



2010: ADAPT electrical subsystem testbed



2011: Habitat Demo Unit

Using Auto-Generated Diagnostic Trees to Support Test Procedures

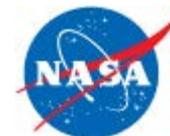
Robyn Lutz (JPL/Caltech), Jeremy Johnson (SGT-NASA Ames), Ann Patterson-Hine (NASA Ames)

NASA OSMA SARP Technical Interchange Meeting
August 4-10, 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.



Executive Presentation



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

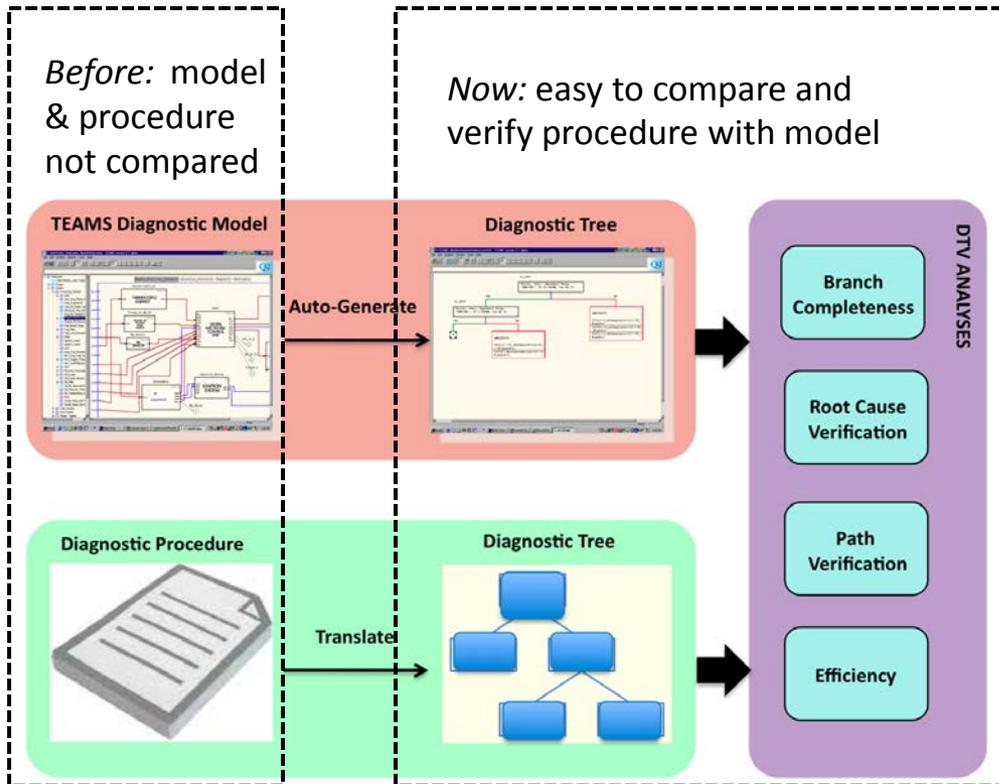
The question: Is this the best procedure?
The problem: Development & review of procedures is labor-intensive and can miss things.
The technique we're investigating: Use comparisons with the auto-generated diagnostic tree from the HDU's model to give a different view in checking out the procedure.

