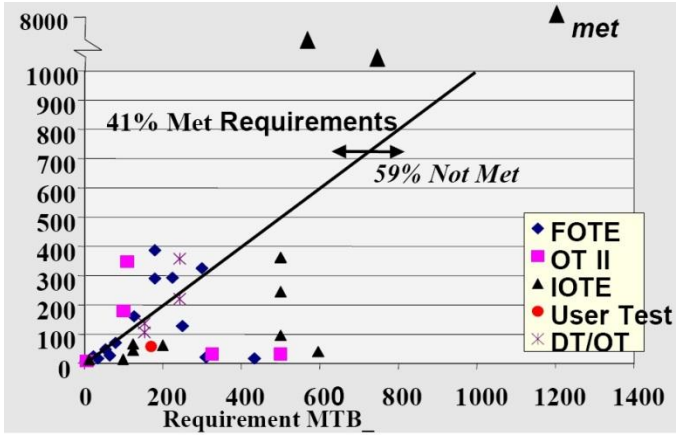
A Recommendation for Specifying Better DoD System Reliability Requirements

David Nicholls, CRE, Reliability Information Analysis Center (RIAC)
Quanterion Solutions Incorporated

15th Annual Systems Engineering Conference
22-25 October 2012
San Diego, CA

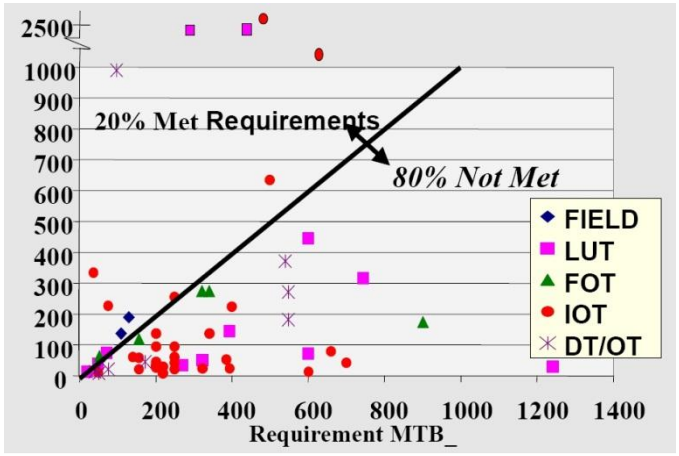
Outline

- Introduction
- Establishing System Design Reliability Requirements (Hypothetical Example):
  - How Good Operational Reliability Requirements Turn Into Bad System Reliability Requirements
  - How to Translate Good Operational Reliability Requirements into Good System Reliability Requirements
- Standardizing the Process
- Conclusions
- Contact Information



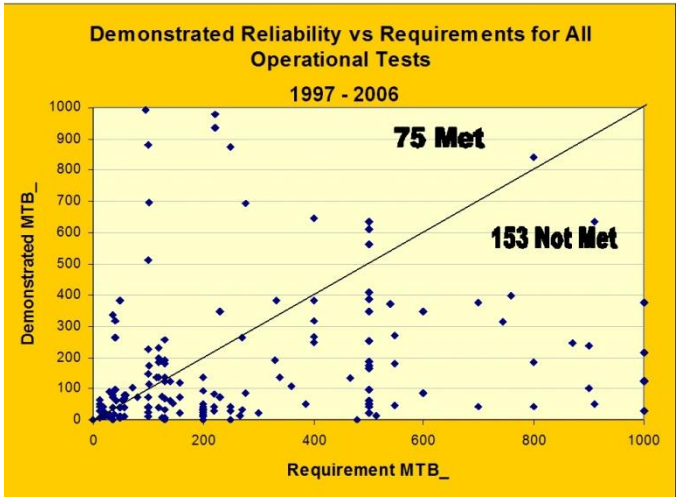
1985-1990

- Demonstrated Reliability vs. Requirements for Operational Tests (DoD RAM Guide)
- Program: MIL-STD-785B



1996-2000

- Demonstrated Reliability vs. Requirements for Operational Tests (DoD RAM Guide)
- Program: MIL-STD-785B (canceled in 1998)
- Commercial Standards IEEE 1332 (1998) and SAE JA1000 (1999)?

