Application of Diagnostic Analysis Tools to the Ares I Thrust Vector Control System

William A. Maul
QinetiQ North America, Cleveland, Ohio

Kevin J. Melcher
Glenn Research Center, Cleveland, Ohio

Amy K. Chicatelli
QinetiQ North America, Cleveland, Ohio

Stephen B. Johnson
Marshall Space Flight Center, Huntsville, Alabama

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to *help@ sti.nasa.gov*

- Fax your question to the NASA STI Help Desk at 443–757–5803

- Telephone the NASA STI Help Desk at 443–757–5802

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

Application of Diagnostic Analysis Tools to the Ares I Thrust Vector Control System

William A. Maul
QinetiQ North America, Cleveland, Ohio

Kevin J. Melcher
Glenn Research Center, Cleveland, Ohio

Amy K. Chicatelli
QinetiQ North America, Cleveland, Ohio

Stephen B. Johnson
Marshall Space Flight Center, Huntsville, Alabama

Application of Diagnostic Analysis Tools to the Ares I Thrust Vector Control System

William A. Maul
QinetiQ North America
Cleveland, Ohio 44135

Kevin J. Melcher
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Amy K. Chicatelli
QinetiQ North America
Cleveland, Ohio 44135

Stephen B. Johnson
National Aeronautics and Space Administration
Marshall Space Flight Center
Huntsville, Alabama 35812

Abstract

The NASA Ares I Crew Launch Vehicle is being designed to send astronauts into Earth orbit in support of missions to the International Space Station (ISS), to the Moon, and beyond. The launch vehicle is an in-line two-stage rocket with the crew vehicle, Orion, on top of the stack. The Ares I is undergoing design and development utilizing commercial-off-the-shelf tools and hardware when applicable, along with cutting edge launch technologies and state-of-the-art design and development techniques to ensure a safe, reliable, cost-effective space transportation system. In support of the vehicle's design and development, the Ares Functional Fault Analysis group was tasked to develop an Ares Vehicle Diagnostic Model (AVDM) and to demonstrate the capability of that model to support failure-related analyses and design integration. The AVDM is a directed graph model of failure effect propagation paths within the vehicle architecture and is a comprehensive representation of the system's failure space behavior. The AVDM is intended to support system engineering activities during the design process, and to provide diagnostic support throughout the development and deployment of the Ares I Launch Vehicle. During the Ares I design phase, the AVDM has been demonstrated to be valuable in the systems engineering process for assessing the completeness of schematics, and improving quality of various system design documents and analyses. The AVDM, along with supporting tools, has provided detection and fault isolation information to determine which components meet the diagnostic requirements for launch pad replacement and to assess system response to off-nominal conditions. One important component of the AVDM is the Upper Stage (US) Thrust Vector Control (TVC) diagnostic model—a representation of the failure space of the US TVC subsystem. This paper first presents an overview of the AVDM, its development approach, and the software used to implement the model and conduct diagnostic analysis. It then uses the US TVC diagnostic model to illustrate details of the development, implementation, analysis, and verification processes. Finally, the paper describes how the AVDM model can impact both design and ground operations, and how some of these impacts are being realized during discussions of US TVC diagnostic analyses with US TVC designers.

I. Introduction

The NASA Ares I Crew Launch Vehicle under the Constellation program is designed to send astronauts into Earth orbit in support of missions to the International Space Station (ISS) and, eventually, to leave Earth orbit on missions returning to the Moon. The launch vehicle is an in-line two-stage rocket with the crew vehicle, Orion, riding on top of the stack. The design and development of the Ares I utilize commercial-off-the-shelf (COTS) tools and hardware when applicable, along with cutting edge launch technologies and state-of-the-art design and development techniques to ensure a safe, reliable, cost-effective space transportation system. In support of the vehicle's design and development, and to ensure that thorough analyses of the system's fault isolation and detection capabilities have been addressed, the Functional Fault Analysis (FFA) team was formed within the Fault Detection, Diagnosis, and Response Working Group, which is under the Avionics and Software Team of the Ares Vehicle Integration project. Representatives from several NASA centers make up the FFA team. FFA team members located at the NASA Glenn Research Center (GRC) are responsible for developing portions of the Ares Vehicle Diagnostic Model (AVDM) associated with the Ares I Upper Stage (US) Thrust Vector Control (TVC) subsystem.

Overall, the FFA team has three major goals, namely:

- to perform analyses of vehicle failure detection (detection of effects generated by system faults) and fault isolation (identification of component faults responsible for the failure) capabilities for prelaunch and ascent,
- to support failure effect propagation time analyses for abort scenarios, and
- to deliver the AVDM to the Ares Ground-Based Diagnostics (AGBD) task.

With regard to these goals, analyses performed during the US TVC design phase identify failure detection and fault isolation gaps that can be addressed while the cost impact can be minimized. In a similar manner, failure effect propagation analyses—performed to determine the time it takes a failure effect to propagate through the entire integrated vehicle—can identify critical disconnects in the system design with respect to response times and allow mitigation strategies to be determined while the design is still fluid. Although the FFA Team is not directly responsible for developing a real-time diagnostic application, the FFA-developed AVDM will be delivered to the AGBD task for integration into a real-time diagnostic system.

A key aspect of the system engineering process is the determination of how the system handles off-nominal situations that may occur during prelaunch or flight operations. Off-nominal situations that may occur during prelaunch will impact logistics, on-site maintenance and ground-based management, and require launch commit criteria for detection. Off-nominal situations impacting flight operations require failure detection, isolation and recovery (FDIR), abort detection, and Caution and Warning (C&W) systems. Current practice is to develop Failure Modes and Effects Analysis (FMEA), which is a "bottom-up" approach to assessing component failures and how they propagate to system-level functionality, and Hazard Analysis (HA), which is a "top-down" approach to determining the causes of system-level failures. With either approach, it is difficult to verify that the system can properly detect and isolate off-nominal conditions. Direct detection may be identified in the analysis, but interactions within the system that impact the propagation of failure effects are difficult, if not impossible, to identify using these FMEA and HA tools. Fault isolation is not possible with either tool as they are not designed for this purpose and do not formally represent failure effect propagation paths, sensors, or the system architecture.

A strategy to address these gaps in failure detection and fault isolation requirement verification is developed by the FFA team through the AVDM (Ref. 1). The AVDM is a directed graph model of failure effect propagation paths within the vehicle's architecture and is intended to be a fundamental representation of the system's failure space behavior. Directed graphs have been utilized extensively in fault diagnostics (Refs. 2 to 4), because they provide a common, abstract representation of any type of

physical component and their physical connections within the system architecture. They are easy to understand as they model architectural connectivity in the same manner as the source schematics, and can be developed from either empirical or fundamental knowledge of the system.

The AVDM is being developed to provide diagnostic support throughout the design, development and deployment of the Ares I Launch Vehicle. In the Ares I design phase, the AVDM has proven to be a valuable systems engineering tool for assessing the completeness of schematics, FMEA reports and interface control documents, and the effectiveness of abort condition detection. The AVDM along with supporting tools has provided failure detection and fault isolation information to determine which components meet the diagnostic requirements for launch pad replaceable component, or Line Replaceable Unit (LRU), and to assess system response to off-nominal conditions. During vehicle development, the AVDM is intended to track the system evolution, providing diagnostic verification for design changes and to provide an off-line diagnostic tool that test personnel can use to diagnose system faults occurring at the test facilities. The AVDM will shadow the Ares I Launch vehicle from assembly and integration, through deployment. It will provide off-line diagnostic analysis of launch data including real-time diagnostics for prelaunch operations, and post-flight analysis for fleet supportability activities.

The AVDM integrates design information (e.g., system schematics, instrumentation program and command list (IPCL), and system specification and requirements documents), traditional systems engineering analysis (e.g., FMEA and Hazard Analysis) and operations information (e.g., concept of operations, mission timeline, operational checkout and testing procedures), into a formal analysis and modeling tool. The model can represent the failure effect propagation paths across all types of system physics, and it can be used to provide failure detection and fault isolation information in support of launch vehicle safety, reliability and availability requirements.

The intent of this paper is to demonstrate benefits of the FFA approach, in general, and the AVDM, specifically, to systems-of-systems architectures. This is accomplished using the US TVC portion of the AVDM to illustrate beneficial implementation and analysis capabilities. Section II provides a description of the AVDM and the associated model development process currently employed by the FFA modeling group. In Section III, application of the FFA development process to the US TVC is presented with an overview of US TVC operation. COTS and custom-designed software tools used to perform diagnostic modeling and analysis are discussed in Section IV; while specific diagnostic analysis techniques enabled by the model are described and demonstrated in Section V. Section VI discusses realized impacts of the FFA modeling process on the US TVC subsystem design and how those benefits translate to Ares I ground and in-flight systems (e.g., abort detection; C&W; FDIR) and, more generally, to system-of-systems applications. The paper closes with Section VII wherein a brief summary and some final remarks are presented.

II. Ares Vehicle Diagnostic Model (AVDM) Development

The FFA utilizes an iterative process in developing the system diagnostic models. The AVDM is partitioned into three major elements corresponding to the major elements of the Ares I vehicle: First Stage which contains the solid rocket boosters of the Ares I launch vehicle and supporting subsystems, Upper Stage which contains the vehicle's avionics, electrical power, thrust vector control and propellant supply subsystems; and the Upper Stage Engine, the J-2X. The diagnostic model for each element is further divided into subsystems; where each diagnostically modeled subsystem is independently developed through an iterative process. The diagnostic modelers gather the subsystem design information, extract the pertinent data and transfer it into the diagnostic model. Then, through a series of interviews and reviews with subsystem designers and domain experts, the subsystem diagnostic model is verified and updated. Resulting subsystem models are then integrated into the appropriate element diagnostic model which is then integrated into the AVDM. Integration requires an established agreement between the subsystem and element models that defines the appropriate propagation paths and the failure effects that are to be transmitted along those paths.