Goal: get the HDU lights back on →



Courtesy of NASA

DTV (Diagnostic Trees for Verification): Current Capability



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



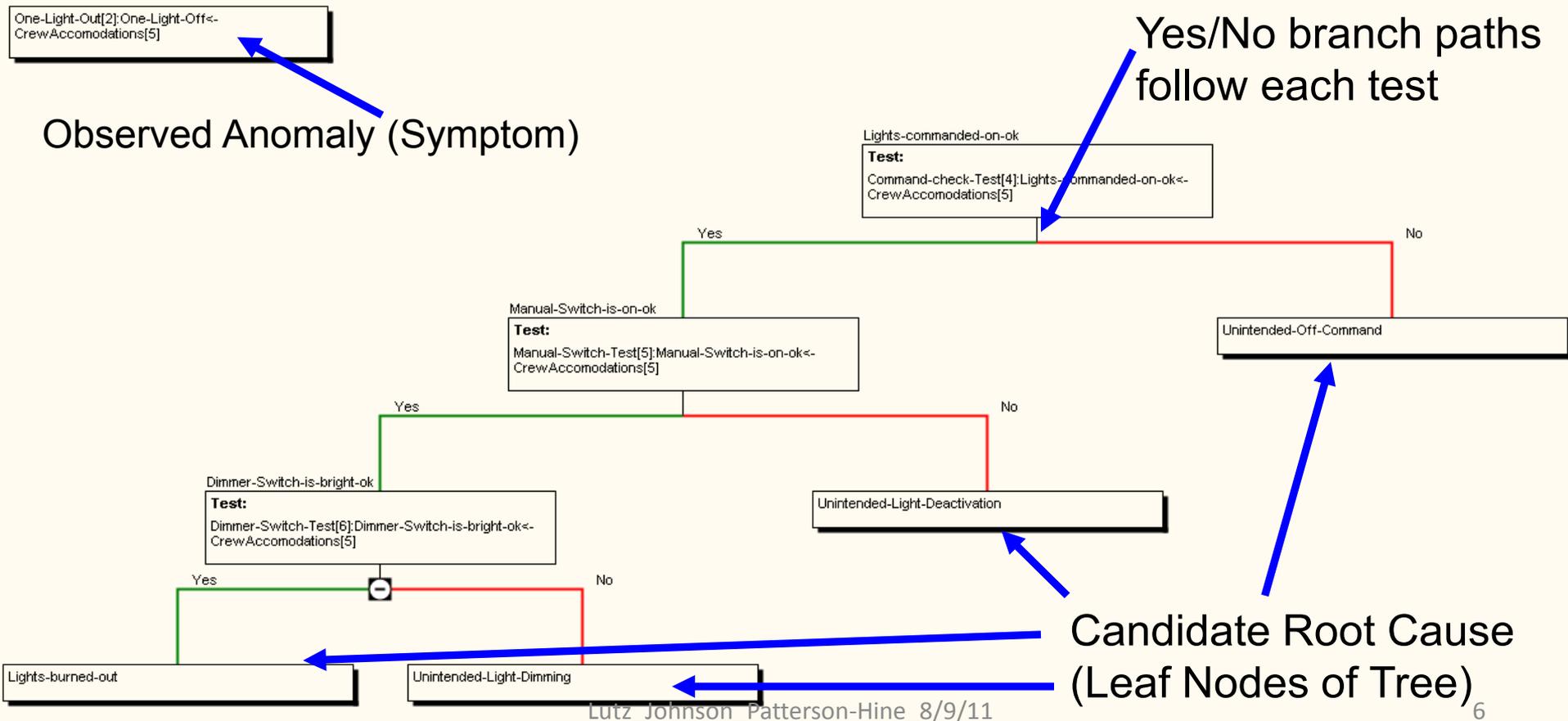
Lights inside the HDU;
Image courtesy of NASA

Diagnostic Tree for Verification Method



- A diagnostic tree describes a branching sequence of checks/tests used for troubleshooting an anomaly