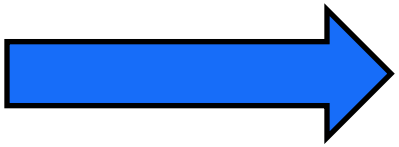


1997-2006

- Demonstrated Reliability vs. Requirements for Operational Tests (Army Systems Only)
- MIL-STD-785B (canceled in 1998)
- Use of IEEE 1332 and SAE JA1000?

Introduction

- The Warfighter Has Critical Operational Reliability Needs
  - "Does Not Care" What Caused a Mission Failure:



  - Inherent hardware (wearout)
  - Hardware quality (random part quality/variability, manufacturing workmanship)
  - Inherent software
  - Induced (maintenance or operator)
  - No defect found/cannot duplicate
  - Inadequate design (e.g., inadequate margins, tolerance stack-up, sneak paths)
  - System management (e.g., requirements issues, insufficient resources)

Introduction

- Failure of DoD Systems to Meet Operational Test and Evaluation (OT&E) Reliability Requirements is Typically Focused on Differences Between Predicted and Observed Reliability
  - Historically blamed on prediction methods
- Objective Analysis Finds Criticism is Misplaced
  - RIAC study of fielded DoD electronic systems (covering ~200 different systems on 9 different fighter/cargo/bomber platforms):
    - 22% of system failures due to random part failures
    - 9% due to wearout
    - 69% due to non-inherent or non-hardware (software) causes
- Debate has Diverted Attention from the Likely Root Cause: Designing to “Bad” System Reliability Requirements
- A More Realistic Process is Needed to Develop Contractual System Reliability Requirements for DoD Systems

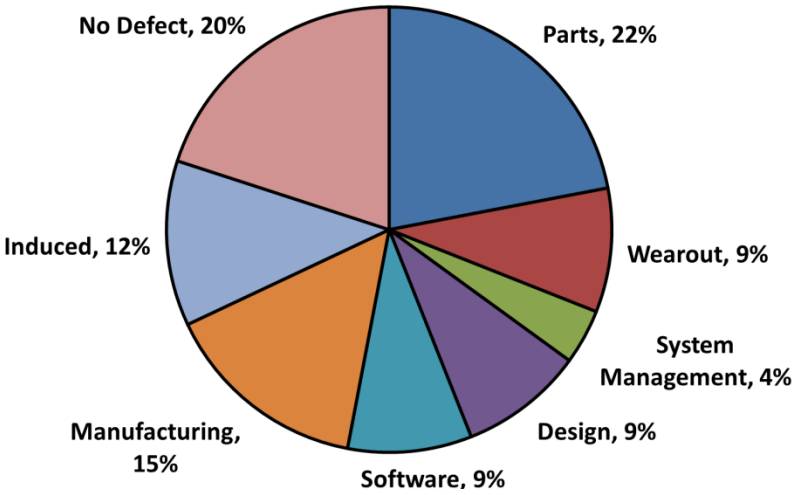
Establishing Reliability Requirements

- Needs of the Warfighter (Hypothetical Example)
  - Warfighter desires an operational MTBF of 100 hours
  - Example basic assumptions (“perfect world”):
    - The operational reliability requirement is realistic and feasible
    - The Warfighter is only concerned that the mission fails, regardless of root cause
    - Any reliability growth planned prior to OT&E is sufficient to ensure compliance with the operational requirement during OT&E
    - If the 100-hour requirement is met in OT&E, then the system is considered compliant

