70
2.7.1	Purpose	70
2.7.2	Constraints	74
2.7.3	Timing.....	74
2.7.4	Application Guidelines.....	75
2.7.5	Applicable Methods/Submethods	78
2.8	Reliability Assessment	78
2.8.1	Purpose	78



2.8.2	Benefits, Enablers, and Constraints.....	82
2.8.3	Timing.....	83
2.8.4	Application Guidelines.....	84
2.8.5	Applicable Methods/Submethods	87
2.9	Failure Definition/Scoring Criteria	88
2.9.1	Purpose	88
2.9.2	Benefits, Enablers, Constraints.....	92
2.9.3	Timing.....	94
2.9.4	Application Guidelines.....	94
2.9.5	Applicable Methods/Submethods	100
2.10	Reliability Program Plan	100
2.10.1	Purpose	100
2.10.2	Benefits, Enablers, and Constraints.....	107
2.10.3	Timing.....	109
2.10.4	Application Guidelines.....	109
2.10.5	Applicable Methods/Submethods	110
2.10.6	Citations	118
2.10.7	For More Information.....	118
2.11	Reliability Verification	119
2.11.1	Purpose	119
2.11.2	Benefits, Enablers, and Constraints.....	123
2.11.3	Timing.....	123
2.11.4	Application Guidelines.....	124
2.11.5	Applicable Methods/Submethods	126
2.12	Technical Reviews	127
2.12.1	Purpose	127
2.12.2	Benefits, Enablers, and Constraints.....	130
2.12.3	Timing.....	131
2.12.4	Application Guidelines.....	131
2.12.5	Applicable Methods/Submethods	132
3.	METHODS	133
3.1	Accelerated Testing Methods	133
3.1.1	Purpose	133
3.1.2	Benefits	133
3.1.3	Constraints	133
3.1.4	Timing.....	134
3.1.5	Application Guidelines.....	134
3.1.6	For More Information.....	137
3.2	Bayesian Techniques.....	138
3.2.1	Purpose	138
3.2.2	Benefits	138
3.2.3	Constraints	138
3.2.4	Timing.....	138
3.2.5	Application Guidelines.....	139
3.2.6	For More Information.....	140
3.3	Benchmarking (Reliability Benchmarking)	140
3.3.1	Purpose	140
3.3.2	Benefits	140
3.3.3	Constraints	140
3.3.4	Timing.....	141
3.3.5	Application Guidelines.....	141
3.3.6	For More Information.....	144
3.4	Block Diagram Development	144
3.4.1	Purpose	144
3.4.2	Benefits	145
3.4.3	Constraints	145
3.4.4	Timing.....	145
3.4.5	Application Guidelines.....	145
3.4.6	For More Information.....	147

3.5	Capability Maturity Model integration (CMMI®)	148
3.5.1	Purpose	148
3.5.2	Benefits	148
3.5.3	Constraints	149
3.5.4	Timing.....	149
3.5.5	Application Guidelines.....	149
3.5.6	For More Information.....	151
3.6	Commercial Off-the-Shelf (COTS) Assessment	151
3.6.1	Purpose	151
3.6.2	Benefits	151
3.6.3	Constraints	151
3.6.4	Timing.....	152
3.6.5	Application Guidelines.....	152
3.6.6	For More Information.....	155
3.7	Component Testing.....	155
3.7.1	Purpose	155
3.7.2	Benefits	155
3.7.3	Constraints	155
3.7.4	Timing.....	156
3.7.5	Application Guidelines.....	156
3.7.6	For More Information.....	158
3.8	Condition-Based Maintenance (CBM)	158
3.8.1	Purpose	158
3.8.2	Benefits	158
3.8.3	Constraints	159
3.8.4	Timing.....	159
3.8.5	Application Guidelines.....	159
3.8.6	For More Information.....	160
3.9	Critical Items List.....	161
3.9.1	Purpose	161
3.9.2	Benefits	161
3.9.3	Constraints	161
3.9.4	Timing.....	161
3.9.5	Application Guidelines.....	161
3.9.6	For More Information.....	164
3.10	Data Collection, Analysis, and Corrective Action System (DCACAS)	164
3.10.1	Purpose	164
3.10.2	Benefits	164
3.10.3	Constraints	164
3.10.4	Timing.....	164
3.10.5	Application Guidelines.....	164
3.10.6	For More Information.....	166
3.11	Data Management Technique (PREDICT)	166
3.11.1	Purpose	166
3.11.2	Benefits	166
3.11.3	Constraints	167
3.11.4	Timing.....	167
3.11.5	Application Guidelines.....	167
3.11.6	For More Information.....	168
3.12	Design for Manufacturing and Design for Assembly.....	168
3.12.1	Purpose	168
3.12.2	Benefits	169
3.12.3	Constraints	169
3.12.4	Timing.....	169
3.12.5	Application Guide	169
3.12.6	For More Information.....	170
3.13	Design of Experiments (DOE) - classical and Taguchi	171
3.13.1	Purpose	171
3.13.2	Benefits	171
3.13.3	Constraints	171

3.13.4	Timing.....	171
3.13.5	Application Guideline	171
3.13.6	For More Information.....	180
3.14	Design Guidelines for Reliable Surface Mount Technology Printed Board Assemblies.....	181
3.14.1	Purpose	181
3.14.2	Benefits	181
3.14.3	Constraints	181
3.14.4	Timing.....	181
3.14.5	Application Guidelines.....	182
3.14.6	For More Information.....	183
3.15	Design Review	184
3.15.1	Purpose	184
3.15.2	Benefits	184
3.15.3	Constraints	184
3.15.4	Timing.....	184
3.15.5	Application Guidelines.....	184
3.15.6	For More Information.....	188
3.16	Durability Analysis.....	188
3.16.1	Purpose	188
3.16.2	Benefits	188
3.16.3	Constraints	188
3.16.4	Timing.....	189
3.16.5	Application Guidelines.....	189
3.16.6	For More Information.....	191
3.17	Durability Verification Test	192
3.17.1	Purpose	192
3.17.2	Benefits	192
3.17.3	Constraints	192
3.17.4	Timing.....	192
3.17.5	Application Guidelines.....	192
3.17.6	For More Information.....	192
3.18	Environmental and Product Usage Profile/Mission Profile	193
3.18.1	Purpose	193
3.18.2	Benefits	193
3.18.3	Constraints	193
3.18.4	Timing.....	193
3.18.5	Application Guidelines.....	194
3.18.6	For More Information.....	200
3.19	Environmental Qualification Test	201
3.19.1	Purpose	201
3.19.2	Benefits	202
3.19.3	Constraints	202
3.19.4	Timing.....	202
3.19.5	Application Guidelines.....	202
3.19.6	For More Information.....	203
3.20	Environmental Stress Screening/Highly Accelerated Stress Screening.....	203
3.20.1	Purpose	203
3.20.2	Benefits	204
3.20.3	Constraints	204
3.20.4	Timing.....	205
3.20.5	Application Guidelines.....	205
3.20.6	For More Information.....	211
3.21	Error/Mistake Proofing (Poka-Yoke)	212
3.21.1	Purpose	212
3.21.2	Benefits	212
3.21.3	Constraints	212
3.21.4	Timing.....	212
3.21.5	Application Guidelines.....	212
3.21.6	For More Information.....	212
3.22	Failure Mode and Effects Analysis/Failure Mode, Effects, and Criticality Analysis.....	215

3.22.1	Purpose	215
3.22.2	Benefits	218
3.22.3	Constraints	220
3.22.4	Timing.....	220
3.22.5	Application Guidelines.....	221
3.22.6	For More Information.....	225
3.23	Failure Reporting, Analysis, and Corrective Action System (FRACAS)	225
3.23.1	Purpose	225
3.23.2	Benefits	225
3.23.3	Constraints	226
3.23.4	Timing.....	226
3.23.5	Application Guidelines.....	226
3.23.6	For More Information.....	228
3.24	Fault Insertion Testing.....	228
3.24.1	Purpose	228
3.24.2	Benefits	228
3.24.3	Constraints	229
3.24.4	Timing.....	229
3.24.5	Application Guidelines.....	229
3.24.6	For More Information.....	230
3.25	Fault Tree Analysis (FTA)	230
3.25.1	Purpose	230
3.25.2	Benefits	231
3.25.3	Constraints	231
3.25.4	Timing.....	231
3.25.5	Application Guidelines.....	231
3.25.6	For More Information.....	235
3.26	Focus Groups.....	236
3.26.1	Purpose	236
3.26.2	Benefits	236
3.26.3	Constraints	236
3.26.4	Timing.....	236
3.26.5	Application Guidelines.....	236
3.26.6	For More Information.....	237
3.27	General RAM Design Considerations	237
3.27.1	Purpose	237
3.27.2	Benefits	240
3.27.3	Constraints	241
3.27.4	Timing.....	242
3.27.5	Application Guidelines.....	242
3.27.6	For More Information.....	249
3.28	Ishikawa Diagram.....	249
3.28.1	Purpose	249
3.28.2	Benefits	249
3.28.3	Constraints	249
3.28.4	Timing.....	249
3.28.5	Application Guidelines.....	250
3.28.6	For More Information.....	250
3.29	Maintainability Demonstration Test.....	250
3.29.1	Purpose	250
3.29.2	Benefits	251
3.29.3	Constraints	251
3.29.4	Timing.....	251
3.29.5	Application Guidelines.....	251
3.29.6	For More Information.....	253
3.30	Human-in-the-Loop Testing (formerly Man-in-the-Loop Testing)	254
3.30.1	Purpose	254
3.30.2	Benefits	254
3.30.3	Constraints	254
3.30.4	Timing.....	254

3.30.5	Application Guidelines.....	254
3.30.6	For More Information.....	255
3.31	Markov Modeling/Analysis	255
3.31.1	Purpose	255
3.31.2	Benefits	255
3.31.3	Constraints	256
3.31.4	Timing.....	256
3.31.5	Application Guidelines.....	256
3.31.6	For More Information.....	257
3.32	Measurement Information Models	257
3.32.1	Purpose	257
3.32.2	Timing.....	257
3.33	Measurement Systems Analysis	258
3.33.1	Purpose	258
3.33.2	Benefits	258
3.33.3	Constraints	258
3.33.4	Timing.....	258
3.33.5	Application Guidelines.....	259
3.33.6	References	259
3.34	Mission Profile Definition	259
3.34.1	Purpose	259
3.34.2	Benefits	259
3.34.3	Constraints	260
3.34.4	Timing.....	260
3.34.5	Application Guidelines.....	260
3.34.6	For More Information.....	262
3.35	One-Shot Device Testing	262
3.35.1	Purpose	262
3.35.2	Benefits	262
3.35.3	Constraints	262
3.35.4	Timing.....	262
3.35.5	Application Guidelines.....	262
3.35.6	For More Information.....	263
3.36	Pareto Analysis	263
3.36.1	Purpose	263
3.36.2	Benefits	263
3.36.3	Constraints	264
3.36.4	Timing.....	264
3.36.5	Application Guidelines.....	264
3.36.6	For More Information.....	266
3.37	Part Derating	266
3.37.1	Purpose	266
3.37.2	Benefits	267
3.37.3	Constraints	267
3.37.4	Timing.....	267
3.37.5	Application Guidelines.....	267
3.37.6	For More Information.....	270
3.38	Parts Obsolescence	270
3.38.1	Purpose	270
3.38.2	Benefits	271
3.38.3	Constraints	271
3.38.4	Timing.....	271
3.38.5	Application Guidelines.....	271
3.38.6	For More Information.....	274
3.39	Parts, Materials, Process Review	275
3.39.1	Purpose	275
3.39.2	Benefits	275
3.39.3	Constraints	275
3.39.4	Timing.....	275
3.39.5	Application Guidelines.....	275

3.39.6	For More Information.....	278
3.40	Physics of Failure (PoF).....	278
3.40.1	Purpose	278
3.40.2	Benefits	279
3.40.3	Constraints	279
3.40.4	Timing.....	279
3.40.5	Application Guidelines.....	279
3.40.6	For More Information.....	282
3.41	Practical Software and Systems Measurement Process	282
3.41.1	Purpose	282
3.41.2	Benefits	282
3.41.3	Constraints	282
3.41.4	Timing.....	283
3.41.5	Application Guidelines.....	283
3.41.6	For More Information.....	284
3.42	Probabilistic Design - Stress and Strength Interference Method (SSI).....	285
3.42.1	Purpose	285
3.42.2	Benefits	285
3.42.3	Constraints	285
3.42.4	Timing.....	285
3.42.5	Application Guidelines.....	285
3.42.6	For More Information.....	286
3.43	Process Failure Modes Effects Analysis/Producibility Analysis.....	286
3.43.1	Purpose	286
3.43.2	Timing.....	287
3.44	Production Process Capability Study.....	287
3.44.1	Purpose	287
3.44.2	Benefits	287
3.44.3	Constraints	287
3.44.4	Timing.....	288
3.44.5	Application Guidelines.....	288
3.44.6	For More Information.....	289
3.45	Program Parts Selection List	289
3.45.1	Purpose	289
3.45.2	Benefits	289
3.45.3	Constraints	289
3.45.4	Timing.....	290
3.45.5	Application Guidelines.....	290
3.45.6	For More Information.....	291
3.46	Pugh Selection	291
3.46.1	Purpose	291
3.46.2	Benefits	292
3.46.3	Constraints	292
3.46.4	Timing.....	292
3.46.5	Application Guidelines.....	292
3.46.6	For More Information.....	295
3.47	Quality and Quality Control	295
3.47.1	Purpose	295
3.47.2	Benefits	295
3.47.3	Constraints	295
3.47.4	Timing.....	296
3.47.5	Application Guidelines.....	296
3.47.6	For More Information.....	297
3.48	Quality Function Deployment.....	297
3.48.1	Purpose	297
3.48.2	Benefits	298
3.48.3	Constraints	298
3.48.4	Timing.....	298
3.48.5	Application Guidelines.....	298
3.48.6	For More Information.....	299

