Raytheon

Customer Success Is Our Mission

Reliability Influenced Requirements for T&E Success

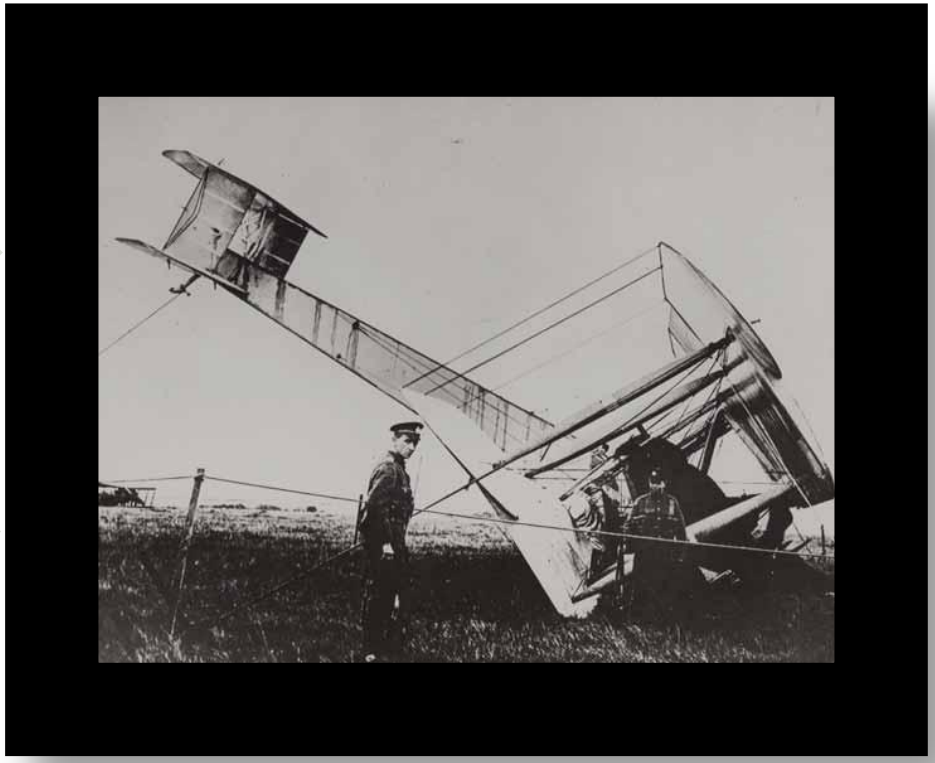
Lou Gullo
Raytheon Missile Systems
Senior Principal Engineer
March 12, 2012

ENGINEERING, TECHNOLOGY & MISSION ASSURANCE

How Do You Know When You Don't Have Good System Reliability Requirements?

Caused by System Failure?

Caused by Poor Requirements?



Caused by Operator Error?

Shot Down by Enemy?

(source: Curtiss-Wright Controls)

Introduction

- How to Influence the Requirements?
- Implicit vs Explicit System Reliability Requirements
- 12 Questions from the National Academy of Science (NAS) Workshop (Sep '11)
  - Design for Reliability (DfR) Requirements Questions Such As:
    - How is/should DfR requirements be presented in proposals
    - How is reliability initially assessed
    - What data are available at the outset for this purpose
    - How are reliability assessments updated (tracked) during development – at the component, subsystem, and system levels
  - Reliability Growth Requirements Questions Such As:
    - What use is made of reliability growth modeling
    - How should reliability growth be specified in the acquisition / RFP process
    - Is the variability of reliability growth modeling assessed and does that assessment play a role in any such decision-making
    - How are software components treated differently in reliability growth or reliability growth modeling, or are they
  - Reliability Management and Test Process Questions
- Responses Provided for Each Question

How to Influence the Requirements?