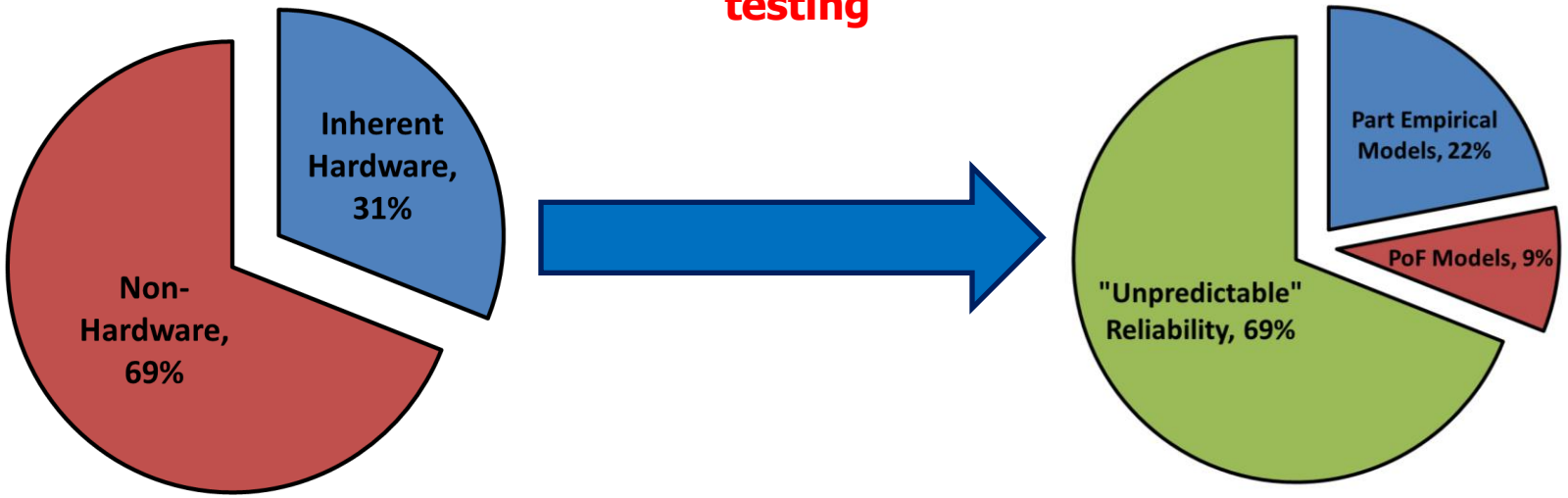
Establishing Reliability Requirements

- Translating Warfighter Needs to Requirements (Hypothetical Contract Language)
  - "…achieve a series configuration MTBF of 100 hours…"
  - "Comparative analyses shall be performed…using field results, similar equipment history, laboratory test data, physics-of-failure (PoF) analysis, data from reliability handbooks (i.e., MIL-HDBK-217, NPRD-2011, etc.), and/or best engineering judgment supported by technical rationale."
- The Systems Engineering Design Approach Taken to Meet Contract Requirements:
  - Use of robust Design for Reliability (DFR) processes
    - Complementary use of empirical and PoF methods
  - Aggressive reliability growth planning and tracking
  - Demonstration of system reliability

How Good Requirements Go Bad



- The system is designed to meet the 100-hour MTBF requirement based on:
  - Inherent hardware design
  - Maybe software design is also considered
- The system reliability prediction of 100 hours is based on empirical models (22%), PoF techniques (9%) and maybe software reliability models (9%)
- The Reliability Growth Planning Curve (RGC) and Testing (RGT) and RDT/RQT are all based on the 100-hour requirement
- **60-70% of potential root failure causes that impact operational MTBF will not be covered by reliability design, analyses and testing**



How Good Requirements Go Bad

- Based on a Robust System Design Approach Using DFR Processes and Reliability Growth Planning/Tracking to Meet the 100-Hour MTBF Requirement…

Failure Category		Original Specified MTBF Reqmt	Contribution to Operational Reliability	Corresponding Operational MTBF
Parts	Inherent Hardware	100 hours	22%	100 hours
Wearout			9%	
System Mgmt	Non-Hardware	N/A	4%	45 hours
Design			9%	
Software			9%	
Manufacturing			15%	
Induced			12%	
No Defect			20%	
TOTAL MTBF			100%	31 hours