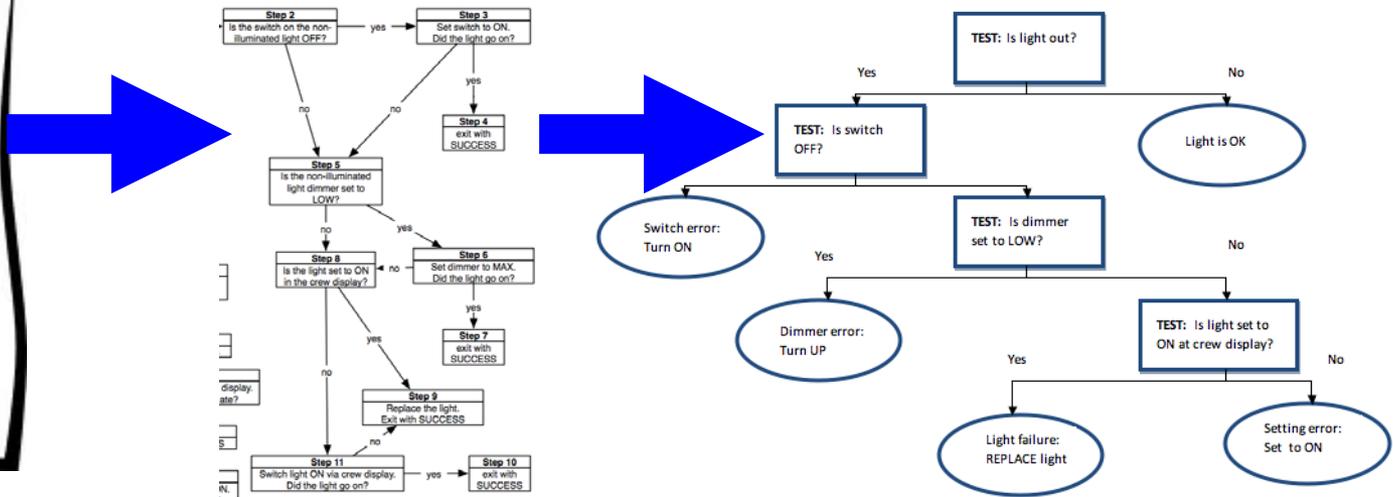
Shown: Diagnostic-tree auto-generated from HDU system modeled in a commercial modeling and analysis toolset called TEAMS (Testability Engineering and Maintenance System, QSI, www.teamsqsi.com).



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.

...



DTV Analysis Methods

Comparing Hand-Generated Procedural Steps and TEAMS Diagnostic Trees

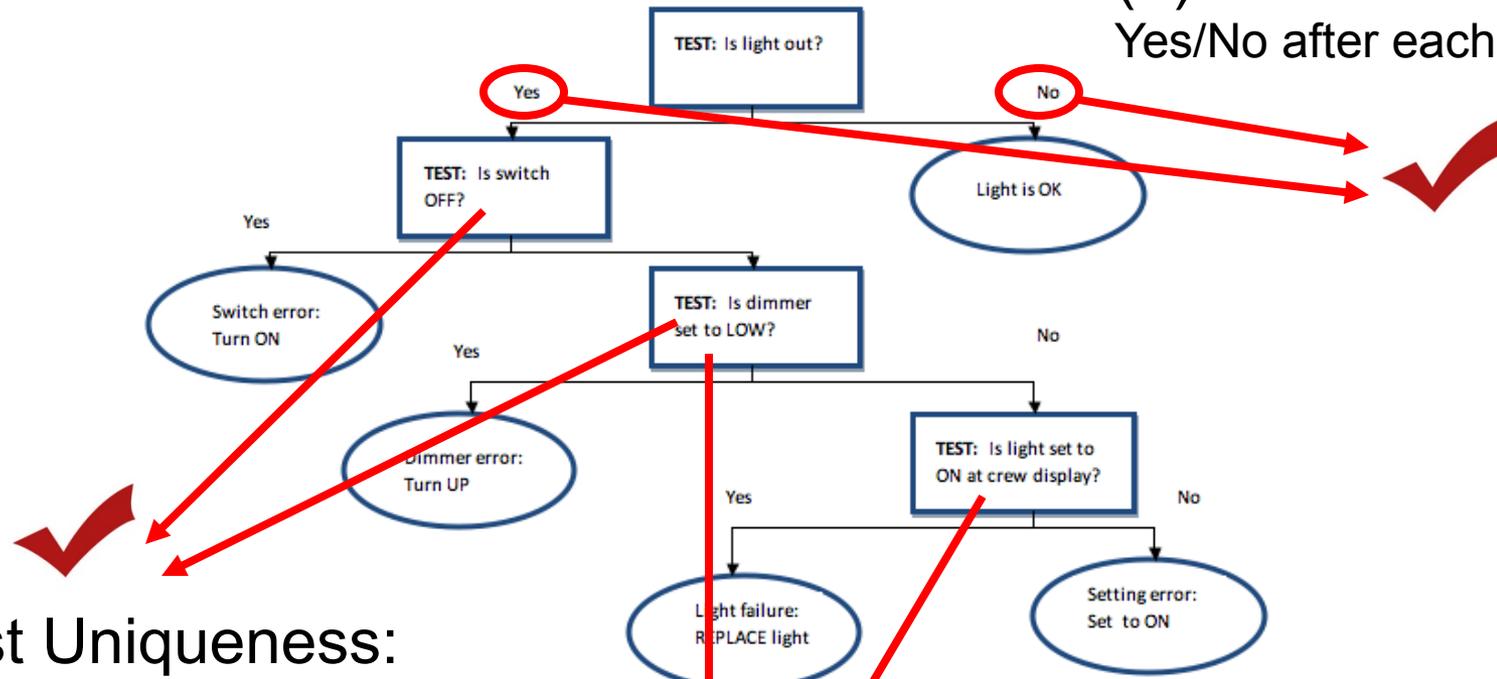
- **Conducted four analyses using tree-to-tree comparisons**
 1. Branch Completeness Analysis – identify inconsistencies in procedural steps
 2. Root Cause Coverage Analysis – verify that all potential root causes of an anomaly/fault are accounted for in the procedure
 3. Efficiency Analysis – identify 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