1. System level requirements and decomposition

- Requirements may be generated for the benefit of reliability without actually stating reliability or related reliability metrics in the requirement language. These are implicit versus explicit reliability requirements.
- The top-level system requirements and functions are apportioned, flowed-down, decomposed and/or allocated to hardware and software designs.
  - Determine the lowest level for hardware and software requirements.
  - Determine the levels for specifications in between top and bottom
- System failure modes are identified and prevented by generation of certain types of requirements, which could be reflected in reliability measures, metrics, and assessment results.

System Reliability Requirements

- Implicit
  - Built-In-Test (BIT)
  - Fault Tolerance
  - Redundancy
  - Design Margin
  - Derating
  - Stress Analysis
  - Prognostics and Health Management (PHM)
  - Condition Based Maintenance (CBM)
  - Performance Based Logistics (PBL)
- Explicit
  - Reliability
  - Availability
  - MTBF or MTTF
  - Failure rate or hazard rate
  - Reliability Growth
  - Design for Reliability (DfR)
  - Reliability Testing
  - Failure Modes Effects and Criticality Analysis (FMEA)
  - Failure Reporting Analysis and Corrective Action System (FRACAS)

How to Influence the Requirements?

2. Failure identification and handling

- Detailed reliability analyses are conducted that are relevant to system engineering and design risk assessments.
- These analyses, such as Functional Design Failure Modes Effects Analysis and Failure Modes Effects and Criticality Analysis (FMEA/FMECA), utilize the risk assessment metrics (e.g., probability of occurrence and severity of the effect or event) as inputs to their processes.
- The output from a FMEA/FMECA provides (1) a list of high risk functions that require risk mitigation, and (2) a list of functions whose risks are mitigated by low probability of occurrence and/or low effect severity.

How to Influence the Requirements?

3. Design feedback loop and reliability improvements

- The feedback loop involves learning about the system, hardware and software design, mitigating the risks of failures, and increasing the design strength.
- For example, in performing an FMECA, the system may operate as designed, but fails to meet customer expectations and top level performance requirements.
  - This type of failure is a requirement defect, which may be caused by:
    - incomplete top level requirements
    - incorrect decomposition of requirements
    - This type of defect is a frequent cause of mission-critical software failures.
  - By uncovering these defects early, cost savings are gained and reliability improves.

Questions (1-5) from NAS Workshop

1. What is meant by design for reliability (DfR)?
2. How is/should DfR be represented in proposals in terms of specific actions to take to improve reliability over time?
   a) How should reliability growth be specifically requested in the acquisition / RFP process and artifacts via requirements and/or technical performance measures?
   b) To what extent should the RFP dictate that the different services and support contractors use similar methods and tools to specify, track, and evaluate reliability on programs?
   c) How should these methods and tools be articulated in the RFP, TEMP, or SEP?
3. How is reliability initially assessed, and what data are available at the outset for this purpose?
   a) If data are primarily available at the component level, how are component-level estimates combined to estimate system-level reliability?
   b) Is information for components mainly from MIL HDBK 217-type sources or through engineering analyses?
   c) How are differences between DT environments and operational profiles accounted for?
4. How are reliability assessments updated (tracked) during development – at the component, subsystem, and system levels?
   a) Is this through engineering analyses, M&S, developmental testing, or operational testing?
   b) How is the adequacy of reliability growth in the early and middle phases of development judged, e.g. for transitioning to the next phase of testing?
   c) Again, how are differences between DT environments and operational profiles accounted for?
5. With respect to testing, what use is made of accelerated life testing and other specific types of reliability tests that are focused on issues like fatigue for finding failure modes and/or for formal input into reliability growth models?