The FFA group has selected a commercial software package called the Testability Engineering and Maintenance System (TEAMS) tool suite (Refs. 5 and 6). The suite includes a number of software tools, including TEAMS-Designer and TEAMS-RT. Teams Designer is the development environment used to create and analyze diagnostic models, while TEAMS-RT is a real-time diagnostic engine. Both utilize a dependency matrix that maps the failure modes to tests available from measurements and observations. This study utilizes only the model development and assessment capabilities of TEAMS Designer. However, it is important to note that TEAMS RT provides a path for moving diagnostic models developed in TEAMS Designer to a real-time hardware/software platform.

TEAMS Designer provides a graphical user interface (GUI) that enables the development of hierarchical modules connected by propagation paths that reflect the design schematics of the system. Using the system schematics and interface control documents, nominal and failure effect propagation paths are defined and established in the diagnostic models. Because the GUI of the model visually reflects system designs, verification with domain experts is straightforward.

Within TEAMS Designer, the modeled system is represented by a series of TEAMS building blocks called modules. These modules can represent a single component or a collection of components enabling the establishment of a hierarchical architecture. Within the hierarchical structure of the model, failure effects are captured in the lowest modules. These modules are called failure modes and are contained within the system components and assembly modules in the same way that the FMEAs and HAs document the failure modes of the system. Alignment of the failure modes with the FMEAs and HAs enhances the verification process. If failure mode probabilities are available they can be assigned within the model and used in the diagnostic analyses. Otherwise the probability of each failure mode is assumed identical.

The failure effects assigned to each failure are propagated along the connections established between the system components. The diagnostic model contains another TEAMS modeling entity called a test point which represents sensors or other observables in the system (e.g., manual measurements or observations). Each test point contains a set of tests that generate a binary pass or fail outcome. One example of a test is a simple monitoring threshold check of a sensor measurement in the presence of a failure. If the sensor value is below the threshold the test fails, meaning it does not detect a designated effect, but if the sensor value exceeds the threshold the test passes. TEAMS Designer allows the model developer to enter test reliability, if available, that attempts to capture test uncertainties that impact detection such as sensor noise, sensor reliability or lack of model fidelity.

Each test is assigned a set of failure effects. The abstract qualitative representation of the failure effects and tests enable the early development of diagnostic strategies without getting dragged into the minutia before they are available. Refinement of the failure effects and the tests are on-going through the development and verification of the diagnostic model. Failure modes are detected by their assigned effect that propagates through a series of links to a test point with a test specifically for that effect. Another model building block called an effect node is similar to a test point, but differs in that it represents system end effects similar to those used in the fault tree analysis of the HA reports.

Beyond capturing design information, the diagnostic model within TEAMS Designer enables a diagnostic analysis of the system to detect failures and isolate faults under a variety of configurations and constraints. The FFA modelers utilize several of the TEAMS modeling features to capture system design information and to enhance the diagnostic analysis process.

- Hierarchical Labels—Each module has a hierarchical label property that defines a level within the diagnostic model. During the diagnostic analysis within TEAMS Designer, the user can set the fault isolation level by selecting the hierarchical label. Specifically, modules representing failures modes are labeled "Failure Modes" and those representing components designated for launch pad replacement are labeled "LRU".
- Naming Conventions—The FFA modeling group has established naming conventions for the various TEAMS modeling entities within the diagnostic model. These naming conventions for the modules, test points and tests enable the capture of system design information.

- Mapping Functions—Within TEAMS Designer, lowest-level modules can either be failure mode or effect mapping modules. An effect mapping module transforms an incoming effect to a new outgoing effect. The purpose of these mapping modules is to simulate the normal transition of effects within components. For example, the effect "Loss of electrical power" might be mapped to "Valve Closed" and "No Propellant Flow." An electrical effect is therefore mapped to a mechanical effect, the valve closing, and a fluid effect, no propellant flow.
- Test Labels—Tests within test points are assigned test labels. These can define the type of instrumentation, the purpose of the test or the sensor's criticality. Selection of test labels restricts the tests used in the diagnostic analysis.
- Technology Labels—The lowest level modules in TEAMS Designer have a technology label property. The technology label can define a failure mode's criticality during various periods of system operation. Selection of technology labels filters the failure modes considered in the diagnostic analysis.
- Switches—Switches are TEAMS modeling entities that establish unique configurations of the effect propagation paths due to the system operational phase. Switches can either have one input and two outputs or two inputs and one output. One input-output path combination is the default setting for the switch and the other path is established by assigning specific operational phases.

Figure 1 illustrates the TEAMS development window for a module of the US TVC diagnostic model. The red-hashed boxes represent failure mode modules and the green-hashed boxes the effect mapping modules. The white boxes are hierarchical modules that represent components and could contain failure modes and effect mapping modules. The lines represent the effect propagation paths within the model and the colors and thicknesses define the expected type of effects transmitted, i.e., electrical effects or mechanical effects. The attachment points for the lines at the module ports are also named with the expected transmitted effect type. These visual features aid domain experts in the verification process, and are developed to match domain documentation as much as possible, such as having colors in the model match the color of similar components or functions in the subsystem schematic.
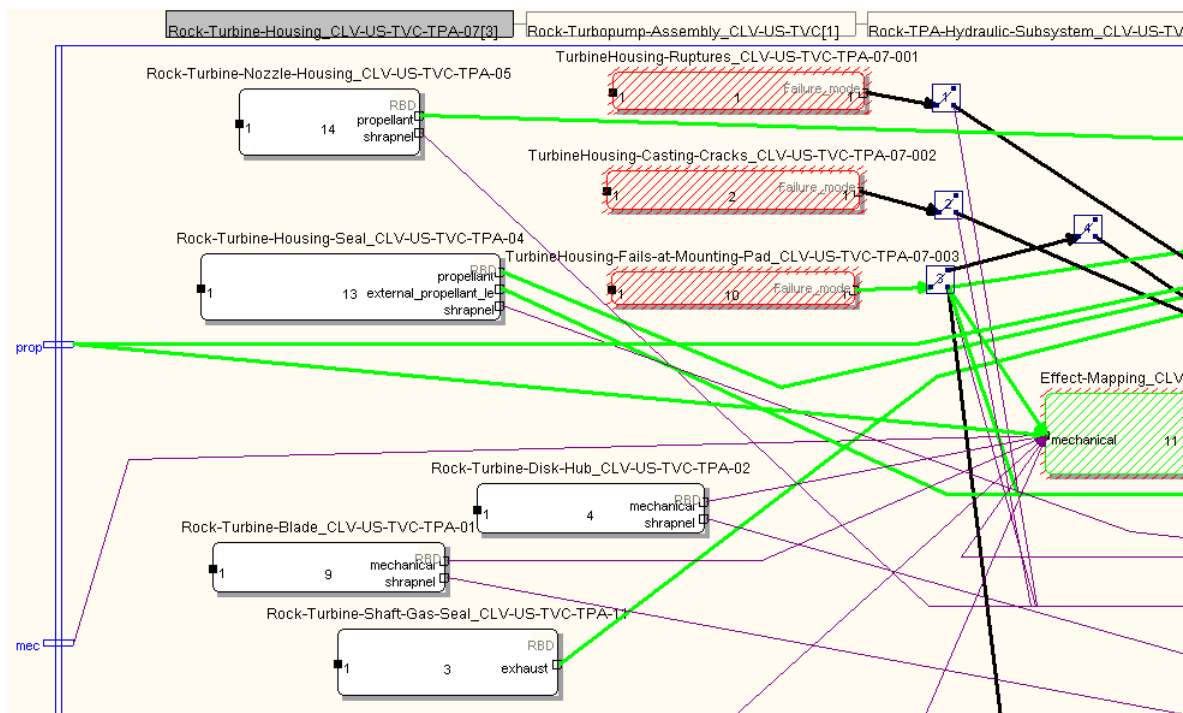

Figure 1.—TEAMS Designer interface displaying the hierarchical structure of a modeled component.

III. US TVC Application

The FFA modeling team at GRC has developed a subsystem model for the AVDM that represents the Ares I US TVC subsystem. As a microcosm of the AVDM, the US TVC subsystem offers numerous challenges in the development of a diagnostic model. This is because the subsystem is composed of components operating on a variety of physical properties: electrical, mechanical, thermal and fluid. The next two subsections provide an overview of the US TVC and the TEAMS-based diagnostic model that has been implemented for that subsystem.

