# Fault Detection and Isolation in the Non-Toxic Orbital Maneuvering System and the Reaction Control System

*Mohammad Azam, *David Pham, §Fang Tu, *Krishna Pattipati, †Ann Patterson-Hine, and ‡Lui Wang

*Dept. of ECE, University of Connecticut, Storrs, CT 06269-1157
†NASA Ames Research Center, MS 269-4, Moffett Filed, CA 94035-1000
‡NASA Johnson Space Center, JSC-ER2, Houston, TX 77058
§Qualtech Systems Inc., 100 Meadow Road, Wethersfield, CT 06109

***Abstract*— In this paper, we consider the problem of test design for real-time fault detection and diagnosis in the space shuttle's non-toxic orbital maneuvering system and reaction control system (NT-OMS/RCS). For demonstration purposes, we restrict our attention to the aft section of the NT-OMS/RCS, which consists of 160 faults (each fault being either a leakage, blockage, igniter fault, or regulator fault) and 128 sensors. Using the proposed tests, we are able to uniquely isolate a large number of the faults of interest in the NT-OMS/RCS. Those that cannot be uniquely isolated can generally be resolved into small ambiguity groups and then uniquely isolated via manual/automated commands. Simulation of the NT-OMS/RCS under various fault conditions was conducted using the TRICK® modeling software.**

## I. Introduction

For safety-critical systems (e.g., aerospace, nuclear, automotive, etc), fast and efficient fault detection and isolation (FDI) techniques are necessary in order to attain a high degree of availability, reliability, and operational safety [2]. The permissible time window for the detection and diagnosis of faults in these systems can be quite narrow, which makes the problem of online detection and isolation all the more difficult.

The space shuttle is a prime example of a safety-critical system. For orbital maneuvering, orbital attitude control, and atmospheric re-entry, the space shuttle employs an orbital maneuvering system and reaction control system (OMS/RCS). Due to the hazards and difficulty involved in maintaining the current OMS/RCS, a new design is currently under development that employs non-toxic propellants. This new system, which we will refer to as the NT-OMS/RCS, is the system of interest in this paper.

FDI in the NT-OMS/RCS poses the following four challenges:

1. A real-time simulation model of the NT-OMS/RCS, called TRICK® [4], is available. However, a complete mathematical model is not available for use. This situation also arises frequently when a subsystem vendor protects the intellectual property of the system details. In this case, the subsystem vendor may provide an executable simulator to the system integrator.
2. The system is reasonably complex with 160 faults and 128 sensors.
3. The system response under normal and faulty conditions is a function of initial conditions of the system (e.g., helium tank pressure, amount of liquid oxygen and fuel in the tanks, etc.). This complicates the test design process because the tests should be insensitive to random initial conditions.
4. The possible combinations of commanded valves, cross-feeds, and active engines causes the number of operating modes of the NT-OMS/RCS to be extremely large ($> 2^{26}$). The design of tests that are (nearly) invariant to operating modes is an engineering challenge.

The lack of a complete mathematical model of the NT-OMS/RCS automatically rules out the possibility of an analytic model-based FDI approach [9]-[15]. However, the NT-OMS/RCS is sensor-rich, providing information on such parameters as temperature, pressure, engine thrust, and fluid flow at many locations in the NT-OMS/RCS network. As a result, a large amount of monitored data is available to the crew members and mission control in real-time. In this situation, a data-driven approach towards fault detection and diagnosis is a feasible solution (given that real-time estimates of the system response variables, under nominal operating conditions, are available; these estimates can often be inexpensively obtained using a simulator) [3].

In data-driven approaches, where failure modes are explicitly known *a priori*, a decision matrix (D-matrix) relating the faults as rows and test results on the features of the residuals as columns is developed off-line. These residuals are computed from simulations of nominal scenarios and scenarios simulated with single faults. Decision fusion (inference) algorithms, using the test results (obtained by performing the same set of tests that was used to develop the D-Matrix on the observed data) and the D-matrix as inputs, provide the FDI solutions. Since a reasonably accurate simulator is available for the NT-OMS/RCS, that uses the commands, fault universe and initial conditions as input parameters and that provides the estimated

sensor readings in real-time, it is an ideal candidate system for the application of data-driven FDI methods.

For data-driven FDI schemes, the design of robust diagnostic tests represents a challenging task. The nature of the observed data (e.g., sampling interval, noise), the number and distribution of sensors, weigh heavily into the effectiveness of the tests. In multi-mode systems, test outcomes for a given fault may vary from one mode of operation to another. When the number of modes is small, separate sets of tests can be designed for each mode. Since the NT-OMS/RCS has an extremely large number of modes (where the number of modes is equal to the number of possible combinations of active RCS and OMS engines), designing a separate set of tests for each mode is impractical. Consequently, the search for tests that are invariant (or nearly so) to the mode of operations is key. Also, the order in which the various tests are considered in diagnostic decisions is another issue that must be addressed.

In this paper, a data-driven FDI scheme for the NT-OMS/RCS is devised. For proof of concept, we focus on the aft section of the NT-OMS/RCS, which contains 160 fault modes with 128 distributed sensors for monitoring temperature, pressure, and thrust-output. Using the proposed tests, we are able to uniquely isolate a large number of the faults of interest in the NT-OMS/RCS. Those that cannot be uniquely isolated can generally be resolved into small ambiguity groups and then uniquely isolated via manual/automated commands. A benefit of the proposed FDI scheme is that it may serve as a template for addressing other FDI problems for which a complete mathematical model of the system is not available.