Questions (6-12)

6. With respect to the collection of data: (a) at what level of aggregation is data on reliability retained, (b) what other related information is linked to it, (c) how long is it saved, and how accessible is it? (d) Is this data set made available to the government?
7. What use is made of reliability growth modeling? If it is used, at what point is it initiated, what are the typical inputs to these models, are they initially implemented for tracking purposes at the component level or the full system level, and does that change through development? Is the variability of reliability growth modeling assessed and does that assessment play a role in any such decision-making?
8. Is the delivery of subsystem or system prototypes to the government dependent on reliability projections from such models? If so, how?
9. How much is the human interface accounted for in contractor DT? Is it clear why performance is so dramatically different between DT and OT?
10. How are software components treated differently in reliability growth or reliability growth modeling, or are they?
11. How do you decide how to allocate testing resources to a system with several subsystems and with varying degrees of uncertainty about the reliability of each? And how do you decide what types of testing and how much testing to use, including M&S, accelerated testing, testing with expert users, testing with military personnel, etc.?
12. What sorts of reliability management processes, including formal reliability reviews and approvals, are defined, and what priority is/should be given to reliability vice schedule, costs, etc.?

Question 1

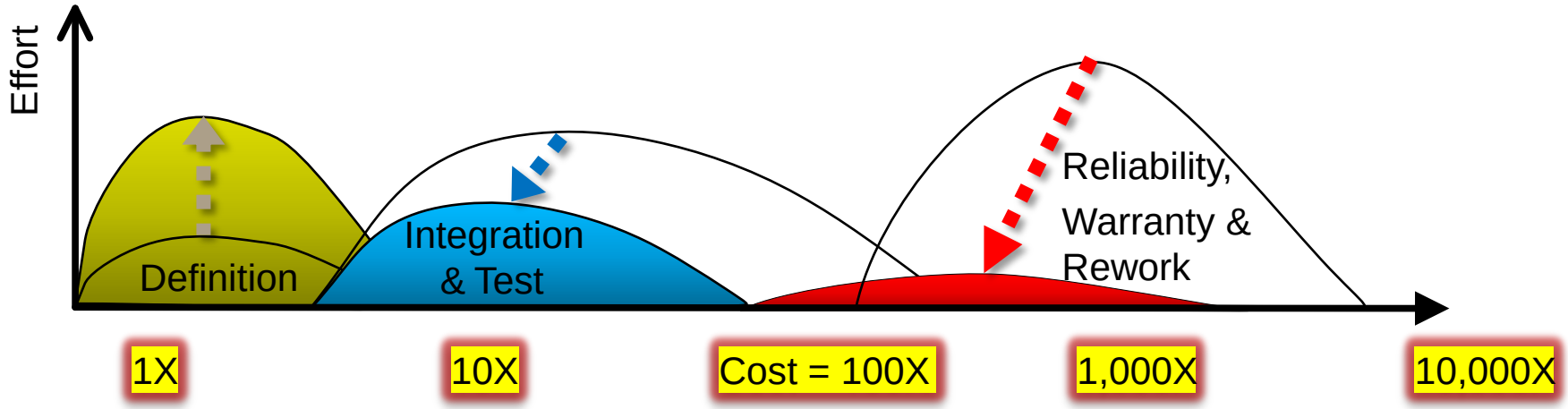
What is meant by Design for Reliability (DfR)?

Response to Question 1 - DfR Process

- Design process includes reliability and design engineering activities/tasks to ensure system or product achieves the reliability specifications or goals.
- Reliability must be designed into the system.
- Design for Reliability (DfR) does not necessarily include reliability growth nor does it require analysis of reliability metrics (e.g. Mean-Time-Between-Failure (MTBF), failure rate, Rate of Occurrence of Failure (ROCOF), etc.).
- During the design trade space in development, DfR requires identification and mitigation of design weaknesses, detection and resolution of mission critical failures, characterization of design margins and continuous design improvements to decrease failures in the field/fleet and reduce Total Cost of Ownership (TCO) over the system/product life cycle to the End of Life (EOL).