3.49	Quality Loss Function.....	299
3.49.1	Purpose	299
3.49.2	Benefits	299
3.49.3	Constraints	299
3.49.4	Timing.....	299
3.49.5	Application Guidelines.....	299
3.49.6	For More Information.....	304
3.50	RAM Design Guide	304
3.50.1	Purpose	304
3.50.2	Benefits	304
3.50.3	Constraints	305
3.50.4	Timing.....	305
3.50.5	Application Guidelines.....	305
3.50.6	For More Information.....	309
3.51	Regression Analysis/Correlation/Prediction Modeling	309
3.51.1	Purpose	309
3.51.2	Benefits	309
3.51.3	Constraints	309
3.51.4	Timing.....	309
3.51.5	Application Guidelines.....	309
3.51.6	For More Information.....	312
3.52	Reliability Allocation	312
3.52.1	Purpose	312
3.52.2	Benefits	312
3.52.3	Constraints	312
3.52.4	Timing.....	312
3.52.5	Application Guidelines.....	313
3.52.6	For More Information.....	314
3.53	Reliability Assessment	314
3.53.1	Purpose	314
3.53.2	Benefits	315
3.53.3	Constraints	315
3.53.4	Timing.....	316
3.53.5	Application Guidelines.....	316
3.53.6	For More Information.....	322
3.54	Reliability Benchmarking.....	322
3.54.1	Cross Reference	322
3.54.2	Timing.....	323
3.55	Reliability Case	323
3.55.1	Purpose	323
3.55.2	Benefits	323
3.55.3	Constraints	323
3.55.4	Timing.....	325
3.55.5	Application Guidelines.....	325
3.55.6	For More Information.....	330
3.56	Reliability-Centered Maintenance	330
3.56.1	Purpose	330
3.56.2	Benefits	330
3.56.3	Constraints	330
3.56.4	Timing.....	330
3.56.5	Application Guidelines.....	331
3.56.6	For More Information.....	333
3.57	Reliability Demonstration Testing	333
3.57.1	Purpose	333
3.57.2	Benefits	334
3.57.3	Constraints	334
3.57.4	Timing.....	334
3.57.5	Application Guidelines.....	334
3.57.6	For More Information.....	336
3.58	Reliability Growth Modeling and Testing.....	337

3.58.1	Purpose	337
3.58.2	Benefits	337
3.58.3	Constraints	337
3.58.4	Timing.....	337
3.58.5	Application Guidelines.....	338
3.58.6	For More Information.....	345
3.59	Reliability Growth Testing and Test-Analyze-Fix-Test (TAFT)	345
3.59.1	Purpose	345
3.59.2	Timing.....	345
3.60	Reliability Modeling and Prediction (Operating and Non-Operating).....	345
3.60.1	Purpose	345
3.60.2	Benefits	345
3.60.3	Constraints	346
3.60.4	Timing.....	346
3.60.5	Application Guidelines.....	346
3.60.6	For More Information.....	353
3.61	Reliability Testing for Engineering Development, Qualification, and Testing	353
3.61.1	Purpose	353
3.61.2	Timing.....	353
3.62	Repair Strategy	353
3.62.1	Purpose	353
3.62.2	Benefits	353
3.62.3	Constraints	354
3.62.4	Timing.....	354
3.62.5	Application Guidelines.....	354
3.62.6	For More Information.....	356
3.63	Repairable Systems Modeling/Analysis	357
3.63.1	Purpose	357
3.63.2	Benefits	357
3.63.3	Constraints	357
3.63.4	Timing.....	357
3.63.5	Application Guidelines.....	357
3.63.6	For More Information.....	360
3.64	Requirements and Architecture Development	361
3.64.1	Purpose	361
3.64.2	Benefits	361
3.64.3	Constraints	361
3.64.4	Timing.....	362
3.64.5	Application Guidelines.....	363
3.64.6	For More Information.....	363
3.65	Risk Assessment.....	364
3.65.1	Purpose	364
3.65.2	Benefits	364
3.65.3	Constraints	364
3.65.4	Timing.....	364
3.65.5	Application Guidelines.....	364
3.65.6	For More Information.....	367
3.66	Root Cause Analysis	367
3.66.1	Purpose	367
3.66.2	Benefits	367
3.66.3	Constraints	367
3.66.4	Timing.....	368
3.66.5	Application Guidelines.....	368
3.66.6	For More Information.....	369
3.67	RQT and Acceptance Testing	370
3.67.1	Cross Reference	370
3.67.2	Timing.....	370
3.68	Sampling Procedures	370
3.68.1	Purpose	370
3.68.2	Benefits	370



3.68.3	Constraints	370
3.68.4	Timing.....	370
3.68.5	Application Guidelines.....	371
3.68.6	For More Information.....	372
3.69	Simulation (Markov Analysis).....	372
3.69.1	Cross Reference	372
3.69.2	Timing.....	372
3.70	Simulation (Warranty)	373
3.70.1	Purpose	373
3.70.2	Benefits	373
3.70.3	Constraints	373
3.70.4	Timing.....	373
3.70.5	Application Guidelines.....	374
3.70.6	For More Information.....	375
3.71	Sneak Circuit Analysis/Sneak Path Analysis	375
3.71.1	Purpose	375
3.71.2	Benefits	376
3.71.3	Constraints	376
3.71.4	Timing.....	376
3.71.5	Application Guidelines.....	376
3.71.6	For More Information.....	380
3.72	Software Reliability Growth Models	381
3.72.1	Purpose	382
3.72.2	Benefits	382
3.72.3	Constraints	382
3.72.4	Timing.....	382
3.72.5	Application Guidelines.....	382
3.72.6	For More Information.....	384
3.73	Sparing Models Assessment Methods.....	385
3.73.1	Purpose	385
3.73.2	Benefits	385
3.73.3	Constraints	385
3.73.4	Timing.....	385
3.73.5	Application Guidelines.....	385
3.73.6	For More Information.....	387
3.74	Specification Generation (Specifying/Establishing RAM Requirements).....	387
3.74.1	Purpose	387
3.74.2	Benefits	388
3.74.3	Constraints	388
3.74.4	Timing.....	389
3.74.5	Application Guidelines for Requirements Generation	389
3.74.6	For More Information.....	394
3.75	Statistical Process Control	394
3.75.1	Purpose	394
3.75.2	Benefits	395
3.75.3	Constraints	395
3.75.4	Timing.....	395
3.75.5	Application Guideline	395
3.75.6	For More Information.....	399
3.76	Surveys/Market Analysis.....	399
3.76.1	Purpose	399
3.76.2	Benefits	399
3.76.3	Constraints	399
3.76.4	Timing.....	399
3.76.5	Application Guidelines.....	400
3.76.6	For More Information.....	400
3.77	Testability Analysis (BIT/Diagnostics/Prognostics).....	400
3.77.1	Purpose	400
3.77.2	Benefits	400
3.77.3	Constraints	401

3.77.4	Timing.....	401
3.77.5	Application Guidelines.....	401
3.77.6	For More Information.....	404
3.78	Warranty Tracking and Information Collection.....	404
3.78.1	Purpose.....	404
3.78.2	Benefits.....	405
3.78.3	Constraints.....	405
3.78.4	Timing.....	405
3.78.5	Application Guidelines.....	405
3.78.6	For More Information.....	407
3.79	Worst-Case Analysis.....	407
3.79.1	Purpose.....	407
3.79.2	Benefits.....	408
3.79.3	Constraints.....	409
3.79.4	Timing.....	409
3.79.5	Application Guidelines.....	409
3.79.6	For More Information.....	411
4.	NOTES.....	412
4.1	Revision Indicator.....	412

ANNEX A	LIST OF REFERENCES (INFORMATIVE).....	413
---------	---------------------------------------	-----

ANNEX B	SYMBOLS AND ABBREVIATED TERMS (INFORMATIVE).....	423
---------	--	-----

Figure 1	Example Objectives and Activities of a defense industry program.....	19
Figure 2	GEIASTD0009 and TAHB0009 traceability.....	20
Figure 3	TAHB0009 Handbook structure and content.....	22
Figure 4	Example of IDEF0 diagram.....	25
Figure 5	IDEF0 for the engineering process modeling diagram.....	28
Figure 6	Systems engineering V-shaped model.....	35
Figure 7	Elements of the engineering process with inputs/outputs and interfaces.....	35
Figure 8	System/product-level user and environmental life-cycle loads.....	41
Figure 9	Life-cycle loads on assemblies, components, and parts.....	47
Figure 10	Integrated growth.....	52
Figure 11	Closed-loop failure-mode mitigation model.....	54
Figure 12	Identify and characterize failure modes and mechanisms model.....	60
Figure 13	Conceptual system/product reliability model.....	66
Figure 14	System/product reliability model.....	71
Figure 15	Principal steps required for evaluation of system/product effectiveness.....	77
Figure 16	Reliability assessment model.....	79
Figure 17	Reliability assessment from developing requirements through use of a system.....	83
Figure 18	System/product failure causes and potential assessment techniques.....	84
Figure 19	Failure definition/scoring criteria model.....	91
Figure 20	Scoring process diagram.....	97
Figure 21	GEIASTD0009 reliability program.....	101
Figure 22	Reliability program plan model.....	103
Figure 23	Reliability equation ²	106
Figure 24	List of RPP Handbook methods.....	107
Figure 25	Roadmap to achieving reliability objectives ²	112
Figure 26	Process to achieve high reliability.....	113
Figure 27	Reliability verification process model.....	120
Figure 28	Technical review process model.....	128
Figure 29	Relative importance of reliability tasks.....	144
Figure 30	Reliability block diagram.....	146
Figure 31	RBD in a series configuration.....	146
Figure 32	RBD in a parallel configuration.....	146
Figure 33	RBD in standby configuration.....	147
Figure 34	RBD for a simple complex structure.....	147
Figure 35	The DCACAS process.....	165



Figure 36	SE objectives	169
Figure 37	DOE elements	173
Figure 38	Coverage of operational envelope	178
Figure 39	Depiction of decision risks.....	179
Figure 40	Example power table.....	179
Figure 41	Comparison of confidence intervals (a)	180
Figure 42	Comparison of confidence intervals (b)	180
Figure 43	Potential stages for design reviews	185
Figure 44	Approach to formal design reviews.....	186
Figure 45	Environmental tailoring process.....	194
Figure 46	Generalized O&M life-cycle histories for military hardware (a).....	195
Figure 47	Generalized O&M life-cycle histories for military hardware (b).....	196
Figure 48	Environmental test chambers	201
Figure 49	Typical ESS process.....	205
Figure 50	Issues to consider for effective reliability screening.....	208
Figure 51	Stress screening and variables relationships	208
Figure 52	Effectiveness of environmental screens (relative strength)	211
Figure 53	Poka-Yoke process steps	213
Figure 54	Comparison table defining different types of reliability assessment techniques.....	216
Figure 55	DFMEA-FMECA-PFMEA-DRBFM decision table	217
Figure 56	Timing of a DFMEA/FMECA/DRBFM/PFMEA.....	221
Figure 57	DFMEA/FMECA/DRBFM/PFMEA and systems engineering connection.....	223
Figure 58	SAE J1739 DFMEA format	223
Figure 59	FMECA format MIL-STD-1629A (section 101 - FMEA).....	223
Figure 60	FMECA format MIL-STD-1629A (sections 101 and 102 - FMEA and CA).....	224
Figure 61	DRBFM format per SAE J2886 DRBFM recommended practice	224
Figure 62	SAE J1739 PFMEA format	224
Figure 63	Comparison table of failure analysis formats.....	224
Figure 64	Generic closed-loop FRACAS	227
Figure 65	Typical fault tree representation.....	232
Figure 66	Sub-level development of the fault tree	234
Figure 67	General RAM design considerations	238
Figure 68	Reliability perspective	239
Figure 69	Applying general RAM guidelines	243
Figure 70	Ishikawa diagram	250
Figure 71	Representation of a Markov model state diagram	256
Figure 72	Typical operational sequence for a military airborne weapons system	260
Figure 73	Service use events in the logistic and operational cycles.....	261
Figure 74	Example of a Pareto chart	265
Figure 75	Example of Pareto stratification	265
Figure 76	OM team structure	273
Figure 77	Mechanical PoF overview	281
Figure 78	PSM measurement process model.....	284
Figure 79	Stress and strength probability density	286
Figure 80	Pugh matrix	294
Figure 81	Detailed Pugh.....	294
Figure 82	The QFD House of Quality.....	298
Figure 83	Loss variance attributes	300
Figure 84	Nominal characteristic.....	302
Figure 85	Smaller-the-Better characteristic.....	303
Figure 86	Larger-the-Better characteristic	303
Figure 87	Systems requirements analysis	306
Figure 88	Fitting a straight line to a set of data points	310
Figure 89	Correlations from scatter plots	311
Figure 90	Relationship of the reliability program plan to the reliability case	324
Figure 91	Reliability case process.....	325
Figure 92	Planned growth and assessments	326
Figure 93	Comparison of exponential and Duane models.....	326
Figure 94	Reliability growth planning curve	326
Figure 95	Extrapolated and projected reliabilities	329

Figure 96	Risk assessment	329
Figure 97	The steps in an RCM approach	332
Figure 98	Determination of optimum PM point based on RCM analysis	333
Figure 99	Defining an RDT/RQT test	335
Figure 100	Reliability growth process	341
Figure 101	General modeling approach	348
Figure 102	Breakdown of potential reliability modeling purposes	349
Figure 103	Breakdown of reliability assessment options	349
Figure 104	Software reliability prediction process	352
Figure 105	DoD program milestones (5000.02)	362
Figure 106	Typical award fee structure	374
Figure 107	Product performance failures	390
Figure 108	Profit motivation for a reliability-based warranty	406
Figure 109	Worst-case analysis	408

