



2010: Advanced Diagnostics & Prognostics  
Testbed for spacecraft electrical systems



2011: Habitat Demonstration Unit



# Using Model-based Assurance to Strengthen Diagnostic Procedures

Robyn Lutz (JPL/Caltech), Jeremy Johnson (SGT-NASA Ames), Ann Patterson-Hine (NASA Ames)



ASE 2011  
University of Kansas, Lawrence, KS  
November 9, 2011



This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, and at NASA Ames Research Center, under a contract with the National Aeronautics and Space Administration. The work was sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program. This activity is managed locally at JPL through the Assurance and Technology Program Office. © 2011 California Institute of Technology. US Government sponsorship acknowledged.



# Lights Back On: An Example Diagnostic Procedure

*To better prepare for contingencies, we use model-based assurance to strengthen diagnostic procedures.*

*The scenario:* While an astronaut works to prepare samples, **all the lights go out** in their quarters (HDU: Habitat Demo Unit). The astronaut then follows the steps in the LightsOut contingency procedure to diagnose the problem.



Courtesy of NASA

NASA Habitat Demonstration Unit Project  
[http://www.nasa.gov/exploration/analogs/hdu\\_project.html](http://www.nasa.gov/exploration/analogs/hdu_project.html)

*The question:* Is this the best procedure?  
*The problem:* Development & review of procedures is labor-intensive and can miss things.  
*The technique we're investigating:* Use comparisons with the auto-generated diagnostic tree from the HDU's model to give a different view in checking out the procedure.

*Goal:* get the HDU lights back on →



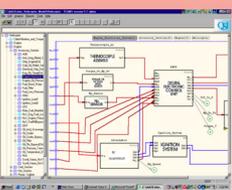
Courtesy of NASA

# DTV (Diagnostic Trees for Verification)

**Status quo:**  
model &  
procedure are  
not compared

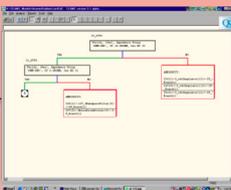
**Contribution:** use model-based  
information to verify procedure

TEAMS Diagnostic Model



Auto-Generate

Diagnostic Tree

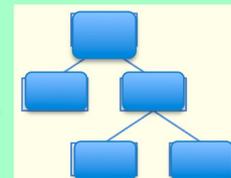


Diagnostic Procedure



Translate

Diagnostic Tree



DTV ANALYSES

Branch  
Completeness

Root Cause  
Verification

Path  
Verification

Efficiency

## Results of application to HDU:

Trouble-shooting trees automatically generated from the diagnostic model gave an independent perspective and found some open issues in the LightsOut diagnostic procedures.

Value to NASA: strengthens preparedness for contingencies

- Makes it easier & quicker to check quality and completeness of procedures
- Uses models already built by NASA projects during development, so low cost
- Catches assumptions that aren't always true
- Explores alternative ways to isolate failure causes
- Reduces risk that updating a procedure can bring



# Diagnostic Trees for Verification (DTV) applied to NASA's Habitat Demonstration Unit (HDU)

- **Problem Statement:** Verify the diagnostic procedures for lighting system failures in NASA's HDU using model-based diagnostic trees.
- Diagnostic procedures provide a set of instructions to help operators and maintenance personnel to monitor a system's parameters and respond to potential problems and anomalies.
- Why verify diagnostic procedures?
  - vehicle/crew safety
  - operational success
  - troubleshooting and maintenance effectiveness
- **Challenge:** Procedure verification is labor-intensive and critically dependent on human expertise