Shift Reliability Effort to the Left

- Early Implementation of Design for Reliability (DfR) and Reliability Growth results in cost savings in the O&S phase
- Benefits Realized with Lower Total Cost of Ownership (TCO)
- $1 spent at the Requirements Development Stage is equivalent to $10 spent at the I&T stage which is equivalent to $100 spent at the initial production stage



Question 2

How is/should DfR be represented in proposals in terms of specific actions to take to improve reliability over time?

a) How should reliability growth be specifically requested in the acquisition / Request for Proposal (RFP) process and artifacts via requirements and/or technical performance measures?

b) To what extent should the RFP dictate that the different services and support contractors use similar methods and tools to specify, track, and evaluate reliability on programs?

c) How should these methods and tools be articulated in the RFP, Test and Evaluation Master Plan (TEMP), or System Engineering Plan (SEP)?

Response to Question 2

- Top-level specification and the contract should specify the system or product reliability requirement, such as a Key Performance Parameters (KPPs), Key System Attributes (KSAs), the reliability engineering activities performed during system/product development, and the means to verify and validate the reliability requirement.
- Reliability growth management as part of DfR represented in proposals is a way to specifically require actions to improve reliability over time with reliability assessment of standard reliability metrics over the system/product life cycle, starting early in the development phase.

Response to Question 2, part a

- The acquisition / RFP should request that the contractor write a Reliability Growth Management Plan (RGMP) and Reliability Growth Test Plan (RGTP) as part of the Integrated Test Planning.
- The acquisition / RFP should include a reliability growth incentive award scale and incentive fee scheduled during intervals in the development cycle so that the contractor is rewarded for favorable reliability growth that exceeds customer expectations.
- Purpose of reliability growth management planning is to develop reliability growth curves for the system, major subsystems, products and assemblies with the plan for achieving specified reliability values.
- RGMP includes reliability assessments and a RGTP that contains types of testing (e.g. Accelerated Life Tests, Highly Accelerated Life Tests), adequate test time in the program schedule, and test samples to demonstrate increasing reliability with increasing confidence over time.
- RGMP provides a means for tracking reliability growth from system level to assembly or configuration item level, and monitoring progress of the RGTP.
- The RGTP includes intervals in the development phase to allow for implementation of design change corrective actions to positively affect reliability with each subsequent design modification.

Response to Question 2, part b

- The RFP should require the different services and support contractors for each major subsystem to provide a Reliability Growth Profile (RGP) using a standard process which can be implemented by a number of approved tools.
- Standard process and tool are used to integrate the inputs from the different services and support contractors' RGPs for a particular system/product and provide standard reporting outputs to program management to verify and validate the reliability growth curve for the particular program.
- The tool should be used to plot reliability growth curves for each major subsystem that shows the following:
  - The expected starting point (initial reliability) with the context in a separate document that supports the data sources and the rationale for its selection
  - The number of tests planned during the development program to be used to verify that starting point
  - The expected reliability growth profile with the context in a separate document that supports the data sources and the rationale for the selection of the points on the graph
  - The number of tests needed to produce that profile, the schedule for these tests and the schedule for implementing design change corrective actions for the failures that are expected to occur, resulting in design reliability improvements.
  - A risk assessment should be performed for the starting point, reliability growth profile, and number of tests necessary to meet the required reliability levels on the growth curve.

Response to Question 2, part c

- The government acquisition / RFP, and TEMP or SEP should require contractors to provide a Reliability Growth Management Plan (RGMP), Reliability Growth Test Plan (RGTP) as part of the Integrated Test Plan, and Reliability Growth Profile.
- Raytheon applies process, tools and methods to meet these requirements.

Question 3

How is reliability initially assessed, and what data are available at the outset for this purpose?

a) If data are primarily available at the component level, how are component-level estimates combined to estimate system-level reliability?

b) Is information for components mainly from MIL HDBK 217-type sources or through engineering analyses?

c) How are differences between Development Test (DT) environments and operational profiles accounted for?