Table 1	Handbook definitions	23
Table 2	GEIASTD0009 reliability activities	24
Table 3	Timing of applicable activity	26
Table 4	Timing of applicable method	26
Table 5	SIPOC for the engineering process model	29
Table 6	Timing of activity	33
Table 7	System product life-cycle loads	42
Table 8	Timing of activity	43
Table 9	Life-cycle loads on assemblies, components, and parts	48
Table 10	Timing of activity	49
Table 11	Closed-loop failure-mode mitigation	55
Table 12	Timing of activity	56
Table 13	Identify and characterize failure modes and mechanisms	61
Table 14	Timing of activity	62
Table 15	Conceptual system/product reliability model	67
Table 16	Timing of activity	68
Table 17	System/product reliability model	72
Table 18	Timing of activity	74
Table 19	Reliability assessment	80
Table 20	Timing of activity	83
Table 21	Failure definition/scoring criteria	92
Table 22	Timing of activity	94
Table 23	Product (mission) reliability and series (logistic) reliability characteristics	94
Table 24	Typical failure categories	95
Table 25	Example failure classifications	96
Table 26	Example relationship matrix	99
Table 27	Reliability program plan	104
Table 28	Timing of activity	109
Table 29	Reliability verification process model	121
Table 30	Reliability verification timing	123
Table 31	Verification techniques	124
Table 32	Technical review process	129
Table 33	Technical review benefits	130
Table 34	Timing of activity	131
Table 35	Timing of method	134
Table 36	Failure mechanisms and acceleration agents	137
Table 37	Timing of method	138
Table 38	Prior distributions from conjugates	140
Table 39	Timing of method	141
Table 40	Most important reliability tasks according to the RIAC benchmarking study survey	143
Table 41	Timing of method	145
Table 42	Timing of method	149
Table 43	CMMI® comparison of continuous to staged representation	149
Table 44	Staged representation maturity level	149
Table 45	CMMI® process areas	150



Table 46	Timing of method	152
Table 47	Advantages and disadvantage of using COTS/NDI.....	153
Table 48	Comparison of reliability activities for new development and for COTS.....	154
Table 49	Potential impacts of modified COTS/NDI hardware/software	154
Table 50	Timing of method	156
Table 51	Screening/test requirements versus maturity	157
Table 52	Relative merits of component screen/test sources	157
Table 53	Commercial and military component testing documentation	158
Table 54	Timing of method	159
Table 55	Timing of method	161
Table 56	Critical item identification techniques	162
Table 57	Critical item control checklist.....	162
Table 58	Countering criticality.....	163
Table 59	Timing of method	164
Table 60	Timing of method	167
Table 61	Timing of method	169
Table 62	Timing of method	171
Table 63	Comparison of classical and Taguchi experiments	172
Table 64	DOE terms	173
Table 65	Timing of method	181
Table 66	Timing of method	184
Table 67	Design review membership.....	186
Table 68	Concept/planning phase reliability review checklist.....	187
Table 69	Design/development phase reliability review checklist.....	187
Table 70	Timing of method	189
Table 71	Basic approach to durability analysis	190
Table 72	Timing of method	192
Table 73	Timing of method	193
Table 74	Various environmental pairs	197
Table 75	Environmental effects.....	199
Table 76	Timing of method	202
Table 77	Timing of method	205
Table 78	Baseline temperature cycling regimen for organizations lacking ESS experience.....	206
Table 79	Baseline random vibration regimen for organizations lacking ESS experience	207
Table 80	Guidelines for performing reliability screening (placement).....	207
Table 81	Discrepancies between actual versus planned defect densities	209
Table 82	Guidelines for performing reliability screening (selection)	210
Table 83	Screening environments versus typical failure mechanics	211
Table 84	Timing of method	212
Table 85	Types of Poka-Yoke approach.....	214
Table 86	Timing of method	220
Table 87	Timing of method	226
Table 88	Timing of method	229
Table 89	Timing of method	231
Table 90	Typical fault tree symbols.....	234
Table 91	Considerations for performing FTA or FMECA/FMEA	235
Table 92	Timing of method	236
Table 93	Timing of method	242
Table 94	Expected operating environment RAM guidelines	243
Table 95	Piece part RAM guidelines.....	244
Table 96	Circuit card assemblies RAM guidelines.....	246
Table 97	Component/subassembly RAM guidelines	247
Table 98	Subsystem/assembly RAM guidelines.....	248
Table 99	System/product RAM guidelines	248
Table 100	Timing of method	249
Table 101	Timing of method	251
Table 102	Timing of method	254
Table 103	Timing of method	256
Table 104	Timing of method	258
Table 105	Timing of method	258

Table 106	Timing of method	260
Table 107	Timing of method	262
Table 108	Timing of method	264
Table 109	Timing of method	267
Table 110	Available derating documents	267
Table 111	Example of electrical/electronic part derating levels	269
Table 112	Timing of method	271
Table 113	Timing of method	275
Table 114	Timing of method	279
Table 115	Timing of method	283
Table 116	Timing of method	285
Table 117	Timing of method	287
Table 118	Timing of method	288
Table 119	Timing of method	290
Table 120	Summary of PPL approach options	291
Table 121	Timing of method	292
Table 122	Timing of method	296
Table 123	Timing of method	298
Table 124	Timing of method	299
Table 125	Timing of method	305
Table 126	Timing of method	309
Table 127	Timing of method	312
Table 128	Reliability assessment purposes	314
Table 129	Timing of method	316
Table 130	Program phase versus reliability assessment purpose	316
Table 131	Summary of reliability assessment options	317
Table 132	Identification of appropriate reliability assessment approaches based on the purpose	320
Table 133	Application guidance for specific reliability assessment methods	321
Table 134	Potential reliability assessment tasks tailored by system/product classification	322
Table 135	Timing of method	323
Table 136	Timing of method	325
Table 137	Timing of method	330
Table 138	Timing of method	334
Table 139	RDT/RQT test plan parameters	336
Table 140	Timing of method	337
Table 141	Differences between RGT and RDT/RQT	338
Table 142	Basic activity options for an effective reliability growth management strategy	342
Table 143	Timing of method	345
Table 144	Timing of method	346
Table 145	Software reliability prediction models	352
Table 146	Timing of method	353
Table 147	Timing of method	354
Table 148	Repair strategy characteristics	355
Table 149	Timing of method	357
Table 150	Redundancy equations for calculating reliability	359
Table 151	Effective failure rate equation approximations	360
Table 152	Timing of method	362
Table 153	Timing of method	364
Table 154	Example risk acceptance matrix	366
Table 155	Timing of method	368
Table 156	Timing of method	370
Table 157	Timing of method	370
Table 158	Timing of method	372
Table 159	Timing of method	373
Table 160	Timing of method	376
Table 161	Checklist for initiating an integrated sneak analysis	377
Table 162	Checklist for monitoring an integrated sneak analysis	377
Table 163	Checklist for evaluating an integrated sneak analysis	378
Table 164	Reasons why software sneaks occur	379
Table 165	General categories of software sneak paths	380



Table 166	Summary of software reliability growth models.....	381
Table 167	Timing of method	382
Table 168	Summary of software reliability models	383
Table 169	Timing of method	385
Table 170	Timing of method	389
Table 171	Activities related to the development of goals and requirements	392
Table 172	RAM parameters	394
Table 173	Timing of method	395
Table 174	Measures of quality.....	397
Table 175a	Process control chart	398
Table 175b	Control chart constants	398
Table 176	Comparison of SPC and DOE	399
Table 177	Timing of method	399
Table 178	Timing of method	401
Table 179	Testability design principles	402
Table 180	Typical testability values	404
Table 181	Timing of method	405
Table 182	Summary of commercial and government warranties	407
Table 183	Timing of method	409

1. SCOPE

1.1 Scope

This Handbook provides “how to” guidance to industry and government for the reliability Activities and Methods contained in GEIASTD0009 for developing reliable products and systems, successfully demonstrating them during test and evaluation, and sustaining them throughout the system/product life cycle.

GEIASTD0009 requires the developers and customer/users working as a team to plan and implement a reliability program that provides systems/products that satisfy the user's requirements and expectations using a systems engineering approach. The four Objectives of GEIASTD0009 are listed below:

- **Objective 1:** Understand customer/user requirements and constraints. The team (developer, customer, and user) includes the Activities necessary to ensure that the user's requirements and product needs are fully understood and defined, so that a comprehensive design specification and Reliability program plan are generated.
- **Objective 2:** Design and redesign for reliability. The developer implements a set of engineering Activities so that the resulting system/product satisfies the customer's documented requirements and needs.
- **Objective 3:** Produce reliable systems/products. The developer performs the Activities that assure the customer that the reliability requirements and product needs have been satisfied.
- **Objective 4:** Monitor and assess user reliability. The team establishes a closed-loop feedback Method for continuous monitoring of reliability trends and incorporation of recommended improvements (corrective actions).

GEIASTD0009 and this Handbook define a systematic approach to engineering a system/product, incorporating best practices that have evolved considerably in recent years.

[Figure 1](#) shows the four Objectives, defined in 1.4.2 of GEIASTD0009, and is a defense industry example of the interaction of the Objectives, supporting Activities and Methods, and strategies for reliable system design in the acquisition cycle.

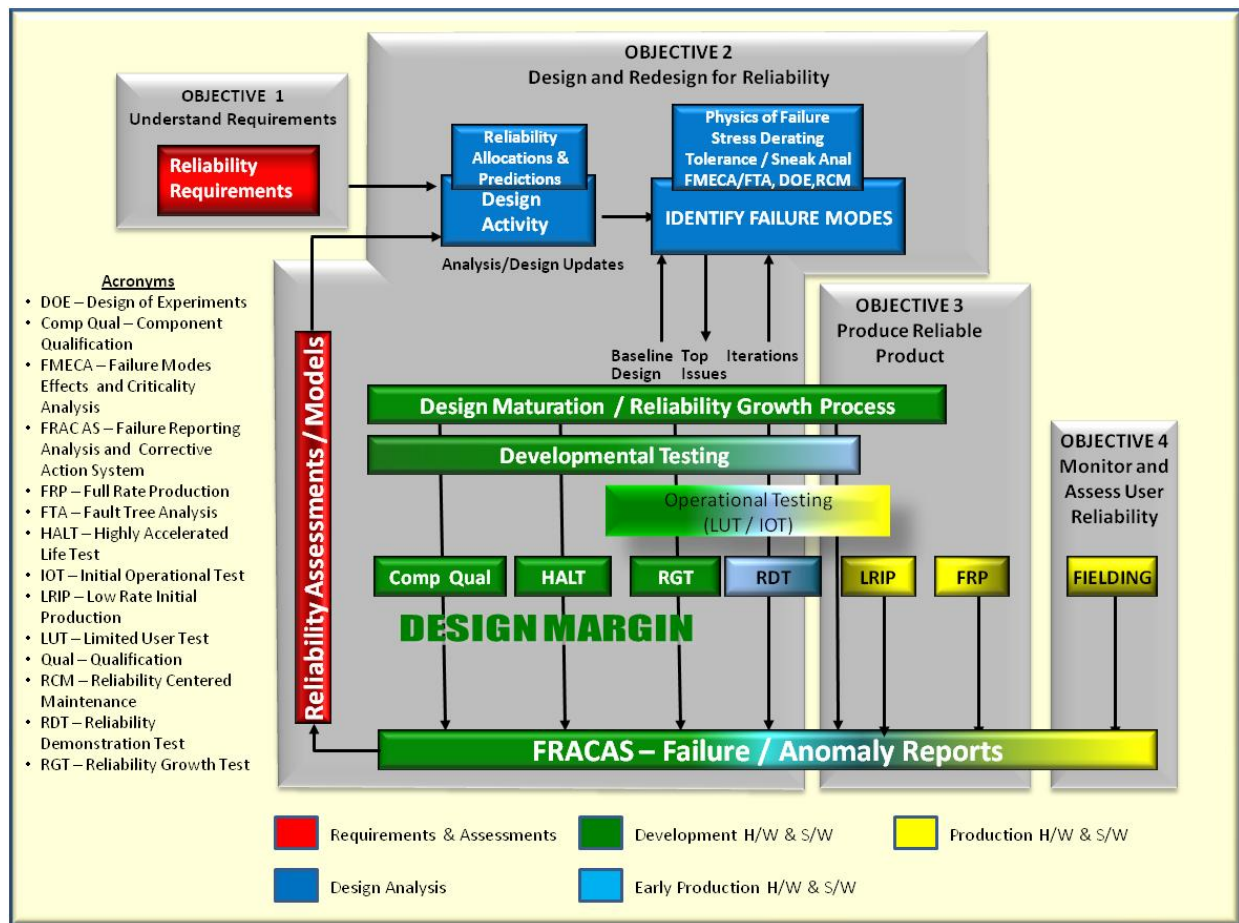


Figure 1 - Example Objectives and Activities of a defense industry program

The four Objectives in GEIASTD0009 have Activities associated with them. These Activities are further developed in this Handbook as shown in [Figure 2](#). The four Objectives of the standard are shown on the left and the derived Activities in the Handbook are on the right.