- …the Warfighter Will Only "See" a 31-Hour MTBF

How Good Requirements Go Bad

- Impact of the "Bad" Design Requirement:
  - The Warfighter operational reliability requirement of 100-Hours **is not met**
  - A Reliability Growth Curve (RGC) based on the 100-hour goal will be optimistic
    - Risk of insufficient reliability growth/test time
  - Minimum acceptable MTBF for reliability demonstration/qualification test (RDT/RQT) based on a 100-hour requirement will be optimistic
    - Risk of not passing the test

How to Keep Requirements "Good"

- Based on a System Design Using the Same Rigorous DFR Processes and Reliability Growth Planning, What Should the Specified Requirement Have Been?

Failure Category		Original Specified MTBF Reqmt	Contribution to Operational MTBF	Corresponding Operational MTBF
Parts	Inherent Hardware	100 hours	22%	323 hours
Wearout			9%	
System Mgmt	Non-Hardware		4%	145 hours
Design			9%	
Software			9%	
Manufacturing			15%	
Induced			12%	
No Defect			20%	
TOTAL MTBF			100%	100 hours

- The Warfighter Will "See" a 100-Hour MTBF

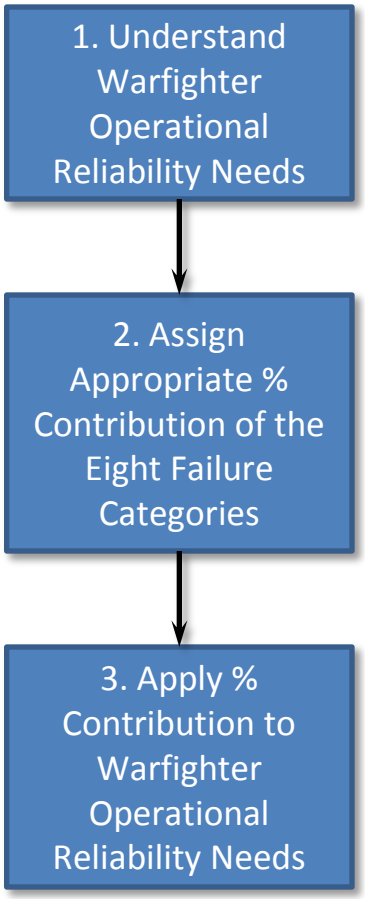
How to Keep Requirements "Good"

- Impact of the "Good" Design Requirement:
  - The Warfighter operational reliability requirement of 100-hours **is met** by the system design
    - Requires the system inherent reliability design MTBF to be 343 hours
      - This is **not** gold plating of the inherent hardware design
  - If the FD/SC is based only on the inherent hardware design, then that same FD/SC would serve as the basis for RGC/RGT
  - If the FD/SC includes all other non-HW factors (145-hour MTBF from Slide 11), then the RGC/RGT and RDT/RQT approaches would be appropriately tailored

Standardizing the Process

- Several Factors Can Influence How "Bad" the Design Reliability Requirements Can Become:
  - Differences in contractual language (HW-only, HW+SW, SW-only)
  - Differences in percent contribution of the eight defined failure categories, influenced by:
    - Different types of equipment
    - Different classes of users
    - Different FD/SC criteria used (initially and as they evolve)
    - Different maintenance skill levels
- A Standardized Process is Needed to Better Specify System Reliability Requirements That Meet Operational Reliability Needs

Standardizing the Process



- Serves as the basis for quantifying a reliability requirement that considers all eight failure contribution categories (HW and non-HW)

a. Obtain/use existing contribution from previous system, or
b. Obtain/use existing contribution from similar system, or
c. Use "informed" engineering judgment
d. Use default values from RIAC Study

- Results in individual (or combined) quantified reliability requirement for each of the eight failure contribution categories (from Slide 11) based on operational reliability needs