Response to Question 3

- Reliability is initially assessed using a combination of 4 data sources.
- The sources of data for initial reliability assessments include field/fleet data sources, test data sources, supplier data sources, and handbook methods (e.g. MIL-HDBK-217, SR-332, etc).
- Supplier data includes stress derating curves and application notes to assist designers in correct electrical part application in circuit schematics. Many failures are due to misapplication of parts and part overstressing, and these failures are mitigated using derating curves early in development.
- Much of the data collected from these data sources are contained in our standard tools (e.g. ASENT and PTC Relex).

Response to Question 3, parts a-c

a) Component-level data from field/fleet sources, test sources, and supplier sources are not always readily available. If data from these various sources are available, they are collected, analyzed and combined using standard tools to calculate system failure rates.

b) Component-level test and design analysis data are combined with calculated component failure rates using handbook methods (e.g. MIL-HDBK-217, SR-332, etc). Engineering analysis information for components from designers are used for electrical and mechanical stress analysis calculations, finite element analysis (FEA), thermal analysis, and reliability assessments.

c) DT environments and operational profiles are accounted for in the selection of pi factors used in the component models from the handbook methods (e.g. MIL-HDBK-217, SR-332, etc). Also, we use MIL-HDBK-338, Electronic Reliability Design Handbook.

Question 4

How are reliability assessments updated (tracked) during development – at the component, subsystem, and system levels?

a) Is this through engineering analyses, Modeling and Simulation (M&S), developmental testing, or operational testing?

b) How is the adequacy of reliability growth in the early and middle phases of development judged, e.g. for transitioning to the next phase of testing?

c) Again, how are differences between DT environments and operational profiles accounted for?

Response to Question 4

- Reliability assessments are updated (tracked) during development at each level of indenture, starting with top-down reliability allocations and apportionments, then with bottom-up reliability assessments/predictions to verify allocations/apportionments.
- The verification may be performed through analysis or testing.
- The verification process involves updates to the reliability assessments from the top-down or from the bottom-up depending on the modeling approach employed (e.g. Model-Based Systems Engineering, System-Level Operational and Supportability Models, Reliability Block Diagrams, Physics of Failure Models, Finite Element Models, etc).

Response to Question 4, parts a-c

a) Results from engineering analyses and M&S are validated through contractor and developmental testing. The DT data collected are made available for independent analysis supporting Operational Test (OT).

b) Adequacy of reliability growth is judged by satisfactory execution of tasks to meet milestones planned on the Integrated Master Schedule (IMS). The IMS will define the build release dates to incorporate design changes that result in reliability improvements that correlate to the points plotted on the reliability growth curve. The achievement of the reliability growth objectives are determined by satisfactorily meeting or exceeding the reliability metrics plotted over time on the curve allows transitioning to the subsequent phases of testing.

c) Raytheon strives to model the DT environments after the operational profiles using a service use profile, as much as possible. Operational profiles are accounted for in the selection of DT verification methods that may be performed through analysis or testing. Particular operational profiles cannot be performed using DT test verification. In these cases, DT verification by analysis is used in lieu of testing.

Question 5

With respect to testing, what use is made of accelerated life testing and other specific types of reliability tests that are focused on issues like fatigue -- for finding failure modes and/or for formal input into reliability growth models?

Response to Question 5

- Accelerated Life Testing (ALT) and Highly Accelerated Life Testing (HALT) are used to focus on issues like fatigue, damage index, acceleration factors and the precipitation and detection of design weaknesses caused by failure mechanisms and failure modes.
- The data collected from these test sources are used to provide input into the reliability growth models, as previously mentioned in the responses to questions 3 and 4 above.
- Raytheon conducts development testing for fatigue on new designs through multiple design engineering activities, which are not explicitly identified as reliability tests.

Question 6

With respect to the collection of data:

a) at what level of aggregation is data on reliability retained,
b) what other related information is linked to it,
c) how long is it saved, and how accessible is it?
d) Is this data set made available to the government?