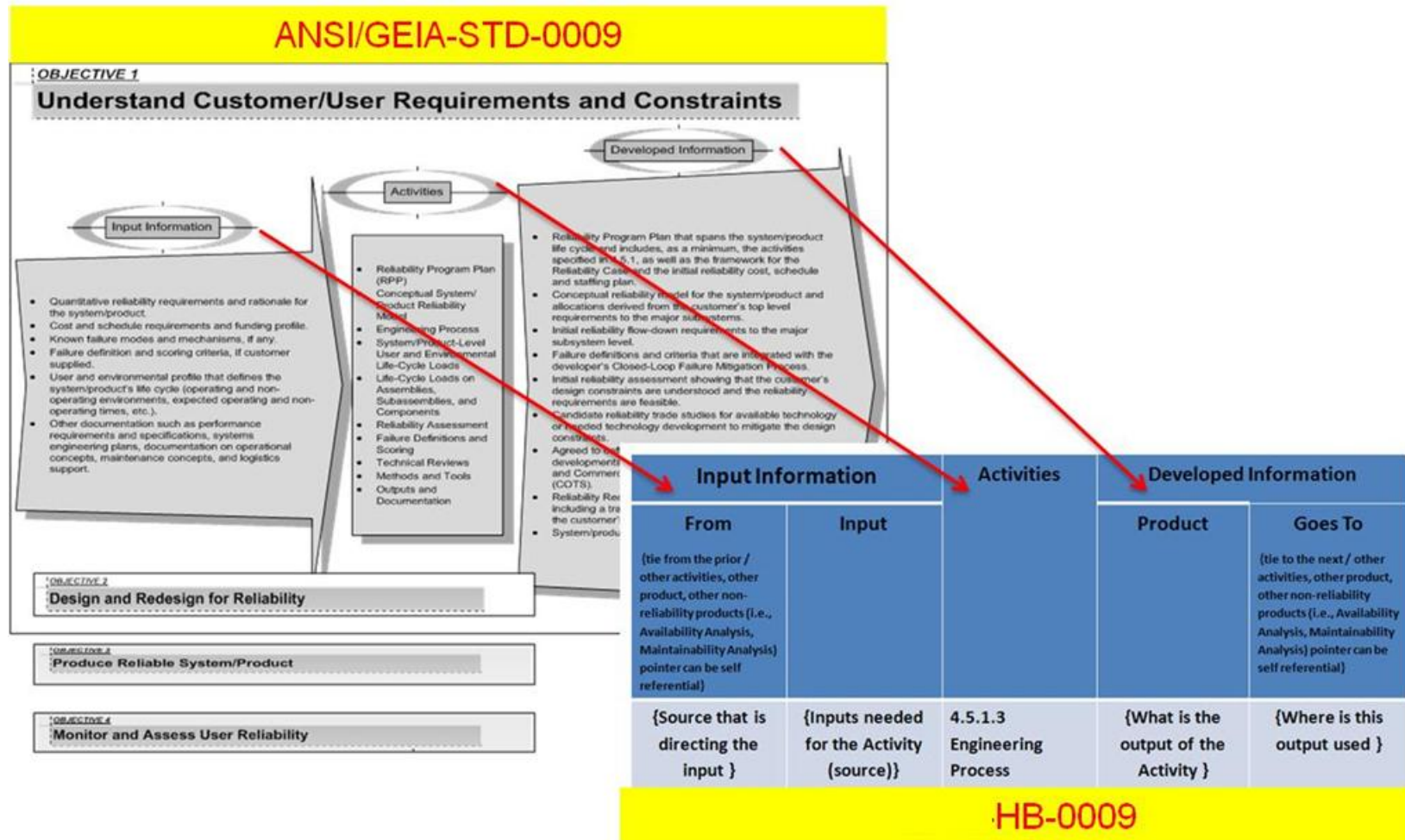


Figure 2 - GEIASTD0009 and TAHB0009 traceability

1.2 Handbook Approach

This Handbook describes each Reliability Activity by stating its purpose, describing the benefits, enablers, and constraints, identifying the timing for the Activity, and providing application guidelines and lessons learned, along with the applicable Methods/Submethods and references.

[Figure 3](#) depicts the Activities taken from GEIASTD0009 (1) as they are translated in the table of contents of the TAHB0009 (2). Within the Handbook, each Activity is described using an integration Definition for Function Modeling (IDEF0) model (for more information, refer to FIPS Publication 183, NIST). The IDEF0 is a functional modeling Method designed to model the decisions, actions, and Activities of a process, an organization, or a system (3), which is, in turn, related to the Activity, input-process-output (IPO). The IPO was then expanded to define the suppliers, inputs, process, outputs, and customers (SIPOC) for each Activity. SIPOC is a Six Sigma tool, and it is completed most easily by starting from the right (customers) and working towards the left (4). The IDEF0 traces the Activity through each of the four Objectives, as applicable, by defining each functional block's inputs, outputs, enablers, and constraints. The SIPOC matrix complements the IDEF0 by adding the supplier for each input and customer for each output of the respective functional block process in the IDEF0. The SIPOC matrix is an expansion of the elements of the IDEF0 diagram but is not necessarily meant to have a one-to-one correspondence. The application guideline (5) provides in-depth detail of the Activity as supported by the SIPOC. This detail may be a combination of graphics and/or text. At the end of each Activity there is a bulleted list of Methods to support the Activity (6). Each of the Methods listed in Annex A of GEIASTD0009 is described in detail in [Section 3](#) of TAHB0009 (7).



1.3 Definitions

For the purposes of TAHB0009 Handbook, the following definitions apply.

Table 1 - Handbook definitions

Term	Definition
Activity	The set of design, development, manufacturing, and maintenance tasks performed in support of the four Objectives of GEIASTD0009. These Activities identify, quantify, and qualify product characteristics in terms of attributes, tolerances, and the test and inspection requirements necessary to produce a reliable, available, and maintainable product.
Constraints	constraints are uncertainties that can affect achievement of the program's Objectives either positively or negatively. The uncertainties that negatively impact the program are those issues that would hinder the program, and the uncertainties that positively impact the program are those issues where the program may benefit from its implementation.
Customer	An individual, organization, or enterprise that commissions the engineering of a product, is a prospective purchaser of the product, or is the acquirer of the product.
Developer	An enterprise or organization that performs the process requirements of this standard.
Method	A reliability best practice used to support an Activity.
Objective(s)	Refers to the four Objectives of GEIASTD0009. Objective 1: Understand Customer/User Requirements and Constraints, Objective 2: Design and Redesign for Reliability, Objective 3: Produce Reliable Systems/Products, and Objective 4: Monitor and Assess User Reliability.
User	Individual, organization, or enterprise that uses, applies, or operates the product.

1.4 Handbook Activities

The Activities from GEIASTD0009 are listed in [Table 2](#). Activities are described in one place in the Handbook allowing the user to easily understand the Activity and how it should be applied across the four Objectives. Each Activity and its implementation applied across the four Objectives of GEIASTD0009 are cross referenced to the TAHB0009 Handbook.

Table 2 - GEIASTD0009 reliability activities

Activity Name	TAHB0009 Section
Engineering Process	2.1
System/Product-Level User and Environmental Life-Cycle Loads	2.2
Life-Cycle Loads on Assemblies, Subassemblies, Components	2.3
Closed-Loop Failure-Mode Mitigation Process	2.4
Identification of Failure Modes and Mechanisms	2.5
Conceptual Reliability Model	2.6
System/Product Reliability Model	2.7
Reliability Assessment	2.8
Failure Definition/Scoring Criteria	2.9
Reliability Program Plan	2.10
Reliability Verification	2.11
Technical Reviews	2.12

Each Activity addresses five key areas, which are described below:

Activity: Purpose. The purpose describes the expected outcome of completing the Activity. An input-process-output (IPO) diagram is used to show the relationship of the expected work required during Objectives 1 through 4, as well as the elements that enable the success of the Activity and the constraints that could hinder it. The IPO was subsequently expanded to a supporting table, SIPOC, which provides a more detailed discussion of the Activity.

[Figure 4](#) is an example of an IDEF0 showing the inputs, outputs, enablers, and constraints associated with a typical Activity defined by GEIASTD0009 across its four Objectives. Each Activity is transitioned from GEIASTD0009 to this Handbook in the same manner. The four-digit reference in the bottom right of each block in the IDEF0 figure corresponds to the appropriate section in GEIASTD0009.

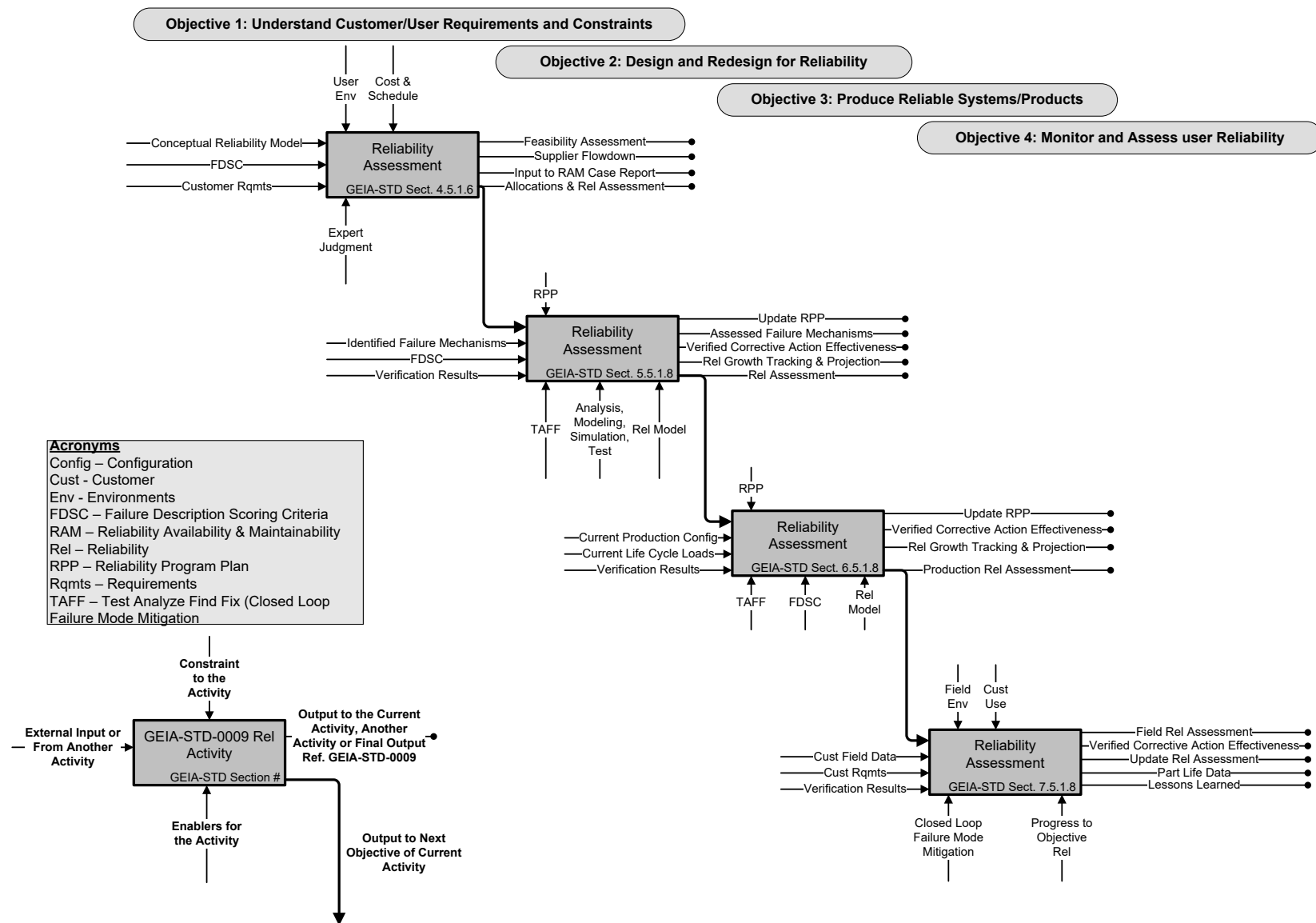


Figure 4 - Example of IDEF0 diagram

Activity: Constraints. Benefits describe those elements of the Activity that promote a robust reliable design and the impacts to the developer and customer. Enablers describe the conditions that must be present to successfully complete the Activity. Constraints are those conditions that restrict or limit the successful application of the Activity.

Activity: Timing of Applicable Activity. A table and description are provided to highlight the Activity's applicability to the four Objectives of GEIASTD0009. The “•” symbol denotes that the Activity is a primary contributor in the Objective. The “Δ” symbol denotes that the Activity may be used, as appropriate, or is updated with available data. Table 3 provides a sample.

Table 3 - Timing of applicable activity

Activity Name	Applicable Objectives			
	Objective 1	Objective 2	Objective 3	Objective 4
Activity	•	•	Δ	•

Activity: Application Guidelines and Lessons Learned. The application guidelines and lessons learned provide a description of how to apply the concepts of the Activity and the expected results. The developer applies the Activity to the system/product or process based on the developer's knowledge of the design genre, as each design genre may have unique considerations (e.g., commercial product designed for use in an office environment versus a product designed for submarine use).

Activity: Applicable Methods. The applicable Methods reference a process or analysis that can be used to develop a robust, reliable design. The Methods listed for each Activity may be tailored as deemed necessary. The Methods listed are those tasks that may be performed over the system's/product's life cycle that have an impact on the total life-cycle cost during design, development, production, delivery, and support. These Methods enable the design to be more reliable (fewer failures), more maintainable (fewer resources needed), and the total life-cycle cost for the system/product to be lower.

1.5 Handbook Methods

A Method can be referenced by one or more Activities. This Handbook describes each Method by stating its purpose, describing the benefits and constraints, identifying the timing for the Method, discussing application guidelines and lessons learned, and providing a list of references for more information. The Handbook does not describe how to use any specific tool referenced. For example, there are no explanations as to how a commercially available reliability prediction program is used. The Handbook assumes that the developer has, or can find, an appropriate subject matter expert trained in the use of the tool.

Method: Purpose. The purpose describes the expected outcome of completing the Method.

Method: Benefits and Constraints. Benefits describe those elements of the Method that promote a robust reliable design and the impacts to the developer and customer. Constraints are those conditions that restrict or limit the successful application of the Method.

Method: Timing of Applicable Method. A table similar to [Table 4](#) is provided for each Method and describes the timing of the applicable Method to the four Objectives of GEIASTD0009. The example reference shown in square brackets corresponds to the appropriate section of the DoD RAM Guide or SAE JA1000-1 standard that is listed in Appendix A of GEIASTD0009.

Table 4 - Timing of applicable method

Accelerated Testing Methods [DoD 4.5.2.16; SAE JA 1000-1 A.1]	System/Product Life-Cycle Phase			
	Objective 1	Objective 2	Objective 3	Objective 4
	•	•	•	

Method: Application Guidelines and Lessons Learned. The Method application guidelines describe lessons learned and how to apply the concepts of the Method.

Method: For More Information. This subsection lists additional industry and/or government resources available for more information.