Standardizing the Process

- Use the FD/SC for OT&E as the basis for specifying contractual reliability requirements. If unknown, assume that all eight failure categories (and corresponding percent contributions) will be covered by the FD/SC.
- The combination of Steps 3 & 4 defines what categories and corresponding reliability should be specified
  - If only inherent hardware reliability requirements are to be designed to, then the "Inherent Hardware Reliability" value should be contractually specified
  - If both inherent hardware and software reliability requirements are to be designed to, then those values (individually or combined) should be contractually specified
- Requiring root failure cause data collection, analysis and categorization into the eight failure contribution areas provides a means for:
  - Verifying accuracy of the process used to determine the contractual reliability needs on the current program
  - Provides data to support the development of reliability requirements for future acquisitions

Standardizing the Process

- RIAC Spreadsheet Excerpt (different from example):
  - Step 1 (Understand Warfighter Operational Reliability Needs) performed in earlier Worksheets (Based on DoD RAM-C Guide Process)

From Step 1

Hours from the INPUTS AND CALCULATIONS Worksheet

Stated End-User Operational Mean Time Between Failure (Hours)
538

Distribution of Root Failure Cause by Category (Percent)		
Category	Default	User Defined
Parts	22%	0%
Wearout	9%	0%
System Management	4%	0%
Design	9%	0%
Software	9%	0%
Manufacturing	15%	0%
Induced	12%	0%
No Defect	20%	0%
	100%	0%

Minimum Mean Time Between Failure at 50% Confidence

Failure Rate Corresponding to Minimum Mean Time Between Failure at 50% Confidence		Minimum Mean Time Between Failure at 50% Confidence (Hours)
Category	Failure Rate	
Parts	0.00040902	2445
Wearout	0.00016732	5976
System Management	0.00007437	13447
Design	0.00016732	5976
Software	0.00016732	5976
Manufacturing	0.00027887	3586
Induced	0.00022310	4482
No Defect	0.00037183	2689
Failure Rate Total	0.00185916	
Resulting Mean Time Between Failure		538
Meets Stated End-User Operational Mean Time Between Failure at 50% Confidence?	YES	

Grouped Minimum Mean Time Between Failure at 50% Confidence

Failure Rate Corresponding to Minimum Mean Time Between Failure Requirement at 50% Confidence		Minimum Mean Time Between Failure at 50% Confidence (Hours)
Category	Failure Rate	
Inherent Hardware Only (Parts + Wearout)	0.00057634	1735
All Other Categories	0.00128282	780
TOTAL	0.00185916	538
OR		
Software Only	0.00016732	5976
All Other Categories	0.00169184	591
TOTAL	0.00185916	538
OR		
Combined 'Inherent Hardware' and 'Software'	0.00074366	1345
All Other Categories	0.00111550	896
TOTAL	0.00185916	538

Step 2: Define Appropriate Failure Category % Contribution

Step 3: Allocate Warfighter Operational MTBF (Individual and Combined) Based on Step 2

Standardizing the Process

C. Based On Hours from the INPUTS AND CALCULATIONS Worksheet

Stated End-User Operational MTBF (hours)
538

From Step 1

Categories of Failure Definition/Scoring Criteria (FD/SC) to be Used During Reliability Test		
Category	User-Defined Failure Category Distribution	Failures in This Category Will Be Scored During Test (Y/N)?
Parts	22%	Y
Wearout	9%	Y
System Management	4%	Y
Design	9%	Y
Software	9%	Y
Manufacturing	15%	Y
Induced	12%	Y
No Defect	20%	Y
	100%	