A. Overview of US TVC Operation

As described in Reference 7, the primary function of the US TVC subsystem is to control the direction of the J-2X engine thrust in order to maintain the vehicle on its commanded flight trajectory. Figure 2 illustrates the US TVC subsystem architecture. A description of its operation is contained in the TVC Operations Concept Document (Ref. 8). Note that while the US TVC design has not been finalized, the architecture shown in Figure 2 is representative of the system as it was defined at the time of this report. Moving across the diagram from right to left, the gaseous hydrogen provided by the main propulsion system (MPS) enters and powers the turbine pump assembly (TPA) via the propellant valves. Once the TPA reaches full power, two independent power strings transport the hydraulic fluid from the pump to two actuators. In the event that one of the power strings fails, the other string can power both actuators. The actuators are positioned 45° from the vehicle pitch axis and are differentiated from each other by the designations Rock and Tilt. The actuators are controlled via a feedback loop using a single command input that is the consolidation of command outputs from three Data Command Units (DCUs). The DCUs receive position commands from the US avionics flight computers based on the vehicle trajectory and orientation measurements relative to the planned flight path.
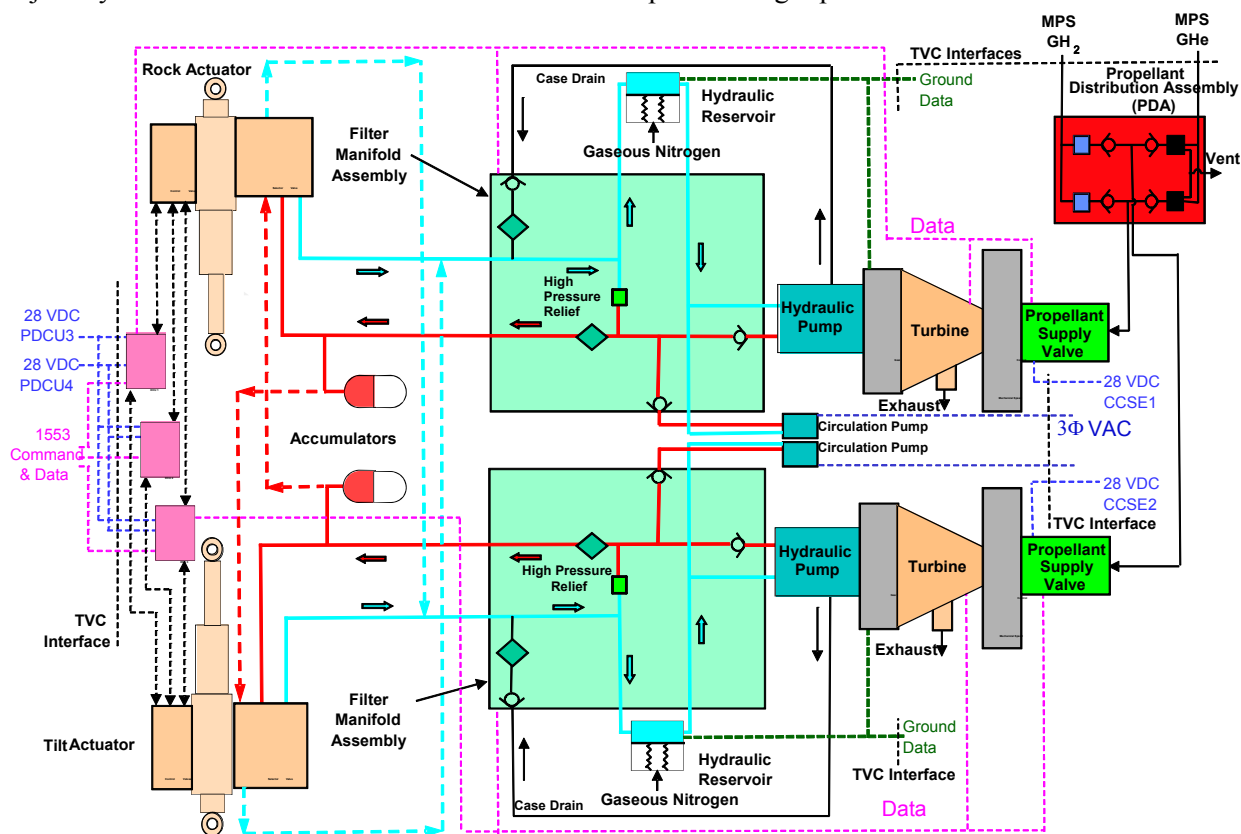

Figure 2.—Ares I upper stage thrust vector control subsystem schematic.

B. Implementation of US TVC Diagnostic Model

The US TVC subsystem contains many features that challenge the diagnostic modeling process. The hydraulic flow path is a closed-loop system, meaning that some failure effects can impact components in any direction along the flow path. This subsystem also interfaces directly with other systems, including the electrical power system, the MPS, the upper stage engine (USE) and avionics flight computers. The US TVC subsystem has several distinct operational phases from prelaunch to the end of the US ascent phases where certain components are active or functioning. Failure modes may be restricted to a single operational phase or common to several operational phases, and failure mode criticality may vary from one operating phase to the next depending on the failure's impact on the vehicle or crew. Further, the subsystem has redundant and single-string sensors located throughout the system to measure the various physical properties needed to determine US TVC operations and health status.

A TEAMS-based US TVC diagnostic model has been completed using the US TVC FMEA partition of the subsystem as a basis for the modeling hierarchical structure. The model reported here includes all of the US TVC components and redundant systems (e.g., both hydraulic strings are represented) and contains a total of 1106 TEAMS modules. This includes 607 failure modes and 222 effect mapping modules. Of the remaining 277 modules in the model, 7 are labeled as LRU and 160 are non-LRU designated components. The rest represent either sensors or higher-level containers within the design structure.

The test points and tests in the US TVC model are based solely on on-board sensors and anticipated tests within the flight computers to detect loss of signal or sensor failure. There are 62 test points in the model, each representing a sensor in the US TVC. There are 234 tests distributed over those test points. These tests may be applicable only for certain stages of operation, but currently within the diagnostic model they are applied uniformly throughout the mission profile. Future versions of the model could be made to distinguish between these tests through the use of test labels, so they are utilized only during appropriate operational phases. This modification would improve the test efficiency assessment for the system.

In addition to the previously described failure modes, the US TVC TEAMS model includes three external failure modes: electrical power system failure, and failures resulting in the loss of MPS Gaseous Hydrogen (GH2) and Gaseous Helium (GHe) to the US TVC. These failures were included in the model to assess their impact on the US TVC and to determine if their detection/confirmation could be obtained within the US TVC sensor suite. The model also includes a set of external test points in the avionics flight computers designed to test for loss of groups of US TVC signals due to cabling or bus failures.

The failure modes and the propagation path switches represented in TEAMS are aligned to specific phases of vehicle operation as defined in the Ares I Integrated Mission Timeline and presented here in Table 1. The unique criticality assigned to each failure mode for each operational phase is based on the values designated in the subsystem's FMEA.

TABLE 1.—TVC OPERATIONAL PHASES DEFINED FOR TEAMS MODEL

US TVC operational phases	System phase	Description
Prelaunch thermal conditioning	Prelaunch phase	Launch pad operational phase that provides thermal conditioning of the hydraulic fluid after cryogenic propellant is loaded on the vehicle. The US TVC circulation pumps are periodically operated to produce a low pressure flow in the hydraulic fluid circuit.
Prelaunch US TVC checkout	Prelaunch phase	Launch pad checkout test of the US TVC TPAs and actuators using GHe propellant.
Flight GHe operation	First stage boost and First stage separation phases	Initial flight bootstrap startup and initial operation of the US TVC using MPS-supplied GHe
Flight GH2 operation	US boost phase	US TVC operation after USE Ignition when GH2 pressure from the USE cooling circuit is sufficient to drive the TPAs, until USE shutdown.

IV. Diagnostic Analysis Process

This section provides an overview of the analysis available in TEAMS Designer and additional analysis capabilities available in the NASA Glenn-developed TEAMS Testability Analysis Tool (TTAT).

A. TEAMS Modeling and Analysis Environment

The TEAMS Designer can perform a diagnostic analysis or testability analysis of the developed model. As part of the diagnostic analysis, TEAMS propagates each failure mode through the model for a given set of user-specified conditions. These conditions include: the technology and test labels, the system mode, and the model fault isolation level. The diagnostic analysis generates a dependency matrix for the model, calculates several model diagnostic figures-of-merit, and enables an interactive mode that allows the user to explore details of the propagation paths within the model.

The dependency matrix is a one-to-one mapping between the failure modes and the tests used to detect them. In the dependency matrix, individual failure modes are associated with specific rows, while a specific test is associated with each column. Values of the dependency matrix may be only one (1) or no value at all. A value of one (1) in a given row and column indicates that the associated failure mode can be detected by the relevant test; no value indicates that it cannot. As an example, Figure 3 shows a portion of the dependency matrix generated by TEAMS for the US TVC diagnostic model.

As a result of the diagnostic analysis, TEAMS Designer generates a series of files that summarize the failure detection and fault isolation capabilities of the system. To facilitate this analysis, TEAMS Designer is capable of incorporating failure mode probabilities, test reliabilities, and fault propagation times, if available. Diagnostic figures of merit generated in the analysis include the Failure Detection Percentage and the Fault Isolation Percentage. The Failure Detection Percentage is equal to the number of failure modes detected by at least one test divided by the total number of failure modes involved in the analysis. The Fault Isolation Percentage is the number of isolated ambiguity groups divided by the total number of ambiguity groups. In this context, an ambiguity group is a set of failure modes that are detected by a unique set of tests referred to as the detection signature and an isolated ambiguity group contains only one member.

B. TEAMS Testability Analysis Tool

FFA model developers have created a TEAMS analysis post-processing tool, called the TEAMS Testability Analysis Tool (TTAT). TTAT extends the diagnostic analysis further, providing additional detail regarding the detection or missed detection of each failure mode. It also provides a breakdown of fault isolation capabilities between failure modes and between components. Result documents generated by the tool can be tailored to meet the expectation of the various verification reviews.

TTAT utilizes output files generated by the TEAMS Designer diagnostic analysis. These files include the model component hierarchy for the system under study, the TEAMS options file, which contains specific selections for the current analysis, and the dependency matrix. The TTAT program also requires an instrumentation description file that contains specific sensor identifiers and a description of the sensor extracted from the Ares I IPCL.

The TTAT detection analysis generates a list of failure modes that were not detected, as well as a detailed detection report that breaks down the detection signature of each individual failure mode. The detailed detection breakdown of the failures also provides information on the detection redundancy of the system. The redundancy demonstration could provide a level of verification for detection system confirmation requirements.

