Is the Cost of Reliability, Maintainability, and Availability Affordable for Software Intensive Systems?

Presented to
IEEE Software Technology Conference
Long Beach, CA

Myron Hecht
April, 2014
Outline

• Consideration of RMA in Systems Acquisition is Required by Law
• New Policies Have Been Created
• Investment in RMA Pays Off
• Reliability Best Practices Have Been Established
• Methods for Calculating Operation and Sustainment Costs Have Been Created
• Tools for Reliability Analysis, Evaluation, and Tracking Exist
  – And advanced tools are being developed
• So What’s the Problem?
• Conclusions
Consideration of RMA in Systems Acquisition is Required by Law

• Public Law 111-123 “Weapons System Acquisition Reform Act of 2009,” Section 102 (codified as 10 USC 4 Section 139d)
  – (b) Director of Systems Engineering-
  – (1) APPOINTMENT- There is a Director of Systems Engineering, who shall be appointed by the Secretary of Defense from among individuals with an expertise in systems engineering and development planning.
  – . . .
  – (5) DUTIES- The Director shall—
    – ``(A) develop policies and guidance for—
    – ``(i) the use of systems engineering principles and best practices, generally;
    – ``(ii) the use of systems engineering approaches to enhance reliability, availability, and maintainability on major defense acquisition programs;
    – ``(iii) the development of systems engineering master plans for major defense acquisition programs including systems engineering considerations in support of lifecycle management and sustainability; and
    – ``(iv) the inclusion of provisions relating to systems engineering and reliability growth in requests for proposals;
New Policies Have Been Created

• CJCSI 3170.01, “Operation Of The Joint Capabilities Integration And Development System,” May, 2007
  – Materiel Availability and Operational Availability as Key Performance Parameters (KPPs)
  – Reliability and Ownership Costs as Key System Attributes

  – PMs for all programs shall formulate a viable Reliability, Availability, and Maintainability (RAM) strategy..... RAM
    • shall be integrated within the Systems Engineering processes,
    • documented in the program’s Systems Engineering Plan (SEP) and Life-Cycle Sustainment Plan (LCSP), and
    • assessed during technical reviews, test and evaluation (T&E), and Program Support Reviews (PSRs).

*superseding 2008 version
Growth of Software Content in DoD Weapons Systems

## Growth of Software Importance in USAF Aircraft

<table>
<thead>
<tr>
<th>Platform</th>
<th>Year</th>
<th>% Functions Controlled by Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>F-4</td>
<td>1960</td>
<td>8%</td>
</tr>
<tr>
<td>A-7</td>
<td>1964</td>
<td>10%</td>
</tr>
<tr>
<td>F-111</td>
<td>1970</td>
<td>20%</td>
</tr>
<tr>
<td>F-15</td>
<td>1975</td>
<td>35%</td>
</tr>
<tr>
<td>F-16</td>
<td>1982</td>
<td>45%</td>
</tr>
<tr>
<td>B-2</td>
<td>1990</td>
<td>65%</td>
</tr>
<tr>
<td>F-22</td>
<td>2000</td>
<td>80%</td>
</tr>
</tbody>
</table>

Investment in RMA Pays Off

- Operations and Support make up 65-80% of the lifecycle cost
- (Predator, Global Hawk, FBCB2) cited as showing Return on Investment of Reliability Improvement of 5:1 to 128:1
- DLA Study of 10-year return of 15.5:1

Reliability Best Practices Have Been Established

Methods for Calculating Operation and Sustainment Costs Have Been Created

- **Expected number of failed items**

  \[ L = p_o \cdot \left[ \sum_{i=0}^{c-1} (c-i) \cdot \frac{n!}{i!(n-i)!} \cdot \left( \frac{\lambda}{\mu} \right)^i \right] + 1 \cdot \frac{1}{c!} \cdot \left[ \sum_{i=0}^{c-1} i \cdot \frac{n!}{i!(n-i)!} \cdot \frac{1}{c^{i-c}} \left( \frac{\lambda}{\mu} \right)^i \right] \]

- **Time waiting to start repair**

  \[ W_q = \frac{L_q}{\lambda \cdot (n-L)} \]

- **Unavailability**

  \[ U = \frac{MTTR + W_q}{MTBO_{unsched} + MTTR + W_q} \]

Number of items awaiting repair

\[ L_q = L - c + p_o \cdot \left[ \sum_{i=0}^{c-1} (c-i) \cdot \frac{n!}{i!(n-i)!} \cdot \left( \frac{\lambda}{\mu} \right)^i \right] \]

- **Unavailability**

  \[ U = \frac{MTTR + W_q}{MTBO_{unsched} + MTTR + W_q} \]