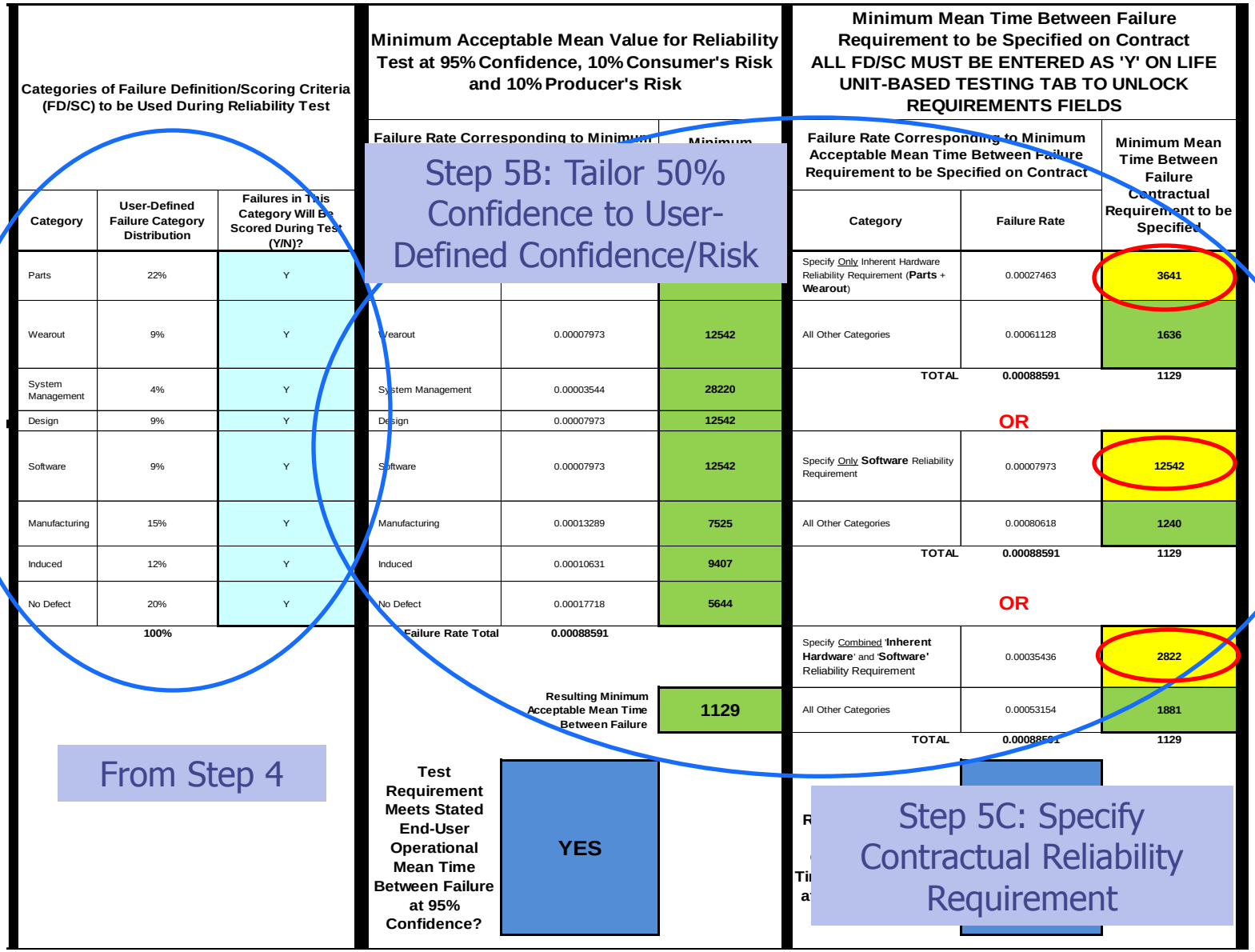
Step 4: Define the FD/SC to be Used

Minimum Acceptable Mean Value for Reliability Test at 50% Confidence Based on User-Defined FD/SC		
	Failure Rate Corresponding to Minimum Acceptable Mean Time Between Failure at 50% Confidence	Minimum Acceptable Mean Time Between Failure at 50% Confidence (Hours)
Category	Failure Rate	
Parts	0.00040902	2445
Wearout	0.00016732	5976
System Management	0.00007437	13447
Design	0.00016732	5976
Software	0.00016732	5976
Manufacturing	0.00027887	3586
Induced	0.00022310	4482
No Defect	0.00037183	2689
Failure Rate Total	0.00185916	
	Resulting Minimum Acceptable Mean Time Between Failure	538