The rest of the paper is organized as follows. The FDI problem for the NT-OMS/RCS is formulated in section 2. An overview of the complete diagnostics process is given in section 3. In section 4, we give detailed descriptions of the diagnostic tests. In sections 5 and 6, we address the problems of sensor faults and fault severity estimation. Test cases and simulation results are presented in section 6 to demonstrate the viability of the idea, and the paper concludes in section 7 with a brief summary.

## II. Problem Formulation

### A. System Description

As shown in Figure 1, the new OMS/RCS consists of 14 forward thrusters, 24 aft thrusters (12 jets on both the left and right sides), 2 orbital maneuvering engines located near the tail of the shuttle, 4 propellant storage tanks (2 ethanol tanks and 2 liquid oxygen tanks), and a large distribution network [1]. Other components in the system include pressure regulators, relief systems, igniters, and an assortment of valves. The propellants are delivered to the engines under high pressure from 4 helium storage tanks where they combine to produce the thrust used for attitude control, rotational maneuvers, and small velocity adjustments.

### B. Fault Universe

The system is subject to four types of faults:

- leakages
- valve blockages
- igniter faults
- regulator faults

In the aft section of the NT-OMS/RCS, there are a total of 160 failure modes which are decomposed as 36 leakage, 26 igniter, 92 blockage, and 6 regulator faults. Of the four fault classes, leakage and blockage represent the most difficult to detect and isolate, since they can occur in various degrees of severity. In addition, many of their characteristics (especially for blockage) are sensitive to the initial conditions and system modes.

### C. Sensors

The aft section of the NT-OMS/RCS contains the following sensors:

- 2 valve position sensors
- 64 pressure sensors
- 28 temperature sensors
- 26 thrust sensors
- 4 propellant mass sensors
- 4 propellant volume sensors

### D. Characteristics of the NT-OMS/RCS Fault Universe

With the exception of leakages and certain types of regulator faults (specifically the "stuck open" fault mode) , all faults in the NT-OMS/RCS are dormant, that is, they will produce no anomalous sensor readings until an engine or a set of engines have been fired. Let $F_i$ be the set of dormant faults that produce error signals when engine $i$ has been fired. Given that the set of engines $E$ have fired, the set of dormant faults $\tilde{F}$ that will produce anomalous sensor readings is given by[1]

$$\tilde{F} = \bigcup_{i \in E} F_i \tag{1}$$

Finally, let us define $F_A$ as the set of leakage faults and "stuck open" regulator faults and $S$ as the set of sensors displaying anomalous readings. The problem then is to determine the fault set $\hat{F} \subseteq (F_A \cup \tilde{F})$ that best accounts for the readings produced by the sensors in $S$.

From further observations of the NT-OMS/RCS, the set $S$ is approximately given by

$$S = \bigcup_{k \in \hat{F}} S_{k|E} \tag{2}$$

where $S_{k|E}$ are the set of sensors producing anomalous readings when fault $k$ has occurred and the set of engines $E$ are firing. The set $S_{k|E}$, in turn, is approximately given as

$$S_{k|E} = \bigcup_{i \in E} S_{k|i} \tag{3}$$

where $S_{k|i}$ are the set of sensors producing anomalous readings when fault $k$ has occurred and engine $i$ fires. These observations reduce the complexity of the FDI scheme.

[1]Equation (1) is based on observations made of the NT-OMS/RCS response behavior via the TRICK® simulator.