Failure Source:182, Tests:253	TPA Propellant Valve Not Energized	Propellant Pressure Low	Propellant Present	Turbine Overspeed	Low Turbine Rotation	Turbine Rotation	High Turbine Rotation		Hydraulic Supply Pressure Low	Hydraulic Supply Pressure High
Rock TVC Supply Valve Power Cable Short Circuit	1	1			1					
Rock TVC Propellant Supply Valve Power Cable Break-in-Wire	1	1			1				1	
Rock TVC Propellant Supply Valve Sticks Intermediate Position		1			1				1	
Rock TVC Propellant Supply Valve Fails to Close			1			1		...		
Rock TVC Propellant Supply Valve Fails to Open		1			1				1	
Rock TVC Propellant Supply Valve External Leak		1							1	
Rock Mechanical Speed Control Fails Causing Turbine Overspeed										1
⋮							⋮			⋮
Rock Mechanical Speed Control Causing Underspeed		1			1			...	1	
Rock GH2 Check Valve Fails to Open		1			1				1	

Columns represent the tests in the TEAMS model

A '1' at the intersection of a row and column indicates that the test is able to detect the failure mode

Rows represent the failure modes in the TEAMS model

Figure 3.—Example of TEAMS dependency matrix.

TTAT also generates another detection report that provides a breakdown of the failure modes detected by each test. This is essentially an examination of the individual columns in the dependency matrix to extract the failure modes detected. A single test may detect multiple failure modes. This report can help verify the importance of a test and/or test point.

The TTAT program performs ambiguity analysis at two distinct hierarchical levels within the model, failure mode and LRU, simultaneously. Ambiguity analysis at the failure mode level identifies the system's ability to isolate individual failure modes. While at the LRU level, the analysis determines the system's ability to distinguish failure modes contained within LRU and non-LRU components. Ambiguity metrics and detailed breakdowns of each ambiguity group are generated at both levels. Included in the breakdowns are the detection signature of the ambiguity group, and detailed information about each failure mode member in the ambiguity group.

LRU fault isolation ambiguity assessment can be complicated. An LRU can have several distinct failure modes with each potentially having a unique detection signature. Across the set of ambiguity groups, an LRU may be included in multiple groups. Therefore, it is possible for a given LRU to be isolated for some of its failure modes, while at the same time being ambiguous with respect to others. The TTAT program provides an additional report specifically for evaluating LRU fault isolation ambiguity.

The TTAT LRU assessment report provides a tabular breakdown of the active LRU failure modes, the associated ambiguity groups, and an indication that a given fault is detectable and isolatable. An example report is shown in Figure 4. For this report, an active LRU is a model component with a hierarchical label of LRU and a failure mode selected by technology label for the given diagnostic

Ambiguity Assessment Report - LRU Assignment to Ambiguity Group

Model Version: CLV_US_TVC_V8.0

Testability Run Date: Mon Mar 01 16:42:05 2010

Test Conditions
TEAMS Model Analyzed:
CLV_US_TVC_V8.0 (*within* CLV_US_TVC_V8.0)
System Modes:
Prelaunch_Thermal_Conditioning
Technology Labels:
Crit-1_Prelaunch-Thermal-Conditioning
Crit-3_Prelaunch-Thermal-Conditioning
Test Labels:
OFI
External

Ambiguity Summary Stats
Number of Active LRUs... 7
Number of Active Non-LRUs... 88
Number of Ambiguity Groups with LRU members............. 16
Number of Isolated Groups.. 10
Number of Isolated LRUs... 2
Tilt-Turbopump_Assembly_CLV-US-TVC
Rock-Turbopump-Assembly_CLV-US-TVC

LRU Ambiguity Output

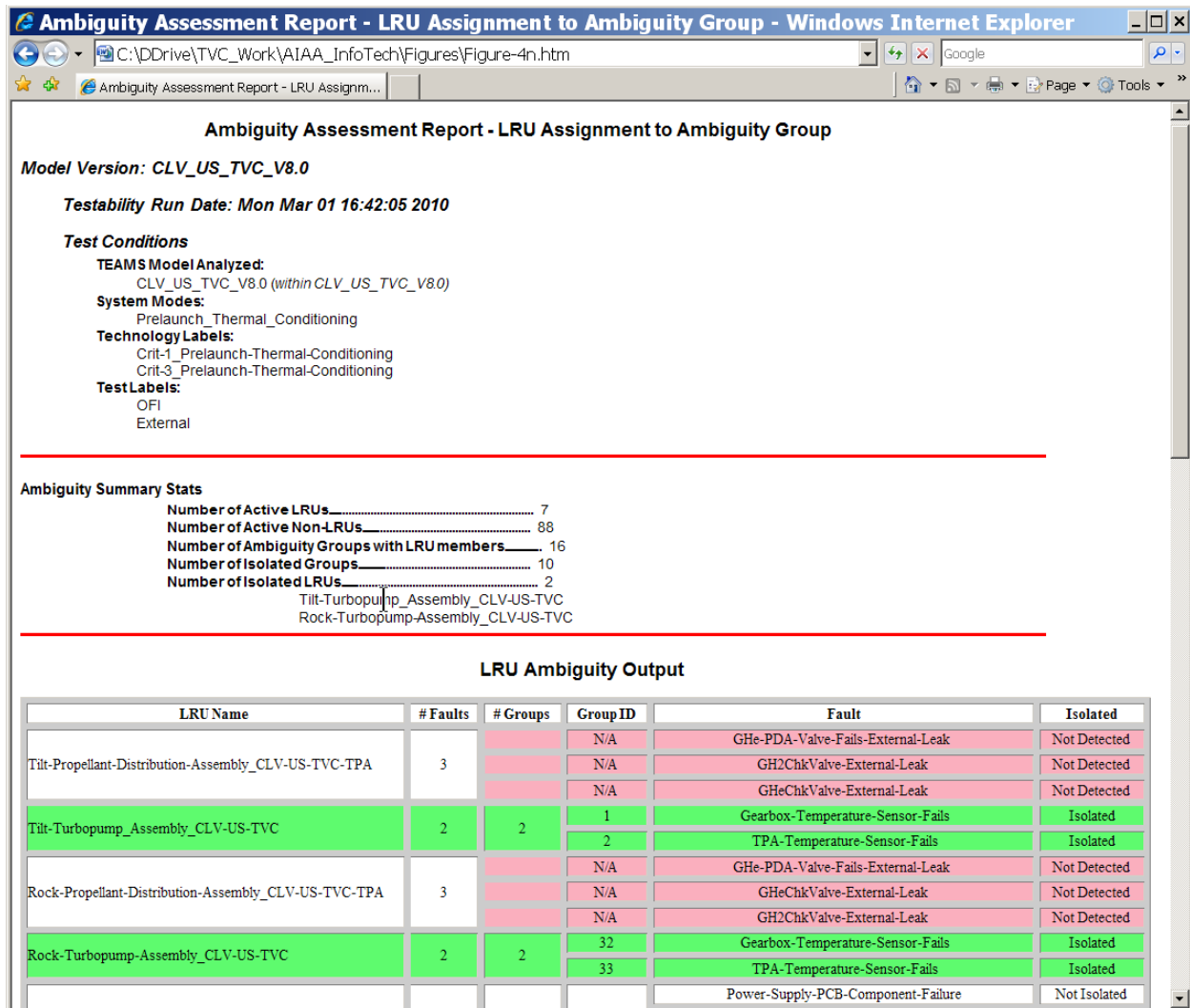| LRU Name	# Faults	# Groups	Group ID	Fault	Isolated
Tilt-Propellant-Distribution-Assembly_CLV-US-TVC-TPA	3		N/A	GHe-PDA-Valve-Fails-External-Leak	Not Detected
			N/A	GH2ChkValve-External-Leak	Not Detected
			N/A	GHeChkValve-External-Leak	Not Detected
Tilt-Turbopump_Assembly_CLV-US-TVC	2	2	1	Gearbox-Temperature-Sensor-Fails	Isolated
			2	TPA-Temperature-Sensor-Fails	Isolated
Rock-Propellant-Distribution-Assembly_CLV-US-TVC-TPA	3		N/A	GHe-PDA-Valve-Fails-External-Leak	Not Detected
			N/A	GHeChkValve-External-Leak	Not Detected
			N/A	GH2ChkValve-External-Leak	Not Detected
Rock-Turbopump-Assembly_CLV-US-TVC	2	2	32	Gearbox-Temperature-Sensor-Fails	Isolated
			33	TPA-Temperature-Sensor-Fails	Isolated
				Power-Supply-PCB-Component-Failure	Not Isolated

Figure 4.—Portion of the tabular display for the LRU assessment report generated by TTAT.

analysis. Highlighted red cells indicate failure modes that are undetected and highlighted green cells indicate failure modes and failure mode groups that are isolated for the LRU components. Rows completely highlighted in green indicate LRU components that are isolatable for the current analysis options. White cells indicate faults that cannot be isolated. This visual display is an important tool for presenting diagnostic results to design personnel unfamiliar with fault isolation issues for LRU components.

Another analysis option available in the TTAT program is a sensor sensitivity analysis. In TEAMS, tests are contained in a test point and the FFA modeling convention is that a test point represents a sensor. The sensor sensitivity analysis uses a user-defined input file that aligns sensors into groups called measurements and categories. Sensor measurements define sensor redundancy groups—a group of sensors measuring the same physical parameter at or near the same physical location. Sensor categories, on-the-other-hand, define groups of sensors that measure the same physical parameter at similar physical locations in redundant parts of the system. An example of this would be the two TPA speed sensors, one in the Tilt hydraulic power string and one in the Rock hydraulic power string.