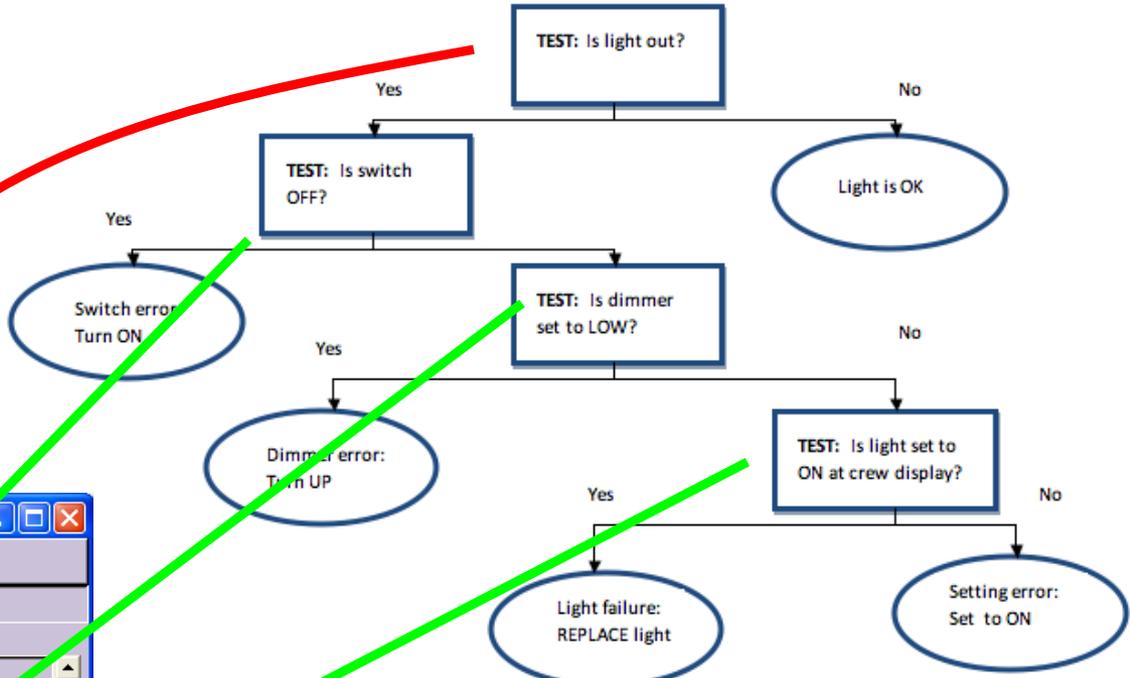
(2) Test Uniqueness:
No duplicate or negated tests