Lights inside the HDU

Courtesy of NASA



## Related Work

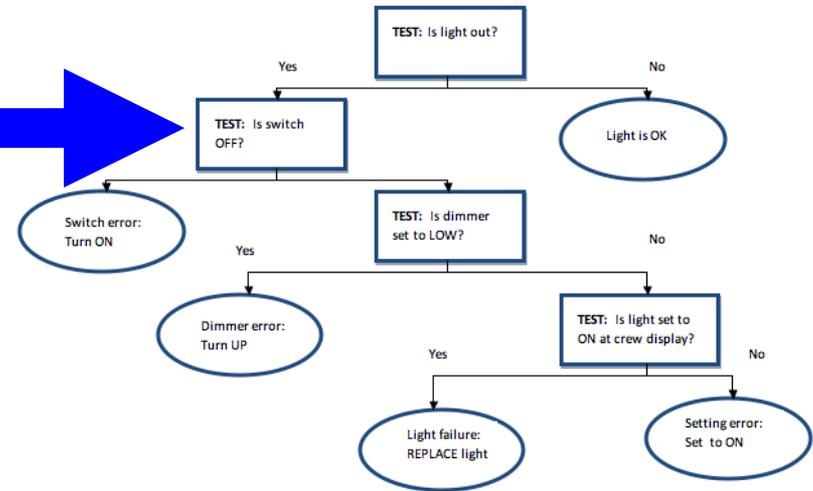
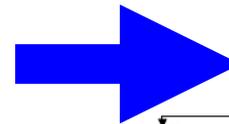
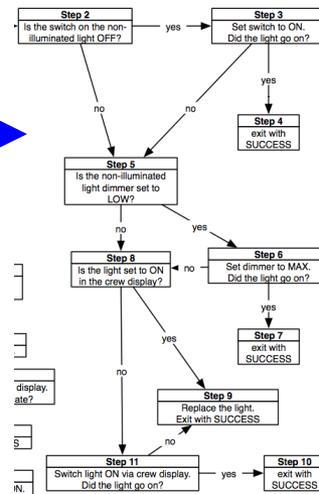
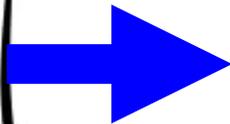
- Verification of procedures [1, 2]
- Generating procedures automatically from models [3]
- Diagnostic software for monitoring and diagnosis of dynamical systems [4]
- Machine-readable representations of natural language procedures [5]

- [1] G. Brat, M. Gherorghiu, D.Giannakopoulou, C. Pasareanu, “Verification of Plans and Procedures” Proc. IEEE Aerospace Conference, 2008.
- [2] C. Damas, B. Lambeau, F.Roucoux and Axel van Lamsweerde, “Analyzing Critical Process Models Through Behavior Model Synthesis”, Proc. 31st ICSE, 2009.
- [3] D. Kortenkamp, R. Peter Bonasso and D. Schreckenghost, “Developing and Executing Goal-Based, Adjustably Autonomous Procedures,” Proc. AIAA InfoTech@Aerospace Conference 2007.
- [4] A. Patterson-Hine, A., et al., “A Review of Diagnostic Techniques for ISHM Applications.” Proc. ISHEM, 2005.
- [5] V. Verma V., T. Estlin, A. Jónsson, C. Pasareanu, R. Simmons, K. Tso, “Plan Execution Interchange Language (PLEXIL) for Executable Plans and Command Sequences, iSAIRAS, 2005.

# Diagnostic Tree for Verification Method



- Manually converted the steps in each procedure to a tree representation similar in style to the trees that TEAMS auto-generates (to aid with comparison methods)



Procedure: Light Out.

Step 1. Check if light is out.

Step 2. Check if switch is off.