2. ACTIVITIES

2.1 Engineering ProcessPurpose

The Objective of the engineering process (EP) is to design and produce a functional, reliable, and robust system/product. This means that the system/product performs its intended function in the full spectrum of the potential environments and use, it is economical to produce, and it is easy to maintain. From a reliability engineering perspective, this goal can be supported by employing a failure mode/mechanism management strategy that is based on robust design for reliability (DFR) principles. An effective EP comprises a two-step reliability process that first proactively identifies a comprehensive set of potential failure modes and their accelerating mechanisms root causes, and secondly, mitigates them based on a specific prioritization Method that accounts for critical functionality from the component level up and the system/product level down. This type of EP will produce not only a functional design, but also a reliable and durable one. An EP that employs DFR principles during design, development, production, and customer use over the system/product life cycle will minimize waste and potential future rework, thereby maximizing the total life cycle cost savings. The inputs, outputs, enablers, and constraints associated with an effective engineering process are shown in [Figure 5](#). Similarly, Table 5 shows the inputs and outputs of the EP, but adds a more detailed discussion of the processes and interfaces that take place. Note that the inputs and outputs of [Table 5](#) are worded differently than those in [Figure 5](#). This is done to further characterize these items because of the complexity of the EP. For instance, the two [Figure 5](#) inputs for Objective 1 (Customer Reliability Requirement and System, Subsystem Component Requirement) are further described as Design Concept Ideal/Intended Functions and Product Boundaries and Levels of Detail, respectively, in [Table 5](#).

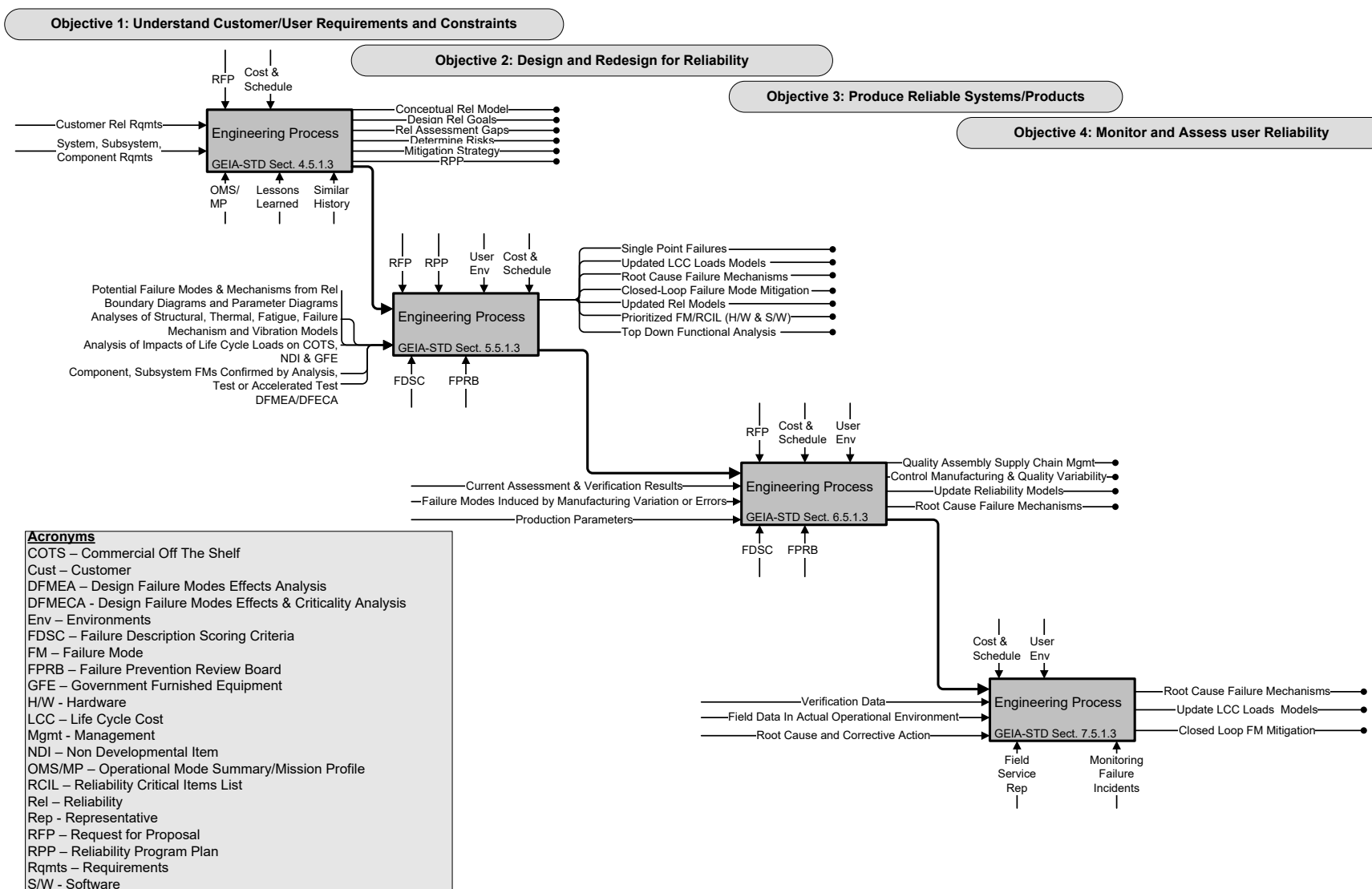


Figure 5 - IDEF0 for the engineering process modeling diagram

Table 5 - SIPOC for the engineering process model

From	Input	Process(es)	Output/Product	To	Ref
System Engineering Architecture (Product Structure and Functional decomposition)	Design concept ideal/intended functions	Bottom-up architectural diagram (components/LRUs) Functional decomposition	Bottom-up component level detail Finalize architecture development (work breakdown structure) Bill of materials	Parameter Diagram	Objective 1
SE Architecture and Trade Studies	Product boundaries and levels of detail	Determine boundaries/interfaces cause and effect relationships and factors that affect system performance Partition system into functional components and subsystems	Functional boundary diagram Error states Noise factors Control factors Unintended functions	Parameter Diagram	
Functional decomposition and Trade Studies	Physical and functional relationships among components/ systems	Tolerance analysis (environmental and physics stresses) Functional decompositions/ tolerance specifications Reliability allocation (component and subsystem reliability requirements)	Reliability block diagram	Failure Definition Parameter Diagram	Objective 2

From	Input	Process(es)	Output/Product	To	Ref
CONOPS	Customer usage profile to establish performance-based reliability requirements	Understand the scope and magnitude of the end-use environments and levels and frequency of stress exposures (temperature, humidity, shock, vibration, and power) to which the product will be exposed throughout its useful life Identify the natural and induced environmental characteristics that the product may experience in its life cycle Quantify the high and low extreme and rate of change conditions for each of the environmental stresses; determine the conditions that have the most impact	Characterization of operational/environmental loads the product can be expected to experience	Failure Definition Ideal Function	
Failure Definition	Failure mechanisms Error states Functional boundary Characterization of operational and environmental loads/stress the product is expected to experience	List of all relevant performance characteristics and the levels at which the product operation is considered unacceptable Fatigue modeling, design for environments, life characteristics	Stakeholder consensus of product failure definitions S:N curves	Parameter Diagram DVP&R (Reliability DOE) FTM DFMEA/FMECA	
Parameter Diagram	Noise factors BOM Error states Ideal/intended functions	Failure definition based DFMEA (Qualitative) BOM based FMECA (Quantitative) Physics-of-Failure analysis (PoF) of pre-production design and components Finite element analysis Failure Prevention and Review Board	Failure modes (failure sites and mechanisms) Root causes Critical components (prioritized list of FMs) Recommended/corrective actions strategies Conceptual design refinement	DVP&R (Reliability DOE) FTM DFMEA/FMECA	

From	Input	Process(es)	Output/Product	To	Ref
DVP&R (Reliability DOE)	Noise factors S:N curve	HALT (assemblies, sub-assemblies and components) HALT (system level) Accelerated life testing (prototype) Environmental testing (prototype) Reliability growth testing (prototype) Failure Prevention and Review Board	Design refinement Inherent reliability estimate from modeling and simulation along with lower level testing	DFMEA/FMECA Closed Loop FRACAS	
FTM (system level-top down)	Functions Failure modes	Identify single failure points Evaluate software and man-machine interfaces Evaluate design change impacts	Qualitative measurement of the consequences and criticality of potential failures	DFMEA	
DFMEA/FMECA (Component Level - Bottom Up)	FMs	FMEA based DVP&R (Reliability DOE)	Reliability demonstration/verification tests	Low Rate Production	
	Root causes/noise factors Ideal/intended functions Control parameters/spec	Root cause failure analysis (system level) Failure Prevention and Review Board Prioritized failure modes	Reliability growth assessment with confidence	Closed Loop FRACAS	Objectives 3 & 4

From	Input	Process(es)	Output/Product	To	Ref
Closed Loop FRACAS	Failures and corrective action information for hardware and software failure modes and mechanisms	Capture data to analytically assess in-process and end-use reliability Identify root failure causes Track the identification and implementation of corrective actions to eliminate the effect of failures on the inherent design reliability of the product Failure Prevention and Review Board Prioritized failure modes	Failure reports Failure analysis Failure modes Failure mode mitigation Risk mitigation decisions Configuration control Lessons learned	Low Rate Production	
FRACAS Low Rate Production	Reliability estimation Control parameters/spec	HALT/HASS of production articles POF test failures Failure Prevention and Review Board	Design refinement Operational reliability estimate	FRACAS Follow on Test and Evaluation FRP and Fielding	

2.1.2 Benefits, Enablers, and Constraints

Engineering processes form the core of the product development system. Such processes are successful when the resulting end products are functional, durable, and economically feasible. This means that the system/product that result from an EP must meet stringent requirements for robustness, feasibility, and economics in order to be competitive and profitable in the marketplace. A delicate balance of enablers and constraints must be found, and each Activity and step must be strategically scheduled, planned, and supported by suitable resources.

2.1.2.1 Benefits

The underlying Product Development System produces a durable and economical system/product that is competitive and profitable. A developer that has a robust and cost-effective EP as the basis of its business strategy will likely have a growing business and expanding market share. Otherwise, the developer risks designing and producing a system/product that may not meet customer requirements and expectations, thereby requiring several iterations of rework or redesign.

2.1.2.2 Enablers

To achieve the potential of the EP to produce a robust system/product, several important conditions must be present:

- Operational Mode Summary/Mission Profile (OMS/MP): Clearly specified system/product environmental loads and service use profiles
- Lessons learned from historical experience with similar product/system
- Failure Definition Scoring Criteria (FD/SC): Clear definitions of critical and essential function failures at the system/product level
- Failure Prevention Review Board (FPRB) and/or a Failure Review Board (FRB)
- Field service performance data
- Failure incident monitoring
- Corrective Action Board

2.1.2.3 Constraints

As with most processes, the EP has constraints that must be accounted for during design, development, production, and customer use:

- Cost and schedule
- Request for Proposal (RFP); restrictive requirements can constrain trade space and conflict with reliability
- Changes to requirements such as environmental user profile

2.1.3 Timing

As shown [Table 6](#), the EP plays a role in each of the four Objectives defined by GEIASTD0009. The primary focus is on DFR (Objective 2), but it has equally important roles in Understanding User Requirements (Objective 1), Produce Reliable System/Product (Objective 3), and Monitor and Assess User Reliability (Objective 4).

Table 6 - Timing of activity

Activity	Applicable Objectives			
	Objective 1	Objective 2	Objective 3	Objective 4
Engineering Process	•	•	•	•

The following paragraphs describe the EP as it relates to Objectives and related tools and Methods:

- During Objective 1, after user requirements are understood and concept selection for a new system/product is made, the EP ensures that the requirements are achievable and that the selected concept is optimized, not only for key performance characteristics, but also for reliable and durable operation over its prescribed life cycle. The use of Reliability Guidelines, design margin principles, system redundancies, and other advanced tools and Methods will ensure that, during Objective 1, the concept and system architecture represents a reliable system/product. In parallel with the EP, the conceptual reliability model is being developed based on the chosen system architecture, so that future refinement of the model will be based on refining and maturing the system/product and its functionality.

- Design and Redesign for Reliability (Objective 2) is based on proven system engineering principles and methodology. During the development phase of the system/product, the EP explicitly manages the product structure/architecture, functionality, and functional decomposition (and then its synthesis) processes, including all identified failure modes, their associated root causes, and their accelerating mechanisms. Consequently, design of the system/product can be completed, with reliability demonstrated at the component level (with a high degree of statistical confidence), and then verified at the system/product level. In other words, the historical concept of reliability growth is being addressed sooner and more proactively in the system/product development process at the lowest feasible levels of the system/product architecture. System/Product-Level Reliability Requirements are being decomposed and allocated to appropriate lower levels of the architecture, and then verified at this level through testing, simulation, etc.
- Software Reliability Design (Objective 2) also focuses on developing a reliable system through continuous software improvements. Proven software reliability techniques are incorporated at each stage of development. The intent is to follow standard software development practices to:
 - Reduce the likelihood of failures
 - Remove defects that cause failures when they are discovered
 - Perform a software and/or firmware failure modes effects analysis
 - Consider the software and firmware in the system fault tree analysis
 - Predict the number of software defects escapes during software development in order to tailor testing to eliminate those errors prior to deployment
 - By implementing these techniques throughout software development, reliability is built into the software at the onset, yielding a quality software product for the customer
- Objective 3 focuses on quality, assembly, and supply chain management. It is extremely important to translate all of the critical design parameters that are controlling the failure mode/mechanism mitigation processes into production parameters during the manufacturing process to control system/product quality. Steps that control manufacturing and quality variability should be planned ahead and employed at this stage. Robust quality practices are necessary to ensure that the inherent reliability built into the product design are not degraded due to poor workmanship, uncontrolled manufacturing processes, deficient documentation, etc.
- Objective 4: After system/product delivery to the customer/user, the engineering process shifts towards a reactive FRACAS approach, while monitoring field data in the actual operational environment. Continuous reliability growth and product improvement is realized by monitoring failure incidents, then analyzing down to their root causes and mitigating them through corrective action that has been verified as effective. The process of failure mode identification shifts to the Service Organization (Field Service Representative), but the failure mode/mechanism mitigation step remains the same as the one established during the design for reliability phase (Objective 2). It should be noted that a robust DFR process during Objective 2 should minimize the number of new failure modes discovered in testing or in the field. If the number of newly discovered failure modes is excessive, then an opportunity presents itself to make the DFR process more robust.