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

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

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[1]___3
SubfloorDuctInletTempTest[2]:SubfloorDuctInletTempTest<-ThermalControl[2]___4
SEGSubfloorTempTest1[3]:SEGSubfloorTempTest1<-ThermalControl[2]___5
SEGSubfloorTempTest2[4]:SEGSubfloorTempTest2<-ThermalControl[2]___6
SEGSubfloorTempTest1[5]:SEGSubfloorTempTest1<-ThermalControl[2]___7
SEGSubfloorTempTest2[6]:SEGSubfloorTempTest2<-ThermalControl[2]___8
SEGSubfloorTempTest1[7]:SEGSubfloorTempTest1<-ThermalControl[2]___9
    
```

Passed Tests: 3 Failed Tests: 1

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

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

Test Fail Outcomes:

Buttons: Send, Close, Diagnosis >>

HDU_JJ_1 - RDS System Health (Diagnosis to: Replaceable Units)

Bad: 1 Suspected: 0 Unknown: 85

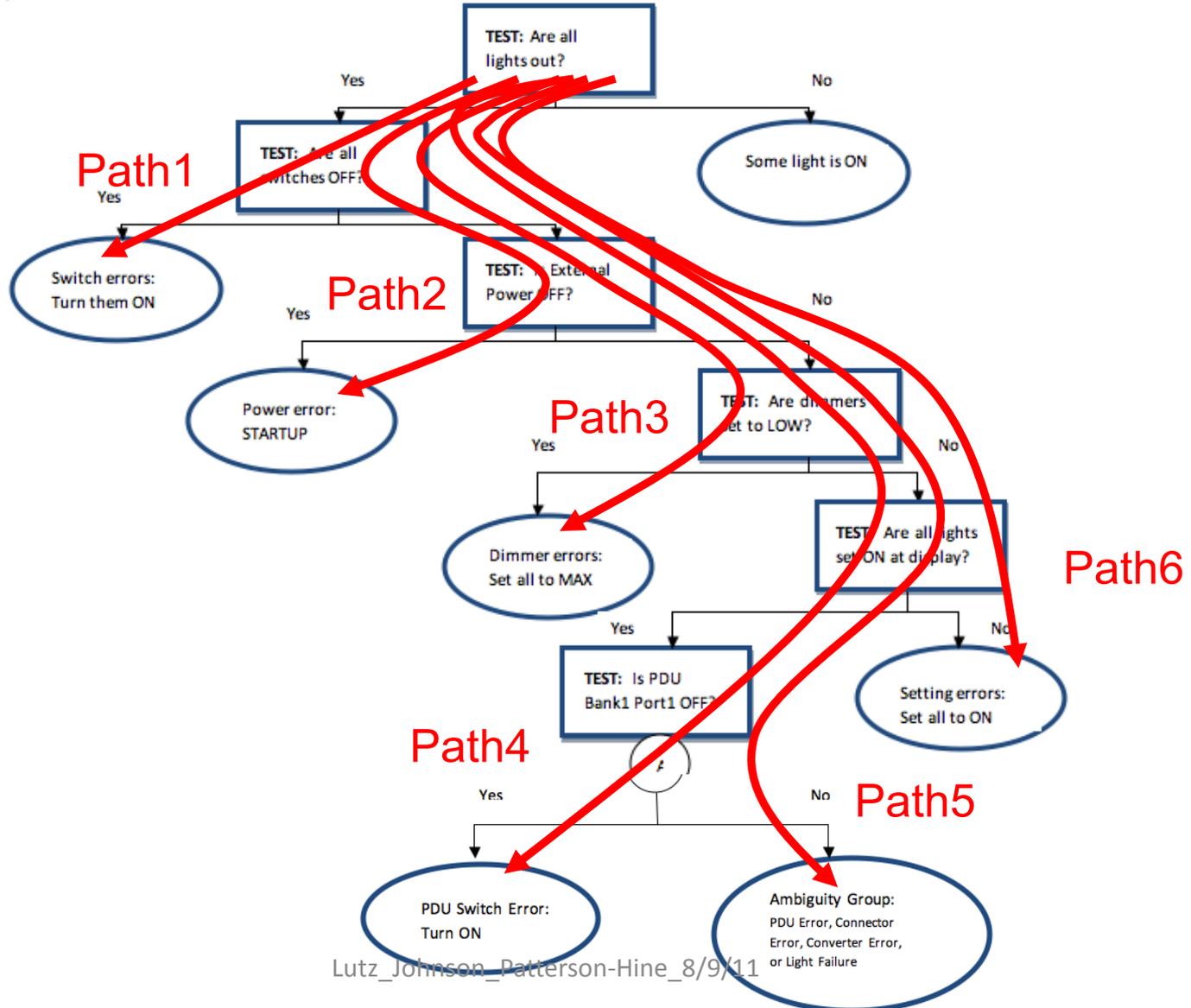
Bad	Suspected	Unknown
Lights-burned-out[1]<-HD		BlockedDuct[1]<-CrewAcc
		Unintended-External-Pow
		SourceFailure[1]<-Source
		JunctionBoxFailure[1]<-H
		PDUFailure[1]<-PDU1_F-
		PDU1DataFailure[2]<-PDI
		PDU2Failure[1]<-PDU2_E
		PDU2DataFailure[2]<-PDI
		PDU3Failure[1]<-PDU3_F
		PDU3DataFailure[2]<-PDI

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

DTV Scales well for larger procedures: Multi-Light Out Symptom - 6 Paths



HDU Light Diagnostic Procedure 1.1 (All Lights Out)
R. Lutz, 4/1/11





Proposed Extensions Useful to HDU, NASA

- Add interfaces with other system modeling tools (SysML, AADL) used by some NASA projects
 - HDU project also interested in SysML modeling
 - Can AADL model in xml format also be imported to TEAMS?
- Add context information for procedures (diagnostic preconditions, assumptions) into the model
- HDU procedures use reconfiguration to aid in failure diagnosis. Add failure isolation after reconfiguration