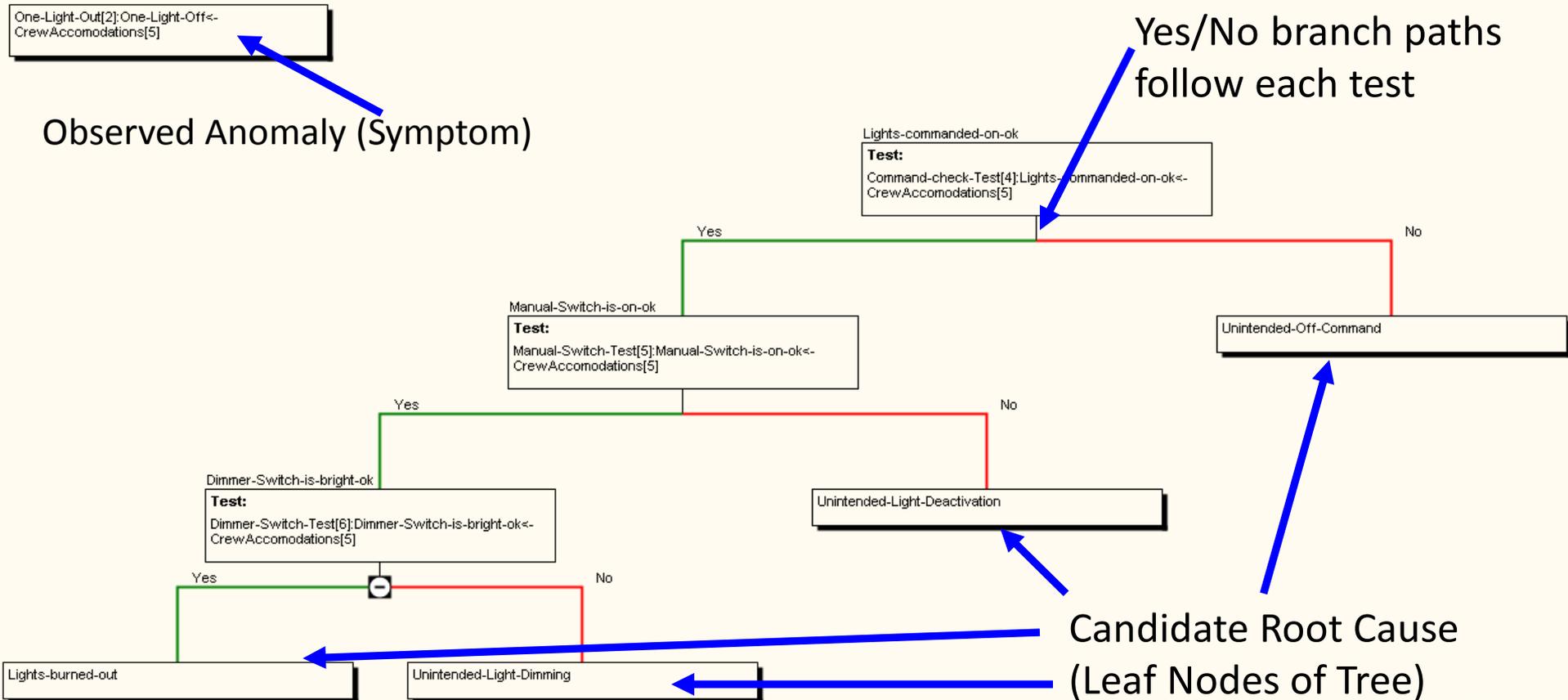
Step 3. Check if dimmer is turned up.

...

# Diagnostic Tree for Verification Method



- A diagnostic tree describes a branching sequence of checks/tests used for troubleshooting an anomaly
- Shown: Diagnostic tree auto-generated from HDU system, modeled in a commercial modeling and analysis toolset called TEAMS (Testability Engineering and Maintenance System, QSI, [www.teamsqsi.com](http://www.teamsqsi.com)).
- HDU TEAMS model has 226 failure modes & 203 tests





