EMSD Technology Exchange
Software Topics

♦ CxP Software and Autonomy Technology Needs,
  • Presented by Ron Morillo

♦ CxP Mission Operations Technology Needs
  • Presented by Ernest Smith

♦ CxP Integrated Build Tool Concepts
  • Presented by Leslye Boyce

♦ CxP Verification, Validation and Accreditation Concepts
  • Presented by Randy Wallace
CxP Software and Autonomy Technology Needs

Ron Morillo
SAVIO Software
11/14/2007
The Constellation Program is interested in software technologies that support the following program objectives:

- Build safer software-intensive systems
  - Mitigate common cause failures

- Reduce development and schedule risk
  - Manage the size and complexity of software interactions in all the phases of the life-cycle.

- Improve fault detection, isolation and recovery techniques

- Lower operational and maintenance cost.

- Enable the move to greater on-board autonomy
  - Intelligent human-in-the-loop automation

- Improve system performance analysis.
  - Timing, trending, forecasting
Specific SW technologies of interest - 1

♦ Requirement Maturation:
  • Ontology systems to determine precise meaning of requirements, avoid possible (mis)interpretations and determine completeness of the requirement set.
  • Requirement analysis for inconsistencies and contradictions
    – Many software-related mishaps, including common cause failures, trace back to incomplete or missing requirements

♦ Design/Architecture:
  • Capture the design knowledge once; use it to code, test and verify, operate the system
  • Physical and behavioral models that capture system properties, cause/effects, environment and interactions:
    – Quantify the complexity of SW code and interfaces
    – Improve model-based analysis and verification, testability and timing analysis.
  • Investigate the true bounds of dissimilar software design.
  • SW fault containment concepts.
Autonomy and FDIR:

- Adjustable levels of autonomy and FDIR.
- Technology for onboard Decision Support and Expert-guided troubleshooting to crew/ Ground.
- Tie diagnostic/prognostic tools to on-board reconfiguration managers and/or intelligent controllers.
- Within tight timing constraints:
  - Minimize false alarms, diagnosis ambiguity.
  - Detect trends
  - Assess failure severity for C&W.
- Better forecasting capability (of system degradation, of remaining useful life, of impending failure..)
- Re-planning following a failure:
  - Decompose high-level objectives onboard, incorporate locally determined information (situational awareness) and create an new execution plan.
- When autonomy meets imperfect information: inductive reasoning techniques for managing certain degree of data inconsistency, limited knowledge or uncertain symptoms; models that manage imprecision and uncertainties
Specific SW technologies of interest - 3

♦ **SW implementation:**
  - Code analyzers and compliance rule checkers
  - Auto coding of critical software functions

♦ **SW Verification and Validation:**
  - Targeting specific tests towards mitigating specific classes or types of software defects.
  - Error injection, tracing and analysis technology
  - Model-based analysis for validation of safety-critical software designs.
  - Test suite generation, including behavioral coverage of safety-critical software functions.
  - Advanced Validation Testing that determines failure boundaries and margins for safety-critical functions.
  - Auto code tools for state estimation, data analysis and to streamline the test activity.
  - Verification and validation of autonomy and automation functions implemented in flight computers.
Special SW technologies of interest - 4

Software reliability

- Quantifying the software risk contribution to the total risk in a system.
- Modeling software failures.
- Mature the technology of predictive SW/system reliability models validating these models with operational data.
Mission Operations Overview For Technology Needs Assessment

Ernest Smith
Mission Operations Directorate

CONSTELLATION

NASA
Mission Operations Overview For Technology Needs Assessment

• Mission Operations at Johnson Space Center is preparing for our support to the Constellation Program
  • Major mission operations systems upgrades/development include the Mission Control Center Systems, the Cx Training Facilities, Mission Ops Reconfiguration System, and Flight Design Applications

• Technologies areas we require include those related to:
  • Autonomy applications related to mission operations
  • Integrated Systems Health Monitoring tools
  • Software development tools (especially JAVA enterprise technology and Workflow tools)
  • Data mining/knowledge management
  • CFDP compatible tools for file transfers (CCSDS-based implementation of FTP)
  • Mission monitoring (telemetry and command) tools and applications
  • Scheduling tools
  • Training support applications and simulations technologies for both stand-alone part-task trainers and full capability simulations of vehicle systems

• We have partnered with Ames for the past 2 years on technology infusion projects to enhance efficiency and capability associated with our plan/train/fly capabilities within Mission OPS, but are interested in other sources for technology infusion
Constellation Program
Integrated Build

ESMD Technology Exchange Conference

Nov 2007
Leslye Boyce
(850) 894-1761
Leslye.a.boyce@nasa.gov
Phased Development Activities

Key enablers for process include

- Planned – Phased Delivery of System Software from Projects
- Reduction in Software Build Cycle Times to reduce risks
- Identification and specification of Infrastructure Support Tools
- Distributed, Early Interface Testing for design validation, risk reduction and Hardware/Software Integration

CxP Integrated Software Planning is a complex task that requires a time phase approach and build up of capabilities

- Builds on multiple System Baselines as time phased capability is developed, integrated and verified (Qual. + Accept.)
- Maintains & integrates multiple System Baselines during concurrent Architectural development
- Provides Increment buildup of capability based on mission objectives
Verification and Validation Interactions

- Project C
- Project B
- Project A Build X.Y
- Integrated Master Schedule
- Delivery Plans/Products/VCNs
- S&A Delivery Schedule
- M&S Capability
- Procedures, Facility Use
- Discrepancy Reporting
- Risk buy down tests
- Sils
- CxP Planning & Coordination
- TR's
- Interconnectivity, Scheduling, coordinating
- Reqt’s, Verification Reqt’s
- Validation Scenarios
- DRM’s
- ConOps
- SIG’s
- DSIL
- PRACA
- Risk Mitigation
- IOS
- IRD’s
- CARD
- M&S Capability