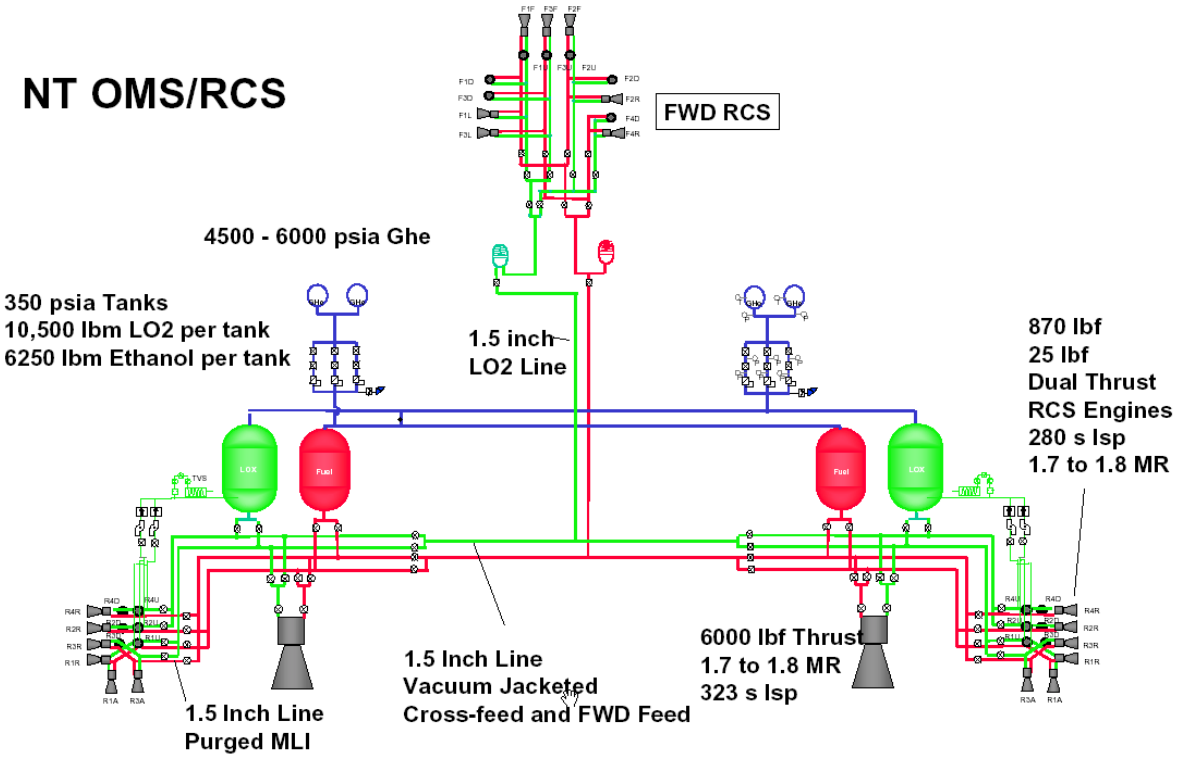


Fig. 1. Schematic of the NT-OMS/RCS

### *E. TRICK® Simulator*

As no mathematical model of the NT-OMS/RCS is available, nominal readings for the computation of error signals is obtained by running the TRICK® [4] simulator in parallel with the physical system (or another simulator with injected faults) as shown in Figure 2. TRICK® is the simulation environment

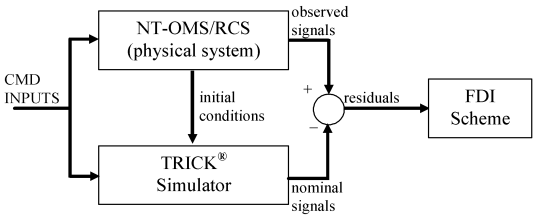


Fig. 2. The role of the TRICK® simulator

at the Johnson Space Center (JSC) that supports the development, operation and analysis, and real-time human-in-the-loop training simulations. The simulation applications range from personal computers to full-scale robotics hardware-in-the-loop facilities and virtual reality systems. TRICK® provides a data-driven real-time scheduling executive, input processing, data recording and automatic code generation (ACG). It uses parsing and ACG utility processors to generate input/output mechanisms as well as mathematical model function calls. TRICK® supports C and C++ programming languages for mathematical modeling, and also has limited support for Fortran and Ada. The TRICK® utility suite also provides graphical, user, developer and run-time interfaces as well as data products including strip charting.

## III. Diagnostics Process Overview

Figure 3 shows the block diagram of the proposed FDI process for the NT-OMS/RCS. The process employs a simulator and the system schematic for test design and fault detection. A quantitative model of the system is created via the EASY5® modeling tool. A TRICK® wrapper serves as the user interface. Using this simulator, different test implementation schemes, discussed in the next section, are applied to evaluate the detection and isolation performance. Simulations (for both the nominal and faulty scenarios) are required to extract the relationships between the fault causes and the observable effects of the system. Information on the system model, such as model parameters, test definition and simulation results, are stored in a database.

A Diagnostic Matrix (D-Matrix) is generated using the results of tests performed on the simulation results of the nominal and faulty scenarios. The D-Matrix is exported in an Extensible Markup Language (XML) format. XML is a flexible text format and is increasingly playing a significant role in the exchange of a wide variety of data on the web and among many different modeling environments. Execution of the tests, construction of the D-Matrix and generation of the XML file can be performed using a design and analysis environment, such as MATLAB®.

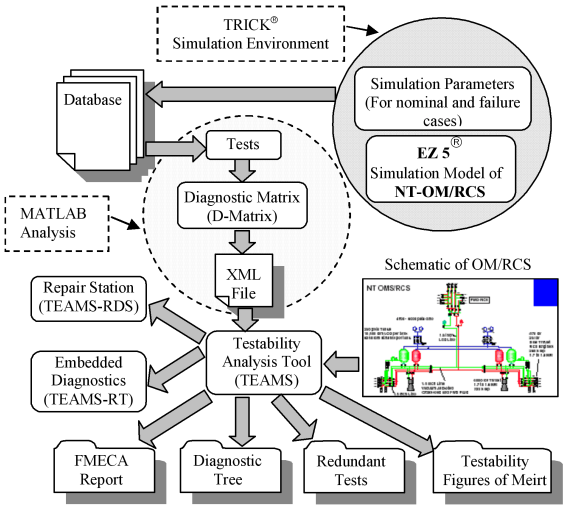


Fig. 3. Diagnostics Process Overview

The XML file is imported into a diagnostic analysis tool, such as TEAMS® (Testability Engineering and Maintenance System) [5][16], to automatically layer in the cause-effect dependencies on a structural model. Multi-signal dependency modeling is employed in order to maintain conformity with the physical structure of the system. This modeling technique has the benefit of capturing the useful and important knowledge about the system for fault diagnosis without unnecessary details. For the NT-OMS/RCS, the fault modes are explicitly associated with sub-modules in the system. However, if one needs to go beneath this layer (to more detailed component models), a cause-effect dependency model becomes necessary. The TEAMS® tool, based on multi-signal dependency modeling, has been used for the testability analysis of large systems, containing as many as 50,000 faults and 45,000 tests. Detailed information about multi-signal modeling can be found in [5].