# DTV Analysis Methods

Comparing Hand-Generated Procedural Steps and TEAMS Diagnostic Trees

## **Conducted four analyses using tree-to-tree comparisons:**

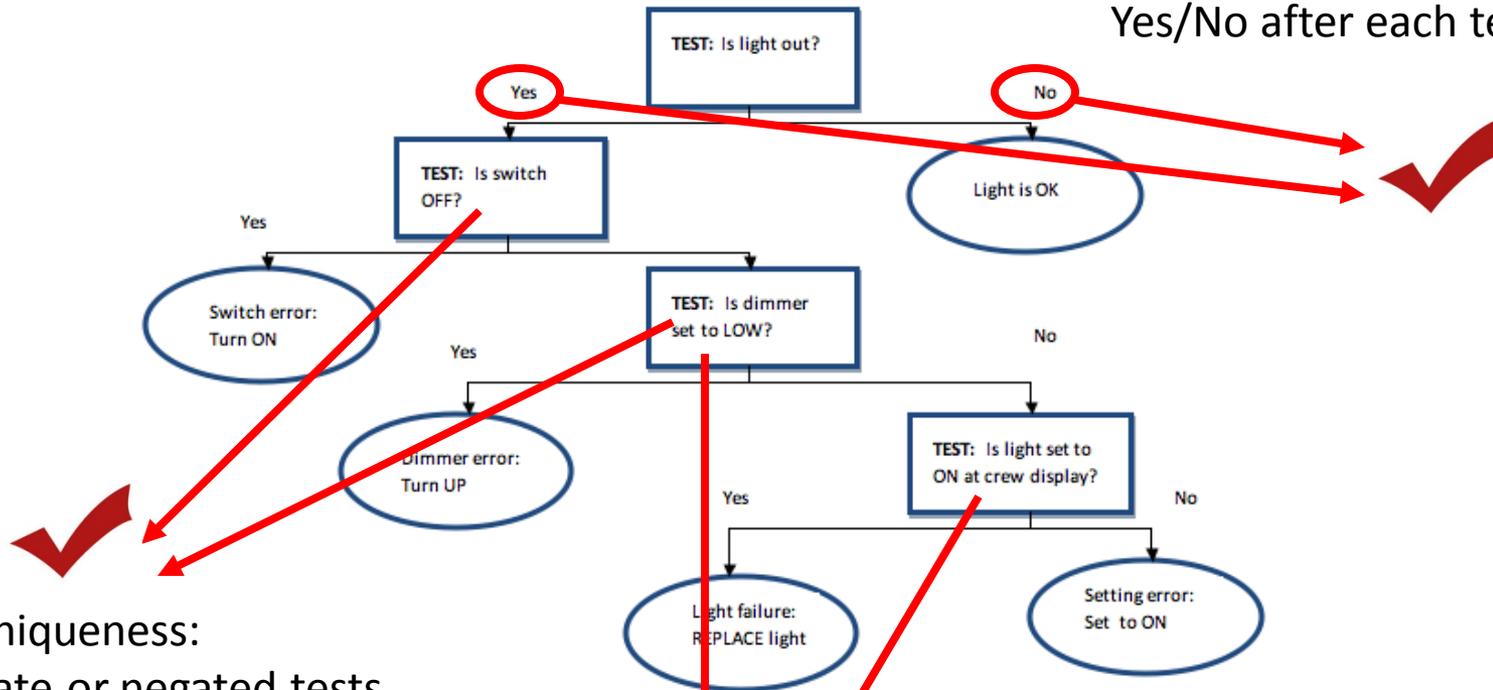
1. Branch Completeness Analysis – identify inconsistencies in procedural steps
2. Root Cause Coverage Analysis – verify that all potential root causes of an anomaly/fault are accounted for in the procedure
3. Efficiency Analysis – identify redundant checks/tests in a path and alternative paths for diagnosis in order to develop optimized strategies for fault handling
4. Path Verification Analysis - verify that a path in a procedure results in the correct diagnosis



# DTV Analysis Method: Branch Completeness Analysis

Three Checks:

(1) Structure OK?:  
Yes/No after each test



(2) Test Uniqueness:  
No duplicate or negated tests

(3) Branch Successors:  
Same successor nodes in both trees

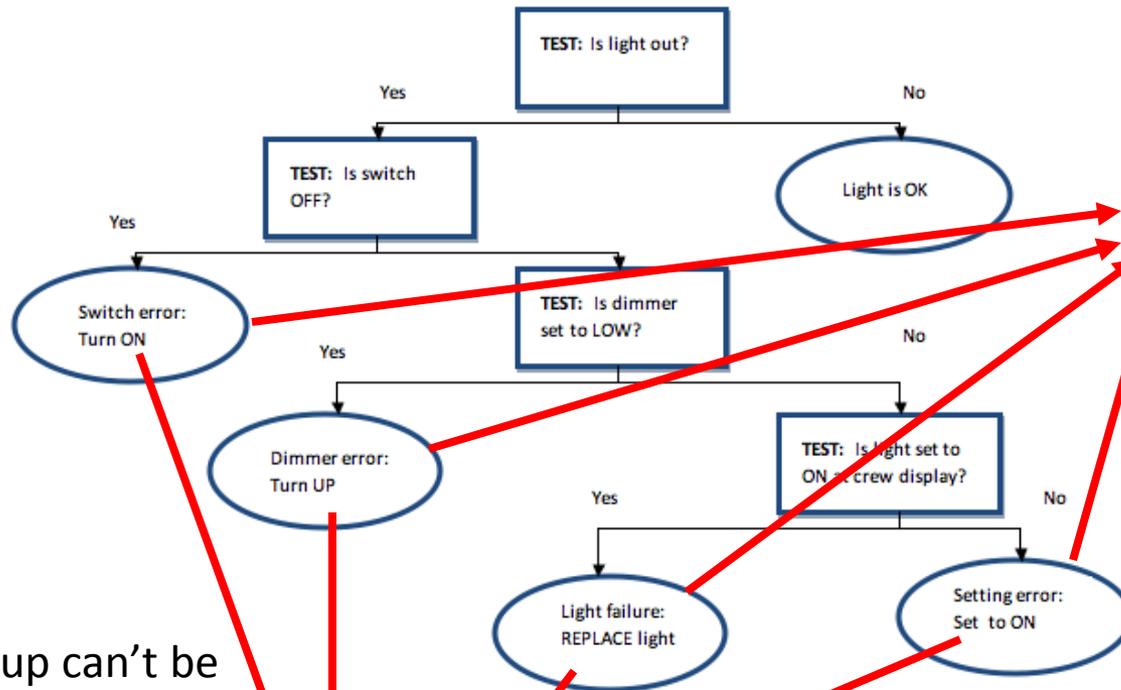
Different: TEAMS suggests checking crew display before implementing manual tests.