- Determine more precisely what should be stored in a system model in order to support its use in developing and assessing diagnostic procedures



Additional Slides for Technical Presentation



HDU TEAMS Model Update

- HDU TEAMS model is being updated to reflect the evolving design in support of selected failure scenarios for Desert RATS 2011
 - Increased model size from 89 failure modes and 76 tests to 226 failure modes and 203 tests
 - Model now includes manual tests proposed by HDU subsystem engineers to reduce failure ambiguity groups
 - Model has been verified using Dependency Matrix and Diagnostic Analysis Output reviews with subsystem engineers



Courtesy NASA



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

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.

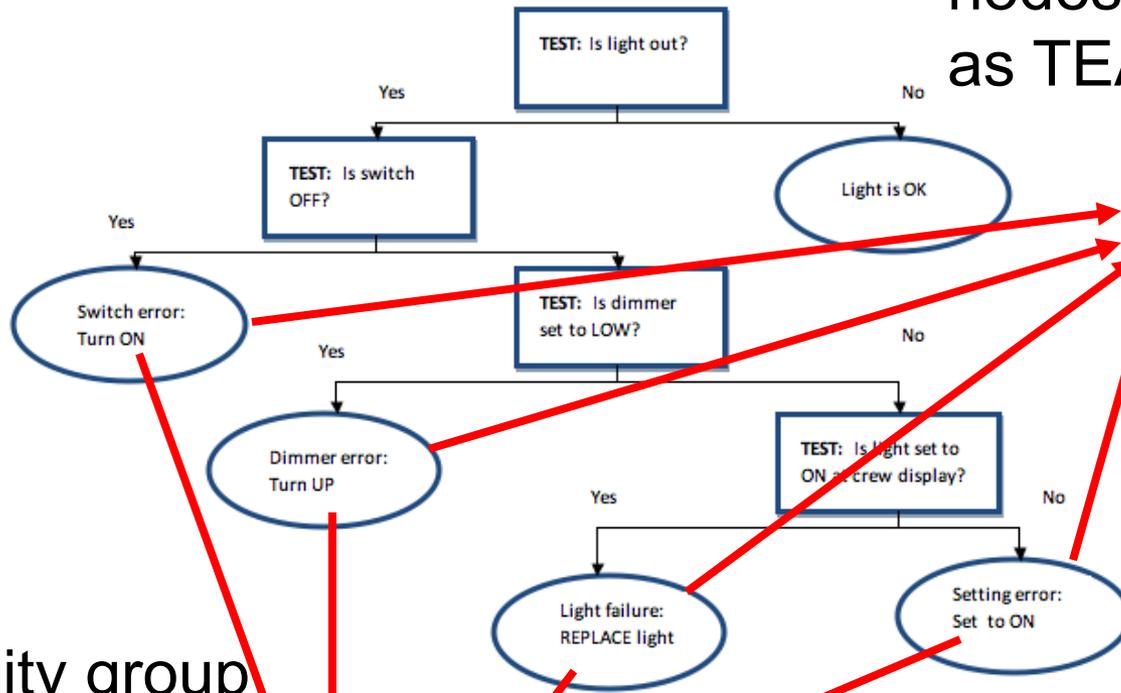
T. Kurtoglu, R. Lutz and M. Feather, “Model-Based Assurance of Diagnostic Procedures for Complex Systems”, Annual Conference of the Prognostics and Health Management Society , 2010.

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.

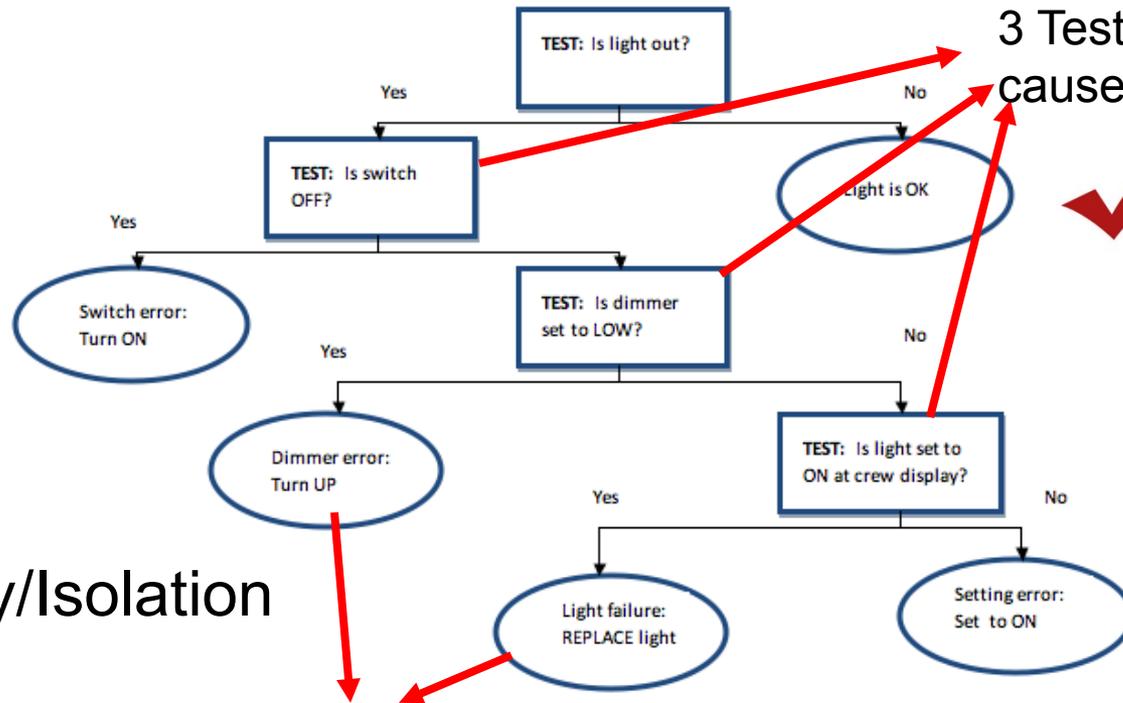
In larger procedure, additional failures were represented in the model-based tree, giving it a more detailed diagnosis of power-system causes of lighting failures.

DTV Analysis Method: Efficiency Analysis



Three Checks:

(1) Same number
of checks?



3 Tests required for root
cause: same as TEAMS

(2) Efficiency/Isolation
tradeoff?

No ambiguity groups to compare.

No interesting results in this case
(which is good news!)

(3) Better Efficiency?
Same number of checks
= same efficiency

Additional Findings for Multi-Light Out Symptom Using Path Verification Analysis



- Paths 1, 2, 3 and 6 verified through TEAMS-RT
- Paths 4 and 5 require a “PDU Bank 1 Port 1 Off” test (not modeled)
- A similar test checks the the current flowing to PDU but does not rule out PDU switch (not currently modeled as a failure)
- Ambiguity group in model larger than in procedure because model’s failure space analyzed was larger than that considered in the procedure