TEAMS® computes the percent fault detection and isolation measures, identifies redundant tests and ambiguity groups, and generates updated Failure Modes, Effects and Criticality Analysis (FMECA) report and the diagnostic tree. It also exports the D-matrix, the test code and structural information to TEAMS-RT® for on-board, real-time diagnosis. The onboard diagnostic data is downloaded to TEAMS-RDS® (remote diagnosis server) for interactive diagnosis (by driving interactive electronic technical manuals), diagnostic/maintenance data management, logging and trending. However, the focus of this paper is on test design and real-time diagnosis.

A detailed picture of the real-time FDI process for the NT-OMS/RCS is presented in Figure 4. For real-time detection, the D-Matrix (generated offline), physical model of the system (TEAMS® model) and the real-time test results are fed into TEAMS-RT®. TEAMS-RT® functions as the decision fusion block, and provides diagnostic decisions that include the list of isolated faults, suspected faults, and the tests utilized. The process depicted here can serve as a generic FDI scheme for systems, whose mathematical models are not available. Customization of the FDI process for a new system requires the design of suitable tests for that target system and loading of its structural model into TEAMS®.

## IV. Robust Test Design

Of key importance in test design is the use of sensor information, which is insensitive to the $2^{26}$ modes[2] of operation of the NT-OMS/RCS (i.e., all possible combinations of active engines). Hence, for test design, we consider only those features from sensor $m$, which satisfy the following criterion:

$$\theta\left(r_m(k|E_i)\right) = \theta\left(r_m(k|E_j)\right) \;\; \forall E_i, \;\; E_j \tag{4}$$

In (4), $r_m(k|E_i)$ denotes the error signal (residual) from sensor $m$ when fault $k$ has occurred and the set of engines $E_i$ are firing and $\theta(\cdot)$ is a function, which extracts the feature of interest from the sensor data.

### A. Determination of fault Onset Time

The fault onset time is determined from the time series associated with a sensor by using the cumulative sum (CUSUM) algorithm [6], a simple test for determining if a random variable has deviated significantly from its statistical mean. Let $e_k$ be the value of the error signal from a sensor at time $t_k$ where $k = 0, 1, 2, \ldots$. Under the CUMSUM test, we treat $e_k \;\forall k$ as an independent random variable with probability function $P_\omega(\cdot)$ where $E[e_k] = \omega$. Define the log likelihood function

$$\Omega(e_k) = \log \frac{P_{\omega_1}(e_k)}{P_{\omega_0}(e_k)} \tag{5}$$

where $E[e_k] = \omega_0 = 0$ prior to the fault and $E[e_k] = \omega_1 \neq 0$ after the fault. Define $g_k$ as

$$g_k = \begin{cases} g_{k-1} + \Omega(e_k) & \text{if } g_{k-1} + \Omega(e_k) > 0 \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

where $g_0 = 0$. From (6), deviations in $e_k$ which favor the hypothesis $E[e_k] = \omega_1$ are accumulated by $g_k$ and those that favor the alternate hypothesis result in $g_k$ being reset back to zero. The alarm time $t_{alarm}$ is given by

$$t_{alarm} = t_a, \quad a = \min\{k \;:\; g_k \geq h\} \tag{7}$$

where $h$ is a threshold which is determined based on the noise levels of the system. The fault onset time $t_{fault}$ is then given as

$$\begin{aligned} t_{fault} &= t_s, \\ s &= \max\{k \;:\; t_{alarm} - t_k > 0, \; g_k = 0\} \end{aligned} \tag{8}$$

[2]The number of operating modes is actually greater than $2^{26}$ when one includes the number of possible commanded valve configurations in the NT-OMS/RCS network of pipes.

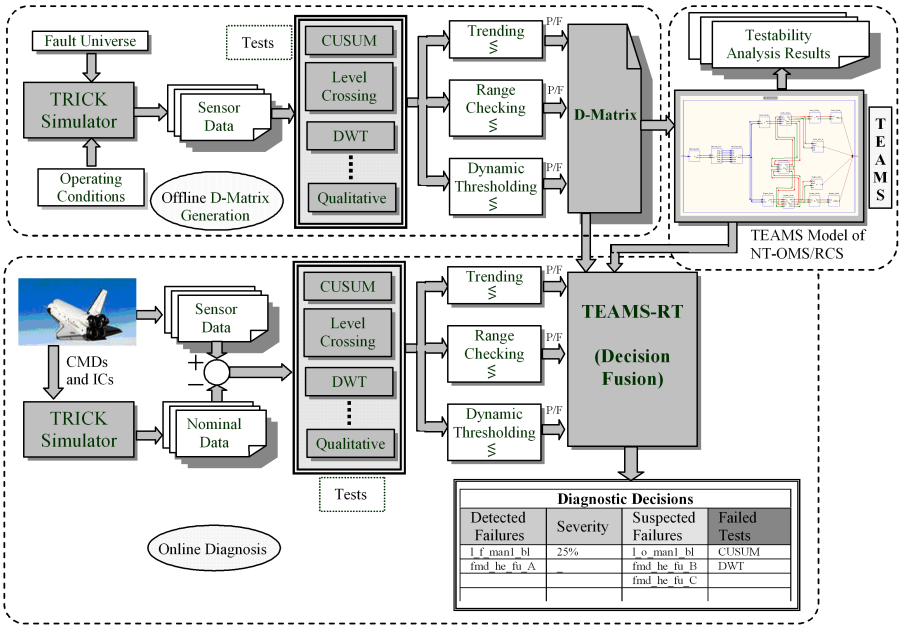


Fig. 4. Block diagram of real-time FDI scheme

### B. Sensor faults

Prior to fault isolation, checks are performed on all sensors reporting off-nominal behavior. Detection of sensor faults is accomplished by invoking a majority rule among groups of correlated sensors. Let $x = \{x_1, x_2, \ldots, x_n\}$ and $y = \{y_1, y_2, \ldots, y_n\}$ be the normalized time series reported by sensors $s_x$ and $s_y$, respectively. The correlation between the normalized time-series $x$ and $y$ is defined as