# DTV Analysis Method: Root-Cause Coverage Analysis

Two Checks:

(1) Sets of leaf nodes the same as TEAMS Tree?

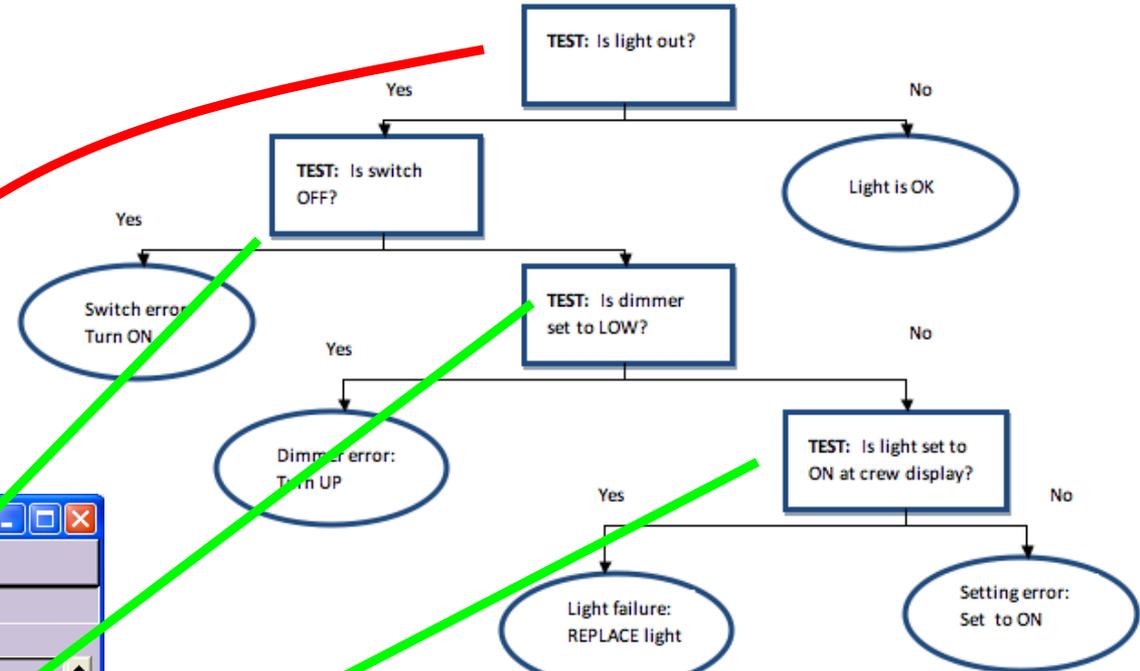


(2) Ambiguity group can't be refined?

All failures are isolated - no ambiguity in either tree.

In larger procedure, additional failures were represented in the model-based tree, giving it a more detailed diagnosis of power-system causes of lighting failures

# Path Verification Analysis: Single Light Out – 1 of 4 Paths



Finding: "Single Light Out" symptom hand generated diagnostic tree *is verified* for each of the four paths to the off-nominal leaf nodes.

Finding: For each of the paths where the other tests in the tree are not exercised, the other failure modes *are considered* in the suspect group.