Response to Question 6, parts a-d

a) Reliability data are retained from system level to component level, where the data are available, collected and analyzed.

b) Reliability data may be linked to environmental conditions, stress conditions, operational or non-operational conditions, operational profiles, pedigree of the data (e.g. system type, part no, serial no), time to failure, time since deployment/shipment, time since last recertification, etc.

c) Raytheon has a standard policy for records retention. Reliability data are maintained for a period of time specified in the policy, which is "delivery of product plus 10 years". The data may be collected by the government and removed from contractor responsibility. Reliability data may be classified with access restricted. Accessibility varies from program to program. Accessibility is usually specified in the contract.

d) Yes, the data set is made available to the government

Question 7

What use is made of reliability growth modeling --- If it is used, at what point is such modeling initiated, what are the typical inputs to these models, are they initially implemented for tracking purposes at the component level or the full system level, and does that change through development?

a) Is the variability of reliability growth modeling assessed and does that assessment play a role in any such decision-making?

Response to Question 7

- The answer is highly dependent on the customer requirements, the type of system and type of contract. Some contracts tie incentive fees or award fees to reliability performance and growth.
- The purpose of reliability growth modeling is to provide an assessment of the demonstrated reliability of the system or product at that time.
- Reliability growth modeling is used to plan phases of development, which involves adding design features to the baseline system or subsequent versions of the system, as the system becomes mature and demonstrates the reliability requirement.

Response to Question 7, part a

- Variability of the reliability growth model for a particular program would be assessed if the system design experiences requirements volatility and extensive changes during the development cycle.
- The changes to the design could affect the system reliability so that the requirements are no longer valid, the reliability growth model is incorrect, and a decision would be made to update the reliability growth model and curve to reflect the future state of the design.
- Design changes may involve an Engineering Change Proposal (ECP) which includes updates to the reliability requirements.
- Early in development, the model changes as we collect data and better understand system performance. In the later phases of development, the model becomes stable and credible, however, it may still evolve as the design changes via FRACAS. Reliability and performance assessments during the RDGT determine whether the reliability requirements are met or if design changes are necessary. If the design does not change after the design is stable and characterized, the model is constant.

Question 8

Is the delivery of subsystem or system prototypes to the government dependent on reliability projections from such models?

a) If so, how?

Response to Question 8, and part a

- The answer is dependent on the situation. There are cases when the prototype is not dependent on reliability projections. If the new system performance is superior to the Program of Record (POR) system as demonstrated in Tech Demo, as an example, an 80% reliable system may suffice for a 95% requirement, given more spares and the allowance of future design enhancements to improve reliability.
- Some contracts require the prototypes to demonstrate reliability, such as a KPP or KSA. If the prototype does not demonstrate the reliability requirement, design changes could be necessary before the prototypes are shipped.

  a) As an example, if test development on a particular program conducts a test that results in detection of a failure mode that is probabilistic in nature, with a potential of a mission critical failure effect, a risk assessment may be performed that warrants a design change before the system is delivered to the government.

Question 9

How much is the human interface accounted for in contractor DT?

Response to Question 9, and parts a-b

- Human interface is accounted for in contractor DT using Raytheon employees, government and contractor personnel with the mix of test resources depending on the system, contract and the program. The human interface is a major part of the DT planning and execution.

  a) Raytheon involves military service members when required by contract, or when possible, we design our DT&E events to use real operators to perform DT operational environments prior to OT. Contracts usually require military involvement on specific integrated test activities, such as Reliability Qualification Tests (RQTs) and Maintainability Demonstrations (M-Demos).

  b) **Raytheon philosophy is "Test as you Fly".** There should be no difference between DT and OT in human performance and the design of the human interface. When there are differences, training, operator experience, selection of test criteria and test scenarios, and familiarity with equipment are some of the factors. Defense contractors can minimize the differences with operationally relevant testing.