$$\rho(x,y) = \frac{1}{(n-1)\sigma_x\sigma_y}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y}) \qquad (9)$$

where

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n}x_i, \quad \bar{y} = \frac{1}{n}\sum_{i=1}^{n}y_i$$

$$\sigma_x = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\bar{x})^2}{n-1}}, \quad \sigma_y = \sqrt{\frac{\sum_{i=1}^{n}(y_i-\bar{y})^2}{n-1}}$$

The sensors $s_x$ and $s_y$ are grouped together, if their normalized time-series are highly correlated. In our simulations, $s_x$ and $s_y$ are placed in the same correlation group if $|\rho(x,y)| \geq \gamma = 0.75$.

From simulations of the NT-OM/RCS, we have observed that while the sign of $\rho(x,y)$ varies from one scenario to another, $|\rho(x,y)|$ itself remains reasonably fixed. Consequently, given the set $S$ of sensors producing anomalous readings, sensor $s_x \in S$ is identified as failed if

$$\sum_{s_y \in C_x \subset S} I_{s_x,s_y} > 0.5|C_x| \qquad (10)$$

where $I_{s_x,s_y}$ is an indicator function of the event that $|\rho(x,y)| < \gamma$, and $C_x$ is the set of sensors in $S$ that are correlated with $s_x$.

Once the faulty sensors have been identified, the failed tests are disregarded from the decision process (see Figure 5). Because each test fuses results from multiple sensors, there is a great deal of built-in redundancy in the process. Hence, the loss of information from failed sensors (provided that they are few in number) will in general not affect the diagnosis.

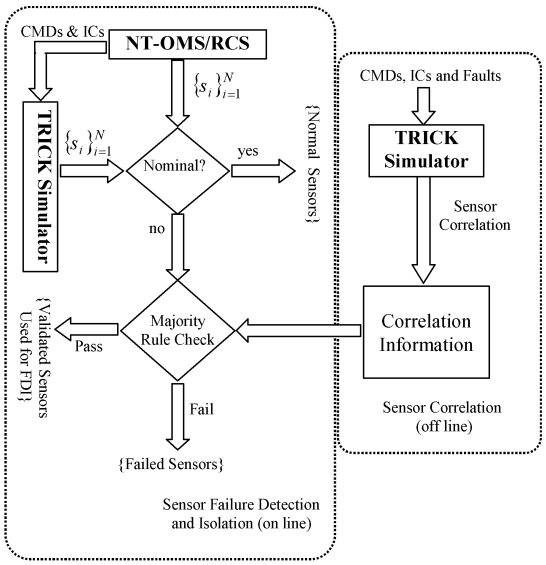


Fig. 5. Sensor Validation Process

### C. Blockage Test

Before proceeding to the actual test, we first identify the sensors that are used to detect and isolate blockage faults. These sensors are identified using the following steps.

1. $\forall k \in F_B$, and $\forall i$, obtain $S^{ini}_{k|i} = S_{k|i} \cap (\bar{S}_{IG} \cup \bar{S}_{REG})$

2. For leakage faults, we observed that the absolute values of the residuals at some sensors continued to increase linearly until the end of the observation interval, which we denote as $t_f$. These sensors were identified using the following criterion:

$$S^{exclude} = \{j \ : \ \theta(r_j) = t_{max} = t_f\}, \quad j \in S^{ini}_{k|i} \quad (11)$$

where $r_j$ is the observed error signal from sensor $j$ over the observation interval and $\theta(\cdot)$ outputs the time at which the error signal has the maximum absolute value.

3. $\forall k \in F_B$, $S^B_{k|i} = S^{ini}_{k|i} \cap \bar{S}^{exclude}$.

Detection and isolation of a particular blockage using the set of sensors $S^B_{k|i}$ $(k \in F_B)$ $i \in E$ is accomplished by using the time difference between the time the error signal first appears and the time when it reaches its peak absolute value as a distinguishing feature. In line with the criterion for what information can be used in the test design, this feature is relatively robust to the mode of operation and initial conditions. In Figure 6, a blockage in the left fuel manifold 1 valve was simulated when engine L1U and L1L were fired respectively. In each of the two cases, the time to peak remained the same.

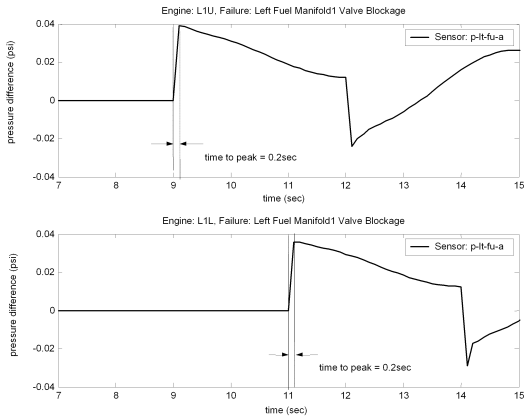


Fig. 6. Blockage: feature invariance to system mode

Define $\tau_{j|(k,i)}$ as the time to peak associated with sensor $j$ ($j \in S^B_{k|i}$) when blockage $k$ has occurred and engine $i$ fires. The decision that blockage $k$ has occurred is made if

$$\sum_{j \in S^B_{k|i}} |\theta(r_j) - \tau_{j|(k|i)}| \leq \epsilon_{k|i} \quad \text{(for any } i \in E) \qquad (12)$$

where $\theta(\cdot)$ in (12) outputs the time to peak of the error signal associated with sensor $j$ and $\epsilon_{k|i}$ is a decision threshold for blockage $k$ given engine $i$.