2.1.4 Application Guidelines

A useful conceptualization of a typical EP is within the context of the systems engineering (SE) V-Model and the Objectives of GEIASTD0009, as shown in [Figure 6](#) (INCOSE. 2010. Systems Engineering Handbook - A Guide for System Life Cycle processes and Activities, Version 3.2). The V-Model illustrates the two general stages of product development - the left side of the "V" representing architecture decomposition and definition, and the right side representing architecture integration and verification.

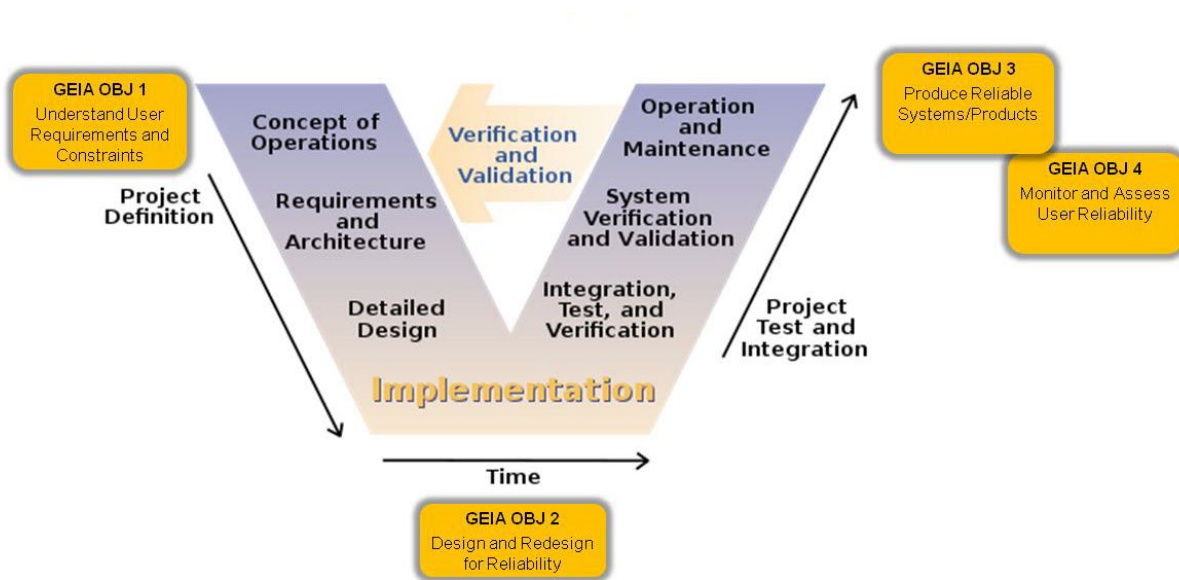


Figure 6 - Systems engineering V-shaped model

During the first part of the failure mode management strategy within the SE process, reliability Activities should identify all potential failure modes that are inherent to the design of the system/product and establish corrective actions to eliminate design deficiencies or mitigate failure consequences. Like Objectives 1 and 2 of the EP, SE practices performed at the end of the design definition and functional decomposition Activities require a prioritized list of potential failure modes that are manageable during subsequent stages of product development.

In the next step of [Figure 6](#), corresponding to Objectives 3 and 4 in the EP, test and integration Activities verify the effectiveness of the corrective actions and demonstrate reliability at all lower levels of the system/product hierarchy. During final demonstration/verification, system/product level reliability should be verified with suitable statistical confidence, ensuring a high probability of future success of the system/product in the customer's hands. Verification and validation methods and approaches should incorporate all potential environmental and operational stress factors that the end item will be expected to be subjected to in the field. Such techniques will verify that the customer requirements and expectations are met and that the system/product is functional, reliable, and durable. These same elements of SE and the EP are shown in [Figure 7](#) within the context of [Table 5](#).

The example characterization in [Figure 7](#) is used with permission from General Dynamics Land Systems (GDLS) and should not be regarded as the only, or the best, EP model. GDLS has applied this model on multiple successful reliability programs and so it has proven itself to be very effective for robust system/product development.

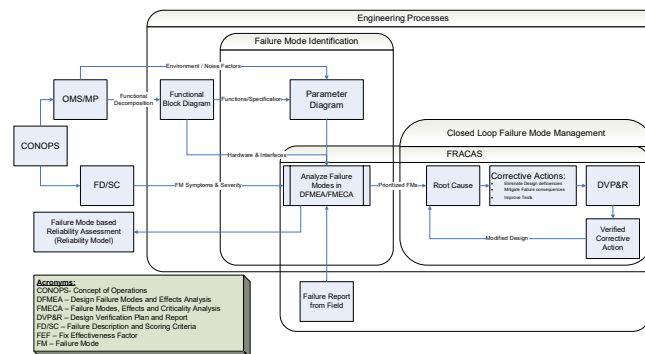


Figure 7 - Elements of the engineering process with inputs/outputs and interfaces

The first step of the failure mode management strategy represented in [Figure 7](#) is proactive failure mode and root cause identification, and elimination of design deficiencies or mitigating failure consequences during the initial DFR process. These efforts are characterized by the tools, Methods, and Activities leading to the DFMEA/FMECA, and are defined as follows (but not necessarily all are depicted in [Figure 7](#)):

- Functional decomposition represents the determination and modeling of ideal functions (desired output function of the subsystem IPO or P-Diagram) at the subsystem and component levels.
- Functional block diagram is used to describe the functional flow within the boundaries of the particular subsystem.
- Functional block/boundary diagram depicts interactions between hardware and software elements and graphically represents the physical architecture of the system. Boundaries of the system define interfaces with the adjacent subsystems, users, operator, and environment.
- Interface matrix is a tabular representation of the functional block/boundary diagram. It describes the interfaces (physical, material exchange, information exchange, energy transfer, etc.) between the hardware and software elements that belong to the system/product of interest.
- Parameter diagram (P-Diagram) aligns the system/product of interest with its operating environment by introducing:
 - The signal or input that triggers the working stage of the system/product.
 - The ideal function that quantitatively describes the output of the system/product.
 - An error state: Any state other than the potential states of the ideal function.
 - Unintended functions: An output of the system/product that is not desired or not intended.
- Control factors: System design parameters that can be changed by the engineering team to fulfill the system functionality.
 - Noise factors: The factors that are not controlled by the developer that affect how a system/product is performing its function.
- Design FMEA (DFMEA) can be a functional, hardware, or software design-based analysis that discovers and consolidates potential failure modes, and recommends actions to eliminate design deficiencies, mitigate failure consequences, and/or improve tests that can be utilized at any level of system/product hierarchy. If based on a P-Diagram, the DFMEA can be a very comprehensive Method for mitigating potential failure modes because it utilizes robust engineering principles in a search for all causes of the potential failure modes. In such an approach, noise factors from the P-Diagram identify conditions the design must withstand, and deficient design selection becomes a potential cause of failure. The DFMEA can be aligned to the fault tree analysis (FTA) when each combination of the item, failure mode, root cause, and mechanism of failure form one basic undesired event in the FTA. Note that the FTA must consider all possible hardware, software, and operator/maintainer events that may contribute to the undesired top-level event.
- FMECA is an extension of the DFMEA methodology. It provides a very detailed analysis of not only the failure mode (FM) and its effect(s), but also each FM's criticality. Criticality measures in an FMECA are typically based on the modal failure rates associated with each failure mode.
- HALT/ALT and other accelerated potential FM discovery Methods are based on a test or simulation approach and typically used at the component level to mature and grow reliability for the specific application and/or environment.

The second step of the failure mode management strategy is mitigation of the identified and prioritized failure modes, so that the required or desired level of product reliability is achieved with some level of confidence. This step is based on the previous step of discovering and prioritizing FMs using DFR principles. In [Figure 7](#), these steps are represented by the Activities leading to and from the FRACAS and are defined as follows:

- A design verification plan and release (report) (DVP&R) is essentially a plan of the verification test(s) that will be used to verify and demonstrate reliability at the subsystem or component level and rolled up to the product level. The DVP&R tests can be based on previously performed inputs to the DFMEA/FMECA FTA, FEA, M&S, etc. These tests address prioritized potential failure modes and their corresponding mechanisms of failure and verify that proposed failure mode management strategies are sound and efficient.
- The failure reporting, analysis, and corrective action system (FRACAS) consists of a failure reporting and analysis system (failure incidents) and associated corrective actions. A FRACAS should be based on two major components of the system/product - the structure that is based on its hierarchy (work-based structure, bill of material, etc.) and the aligned potential failure modes. Ideally, the FRACAS must capture all failures associated with the design, test, production and use of the system/product, and can be used to evaluate the robustness of a previously created DFMEA (with recommended corrective actions aligned to the components of the product hierarchy) or any other DFR Activity. The FRACAS provides the necessary data/information to support the qualitative and quantitative analyses of the system/product reliability performance during testing, or in the field. Thus, the FRACAS can be a very powerful tool in continuous reliability assessment, as well as a mechanism for continuous reliability growth during the design, development, production and fielding stages of the system/product life cycle. A comprehensive FRACAS is the critical element of the closed-loop failure mode management system.
- Many companies have found that relying on FRACAS as the primary engineering process to mitigate/address failures (test and fix) can result in a potentially lengthy product development process that may exceed time-to-market timing requirements. An alternative is to use the FMEA/FMECA to recommend and execute corrective actions to eliminate design deficiencies, mitigate failure consequences, and improve test procedures, followed by confirmatory testing or analyses.

Managing failure modes throughout the design process by first comprehensively identifying them, and then fixing them in prioritized order so that the system/product meets its intended level of reliability, is a DFR approach discussed in this Handbook. An engineering process that follows the system engineering model creates a product Structure and hierarchical functional requirements for the software, parts and components that can be subsequently used to derive FMs of the component or software that are based on their intended function (described in a System/product Specification). Such an approach can connect and naturally merge the system engineering and DFR processes into an overall strategy that results in not only a system/product that is capable of performing its intended function, but one that can do this reliably and robustly in the presence of uncontrolled noise factors such as aging, environment, user/operator skill levels, etc. A properly set up process, coupled with an established reliability program plan (RPP), initiates a closed-loop failure mode management system during the design stage, and then follows through with a comprehensive FRACAS process during the production and fielding life-cycle phases.

Finally, lessons learned for the developer in the implementation and potential enhancement of the EP include:

- If reliability data indicates that changes should be made to the EP, any potential reliability improvements that can be achieved should be reported to the appropriate engineering organization(s). Similar reliability improvement opportunities should be reported back to the appropriate manufacturing, test or administrative organizations if the data warrants it. See the closed-loop failure mode mitigation process activity in this Handbook for more information.
- If the engineering process is changed at any time, regardless of whether it is in response to data obtained from in-house engineering Activities or from field use, the reliability impact of those changes should continue to be monitored and assessed as part of field use.
- Items that have been identified as reliability-critical during the design and development phases of the EP should continue to be evaluated, managed, and controlled throughout the useful life of the product.

2.1.5 Applicable Methods/Submethods

Due to the complexity of the EP there are a large number of Methods/Submethods. For further application guidance, see the individual Method.

- [Method 3.1](#): Accelerated Testing Methods (such as TAFT, RDGT, HALT, ALT)
- [Method 3.3](#): Benchmarking (Reliability Benchmarking)
- [Method 3.5](#): Capability Maturity Model Integration (CMMI®)
- [Method 3.6](#): Commercial Off-the-Shelf (COTS) Assessment
- [Method 3.7](#): Component Testing
- [Method 3.9](#): Critical Items List
- [Method 3.10](#): Data Collection, Analysis, and Corrective Action System (DCACAS)
- [Method 3.12](#): Design for Manufacturing and Design for Assembly
- [Method 3.13](#): Design of Experiments (DOE) - Classical and Taguchi
- [Method 3.14](#): Design Guidelines for Reliable Surface Mount Technology Printed Board Assemblies
- [Method 3.15](#): Design Review
- [Method 3.16](#): Durability Analysis
- [Method 3.17](#): Durability Verification Test
- [Method 3.18](#): Environmental and Product Usage Profile/Mission Profile
- [Method 3.19](#): Environmental Qualification Test
- [Method 3.20](#): Environmental Stress Screening/Highly Accelerated Stress Screening
- [Method 3.21](#): Error/Mistake Proofing (Poka-Yoke)
- [Method 3.22](#): Failure Mode and Effects/Failure Mode, Effects, and Criticality Analysis
- [Method 3.23](#): Failure Reporting, Analysis, and Corrective Action System (FRACAS)
- [Method 3.24](#): Fault Insertion Testing
- [Method 3.25](#): Fault Tree Analysis (FTA)
- [Method 3.28](#): Ishikawa Diagram
- [Method 3.30](#): Human-in-the-Loop Testing (formerly Man-in-the-Loop Testing)
- [Method 3.33](#): Measurement Systems Analysis
- [Method 3.34](#): Mission Profile Definition
- [Method 3.35](#): One-Shot Device Testing

- [Method 3.36](#): Pareto Analysis
- [Method 3.37](#): Part Derating
- [Method 3.40](#): Physics of Failure (PoF)
- [Method 3.42](#): Probabilistic Design - Stress and Strength Interference Method (SSI)
- [Method 3.43](#): Process Failure Modes Effects Analysis/Producibility Analysis
- [Method 3.44](#): Production Process Capability Study
- [Method 3.45](#): Program Parts Selection List
- [Method 3.46](#): Pugh Selection
- [Method 3.47](#): Quality and Quality Control
- [Method 3.49](#): Quality Loss Function
- [Method 3.50](#): RAM Design Guide
- [Method 3.55](#): Reliability Case
- [Method 3.56](#): Reliability-Centered Maintenance
- [Method 3.57](#): Reliability Demonstration Testing
- [Method 3.58](#): Reliability Growth Modeling and Testing
- [Method 3.59](#): Reliability Growth Testing and Test-Analyze-Fix-Test (TAFT)
- [Method 3.61](#): Reliability Testing for Engineering Development, Qualification, and Testing
- [Method 3.62](#): Repair Strategy
- [Method 3.64](#): Requirements and Architecture Development
- [Method 3.65](#): Risk Assessment
- [Method 3.66](#): Root Cause Analysis
- [Method 3.67](#): RQT and Acceptance Testing
- [Method 3.71](#): Sneak Circuit Analysis/Sneak Path Analysis
- [Method 3.74](#): Specification Generation (Specifying/Establishing RAM Requirements)
- [Method 3.79](#): Worst-Case Analysis
- [Activity 2.10](#): Reliability Program Plan

2.2 System/Product-Level User and Environmental Life-Cycle Loads

2.2.1 Purpose

It is beneficial to account for all user and environmental life-cycle loads as early in the design process as possible, and keep them up to date throughout the entire life cycle, as more detailed information becomes available (Figure 8). Good understanding of the potential factors that the end product will be exposed to will ensure the success of the developmental process and make systems robust and reliable. Many future failures or failure modes can be categorized as either lack of design margin (strength) in response to specific stresses and loads or complete omission of these factors in the design process. A complete and comprehensive list of user and environmental loads must be presented and discussed at the level of system requirements ([Table 7](#)). In order to fully describe such loads that later will be disseminated and propagated to subsystem level and components (see [2.3](#)), it is critical to describe each load in terms of physical influence or noise factors (mechanical, thermal, vibration, etc.), with a corresponding estimated mean level variance, the spread or deviation of the expected values, the rate of change, frequency, etc.