13
Requirements Highlights

- The IBT is the authentic source for all software, associated data and meta data for the CxP

- The IBT supports the planning, tracking, submittal, and distribution of software and data between the various Constellation projects and elements

- The IBT supports the decisions and manages the activities for the Computing Systems Control Panel as directed by the Constellation System Engineering Control Board

- The IBT supports the planning and tracking for System Integration Plan
## Desired End-State Captured in the SIP

**Focused Look at ISS IOC - Draft**

### ISS Program Phase

<table>
<thead>
<tr>
<th>Design Synthesis</th>
<th>Initial Operational Capability</th>
<th>Full Operational Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>VV&amp;A VV&amp;A VV&amp;A</td>
<td>VAC VAC VAC</td>
<td>DGT DGT</td>
</tr>
<tr>
<td>Intg Phase</td>
<td>GT GT GT Stack FEIT CoFR Ares 1-Y</td>
<td>CoFR PFA CoFR PFA CoFR PFA</td>
</tr>
<tr>
<td></td>
<td>GT GT GT GT MEIT Stack FEIT</td>
<td>Orion 1</td>
</tr>
<tr>
<td></td>
<td>GT GT GT GT GT</td>
<td>Orion 2</td>
</tr>
</tbody>
</table>

### Each Mission will have an assessment to generate the final information needed to satisfy their respective CoFRs. The results for each will drive the larger integration phase/system assessments.

### Documented in the SIAP
- Documented in the flight test strategy

### Using the anchor points, vertical and horizontal assessments can be done to drive the integration

### Integration is complete when the what is needed and when it is need matches what is provided

### Gather the project build plans to see what is provided

### Template/Framework

<table>
<thead>
<tr>
<th>LOC/LOM</th>
<th>Crew Survival</th>
<th>C3I</th>
<th>Flight Rate</th>
<th>GPS Metric Tracking</th>
<th>Safe Design</th>
<th>Ec, Ep, Pi</th>
<th>Orbital Debris</th>
<th>Imagery</th>
<th>Operability</th>
<th>D&amp;C Stds</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Threads/What is needed

- Ares
- Orion
- GO
- MO
- EVA
- DSIL
- MS&DA

### SIP to provide the Template or framework to provide anchors for all
Modeling and Simulation Verification, Validation and Accreditation

ESMD Technology Exchange Conference
Nov 2007
Randy Wallace
(256) 544-2940
Randal.L.Wallace@nasa.gov
Over 400 existing simulations
Various conditions
Numerous development efforts
Over 700 identified needs for M&S
Compressed schedules
M&S VV&A

VERIFICATION
The process of determining that a model [or simulation] implementation and its associated data accurately represents the developer’s conceptual description and specifications…*Did we build the thing right?*

VALIDATION
The process of determining the degree to which a model [or simulation] and its associated data provides an accurate representation the real world from the perspective of the intended uses of the model or simulation…*Did we build the right thing?*

ACCREDITATION
The official acceptance of a model or simulation or federation of models and simulations and its associated data to use for a specific purpose…*Should it be used?*

Verification, Validation, and Accreditation (VV&A):
A process for substantiating the credibility of models and simulations.
Benefits of VV&A

- Increase the credibility of M&S used.
- Supports NASA M&S Standard 70009
- Reduce the risks associated with the M&S used.
- Establish a solid understanding of M&S strengths and weaknesses, and the bounds within which they can credibly support decision-making.
- Ensure informed decision-making.
- Reliably realize the benefits of simulation

VV&A provides a mechanism to communicate credibility between M&S developers, analysts and decision makers.
A Three Phased NASA Process

MSDA M&S VV&A Process Objectives

- Document M&S credibility
- Accredit key M&S

VV&A Process

MV & APrioritization Process Phase 1 Initialization

MSA VV&A Process INPUTS

- M SSP
- SIA
- IDA/Chedules
- M&S Plans
- TDSs
- MVOs

M&S Needs

(M&S V V&A Prioritization Process)

Prioritized VV&A List

Phase 1
Initialization

Decision

Phase 2
Planning

Decision

Phase 3
Execution

Products per M&S Tool

- M&S Initial Assessment
- Data Analysis Flow Diagram
- Accreditation Criteria
- Credibility Assessment
- ROM for Phase 2 Efforts
- Accreditation Memo, or Memorandum of Record

- Accreditation Plan
- V&C Plan
- Accreditation Memo, or Memorandum of Record

- V&C Report
- Accreditation Report
- Accreditation Memo, or Memorandum of Record

V V&A
Inputs & Outputs
are stored in MSDB

MSDB

VV&A Process Resources

- VV&A Policy (found in IMDD)
- VV&A RPG
- Integrated Collaborative Environment, M&S Database
- Access to M&S tool-developers and Analyst-users ??
NASA M&S VV&A Needs

- Increased Awareness of VV&A requirements and applicability
- Tools to automate the verification process
- Consistent information management systems
- Real-world referent data on developmental systems
- Analysis Standards
- Analysis Recommended Practices Guide
The Fundamental Questions

How Good Is It?

Is It Good Enough?

VV

&A
Contact Information

♦ Randy Wallace
  • M&S VV&S Lead, CxP Software and Avionics Integration Office (SAVIO)
  • randal.l.wallace@nasa.gov
  • 256-544-2940

♦ Lisa Caine
  • Aegis Technologies
  • Lcaine@aegistg.com
  • 256-922-0802