### *D. Igniter fault Test*

An igniter fault results in a significant drop in the chamber pressure and thrust output of the corresponding engine (which is firing at the time). It also causes large deviations in the nominal fuel injector temperature of the engine. Each engine is monitored by three sensors (each monitoring one of the aforementioned parameters). Consequently, we use a majority rule to isolate an igniter fault. Define $I_{p,j}$, $I_{t,j}$, and $I_{f,j}$ as indicator functions for the event that a large deviation is observed in the sensors that monitor chamber pressure, fuel injector temperature, and thrust output of engine $j$, respectively. Engine $j$'s igniter has failed if

$$I_{p,j} + I_{t,j} + I_{f,j} \geq 2 \qquad (13)$$

The use of a majority rule also makes this test robust to sensor faults.

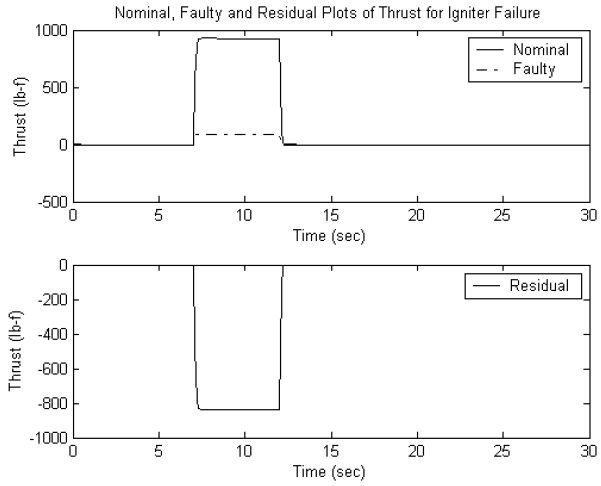


Fig. 7. Thrust anomaly

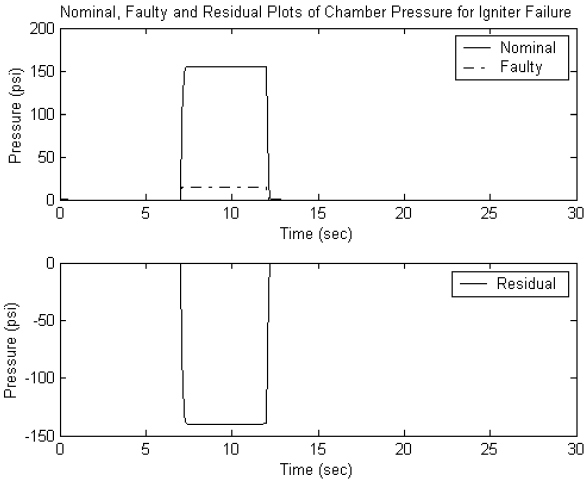


Fig. 8. Igniter: pressure anomaly

### *E. Regulator fault Test*

The NT-OMS/RCS system is equipped with six helium regulators; three of each are located in the fuel-helium legs (A, B, C) and the oxygen-helium legs (A, B, C). We have observed that the sensor that monitors the pressure at the fuel-helium manifold has a distinct waveform (see Figure 9)

whether the heilum valves fail "stuck open" or "stuck closed". For simplicity, we will refer to this sensor as sensor $s_{fu}$. The same waveform was observed at the sensor that monitors the pressure at the oxygen-helium manifold; we will refer to this sensor as $s_{ox}$. From Figure 9, the residuals produce a narrow spike and then settle down to a steady state value. Since the transient is quite narrow, for identification of this waveform, we employed a multi-resolution analysis technique in the time-frequency plane. Discrete wavelet transform (DWT) is a multi-resolution analysis that provides coefficients, which represent the rate of deviation of a signal at their corresponding locations on a time scale[7] [8]. Consequently, DWT is used to isolate the coefficients belonging to the transient region and compare them with our expectations of the fault; helium regulator faults are detected and isolated via this comparison.

The procedure for detecting and isolating a helium regulator fault in the fuel legs is as follows. Define $\{d_i\}_i \ i = 0, 1, \ldots$ as the set of level 2 detailed coefficients (obtained via wavelet transform using a Duabechies 10 mother wavelet) associated with the residual at sensor $s_{fu}$. Define $i_{max}$ as the index of the coefficient with the maximum absolute value. Then, the significant coefficients are determined via the set $\{c_i\} = \{d_i\}_{i_{max}-q}^{i_{max}+q}$ where $q$ is a user selected parameter which determines the range of significant coefficients. The decision that a helium regulator in a fuel leg has failed is made if

$$\max_i\{c_i\} - \min_j\{c_j\} \geq \beta \tag{14}$$

where $\beta$ is a threshold. To detect and isolate a helium regulator fault in the oxygen legs, we repeat the above procedure by replacing $s_{fu}$ with $s_{ox}$.