Given a user-defined input file, the TTAT software systematically removes sensors or groups of sensors from the analysis and determines changes in the fault detection and failure isolation metrics. The TTAT program does not simply remove the sensor tests from the dependency matrix, but also the failure modes contained within those sensors. If there is a change, then it is highlighted and reported. The TTAT also identifies sensors that provide no diagnostic information beyond their own internal failure modes. Figure 5 illustrates a portion of one of the sensitivity analysis reports generated by the TTAT program. The report presents the test conditions for the diagnostic assessment. In this example, removal of a single sensor, Rock Hydraulic Supply Pressure, results in the loss of detection of the ten failure modes presented in red text.
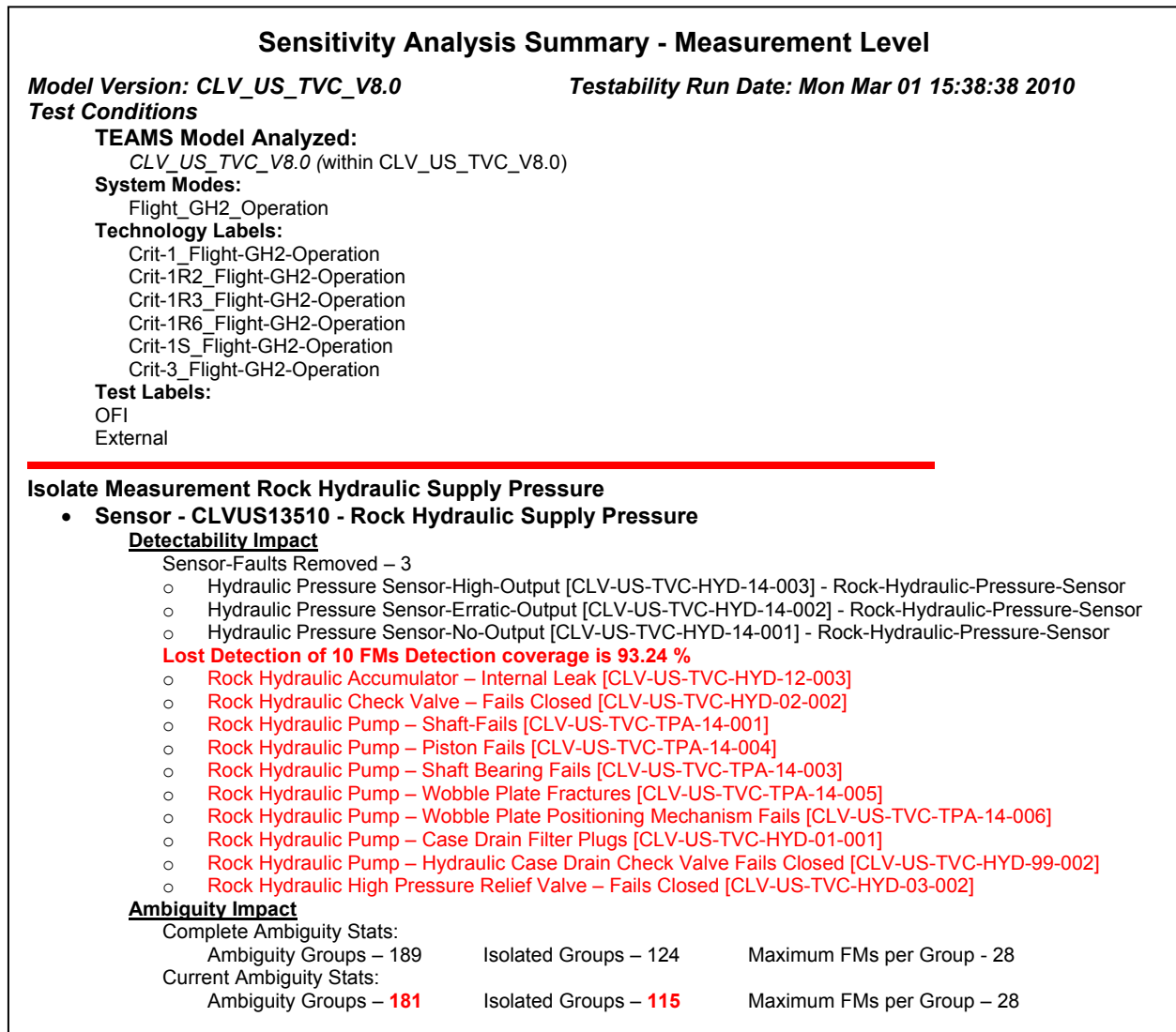

Sensitivity Analysis Summary - Measurement Level

Model Version: CLV_US_TVC_V8.0   **Testability Run Date: Mon Mar 01 15:38:38 2010**

Test Conditions
    TEAMS Model Analyzed:
      *CLV_US_TVC_V8.0 (*within CLV_US_TVC_V8.0)
    System Modes:
      Flight_GH2_Operation
    Technology Labels:
      Crit-1_Flight-GH2-Operation
      Crit-1R2_Flight-GH2-Operation
      Crit-1R3_Flight-GH2-Operation
      Crit-1R6_Flight-GH2-Operation
      Crit-1S_Flight-GH2-Operation
      Crit-3_Flight-GH2-Operation
    Test Labels:
    OFI
    External

_____

Isolate Measurement Rock Hydraulic Supply Pressure
- **Sensor - CLVUS13510 - Rock Hydraulic Supply Pressure**
    Detectability Impact
    Sensor-Faults Removed – 3
  - Hydraulic Pressure Sensor-High-Output [CLV-US-TVC-HYD-14-003] - Rock-Hydraulic-Pressure-Sensor
  - Hydraulic Pressure Sensor-Erratic-Output [CLV-US-TVC-HYD-14-002] - Rock-Hydraulic-Pressure-Sensor
  - Hydraulic Pressure Sensor-No-Output [CLV-US-TVC-HYD-14-001] - Rock-Hydraulic-Pressure-Sensor

  Lost Detection of 10 FMs Detection coverage is 93.24 %
  - Rock Hydraulic Accumulator – Internal Leak [CLV-US-TVC-HYD-12-003]
  - Rock Hydraulic Check Valve – Fails Closed [CLV-US-TVC-HYD-02-002]
  - Rock Hydraulic Pump – Shaft-Fails [CLV-US-TVC-TPA-14-001]
  - Rock Hydraulic Pump – Piston Fails [CLV-US-TVC-TPA-14-004]
  - Rock Hydraulic Pump – Shaft Bearing Fails [CLV-US-TVC-TPA-14-003]
  - Rock Hydraulic Pump – Wobble Plate Fractures [CLV-US-TVC-TPA-14-005]
  - Rock Hydraulic Pump – Wobble Plate Positioning Mechanism Fails [CLV-US-TVC-TPA-14-006]
  - Rock Hydraulic Pump – Case Drain Filter Plugs [CLV-US-TVC-HYD-01-001]
  - Rock Hydraulic Pump – Hydraulic Case Drain Check Valve Fails Closed [CLV-US-TVC-HYD-99-002]
  - Rock Hydraulic High Pressure Relief Valve – Fails Closed [CLV-US-TVC-HYD-03-002]

    Ambiguity Impact
    Complete Ambiguity Stats:
      Ambiguity Groups – 189   Isolated Groups – 124   Maximum FMs per Group - 28
    Current Ambiguity Stats:
      Ambiguity Groups – **181**   Isolated Groups – **115**   Maximum FMs per Group – 28

Figure 5.—Portion of the main output page from TTAT software that displays the sensitivity analysis summary.

V. Diagnostic Analysis for Upper Stage Thrust Vector Control Application

This section provides two example case studies performed on the US TVC diagnostic model. The first case study demonstrates the application of TTAT to the US TVC model for flight operation and includes a sensor sensitivity assessment. The second case study demonstrates the application of TTAT to the US TVC model for Prelaunch LRU assessment.

A. Case Study 1—Failure Mode Ambiguity Analysis

For the Ares I flight phases, two distinct US TVC operational phases were available for testing: Flight GHe Operation and Flight GH2 Operation. For Flight GHe Operation, GHe supplies power to the TPA during initial boot-up and operation of the US TVC. This operational phase begins just prior to the end of first stage operation, continues through the US separation, and ends during the initial phase of upper stage operation. For Flight GH2 Operation, GH2 from the J-2X cooling circuit provides the working fluid for the US TVC TPAs. This operational phase is conducted entirely within the upper stage operation. Since there is significant similarity between the two operational phases, only the Flight GH2 Operation mode is evaluated here.

Failure modes are restricted through technology labels consistent with the US TVC FMEA assigned criticalities. Technology labels contain a criticality of "1", "1R" or "1S". The "1" critical failure modes result in worst-case effects leading to loss of vehicle or loss of crew. The "1R" critical failure modes contain at least one level of fault tolerance prior to a criticality 1 failure. The "1S" critical failure modes are the failure of a safety device intended to mitigate a criticality 1 failure or a safety monitoring device used for mitigation purposes. The remaining failure modes are considered benign failures, having little or no effect on the system, and are designated with technology labels of "3".

For the Flight GH2 Operation operating phase, the model contained 567 active failure modes and 253 tests. The detection coverage was found to be 95.04 percent with 28 undetectable failure modes. There are 189 ambiguity groups generated for the ambiguity analysis. At the failure mode level, 124 of the 189 ambiguity groups are isolatable, meaning they have a single failure mode.

During flight operation, ambiguity metrics at the LRU level are not important since no in-flight repairs are possible, but at the failure mode level an ambiguity analysis would reveal any inability to distinguish between failure modes with differing levels of criticality. For example, it is critical that the detection signature for failure modes that results in an identified C&W condition not be confounded with faults that do not. Each ambiguity group must be reviewed at the failure mode level. Ambiguity groups containing failure modes with differing criticalities need to be reviewed by the subsystem designers as well as those with differing mitigation actions. Assuming that criticality assignments and the TEAMS model are verified, designers need to assess the impact of an inaccurate diagnosis. Currently mitigation actions are not identified in this analysis, but they could be, using test points aligned to system end effects.