Meets Sta
User Op
Mean
Between
50% Con

Step 5A: Apply FD/SC to Step 3 Results for 50% Confidence Requirements

Standardizing the Process



Categories of Failure Definition/Scoring Criteria (FD/SC) to be Used During Reliability Test

Category	User-Defined Failure Category Distribution	Failures in This Category Will Be Scored During Test (Y/N)?
Parts	22%	Y
Wearout	9%	Y
System Management	4%	Y
Design	9%	Y
Software	9%	Y
Manufacturing	15%	Y
Induced	12%	Y
No Defect	20%	Y
	100%	

From Step 4

Minimum Acceptable Mean Value for Reliability Test at 95% Confidence, 10% Consumer's Risk and 10% Producer's Risk

	Failure Rate Corresponding to Minimum	Minimum
Wearout	0.00007973	12542
System Management	0.00003544	28220
Design	0.00007973	12542
Software	0.00007973	12542
Manufacturing	0.00013289	7525
Induced	0.00010631	9407
No Defect	0.00017718	5644
Failure Rate Total	0.00088591	
Resulting Minimum Acceptable Mean Time Between Failure		1129

Test Requirement Meets Stated End-User Operational Mean Time Between Failure at 95% Confidence? **YES**

Step 5B: Tailor 50% Confidence to User-Defined Confidence/Risk

Minimum Mean Time Between Failure Requirement to be Specified on Contract
ALL FD/SC MUST BE ENTERED AS 'Y' ON LIFE UNIT-BASED TESTING TAB TO UNLOCK REQUIREMENTS FIELDS

Category	Failure Rate Corresponding to Minimum Acceptable Mean Time Between Failure Requirement to be Specified on Contract	Minimum Mean Time Between Failure Contractual Requirement to be Specified
Specify Only Inherent Hardware Reliability Requirement (**Parts** + **Wearout**)	0.00027463	3641
All Other Categories	0.00061128	1636
TOTAL	0.00088591	1129
OR		
Specify Only **Software** Reliability Requirement	0.00007973	12542
All Other Categories	0.00080618	1240
TOTAL	0.00088591	1129
OR		
Specify Combined '**Inherent Hardware**' and '**Software**' Reliability Requirement	0.00035436	2822
All Other Categories	0.00053154	1881
TOTAL	0.00088591	1129

Step 5C: Specify Contractual Reliability Requirement

Standardizing the Process & Recommendations

Step 6: Place Data Requirements on Contract

- Contractually Impose Requirements for Collection/ Analysis of Data & Classification of Failures Based on Standardized "Failure Cause" Definitions
- Ensure Government Access to Appropriate Details of Data Generated Over the System Life Cycle, Down to Root Failure Cause, if Possible
- Recommendations – the DoD should:
  - Gain a Better Understanding of All Eight Root Failure Cause Categories Through Data Collection/Analysis
  - Gain a Better Understanding of Current Prediction Methodology Benefits/Limitations & How They Relate to Failure Categories
  - Support Development of System Reliability Assessment Methods That Address All Hardware & Non-Hardware Failure Categories

Conclusions

- The Root Cause of Systems Not Meeting Operational Reliability Requirements (and the Differences Between Predicted and Observed MTBF) is:
  - "Good" operational reliability requirements that are translated to "bad" specified system design reliability requirements
- A Formal Process was Presented that Allocates Contractual Reliability Requirements Based on Eight "Real World" Failure Categories that Impact Operational Reliability
- Recommendations were Provided to Improve the DoD Acquisition Process for Reliable Systems

Contact Information

- David Nicholls, CRE
  Reliability Information Analysis Center (RIAC)
  Quanterion Solutions Incorporated
  100 Seymour Rd, Suite C101
  Utica, NY 13502-1311
  Ph: 315.351.4202
  Fax: 315.351.4209
  Email: dnicholls@theRIAC.org