Physical loads acting on the whole system during a particular mission or function generate specific duty cycles for the system that can be used to define the specification of the components and subsystems. Different physical loads can lead to potential failure modes or accelerate the failure based on specific Physics of Failure. Sometimes, different loads can be amplified by other loads, thus increasing their effect multiple times and accelerating the failure mechanism. So, the design should account for different loads in unison and not independently. Design of experiments is an effective approach to evaluate the effect of user and environmental loads, thus employing robust engineering principles.

As will be discussed in [2.2.4](#), the assessment of the life-cycle loads is an iterative process that starts from analysis of the mission profile and functional behavior and continues through prototype testing that assesses, measures, and categorizes actual loads. The load case can be established by using a prototype in the actual environment and measuring the impact on the system. This information can be used as an input for subsystem, component, and part level acceleration tests, which are very useful to discover and then mitigate failure modes, find weak links, and measure (demonstrate) reliability at progressively lower levels of assembly, down to the lowest appropriate level.

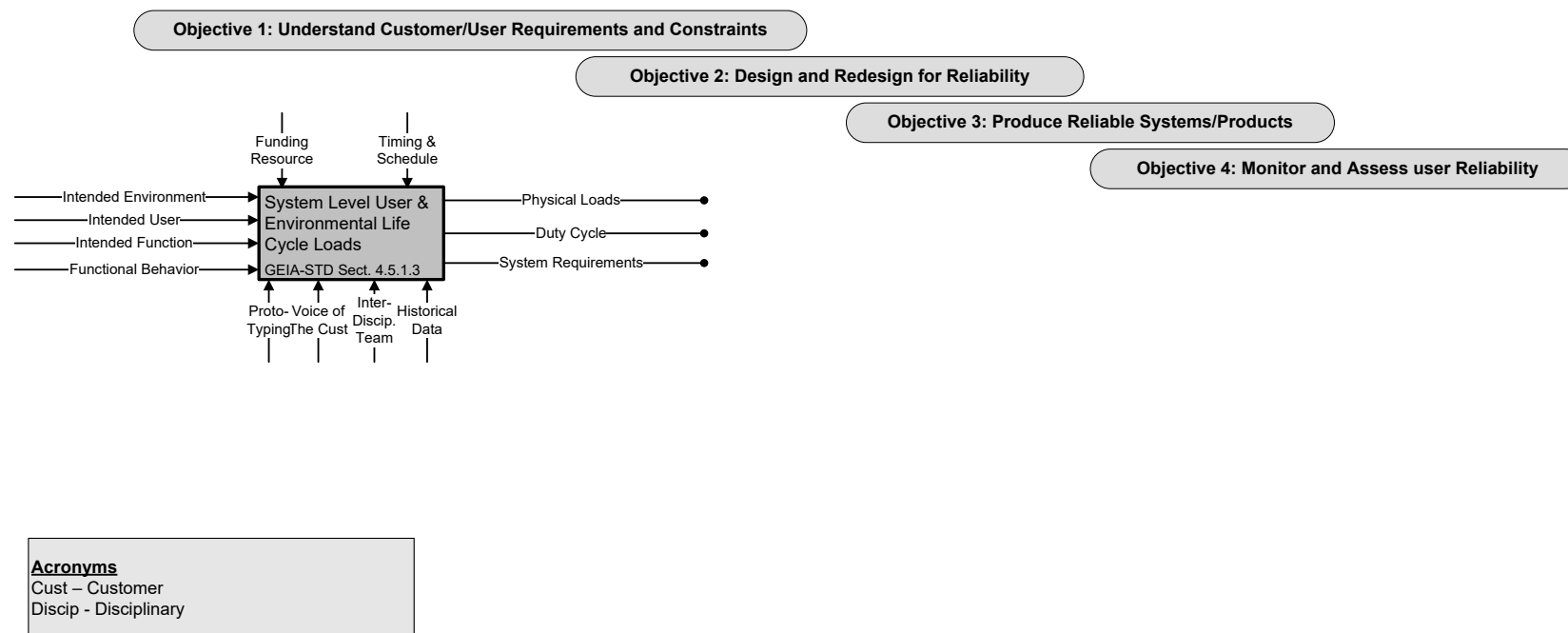


Figure 8 - System/product-level user and environmental life-cycle loads

Table 7 - System product life-cycle loads

From	Input	Process(es)	Output/Product	To	Ref
OMS/MP FD/SC	System level loads System level noise factors (environmental and user)	Qualitative and quantitative analysis of physical loads acting on system/product System level parameter diagram	System level physical loads System level duty cycle System requirements	Life-Cycle Loads on Assemblies and Subsystems Engineering Processes	Objective 1

2.2.2 Benefits, Enablers, and Constraints

2.2.2.1 Benefits

System/product level user and environmental life-cycle loads dictate the external operational environment of the end item that the design must adhere to. Proper and complete assessment of loads acting on the end item, either through analysis, or (preferably) through direct measurement, is a crucial component of the design process. An output of this process is the subsequent decomposition of the loads to lower levels of assembly, to define the specifications duty cycles of newly developed designs or non-developmental items (NDI). Without this flow-down analysis, it is impossible to truly design reliable and robust systems that are capable of performing their mission and function in the given environment and in field usage.

2.2.2.2 Enablers

In order to achieve the full potential of the robust load assessment process and then produce a reliable product, several important conditions must be met:

- Good understanding of the planned mission and/or function to be performed by the product (OMS/MP)
- Full gamut of the intended functions that are measured, producing a feasible and attainable duty cycle for lower-levels of assembly
- Study of the voice of the customer (VOC) that portrays the user-type of loads, as well as exposure to environmental stresses
- Study of functional behavior that accounts for the human-in-the-loop and different stages of the mission
- Prototyping and testing of the total system in the conditions that mimics the real environment
- Establishing characterization of the loads through actual testing and measuring the system reaction to these loads

2.2.2.3 Constraints

System/product level user and environment life-cycle load assessment can have constraints through the following factors:

- Resources, funding
- Timing, schedule, time to market
- Proper understanding of the actual environment and inability to test at the extreme level of the loads

2.2.3 Timing

Table 8 - Timing of activity

Activity	Applicable Objectives			
	Objective 1	Objective 2	Objective 3	Objective 4
System/Product-Level User and Environmental Life-Cycle Loads	.			

System/product-level user and environmental loads assessment and monitoring is extremely important at the inception of the program, when the developer understands and assesses user requirements. During Objective 1, system level loads are assessed and analyzed, and such Activity defines the design guidelines and processes to be used during the developmental process for the Objective 2. The main goal of loads assessment during Objective 1 is to establish a comprehensive set of potential loads on the end product during its useful life and to realistically estimate their distributions.

When implicit and generic user and environmental life-cycle loads are translated into measurable physical loads during Objective 2, design Activities and engineering processes decompose them into progressively lower level assembly loads (2.3), thus creating the specification requirements for their design. It is important to maintain the traceability of these detailed specifications to system level loads, as well as to verify their accuracy throughout the development process. When a detailed design passes the critical design review (CDR) and starts a synthesis stage of the system engineering V-model (2.1), it is important to validate and verify subsystem level requirements by exposing the component to previously derived subsystem level loads. Ultimately, this process will arrive at the system level verification of the robustness and reliability of the end product in the presence of the system level user and environmental life-cycle loads. Hence, the main role of system level load assessment during Objective 2 is verification and validation of the design by properly defining and executing the appropriate customer-level testing such as Developmental and Operational Tests (DT/OT).

After fielding the product during Objective 4, it is essential to monitor actual system level user and environmental loads during normal operations. Due to potential limitations of the sample size in Developmental Test (DT) and Operational Test (OT), some important factors contributing to the loads acting on the system will likely be missed, or its impact will be over/under estimated. Ultimately, the system/product may be used in environmental conditions or different mission profiles than what was intended or required in the initial specification requirements. For example, the original operating concept for the B-52 aircraft was to penetrate enemy airspace at high altitude. When this concept was modified to require low-level penetration, the service life of the airframe was significantly reduced due to the higher aerodynamic loads caused by low-level flight. In these cases, the changes in environmental and user loads must be factored into a reliability assessment of the impact on system/product reliability (Tagg, 2004).

2.2.4 Application Guidelines

As was discussed before, the main purpose of the system/product level user and environmental life-cycle loads assessment and analysis is to (1) comprehensively and entirely describe all potential loads on the end product, (2) translate all loads into physical loads with realistic numerical values at progressively lower levels of assembly, (3) design to those load levels, (4) verify that design of the system is capable of performing its intended function under these loads and, finally, (5) monitor the effect of the user and environmental loads after the product is fielded.

One of the best tools employed to comprehensively study system level loads is the parameter diagram (P-Diagram), which is described in greater detail in 2.1.4. This tool allows understanding of the system operation in the presence of noise factors, which resemble system (and subsystem) levels of loads. The P-Diagram constructs the notional picture of the energy transformation of the system and generates the intended function(s) from the input(s). Such energy transformation is controlled by the specification of the system or control factors in the presence of five groups of noise factors:

- Variability
- Change over time, degradation, aging
- Environmental loads
- User/operator factor
- Subsystem interaction (will be used at the subsystem level loads analysis)

- From the physical load analysis, user and environmental life-cycle loads can be described as:
- Mechanical loads
- Vibration
- Shock
- Pressure
- Thermal
- Thermal cycling
- Heat/cold extremes
- Electrical
- Humidity
- Salt fog
- Aggressive environmental exposure
- Chemical
- Biological
- Nuclear

The operational aspects of the system level life-cycle loads are:

- Operator/user interaction
- Maintenance

All these aspects need to be analyzed, studied, and accounted for during the system level load assessment. During prototyping and initial system-level testing, it is possible to discover the impact of the user and environmental loads that were omitted during planning phase. At this point, it is important to not only create corrective action that mitigates the effect of a newly discovered failure mode, but also to analyze the overall impact of this load factor/failure mechanism on the design performance.

2.2.5 Applicable Methods/Submethods

- [Method 3.4](#): Block Diagram Development
- [Method 3.18](#): Environmental and Product Usage Profile/Mission Profile
- [Method 3.22](#): Failure Mode and Effects/Failure Mode, Effects, and Criticality Analysis
- [Method 3.25](#): Fault Tree Analysis (FTA)
- [Method 3.48](#): Quality Function Deployment

2.3 Life-Cycle Loads on Assemblies, Subassemblies, Components

2.3.1 Purpose

System level loads were first defined in [2.2](#). These loads must be disseminated and propagated to lower level assemblies, subassemblies, components and parts. System level loads include any stress, acting physically or chemically on the subject of the study (system, subsystem, component, etc.), that affects the output of the operating system or changes its operating state, leading to an unintended function, error state, or failure. Examples of such loads would be mechanical vibration coming through the mounts of the subsystem, mechanical shock, temperature variation of the environment, humidity, unexpected user/operator input, heavy network traffic, high number of end users, etc. Such loads result from the external environment of the system/product; thus, are the function of system operating conditions and overall duty cycle, or from adjacent systems or the user/operator. Both software and hardware components are affected by life cycle loads.

From a robust engineering perspective, all loads acting on a system can be divided into control factors that are required for the system to operate and produce an intended function and noise factors that are not controlled by design engineers and still affect the output of the system (see the parameter diagram definition in [2.1.4](#)). For software components, the control factors include but aren't limited to validation of user inputs, robust design to handle heavy usage, alternative paths, software faults, hardware faults, I/O faults, off nominal conditions, etc. For software noise factors might be a sudden system shutdown, loss of power to the processing unit, etc. jointly, control factors, i.e., material specification, geometry, assembly procedures, etc., and noise factors or loads, such as vibration, environmental conditions, user inputs, network traffic, number of end users, etc., form the specifications and/or requirements for the subsystem and parts. Hence, it is extremely important to comprehensively capture and verify all life-cycle loads and noise factors in order to produce proper specifications for components, thus designing reliable and robust products ([Figure 9](#)). The software specifications should also address how the software will handle invalid inputs, heavy network traffic, heavy end-user volume, hardware faults, I/O faults, faults in other software, and off-nominal conditions.

Ultimately, for the reliability assessment of the subsystem or component, any noise factor or load can be a potential root cause of the failure modes. Therefore, such loads must be considered in mechanisms of failures and described in design failure modes effects analysis (DFMEA), failure modes effects and criticality analysis (FMECA), and software failure modes effects analysis (SFMEA) when analyzing and assessing the subsystem performance and robustness. The software FMEA analyzes the effects of both control factors and noise factors. For example, what does the software do if the processing unit shuts down while storing critical data? What does the software do if the hardware is in a faulty state?