Included in the TTAT ambiguity group breakdown report are the failure mode criticalities for each failure mode in the ambiguity group. For this case study, several ambiguity groups had failure mode members that did not have identical criticalities assigned. Each of these discrepancies will need to be reviewed and resolved by the subsystem designers. As an example, notice ambiguity group #127 in Figure 6 where several criticality 1 and criticality 1R failure modes are listed. The red highlighted boxes indicate two failures modes with a criticality 1 setting. Since they exhibit the same detection signature as other criticality 1R failure modes, the questions to be explored are:

- Are the criticality assignments for the failure mode in this group correct and appropriate?
- Are the failure modes accurately modeled within TEAMS?
- What is the impact of improper diagnosis between the failure modes with differing criticalities?
- Are additional tests needed to be able to distinguish these failure modes from one another?
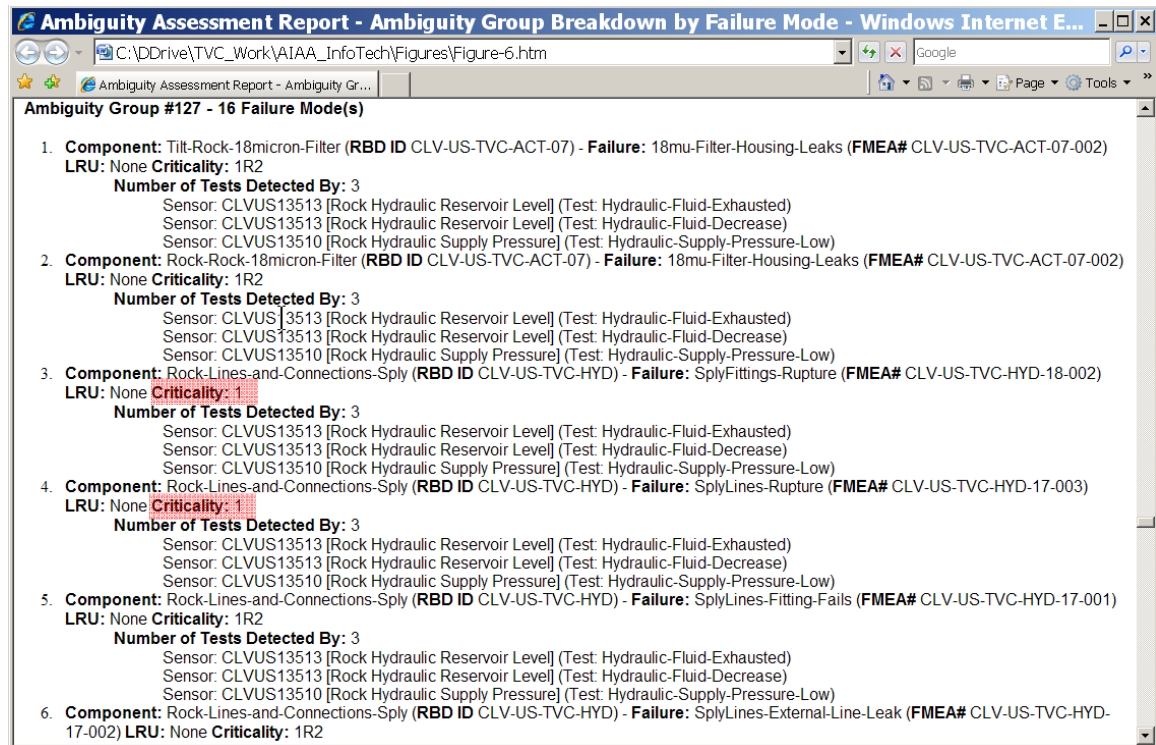
Figure 6.—Screen capture of the TTAT ambiguity group breakdown from failure mode report for the US TVC flight GH2 operation diagnostic analysis.

Extending this case study further, the TTAT program was used to generate a sensor sensitivity analysis on the diagnostic performance of the model. A summary of the sensitivity analysis is presented in Figure 7. Sixteen (16) sensors are identified as providing no diagnostic contribution for the current analysis. Included in this set are temperature measurements of the DCUs and the TPAs. These sensors were recently added to the US TVC design and, subsequently, to the diagnostic model. Although they have tests assigned in the test points, the associated failure effects are not yet linked to any modeled failure modes in the model. Also, actuator differential pressures, used mainly for trim control of the actuator movement, have no detection tests associated with them.

Table 2 shows the impact of the removal of individual or groups of sensors on the detection of failure modes. Columns 1, 3, and 5 from the table identify the sensor or groups of sensors removed in each sensitivity analysis cycle. For the first analysis cycle, individual sensors are removed iteratively from the sensor suite and the diagnostic metrics for failure detection and fault isolation are performed. For the second analysis cycle, sensors that are redundant in measuring the same physical parameter are removed as a group iteratively, and again the diagnostic metrics are re-computed. For the final analysis cycle, sensors measuring similar physical measurements across redundant components in the system are removed as a group iteratively prior to computing the same diagnostic metrics. The diagnostic metrics for each iteration is compared to the case where all the sensors are available. In the table, the complementing columns 2, 4, and 6 report the failure modes that are no longer detected upon removal of the sensor or group of sensors.
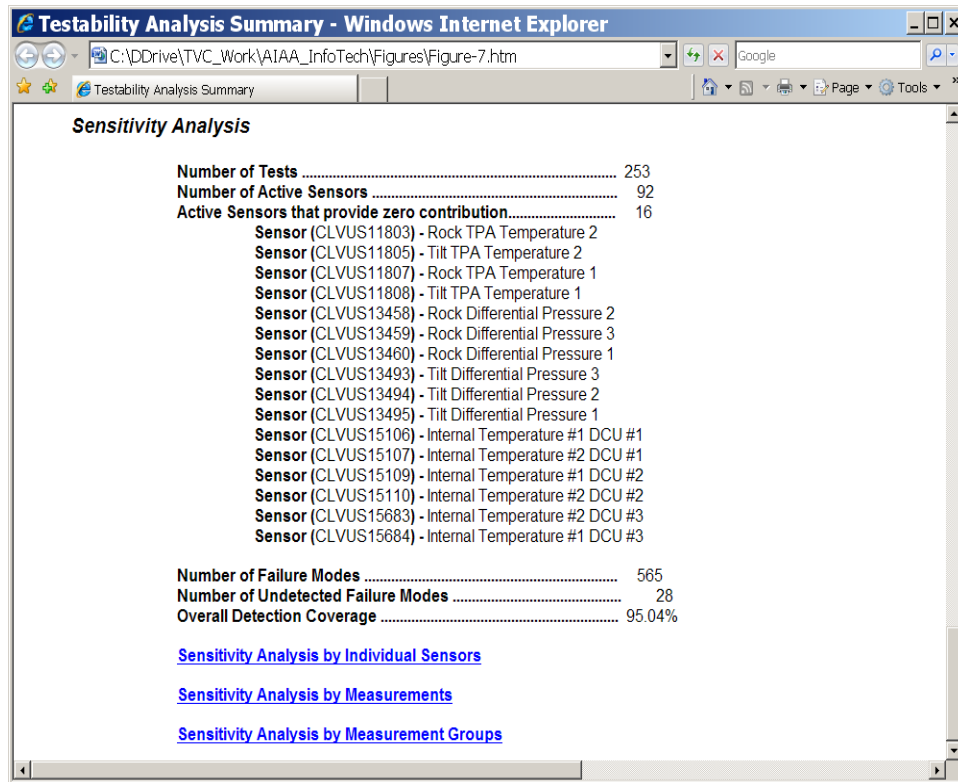
Figure 7.—Portion of the main output page from TTAT that displays the sensitivity analysis summary for US TVC diagnostic analysis for the flight GH2 operation phase.

TABLE 2.—DETECTABILITY IMPACTS SUMMARIZED FROM THE US TVC SENSITIVITY ANALYSIS

Individual sensors removed		Redundant sensors removed		Sensor groups removed	
Sensor identifier	Failure modes undetected	Parameter	Failure modes undetected	Category	Failure modes undetected
CLVUS13510	13	Rock hydraulic supply pressure	13	Hydraulic supply pressure	26
CLVUS13518	13	Tilt hydraulic supply pressure	13		
CLVUS13514	0	Rock hydraulic reservoir temperature	1	Hydraulic reservoir temperature	2
CLVUS17366	0				
CLVUS13522	0	Tilt hydraulic reservoir temperature	1		
CLVUS17367	0				

Table 2 also displays a selection of sensors that demonstrate the loss of detection when those sensors are removed, either individually or as a group. For example, the Rock and Tilt hydraulic supply pressures are single sensors with no redundancy. The removal of either sensor results in an inability to detect 13 failure modes. The Rock and Tilt hydraulic reservoir temperatures do have redundant sensors. The loss of a single sensor does not impact failure detection capability, but the loss of both results in a loss of failure mode detection capability. This indicates that for this failure mode, the hydraulic temperatures currently provide the only detection test. This illustrates the affect of no redundancy and the lack of independent confirmation for failure mode detections. The sensor sensitivity analysis allows the designer to not only determine the loss of failure detection with the removal of a sensor, but also to begin to explore the impact on fault isolation with each removal.

B. Case Study 2—LRU Ambiguity Analysis

The US TVC has two distinct prelaunch operational phases: Prelaunch Thermal Conditioning and Prelaunch US TVC Checkout. Prelaunch Thermal Conditioning covers the US TVC thermal conditioning operation that begins after cryogenic propellant is loaded on the vehicle and ends at US TVC prelaunch checkout testing and Prelaunch US TVC Checkout covers the US TVC prelaunch checkout testing period just prior to vehicle launch.