- Avionics failures, as well as failures leading to avionics failure (e.g., loss of avionics power or thermal conditioning), not considered in model or procedure



Some 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.



Research Challenges

- Cost function
 - Needed to evaluate alternative paths
 - TEAMS has the capability to include cost information
- Situation-based sequencing
 - Example: if an astronaut is alone in the HDU then the best sequence of diagnostic steps may be different from the best steps if there are several astronauts who can distribute the tasks.
 - TEAMS can represent situations as distinct modes
- Reconfiguration to isolate faults
 - Some diagnoses reconfigure the system during the troubleshooting process
 - Available in TEAMMATE but out of scope of HDU work to date

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



- Together, provides *more thorough coverage of failure space*
 - Model (but not procedure) included avionics failures that led to lights out & used automatic tests to disambiguate failure groups
 - Procedure contained failure modes and tests initially not included in the model, likely due to the expertise of procedure author.
- DTV uncovers possible *undocumented assumptions*
 - Adds 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.
 - If the technician has the ability to command lights through the crew display, this implies passed tests indicating nominal avionics behavior.
- Model based approach suggests a *more optimal order of checks*, moving expensive/manual tests to the end
- Model requires standard test outcome, so *caught inconsistent usage* that could cause 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.



Backup Slides

Results of Verification Methods



<i>Analyses</i>	<i>Single_light_out</i>	<i>Multi_lights_out</i>
1. Branch completeness analysis:		
Structure OK	Yes	Yes