Question 10

How are software components treated differently in reliability growth or reliability growth modeling, or are they?

Response to Question 10

- New start programs with large software content are considering software reliability and reliability growth.
- Some programs treat software components as part of the system, along with the hardware components. System Reliability requirements are flowed down or decomposed to the components, software and hardware.
- Many reliability growth attributes (e.g. MTBF vs Time, Defect Density vs Time, Test Analyze Fix, Design Change vs Time, Test Coverage vs Time), applied to hardware can also be applied to software.
- Following a spiral development process, software design features are added to software components in the baseline system or subsequent versions of the system. As the system becomes mature, software testing demonstrates the reliability requirements along a growth curve with each software build release.

Question 11

How do you decide how to allocate testing resources to a system with several subsystems and with varying degrees of uncertainty about the reliability of each?

a) How do you decide what types of testing and how much testing to use, including M&S, accelerated testing, testing with expert users, testing with government personnel, etc.?

Response to Question 11

- Test resources are planned during the proposal stage and included on the IMS after contract award. A risk assessment is conducted during the proposal to ascertain which subsystems require test resources. The maturity, performance history and degree of uncertainty about the reliability of each subsystem are considered in the risk assessment and factored into the program plans. The program executes the test resource plan in accordance with the IMS.
- For example, mature Commercial Off-The-Shelf (COTS) subsystems are tested, but require fewer resources than new design subsystems. The maturity of the COTS must be considered and assessed against the Technology Readiness Level (TRL levels) definitions.

Response to Question 11, part a

- Raytheon follows the Integrated Product Development System (IPDS) for system and product development which includes use of various types of M&S, tests and analyses.
- IPDS enablers promote M&S and test planning to include integrated testing. M&S is integrated with testing for mission profile use case testing when actual hardware and in-service applications are not available.
- Through requirements analysis, test plans are created, with a requirements verification cross-reference matrix. This matrix includes verification by analysis, test, demonstration, or inspection. Design of Experiments (DOE) may be used to select the types of M&S (e.g. ProE and PSPICE), tests and quantity of tests.

Question 12

What sorts of reliability management processes, including formal reliability reviews, and what priority is/should be given to reliability vice schedule, costs, etc.?

Response to Question 12

- Raytheon's IPDS defines our management process.
- Reliability is an element of all milestone reviews.
  - Reliability is assessed early in development and at every major gate review (e.g. SFR, PDR, CDR, etc) in IPDS, and a reliability output products are independently reviewed at each gate.
- Many reliability tasks result in reliability management plans, procedures and reports that are internally peer reviewed, and some may be formally reviewed by customers.
- Some contracts put high priority on the reliability and performance of the system compared to cost and schedule.

Questions

Acknowledgements from Raytheon

- Thanks to the following Raytheon individuals who provided responses which were integrated with my responses:
  - Carla Head, R Miguel Peterson, Phil Conde and Gary Bolla
- Thanks to the following Raytheon individuals who provided peer reviews of the integrated responses
  - Brian Wells, Ray Lytle, Jeff Thomas, Beth Wilson, Jonathan Green, Louisa Guise, Paul Shedlock, Roger Abbott, and Martin Woznica

Biography

– **Lou Gullo,** Raytheon Missile Systems, Engineering Product Support Directorate (EPSD), Reliability Engineering Department located in Tucson, AZ. Leader of several Enterprise-wide Engineering Council-sponsored special projects including IEEE reliability standards development, software reliability methods and the automation of electrical stress analysis methods. 30 years experience in military, space and commercial programs. Retired US Army Lieutenant Colonel. Senior Member of the IEEE. IEEE Reliability Society Standards Committee Chair. Member of the Reliability and Maintainability Symposium (RAMS) Management Committee.

Louis J Gullo
Sr Principal Systems Engineer
Lou.Gullo@Raytheon.com
520-746-2392