For these two operational phases, diagnostic analysis was conducted on the US TVC model using both the TEAMS Designer software and the FFA-developed TTAT software. Failure modes are restricted to criticalities of "1", (indicating worst-case effects leading to loss of vehicle or crew) and "3" (indicating a potential launch scrub or delay), as recorded in the US TVC FMEA.

1. Diagnostic Analysis for US TVC Thermal Conditioning During Prelaunch

For the Prelaunch Thermal Conditioning (PTC) operating phase, the US TVC has two circulation motors that are operated periodically to produce a small hydraulic flow through the fluid circuit in both the Rock and Tilt hydraulic power strings. The purpose is to prevent the fluid from freezing due to the close proximity to the cryogenic propellants. Since the hydraulic flow is not routed through the TPAs, those components are heated independently using electrical heaters that are not yet included in the diagnostic model. For the diagnostic analysis during PTC, 260 failure modes were active and 253 tests were available. The detection coverage was found to be 96.92 percent with 8 failure modes undetected. These eight failure modes represent external leakages of GHe propellant at four different locations in the propellant supply legs of the Rock and Tilt hydraulic power strings. Discussions with US TVC designers indicate that monitoring of unexpected loss of GHe in the MPS is being considered. A determination of the exact monitoring capability is still being developed. If such a monitoring capability were implemented, then the eight (8) undetected failures would presumably be detected by external tests in the MPS, which stores and distributes the GHe.

PTC ambiguity analysis results show that 89 ambiguity groups were generated with 16 ambiguity groups containing failure modes from LRU components. Further, for this PTC analysis, the US TVC has seven (7) LRUs and 88 non-LRU components with at least one active failure mode. Performing the ambiguity analysis for failure mode isolation, 51 of the 89 ambiguity groups, 57.3 percent, are isolated, meaning these groups contain a single failure mode. Ambiguity analysis for LRU isolation reveals 10 of the 16 ambiguity groups, 62.5 percent, that contain LRU component failure modes are isolated, meaning they contain failure modes that are specific to a single LRU component. Figure 8 is a snapshot of output from the TTAT-generated report that indicates ambiguity group distribution by number of LRU or Non-LRU component elements. The other six (6) ambiguity groups that contain at least one LRU component have only two (2) members.

The TTAT LRU assessment shows that 2 LRUs, the Rock and Tilt TPAs, are isolated. In addition, the three (3) DCUs are nearly isolatable except for the inability to distinguish between the loss of power due to internal DCU power-supply printed circuit board failure and the external power supply cables. The remaining two LRU components are the Rock-side and Tilt-side propellant distribution assemblies, and based on the analysis, none of their failure modes were detectable. Figure 9 shows a portion of the TTAT-generated LRU Assessment report with a failure mode breakdown for the various LRUs displayed. Failure mode entries highlighted in red indicate that the failure mode was undetected. Failure modes highlighted in green are isolated with respect to the LRU component. If the entire set of failure modes for a given LRU is isolated, the entire row is highlighted in green. Other reports provided by the TTAT identify the members of each ambiguity group. By reviewing these reports, the user can identify what other non-LRU components are confounded with the LRU faults; and determine the reason for the ambiguity. Figure 10 provides a screen capture portion of this report which shows that the DCU power supply PCBs faults are confounded by the power supply cable faults.
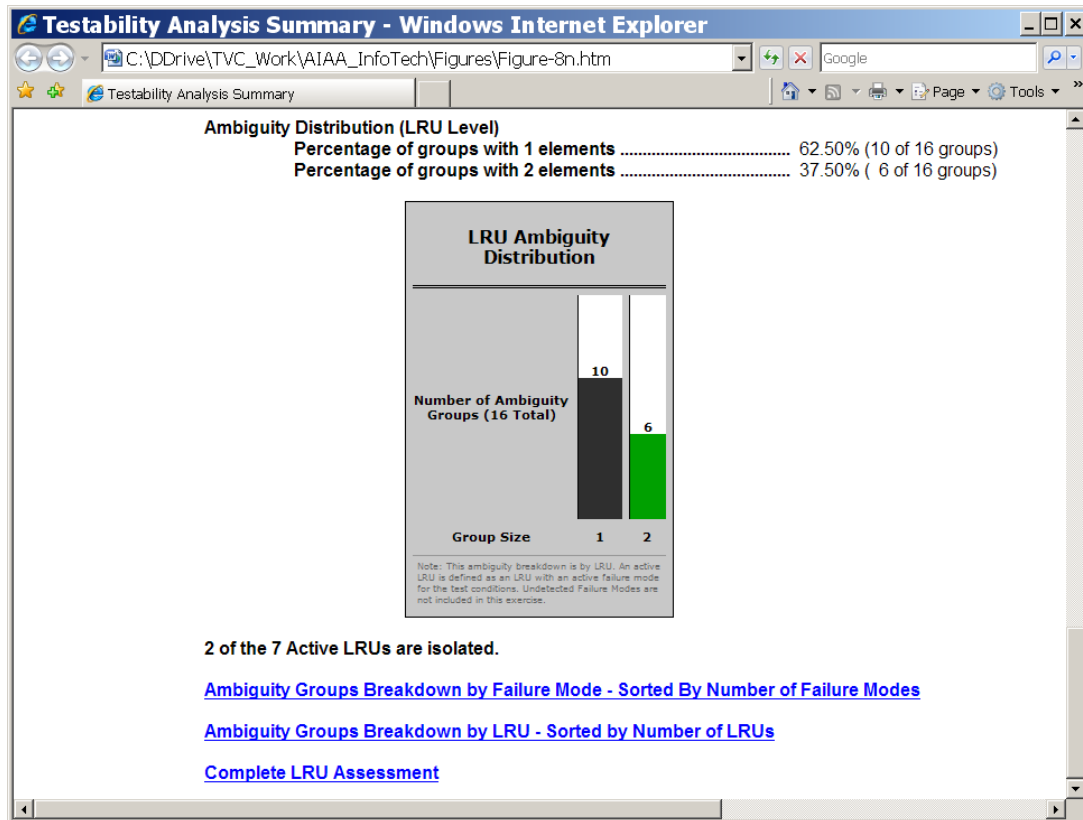
Figure 8.—TTAT LRU ambiguity distribution for US TVC prelaunch thermal conditioning case study.

Figure 9.—TTAT LRU assessment report generated for US TVC prelaunch thermal conditioning case study.
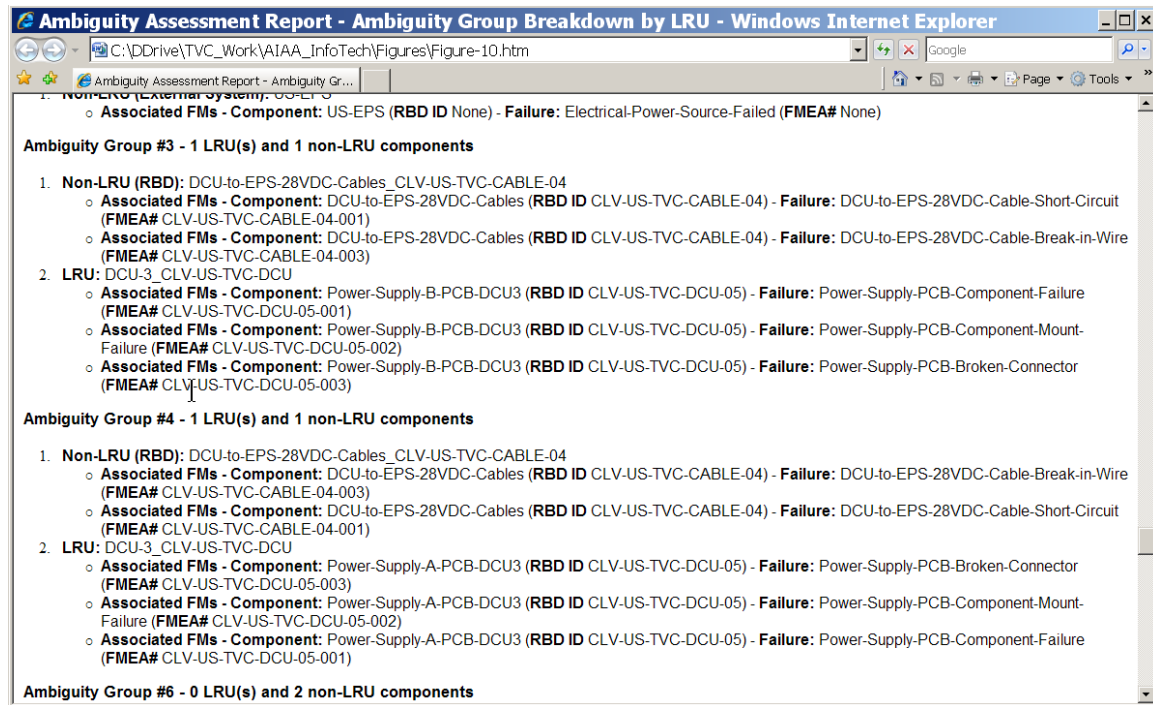
Figure 10.—Screen capture of the TTAT report providing a detailed breakdown of the LRU ambiguity groups for the US TVC prelaunch thermal conditioning diagnostic analysis.

2. Diagnostic Analysis for US TVC Checkout During Prelaunch

During Prelaunch US TVC Checkout, the US TVC is pressurized using MPS-supplied GHe propellant to drive the TPAs. The actuators gimbal the engine through predefined patterns and proper operation is verified by various performance parameters. For the ambiguity analysis associated with this operating phase, 567 failure modes were active and 253 tests were available. The detection coverage was found to be 94.71 percent with 30 failure modes undetected.