An excellent tool for capturing noise factors or loads acting on the subsystem is Parameter Diagram (P-Diagram). The P-Diagram aligns the system/product of interest with the requirements of its operating environment by introducing:

- The signal or input that triggers the working stage of the system/product
- The ideal function that quantitatively describes the output of the system/product
- An error state: Any state other than the potential states of the ideal function
- Unintended functions: An output of the system/product that is not desired or not intended
- Unintended user inputs: A user input is allowed which should not be
- Unintended software functions: The right software function is executed at the wrong time or in the wrong state or the wrong software function is executed
- Heavy network traffic
- Heavy volume of end users or heavy usage

- Using the software for an extended period of time without turning it off or rebooting
- Control Factors: The factors that control the energy transfer between an input and output of the system/product
- Noise Factors: The factors that are not controlled by the developer that affect how a system/product is performing its function

Comprehensive analysis of the product reliability during field operation usually reveals two major design deficiencies: either the particular load or noise factor was not considered and later led to the unexpected failure of the system, or such load was considered, but it exceeded the strength of the component and led to an unanticipated failure. The latter failure mechanism is also called inadequate design margin. In some instances, the nominal values for strength and stress are substantially separated and the reason for failure is not due to lack of the design margin, but rather variability of the stress (load uncertainty) or variability of the strength (manufacturing variability). For software, the software design or specifications may not have considered either the control factors or the noise factors and hence failures occur because only the nominal conditions were considered and hence the code is written so as to not address the factors.

In addition, loads that do not immediately cause failure due to exceeding limits may cause smaller, non-failing strains and deformations in the materials. These can accumulate during the life-cycle of a product and result in fatigue failures. Fatigue failure may be assessed early in design using Physics-of-Failure Methods, and mitigated by adding protections from the loads, by inclusion of design protections such as conformal coatings, or by scheduling inspections and maintenance.

Life-cycle load analysis on every level of the product hierarchy, if properly conducted, will lead to capturing all potential failure modes and consequently designing them out or mitigating them in the early stages of the design process. It is essential to capture not only environmental or system level loads, but also subsystem or component interactions, manufacturing variability, and aging of the system. A comprehensive and well thought-out design verification plan and release (DVP&R) will verify and confirm the robustness of the subsystem design only if all significant loads are captured and employed during an accelerated life test. For software it is essential to capture the factors that affect software and firmware interfaces. One common interface factor is incorrect scale or units of measure between two software programs. With regards to aging, software components that aren't updated over time may eventually result in an interface failure. For example, many modern software programs can't run on older operation systems.

The DVP&R is essentially a plan of the verification test(s) that will be used to verify and demonstrate reliability at the subsystem or component level and then rolled up to the product level. The DVP&R tests can be based on previously performed inputs to the DFMEA/FMECA/SFMEA, FTA, FEA, M&S, etc. These tests address prioritized potential failure modes and their corresponding mechanisms of failure and verify that proposed failure mode mitigation strategies are sound and efficient. Such tests should be based on design of experiment principles in order to introduce significant loads and their interactions simultaneously. The end result will be realistic and represent the real life environment.

Objective 1: Understand Customer/User Requirements and Constraints

Objective 2: Design and Redesign for Reliability

Objective 3: Produce Reliable Systems/Products

Objective 4: Monitor and Assess user Reliability

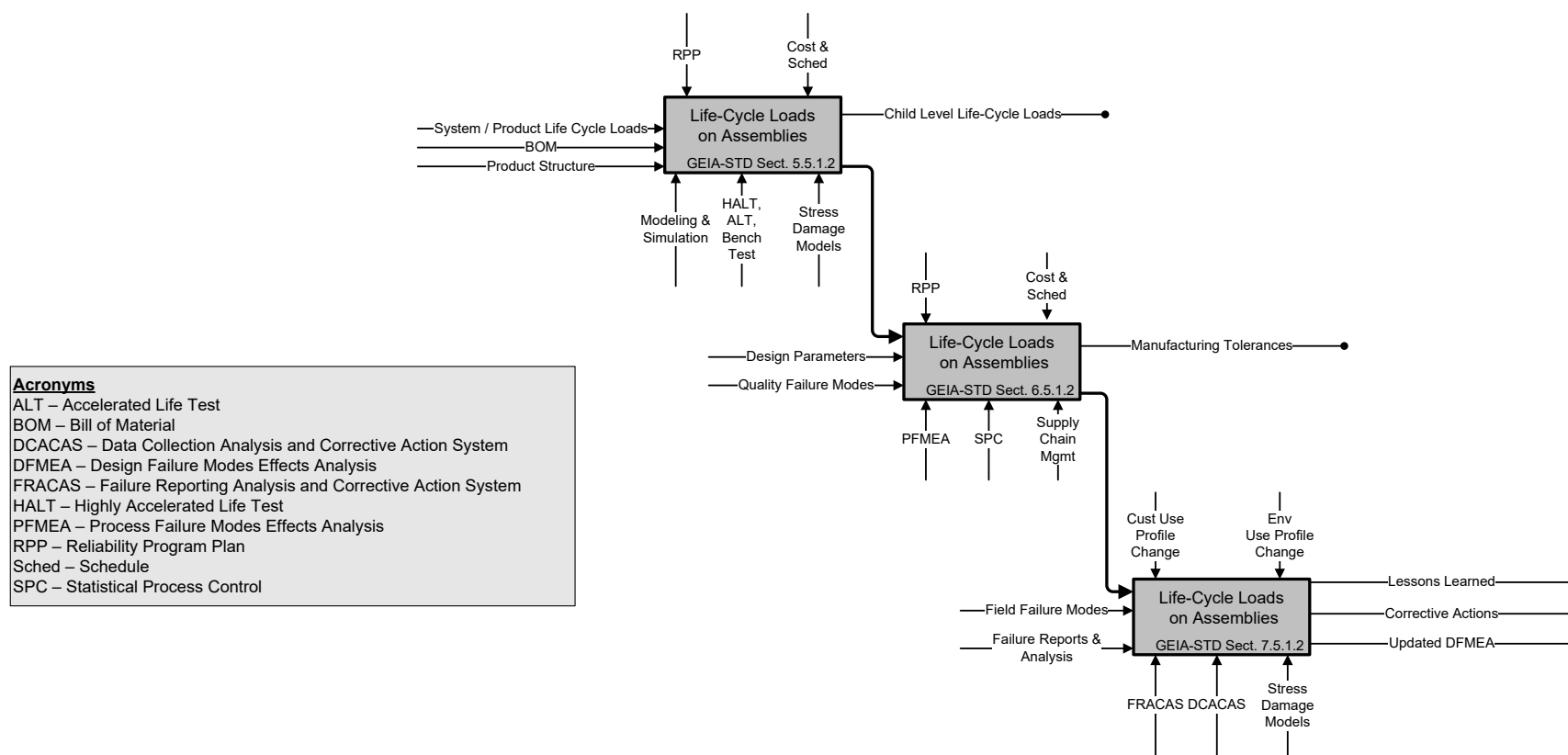


Figure 9 - Life-cycle loads on assemblies, components, and parts

Table 9 - Life-cycle loads on assemblies, components, and parts

From	Input	Process(es)	Output/Product	To	Ref
System/Product Life Cycle Loads Life-Cycle Loads on Assembly, Subassembly, and Component	Parent assembly life-cycle loads Adjacent subsystem/assembly unintended functions, loads	Loads propagation and dissemination at lower level of product structure Loads generation at Subsystem level as an unintended functions Planning the test, establishing traceability of the requirements Key life test (ALT/HALT/DOE)	Child level life-cycle loads	Life-Cycle Loads on Assembly, Subassembly, and Component P-Diagram DVP&R	Objective 2
Engineering Processes DFMEA/FMECA/SFMEA	Design parameters Control parameters	Control critical design parameters during assembly using PFMEA Control component quality Statistical process control	Controlled manufacturing tolerances	Engineering Processes	Objective 3
FRACAS DCACAS	Failure reports Failure analysis	Monitoring field life-cycle loads Update DFMEA/FMECA and P-Diagrams	New or updated life-cycle loads Updated duty cycle	Lesson Learned Corrective Actions Engineering Processes	Objective 4

2.3.2 Benefits, Enablers, and Constraints

2.3.2.1 Benefits

Life-cycle loads on assemblies, subassemblies, and components dictate the operational environment for each component at all levels of the end system hierarchy. Proper decomposition of the loads to the component level defines specifications and the duty cycle of the newly developed or COTS parts and components. Without this analysis it is impossible to truly design a reliable and robust system that is capable of performing its mission and function in the given environment and in the user's hands.

2.3.2.2 Enablers

In order to comprehensively and completely identify and assess loads at every level of the product hierarchy and then manufacture an excellent product, several important conditions must be present:

- Good understanding of the planned mission and/or function to be performed by the product (OMS/MP) at the system level
- The full gamut of the intended functions that produce feasible and attainable duty cycle for the subsystem and component level

- Prototyping and testing of the subsystems under conditions that mimic the real environment
- Establishing characterization of the loads on actual test and measuring the system reaction to these loads

2.3.2.3 Constraints

System/product level user and environment life-cycle load assessment can be constrained by the following factors:

- Resources, funding
- Timing, schedule, time to market
- Improper understanding of the actual environment and inability to test at the extreme level of the loads
- Lack of supplier design data for COTS devices

2.3.3 Timing

Table 10 - Timing of activity

Activity	Applicable Objectives			
	Objective 1	Objective 2	Objective 3	Objective 4
Life-Cycle Loads on Assemblies, Subassemblies, and Components		•	•	•

During Objective 2, life-cycle loads on assemblies, subassemblies, and components decomposition, assessment, and validation are extremely important at the design phase of the program, when the developer establishes the specification of the components and makes a decision about COTS. Proper understanding of system level loads and then their decomposition into subsystem and component loads will greatly influence not only the specification of parts and components of the end product, but also the system architecture and overall design. Indeed, the discussion on life-cycle loads acting upon subsystems should initiate a trade study earlier in the design phase. Hence, capturing and assessing the life-cycle loads at lower than system level and their consecutive verification through bench-testing and DOE should take place at the initial functional review of the design.

During preliminary and critical design stages, life-cycle loads must be comprehensively captured, assessed, and analyzed. Test engineers must be involved in the design process and they should construct comprehensive test plans to verify and validate the component design in the presence of most important and critical loads or noise factors. Hence, verification and testing of life-cycle loads acting on the component level should start very early in the design phase. Depending on the chosen testing strategy, reliability components can be either measured using the test-to-failure approach or just confirmed using test-to-bogie (no failure test, similar to a qualification test, which runs for a prescribed amount of time, during which the system does not fail) accelerated life test strategy. Either way, appropriate and allocated reliability will be verified and demonstrated at the component or parts level, thus saving time and money for the business.

During Objective 3, life-cycle loads must be translated into critical assembly parameters and vendor/parts quality using FMEA tools. In short, potential failure modes and associated noise factors or loads can be controlled by design factors that are confirmed and verified in DFMEA. Those critical design factors need to be monitored through an assembly process to avoid quality and assembly errors that can potentially lead to a failure mechanism identified in DFMEA. Thus, monitoring quality of the components and their assembly must be accomplished based on potential failure modes and their corresponding mechanisms of failures.

During Objective 4, life-cycle loads acting on assemblies, components and parts will be ultimately verified in the real operational environment and actual user hands. It is interesting to note that the majority of failures discovered in the field happened due to either unaccounted noise factors (unexpected loads) inadequate design margins (an acting load statistically exceeds the strength of the component), or the manufacturing process/parts quality does not control the strength variability of the components adequately. These three factors are the most common causes for failures discovered in the real, operational environment.

Consistent and comprehensive use of FRACAS during fielding of the end product and system is crucial for capturing life-cycle loads at the component level and monitoring associated failure modes and root causes. Analyzing and understanding life-cycle loads and noise factors acting at the component and assembly levels during normal use will help extend useful life of the current product as well as capture lessons learned for a future product development.

Therefore, analyzing, understanding, and managing life-cycle loads on assemblies, subassemblies, and components are extremely important engineering Activities during design, production, and fielding of the product that shape the component specification and have direct impact on product reliability and performance.

2.3.4 Application Guidelines

Detailed descriptions of the capturing and analysis of the life-cycle loads on assemblies, subassemblies, and components have been discussed in great detail in [2.1](#). Also, the main strategy and application guidelines were characterized in [2.2](#). Here are some main points to consider during life-cycle loads analysis on different levels of the product structure:

- System/product level user and environmental life-cycle loads must be comprehensively disseminated to lower levels of the product hierarchy and propagated to the lowest level of the product structure. The traces of each environmental load or user impact can be found for each subsystem and component. Such traceability of the system level loads to the component and parts of the product is extremely useful for verification of the system level requirements and establishing component level requirements and specifications.
- Besides the impact of system level loads, each subsystem, assembly, and component will be subjected to the gamut of other loads either generated by adjacent subsystems/components or specific user/operator/maintainer intervention that can lead to a negative impact on the system operation or system failure. Excellent tools for propagating, analyzing, and capturing loads and noise factors are functional boundary and parameter diagrams. These tools are described in [2.1](#).
- Using both functional decomposition and the subsystem specification generation process can be very useful for the loads and noise factors propagation and dissemination study. Combining those two work streams can ensure completeness and comprehensiveness of the life-cycle loads analysis at the lowest level of the product hierarchy, thus generating proper specification for parts and components.
- Comprehensive analysis of the life-cycle loads in conjunction with functional analysis and hardware selection process is the basis for the analysis of the potential failure modes and failure mechanisms during FMEA/FMECA tasks. Hence, each understood failure mechanism will have one or many loads or noise factors associated with it.
- Properly disseminated and propagated life-cycle loads at the component level are the key for DVP&R input. They provide traceability to a system level test and requirement verification. Prioritizing loads based on importance and influence at the subsystem level can significantly improve failure mode mitigation and the overall reliability of the system.

2.3.5 Applicable Methods/Submethods

- [Method 3.1](#): Accelerated Testing Methods (such as TAFT, RDGT, HALT, ALT)
- [Method 3.3](#): Benchmarking (Reliability Benchmarking)
- [Method 3.4](#): Block Diagram Development
- [Method 3.13](#): Design of Experiments (DOE) - Classical and Taguchi
- [Method 3.22](#): Failure Mode and Effects/Failure Mode, Effects, and Criticality Analysis
- [Method 3.25](#): Fault Tree Analysis (FTA)
- [Method 3.40](#): Physics of Failure (PoF)
- [Method 3.43](#): Process Failure Modes Effects Analysis/Producibility Analysis
- [Method 3.56](#): Reliability-Centered Maintenance