Since only one sensor is available for monitoring the three helium regulators in legs A, B, and C, a helium regulator fault in a fuel leg is detected with an ambiguity group of size three. The same is true of detecting a regulator fault in an oxygen leg.

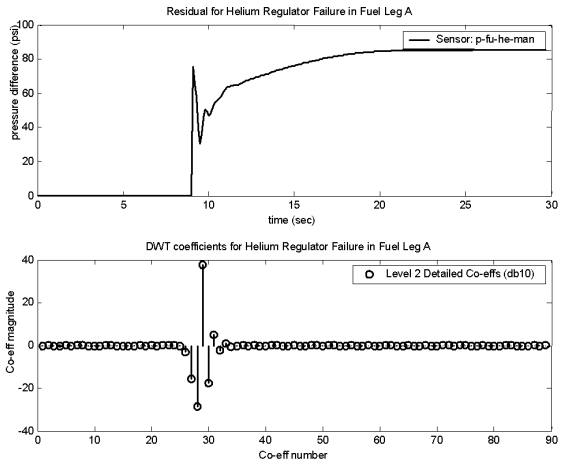


Fig. 9. Fuel Reg. C: pressure anomaly detected by DWT

### F. Leakage Test

Having ruled out regulator faults which produce distinct, transient signatures (whether in the "stuck open" or "stuck closed" fault mode), any continual off-nominal behavior that occurs while the engines are off and the system has reached steady state, is the result of leakages. Consequently, the detection of leakages should be made while the system is at rest (i.e., no active engines).

Isolating the location of a leakage is conducted in two stages using qualitative relationships. The first stage examines the direction of change $(+/-)$ of the error signals associated with each leakage fault. Note, in Figure 10, that the sign of the error signal for a particular leakage (in this case a helium leakage in the left fuel tank) remains the same regardless of which engine fires.

Given that a single leakage has actually occurred, the test produces an ambiguity group that is typically of size 7 or lower. Leakage $k$ is a member of the group if

$$\sum_{i \in S_{k|\emptyset}} |\theta(r_i) - \xi_{i|k}| = \gamma \tag{15}$$

where $r_i$ is the observed error signal from sensor $i$, $\xi_{i|k} \in \{-1, 1\}$ is the known direction of change of the error signal associated with sensor $i$ when leakage $k$ has occurred[3], $\theta(\cdot)$ outputs the sign of the sample point in $r_i$ with the largest absolute value if that value exceeds a threshold $\epsilon$; otherwise, it outputs a zero, and $\gamma$ is the minimum of (15):

$$\gamma = \min_{k \in F_L} \left\{ \sum_{i \in S_{k|\emptyset}} |\theta(r_i) - \xi_{i|k}| \right\} \tag{16}$$

In the second stage, the size of the ambiguity group is reduced by comparing the steady state pressure at each leakage location[4]. As the actual leakage faults will be associated with the lowest steady state pressure drop, leakage $k$ is selected as a possible candidate if

$$p_j - p_k \geq \lambda, \text{ for some } j \neq k, \ j, k \in A \tag{17}$$

where $p_j$ and $p_k$ are the steady state pressures associated with leakages $j$ and $k$, respectively; $A$ is the ambiguity group obtained in stage 1; and $\lambda$ is a threshold. Using (17), we can generally reduce the ambiguity groups of size 7 to groups of size 3 or 4.

Based on the structure of the NT-OMS/RCS, there exist four primary ambiguity groups:

- Leakages on the left side that are associated with the liquid oxygen line.
- Leakages on the left side that are associated with the fuel line.
- Leakages on the right side that are associated with the liquid oxygen line.

[3]This information is known by observing the effects of the various leakages on the NT-OMS/RCS.

[4]The pressure information for each leakage fault is provided by a local sensor.

- Leakages on the right side that are associated with the fuel line.

Consider the case when the ambiguity group $A$ contains leakage faults from more than one primary group. If the suspected leakages in $A$ were partitioned according to their associated primary groups, then we can expect there to be at least one leakage fault in each of the resulting groups. The reasoning for this is that in the single leakage scenario, the ambiguity group $A$ almost always contains leakage faults from a single primary group. Hence, if $A$ contains leakage faults from different primary groups, there is at least one leakage fault from each of the representative primary groups in $A$. So, adopting a divide and conquer strategy, the procedure in these instances is to partition $A$ into groups where each group contains members from only one primary group, and then to apply stage 2 to each of the new groups.

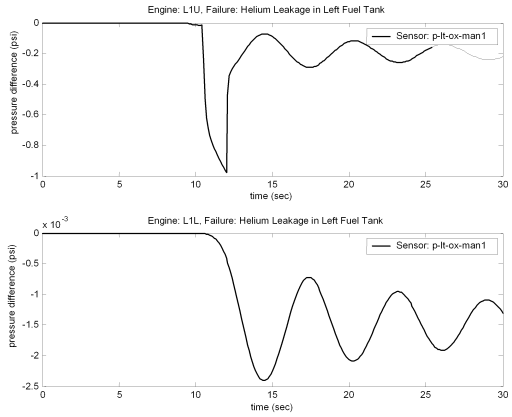


Fig. 10. Leakage: feature invariance to system mode

## V. Estimation of Leakage and Blockage Severity

Once a leakage or blockage has been isolated, its severity is estimated using the following variables:

- pressure in the (fuel) helium tank
- pressure in the (oxygen) helium tank
- volume of the right fuel tank
- volume of the right oxygen tank
- volume of the left fuel tank
- volume of the left oxygen tank

In addition to the above variables, which comprise the initial conditions of the NT-OMS/RCS, data is taken from pressure sensors near the isolated fault.