There are 184 ambiguity groups generated for the ambiguity analysis, with 50 ambiguity groups containing failure modes associated with LRU components. The US TVC in this analysis has seven (7) active LRUs and 123 non-LRU components with at least one active failure mode. At the failure mode level, 120 of the 184 ambiguity groups, 65.22 percent, are isolated. At the LRU level, 38 of the 50 ambiguity groups, 76 percent, are isolated, and only two (2) of the ambiguity groups contain more than three (3) component elements as failed candidates. The TTAT LRU Assessment reports that none of the LRUs were completely isolated across all of their failure modes.

A more detailed look at the Rock and Tilt TPAs reveals that each TPA has 46 active failure modes for the mode of operation analyzed. Four failure modes are undetectable. Of the undetectable failure modes, two involve parts that fall off the vehicle, and two are very minor faults that result in no impact on TPA performance. The minor faults are retained in the TEAMS model for alignment with the FMEA.

Of the detected failure modes, all but 9 of the failure modes are isolatable with those being contained in three ambiguity groups. Further investigation of the three ambiguity groups for each TPA reveals that one ambiguity group is a collection of failure modes that result in the loss of hydraulic fluid. There are a number of components along the hydraulic flow path that could fail causing external leakage and this would be difficult to distinguish without visual inspection. A second ambiguity group confounds the loss of function of the hydraulic pump to produce hydraulic pressure and the failure of the hydraulic fluid check valve opening. The last ambiguity group contains a TPA fault in the mechanical speed control mechanism which would result in the propellant supply path to the TPA turbines being closed. This fault is confounded with other losses of propellant supply at the propellant supply valve and the propellant distribution assembly.

Results from diagnostic analyses, like those discussed here, provide designers with knowledge about the strengths and weaknesses of their design from a diagnostic viewpoint. Designers can use this diagnostic knowledge about their system to identify new approaches that improve failure detection and fault isolation or to further evaluate the effects reported by the FMEA and captured in the model.

VI. Impact of the Diagnostic Model on the Design Process

The US TVC diagnostic model, described in this report, has been utilized in several areas of the subsystem's design process. While the diagnostic metrics are important and useful, it is often the interrogation of the model and the associated results that offer the larger rewards and benefits.

In the development of the US TVC diagnostic model, inconsistencies and omissions in the FMEA, design schematics and operations concept were uncovered. While similar findings would be encountered during the development of any simulation, hardware or software, the diagnostic model is unique in that it is modeling the failure mode effects, rather than nominal operation. Also, the diagnostic model is abstract enough to incorporate a large number of failure conditions with minimal detailed design information. This enables a useful level of diagnostic analysis early in the design process when modifications can be implemented with minimal impact to cost and schedule.

There is a process to determine whether or not a component should be designated as an LRU. The component is first assessed to determine if it is life limited or of high criticality. If the component meets either of those criteria, the next requirement is that the failures of the potential LRU must be detectable and isolatable. The ambiguity analysis provided by the TEAMS Designer and TTAT offers a verification of the fault isolation requirement not achievable with other system engineering tools. For US TVC, ambiguity analysis was provided for the LRU assessment of the hydraulic filter manifold assembly. The analysis provided a backdrop for discussions about the various failure modes and their probabilities of occurrence. The hydraulic filter manifold assembly was later removed from the LRU component list due primarily to the complexity of launch pad removal and replacement; nevertheless, the ambiguity analysis did provide insight into failure detection and fault isolation considerations.

The US TVC diagnostic model has also been utilized in a series of off-nominal analysis discussions where design engineers walk through the subsystem, component-by-component, investigating each failure mode. This includes evaluating each failure mode's impact on system performance and what sensors, if any, could be used to detect the failure effects. Early discussions surrounding the propellant distribution assembly revealed an inability to detect leakage of GHe due to faults in several elements in that assembly. As a result, discussions have been initiated with the MPS design personnel to define a monitoring strategy for this failure condition.

The US TVC diagnostic model is also involved in several other on-going activities. The model is being utilized as a verification tool for requirements to detect and isolate recoverable faults of the subsystem. Further, the diagnostic and sensor sensitivity analysis from the model are expected to support the justification of proposed subsystem instrumentation. And finally, the US TVC model will be used to demonstrate FMEA-Fault Tree linkage with probabilistic risk assessment tools.

VII. Summary

A diagnostic model is being developed for the Ares I Launch Vehicle based on a directed graph representation of failure effect propagation paths within the system. The purpose of the diagnostic model is to support the design of the vehicle through assessment of the diagnostic capabilities of the system and to support the development of a real-time diagnostic tool for testing and prelaunch operations.

This paper has presented a diagnostic model for the Upper Stage (US) Thrust Vector Control (TVC) subsystem of the Ares I vehicle as well as the diagnostic analysis tools used to evaluate that model. The diagnostic model was developed with the aid of TEAMS-Designer, a commercial software tool. Features of the model and the utilization of those features in developing and using associated analysis tools were described. Two case studies were presented that demonstrate the potential application of the results from

the diagnostic analysis of this model. The first case study illustrated how the fault detection assessment could be applied to flight operations, including sensor sensitivity studies. The second case study explored the failure detection and isolation for prelaunch operations, focusing on failure isolation assessment of components that are replaceable on the launch pad. These studies demonstrate that the diagnostic model can be utilized to verify failure detection and fault isolation capabilities for both prelaunch and in-flight operations.

Even during its development, the diagnostic model can support a number of system engineering activities. The model essentially is an actionable Failure Mode and Effects Analysis (FMEA), capable of being exercised interactively to extract useful information. While the diagnostic metrics are important and useful, it is often the detailed interrogation of the model and the diagnostic results that offer the larger rewards and benefits to the system engineering process. The model uses a common, abstract representation that can be applied to any system and eases verification by providing a model architectural connectivity that is similar to the source schematics. Further, the abstract qualitative representation of the failure effects and tests enable the early development of diagnostic strategies. This diagnostic model has the potential to become an integral tool in the systems engineering arsenal, providing information through subsystem development and vehicle integration.

References

1. Kurtoglu, T., Johnson, J., Barszcz, E., Johnson, J., and Robinson, P., "Integrating System Health Management into the Early Design of Aerospace Systems Using Functional Fault Analysis," 2008 International Conference on Prognostics and Health Management, Denver, Colorado, October 7, 2008.
2. Mohindra, S., and Clark, P., "A Distributed Fault Diagnosis Method Based on Digraph Models: Steady-State Analysis, Computers and Chemical Engineering," Volume 17, Issue 2, February 1993, pp. 193–209.
3. Yang, F. and Xiao, D., "Sensor Location Strategy in Large-Scale Systems for Fault Detection Applications," Journal of Computers, Vol. 3, No. 11, November 2008.
4. Zhang, Z., Wu, C., Zhang, B., Xia, T., and Li, A., "SDG Multiple Fault Diagnosis by Real-Time Inverse Inference, Reliability Engineering and System Safety," Volume 87, Issue 2, February 2005, pp. 173–189.
5. Deb, S., Pattipati, K.R., Raghavan, V., Shakeri, M., Shrestha, R., "Multi-Signal Flow Graphs: A Novel Approach for System Testability Analysis and Fault Diagnosis," IEEE Aerospace and Electronics Systems Magazine, Vol. 10, No. 5, pp. 14–25, 1995.
6. QualTech Systems Incorporated website, http://www.teamsqsi.com.
7. GRC-TVC-REQ-001 Thrust Vector Control Subsystem Requirements Document, Revision A, National Aeronautics and Space Administration, March 5, 2009.
8. GRC-TVC-OPS-001 Thrust Vector Control Operations Concept Document, Baseline (Draft), National Aeronautics and Space Administration, March 10, 2009.

1. REPORT DATE (DD-MM-YYYY) 01-06-2010	2. REPORT TYPE Technical Memorandum	3. DATES COVERED (From - To)

4. TITLE AND SUBTITLE
Application of Diagnostic Analysis Tools to the Ares I Thrust Vector Control System

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Maul, William, A.; Melcher, Kevin, J.; Chicatelli, Amy, K.; Johnson, Stephen, B.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
WBS 136905.08.05.07.01.03

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field
Cleveland, Ohio 44135-3191

8. PERFORMING ORGANIZATION REPORT NUMBER
E-17268

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITOR'S ACRONYM(S)
NASA

11. SPONSORING/MONITORING REPORT NUMBER
NASA/TM-2010-216333

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Categories: 12 and 19
Available electronically at http://gltrs.grc.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 443-757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The NASA Ares I Crew Launch Vehicle is being designed to support missions to the International Space Station (ISS), to the Moon, and beyond. The Ares I is undergoing design and development utilizing commercial-off-the-shelf tools and hardware when applicable, along with cutting edge launch technologies and state-of-the-art design and development. In support of the vehicle's design and development, the Ares Functional Fault Analysis group was tasked to develop an Ares Vehicle Diagnostic Model (AVDM) and to demonstrate the capability of that model to support failure-related analyses and design integration. One important component of the AVDM is the Upper Stage (US) Thrust Vector Control (TVC) diagnostic model-a representation of the failure space of the US TVC subsystem. This paper first presents an overview of the AVDM, its development approach, and the software used to implement the model and conduct diagnostic analysis. It then uses the US TVC diagnostic model to illustrate details of the development, implementation, analysis, and verification processes. Finally, the paper describes how the AVDM model can impact both design and ground operations, and how some of these impacts are being realized during discussions of US TVC diagnostic analyses with US TVC designers.

15. SUBJECT TERMS
Fault detection; Graph theory

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON STI Help Desk (email:help@sti.nasa.gov)
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	UU	25	19b. TELEPHONE NUMBER (include area code) 443-757-5802