Test uniqueness: no duplicate or negated tests	Yes	Yes
Branch successors: same successor nodes in both trees	No: Ex: Proc. manually tests the light's switch & dimmer setting before checking if light was commanded on OK at the crew display. Procedure tests negative ("dim?") while TEAMS tests positive ("bright?")	No Ex: TEAMS puts manual tests to the bottom
2. Root cause coverage analysis		
Sets of leaf nodes the same	Yes	No: procedure incomplete Ex: TEAMS includes Heat Pump failure, & other failures not in procedure TEAMS includes all tests in procedure
Ambiguity group can't be refined	None in either	Yes, for TEAMS No, for procedure's tree (need to update)
3. Efficiency analysis		
Same number of checks	Same, except I put symptom in as an extra test	No, TEAMS has more
Efficiency/isolation tradeoff	NA	1 ambiguity group in TEAMS: failures can't be distinguished?
Better efficiency	NA	Hard to compare due to different number of failures considered

Differences in Ambiguity Groupings: Model has more detail



Hand-generated DT ambiguity group after PDU 1 test passes	TEAMS-RT reported ambiguity group after current to PDU 1 is lost	Discussion
PDU Error	PDU 1 failure	
Connection Error		Not modeled in TEAMS
ACDC Conv. Error	ACDC failure	
Light Failure	Lights Burned Out	
	Source failure	Diesel generator failed
	Junction Box failure	Feeds electricity from generator to the 3 PDUs
	PDU 2 failure	Feeds electricity to the avionics
	Heat Pump failure	If thermal conditioning is lost, this will lead to avionics overheating and shutdown.
	Obstruction in seg D	Segment D and E obstructions refer to the thermal conditioning ducts for the segments housing the avionics
	Obstruction in seg E	
	Lighting RIU failure	Avionics function that will lead to lights out
	Lighting Control sw failure	Avionics function that will lead to lights out
	CDH switch failure	Avionics function that will lead to lights out
	OC 1 failure	Avionics function that will lead to lights out