L = number of items waiting to be fixed

\( W_q \) = waiting time for items to be fixed

\( p_o \) = probability of an empty queue

\( U \) = unavailability

\( MTTR \) = mean time to repair

\( MTBO \) = mean time between outages

Tools for Reliability Analysis, Evaluation, and Tracking Exist

- General Math / Statistics
- Maintainability
  - Design
    - Human Factors
    - Maintenance Concept
    - Not Otherwise Categorized
  - Other
  - Prediction
    - Detection
    - MTTR
    - Not Otherwise Categorized
  - TQM
- Quality
  - ISO-9000
  - Manufacturing
  - Not Otherwise Categorized
  - Other
  - Statistical Process Control
- Reliability
  - Availability
    - Components
      - Applications
        - Mechanical
      - Data
        - Discrete
      - Other
        - Passive
    - Design / Analysis
      - De-rating
      - Failure Analysis
      - Finite Element Analysis
      - FME(C)A
        - Design
        - Process
      - FRACAS
      - FTA
      - Markov
      - Mechanical
      - Modeling / Simulation
        - RBD
      - Other
      - Parts Control
  - EOS / ESD
    - Susceptibility
  - Non-operating
  - Prediction
    - Bayesian
    - CNET
    - Mechanical
    - MIL-HDBK-217
    - Non-operating
    - Other
    - 217
    - Telcordia (Bellcore)
- Risk
- Supportability
  - Life Cycle Cost
  - Logistics
    - Data
    - Maintenance Concept
  - Other
  - Spares
  - Referral
  - Warranty
- Thermal Analysis
- Weibull
- Software Reliability
- System
- Data
- Testing
  - Accelerated Life
  - Source: The Reliability Information Analysis Center, Software Tools Page
  http://www.theriac.org/informationresources/softwaretools.html
…and advanced tool sets are being developed

Model Driven Design and Analysis Tool Set
(Aerospace Corp)

Architecture and Error Models

Stochastic Network Model

Results

On-Orbit Operating Hr

Bus Computer Uptime

Payload Computer Uptime

Software Recovery Time (Hours)
...and advanced tool sets are being developed

**ASSERT* (European Space Agency)**

- **Source**
  - European Space Agency and Collaborating Tool Developers
- **ESA Autonomous Transfer Vehicle Control System Development Example**
  - Specify arbitration logic
  - Define finite state machine (using SDL)
  - Verify (check for exceptions, deadlocks, stop conditions)
  - Autogenerate code
  - Deploy on runtime environment

* Automated proof-based System and Software Engineering for Real-Time applications

http://www.assert-project.net
So What’s the Problem?

• Programs not managing to requirements
• Lack of incentives
  – *RMA Efforts have costs*
    • Impact on design
    • Impact on cost and schedule
    • Addition of uncertainty – particularly if RMA group is less competent than Government oversight
  – *No discernible benefit*
    • Insufficient EVM and cost accounting techniques
• Programmatic Attention Elsewhere
• Poor Systems Engineering

What to do

• Accurate Valuation Of RMA-related Benefits As Well As Costs In DoD Affordability Initiatives
• Effective Earned Value Tracking Of RMA Engineering Tasks
• Early and Frequent Feedback From RMA Into The Design And Implementation Activities
Valuation Of RMA-related Benefits As Well As Costs In DoD Affordability Initiatives

• Cost:
  – NRE in engineering and analysis

• Benefits
  – Greater operational or mission effectiveness
  – Fewer units required (fleet availability is higher when unit availability is higher)
  – Smaller sustainment organization
  – Lower spares inventory and logistics costs
Accurate Earned Value Tracking Of RMA Engineering Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Program Milestone Review</th>
<th>Proportion of Earned Value*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability Program Plan</td>
<td>System Requirements Review (SRR)</td>
<td>5%</td>
</tr>
<tr>
<td>Reliability/Availability Allocations</td>
<td>System Design Review (SDR)</td>
<td>5%</td>
</tr>
<tr>
<td>Preliminary Reliability Predictions and Failure Modes and Effects Analysis (FMEA)</td>
<td>Preliminary Design Review (PDR)</td>
<td>5%</td>
</tr>
<tr>
<td>Final Reliability Models Predictions and FMEA</td>
<td>Critical Design Review (CDR)</td>
<td>20%</td>
</tr>
<tr>
<td>Failure Reporting and Corrective Action System (FRACAS)</td>
<td>Test Readiness Review (TRR)</td>
<td>10%</td>
</tr>
<tr>
<td>Life, Stability and Failure Recovery testing (may be part of Day in the Life Testing) and Maintainability Testing Complete</td>
<td>Functional Configuration Audit (FCA)</td>
<td>30%</td>
</tr>
<tr>
<td>Requirements Verification Complete</td>
<td>Physical Configuration Audit (PCA)</td>
<td>25%</td>
</tr>
</tbody>
</table>

*notional values, actual values should be program specific
Recommended RMA Activities in a Software Intensive Development Program

- Definition of Degraded Modes, Acceptable Outage Durations, Maintenance Concepts
- R&M Testing (incl. SW)
- Redundancy, Failure Containment, Degraded Modes, FMEA* (initial)
- R&M Requirements Allocation (incl. SW)
- FD&R** Design, FMEA, predictions, FMEA (detailed)
- DR Data tracking, ID of unanticipated failure modes, FD&R verification
- FD&R Implementation, Static Analysis (coding standard conformance), FMEA revisions

* Failure Modes and Effects Analysis
** Failure Detection and Recovery
Next Steps

- Valuation techniques to link between RMA engineering to affordability
  - *Methods of measurement and accounting of operational suitability, effectiveness, and sustainment engineering for acquisition managers*
  - *Is the link really as strong as congress, the GAO, and RMA advocates believe?*

- Methods to assess the RMA-related Key Performance Parameters (KPPs) and Key System Attributes (KSAs) during development
  - *Metrics*
  - *Models*

- Methods to identify operations and sustainment costs
  - *Access and analysis of operations and maintenance databases*
  - *Methods to improve data recording and collection*

- Policies and metrics linked to award fees for incentivizing contractors to invest in RMA engineering
  - *Linking operational and sustainment costs to award fees and past performance ratings*