Current Research in IV&V techniques at JAXA

9/27/2007, WV

Yuko MOMO MIYAMOTO*1
Masa KATAHIRA*1, Shigeo YOSHIKAWA*2
*1 Japan Aerospace Exploration Exploration Agency
*2 Japan Manned Space System Co.
Contents

- IV&V in JAXA
- Overview of Research
- Model-based IV&V
- New research areas
  - Case 1: ODF verification
  - Case 2: Operation procedure verification
- Lessons Learned
- Future work
IV&V in JAXA

- **History**
  - JAXA started performing IV&V in 1996 based on an agreement for the ISS program.
  - Up to now, JAXA has performed IV&V on:
    - Manned System: 6 subsystems
    - Satellite: 6 satellites (15 subsystems)
    - Ground Segment: 3 subsystems
    - Operational Procedure: 1 system

- **Research strategy**
  - Cost-effective plan for IV&V
    - Strategic IV&V planning research
      - In corporation with University of Hawaii
  - Appropriate technique for IV&V
    - Research of techniques applicable for IV&V
Overview of Research - Strategic IV&V planning

- Motivation
  - Cost-effective IV&V planning
    - Plan cost effective IV&V activities by considering target project characteristics.
    - Assess risk of target system, and select most cost effective and efficient IV&V perspectives and techniques to reduce risk.
  - Appropriate selection and combination of IV&V techniques

- Target project characteristics
- IV&V conditions

Model
- Risk size
- Risk probability
- Risk reduction level
- IV&V technique and its Cost

Strategic IV&V Planning Model

Strategic IV&V Plan
Overview of Research
- IV&V Techniques -

- Categories
  - Review of Document (ROD)
    - Checklists
    - Parsing
    - Inspection
  - Analysis
    - System Hazard Analysis / Software Hazard Analysis
    - Traceability analysis
    - Static Code analysis
  - Model checking (MC)
    - State machine
    - Time automaton
  - Simulation
    - Model and Simulation (M&S)
    - Simulation using artifacts
Overview of Research
- Techniques Selection and Combination-

**Compliance**
- Traceability
- Correspondence

**Artifacts Correctness**
- Completeness
- Consistency
- Correctness

**Coverage**
- Robustness

**Safety**
- Consistency
- Reachability

In Each Phase, work with System level Safety Analysis.
Model Based IV&V
Model checking (MC) & SIMulation (Spec. Execution)

- Why use?
  - To confirm,
    - No unexpected behaviors
    - No incompleteness
    - No inconsistencies

- When done?
  - Subsystem Requirement Analysis, typically

- How to use?
  - Model Checking and Simulation
  - Focus on Safety critical functions
New Research Topics
- Verification of Operation design using
  - Model checking
    - How to develop models?
    - How to introduce automated and accurate evaluation?
- Simulation
  - Investigate the possibility and benefit of having simulator for verification of operation.

To verify
- Operation Data File (ODF)
- Operation Procedure (OP)
Case 1: ODF verification (1)  
- Model checking -

- Verification targets
  - ODF for Malfunction cases (MAL ODF)
    - Developed by operation support team
    - Describe how to determine failure causes during operation in orbit using telemetries (34 files, ~120 failure causes)

- Reference
  - FDIR Sheets
    - Developed by satellite developer
    - Describe failure modes and its effects in terms of Telemetry (~ 200 FMEA files)

- Perspectives of IV&V
  - Consistency
    - MAL ODF is consistent with contents of FDIR sheets
  - Uniqueness
    - One failure determination flow identify one failure cause

- Issue
  - It is impossible for human to verify about 120 failure determination flows by referring ~200 failure mode descriptions.
Case 1: ODF verification (2) - Model checking -

- Modeling
  - Model MAL ODFs using UPPAAL ([http://www.uppaal.com/](http://www.uppaal.com/))
  - Develop model for each subsystem
  - Model the failure determination flow from initial condition to final determination.
  - Easy to model flows and branches by UPPAAL

Modeling diagram showing transitions and conditions for model checking.
Case 2: Operation procedure verification

- HLA based Distributed Simulation -

- Distributed Simulation configuration

JAXA’s Ground System

ISS Ground System

Transfer vehicle Simulator

ISS Simulator

Simple ISS SIM For IV&V

TLM/CMD DB

Scenario

Operation Procedure

Operation procedure verification by operator

HLA
Lessons Learned
- Model checking VS Simulation -

● Model checking
  ● Develop model of operation procedures and verify the procedures using the model
  ● Hard to maintain traceability between artifact (ODF) and Models
  ● High number of false negatives in automated checking
    ● Needs more review by examiner and development members

● Simulation
  ● Execute simulation of using on-board software and verify operation procedures.
  ● Hard to prepare the environment