TEST OUTCOMES - HDU\_JJ\_1

Unknown: 72

Tests (Unknown)

- PDU1CurrentTest[1]:PDU1CurrentTest<-Power[1]\_\_\_0
- PDU2CurrentTest[2]:PDU2CurrentTest<-Power[1]\_\_\_1
- PDU3CurrentTest[3]:PDU3CurrentTest<-Power[1]\_\_\_2
- SubfloorDuctInletFlowRateTest[1]:SubfloorDuctInletFlowRateTest<-ThermalControl[2]\_\_\_3
- SubfloorDuctInletTempTest[2]:SubfloorDuctInletTempTest<-ThermalControl[2]\_\_\_4
- SEGESubfloorTempTest1[3]:SEGESubfloorTempTest1<-ThermalControl[2]\_\_\_5
- SEGESubfloorTempTest2[4]:SEGESubfloorTempTest2<-ThermalControl[2]\_\_\_6
- SEGFSubfloorTempTest1[5]:SEGFSubfloorTempTest1<-ThermalControl[2]\_\_\_7
- SEGFSubfloorTempTest2[6]:SEGFSubfloorTempTest2<-ThermalControl[2]\_\_\_8
- SEGGSubfloorTempTest1[7]:SEGGSubfloorTempTest1<-ThermalControl[2]\_\_\_9

Passed Tests: 3      Failed Tests: 1

Tests Passed: Command-check-Test[4]: Manual-Switch-Test[5]: Dimmer-Switch-Test[6]: Di

Tests Failed: One-Light-Out[2]: One-Light

Test Fail Outcomes

Buttons: Send, Close, Diagnosis >>

HDU\_JJ\_1 - RDS System Health (Diagnosis to: Replaceable Units)

Bad: 1      Suspected: 0      Unknown: 85

Bad	Suspected	Unknown
Lights-burned-out[1]<-HD		BlockedDuct[1]<-CrewAcc
		Unintended-External-Pow
		SourceFailure[1]<-Source
		JunctionBoxFailure[1]<-HD
		PDUFailure[1]<-PDU1_F-
		PDU1DataFailure[2]<-PDI
		PDU2Failure[1]<-PDU2_E
		PDU2DataFailure[2]<-PDI
		PDU3Failure[1]<-PDU3_F-
		PDU3DataFailure[2]<-PDI

Buttons: No Colors, Send Once, Close, Show Minimal >>

# DTV: What does a model-based approach contribute over expert review?



- Together provide *more thorough coverage of failure space*
  - Model (but not procedure) includes avionics failures that led to lights out & uses automatic tests to disambiguate failure groups
  - Procedure contains failure modes and tests initially not included in the model, likely due to the expertise of procedure author
- DTV uncovers possible *undocumented assumptions*
  - Else, add risk when architecture changes and old procedures become invalid
  - Example: Attic gets added to the HDU which adds another lighting circuit. Old procedure assumes an avionics failure path that is no longer valid.
- Model based approach suggests a *more optimal order of checks*, moving expensive/manual tests to the end
- Model requires standard test outcome, so *catches inconsistent usage* that can cause crew confusion:
  - In procedure, “yes” sometimes meant “passed” and sometimes meant “failed”
  - One procedure checked that the light was ON while another checked that the light was OFF.

# Thank you!

**For more information:**

[Robyn.R.Lutz@jpl.nasa.gov](mailto:Robyn.R.Lutz@jpl.nasa.gov)

[Ann.Patterson-Hine@nasa.gov](mailto:Ann.Patterson-Hine@nasa.gov)

[Jeremy.R.Johnson@nasa.gov](mailto:Jeremy.R.Johnson@nasa.gov)

- T. Kurtoglu, R. Lutz and M. Feather, “Model-Based Assurance of Diagnostic Procedures for Complex Systems ,” Annual Conference of the Prognostics and Health Management Society , 2010.
- T. Kurtoglu, R. Lutz and A. Patterson-Hine, “Towards Verification of Operational Procedures using Auto-Generated Diagnostic Trees, “Annual Conference of the Prognostics and Health Management Society, 2009.
- R. Lutz, A. Patterson-Hine, S. Nelson, C. Frost, D. Tal and R. Harris, “Using Obstacle Analysis to Identify Contingency Requirements on an Unpiloted Aerial Vehicle,” Requirements Engineering Journal 12(1), 2007.