The aforementioned variables, which we denote as $\{x_1, x_2, \ldots, x_k\}$, are the inputs to a severity estimator

$$f(x_1, x_2, \ldots, x_k) = \sum_{i=1}^{k} \boldsymbol{c}_i^T \mathbf{x}_i + c_0 = \hat{y} \qquad (18)$$

where $c_0$ is a bias term and

$$\begin{aligned} \boldsymbol{x}_i &= [\ x_i \quad x_i^2 \quad \ldots \quad x_i^k\ ]^T \\ \boldsymbol{c}_i &= [\ c_{i1} \quad c_{i2} \quad \ldots \quad c_{ik}\ ]^T \end{aligned}$$

The coefficient vectors $\{\boldsymbol{c}_i\}_{i=1}^k$ were estimated from the simulation data and were optimized in the least squares sense.

For blockages above $30\%$, the blockage severity can be estimated to within $\pm 5\%$ of the true blockage value. In the case of leakages, holes greater than $0.6\text{in}^2$ can be estimated to within $\pm 0.3\text{in}^2$ of the true hole size. For both leakages and blockages, $k = 4$ was the polynomial order.

## VI. Simulation Results

In this section, we present several examples to demonstrate the feasibility of the proposed FDI scheme. In each example, the observed sensor data at each instant of time is perturbed with zero mean additive white Gaussian noise with a standard deviation of 0.2 to examine the effects of imperfect data on the diagnosis. Leakage faults were simulated with $0.5\text{in}^2$ holes and blockage faults were simulated with severity at $25\%$.

### A. Leakage faults

**Example 1**: In this example, the Left OMS and R1R RCS engines were fired at $t = 6$ and $t = 8$ seconds, respectively. A leakage fault in the left fuel helium tank occurred at $t = 10$ seconds. Both engines stopped firing at $t = 12$ seconds. For this case, the FDI scheme uniquely isolated the leakage fault.

**Example 2**: The same firing scenario used in example 1 is applied here. A leakage in manifold 1 of the right oxygen line took place at $t = 4$ seconds. The fault in this case was uniquely isolated.

**Example 3**: In this example, we fire the L3D and R2R RCS engines at $t = 15$ and $t = 17$ seconds, respectively. A leakage in flow path A of the left fuel line took place at $t = 18$ seconds. The L3D and R2R RCS engines stopped at $t = 20$ and $t = 21$ seconds, respectively. In this case, the FDI scheme produced an ambiguity group of size 3, where the actual leakage fault was a member of the group. It should be noted that unique isolation is possible if manual/automatic tests are applied, that is, commanding certain valves to open and close to pinpoint the exact location of the leakage.

**Example 4**: In this example, the Left OMS engine and L2L RCS engine were both fired at $t = 9$ seconds. The L2L RCS engine and Left OMS engine stopped at $t = 11$ and $t = 15$ seconds, respectively. A leakage in the oxygen crossfeed line occurred at $t = 16$ seconds. This fault was uniquely isolated.

### B. Igniter faults

**Example 5**: In this example, we failed the igniter for the L1U RCS engine which was activated for a two second duration. This fault was uniquely isolated.

**Example 6**: In this example, we failed the igniters for the L4D and R3A RCS engines. These engines were fired for a period of 1 second. Both igniter faults were isolated uniquely.

### C. Regulator faults

**Example 7**: In this example, the L1U RCS engine was fired at $t = 7$ seconds. The helium regulator in fuel leg B was failed at $t = 9$ seconds and the engine stopped firing at $t = 12$ seconds. The outcome of the FDI scheme was an ambiguity group consisting of the three heilum regulators in the fuel legs.

**Example 8**: In this example, the L1U and L2D RCS engines were fired at $t = 5$ seconds and the right OMS engine was fired at $t = 6$ seconds. The L1U RCS engine was stopped at $t = 7$ seconds. The helium regulator in fuel leg C was failed at $t = 8$ seconds followed by the helium regulator fault in oxygen leg A at $t = 9$ seconds. The L2D RCS and right OMS engines stopped firing at $t = 11$ and $t = 13$ seconds, respectively. The outcome of the FDI process was an ambiguity group of size 6 consisting of the helium regulators.

### *D. Blockage faults*

**Example 9**: In this example, the L2D and R1U RCS engines were fired at $t = 10$ seconds and $t = 12$ seconds, respectively. A blockage in the fuel line of the engine L2D occurred at $t = 13$ seconds. Both the engines stopped at $t = 14$ seconds. The outcome of the FDI process was an ambiguity group of size 3. The actual blockage fault was a member of that group (other 2 faults were blockage in the oxygen line of the engine L2D and blockage in left fuel manifold 2).

**Example 10**: In this example, the Left OME and the L2D RCS engines were both fired at $t = 7$ seconds. A blockage in the right oxygen manifold1 occurred at $t = 9$ seconds. The L2D RCS engine and the Left OME stopped at $t = 11$ seconds and at $t = 15$ seconds, respectively. The outcome of the FDI process was an ambiguity group of size 2. The actual blockage fault was a member of that group and the other member was blockage in the right fuel manifold 1.

### *E. Sensor faults*

**Example 11**: The scenario that was presented in Example 3 is duplicated here with the exception that the sensor that monitors pressure in flow path A of the left fuel line was failed in addition to the leakage in that same location. The time series from this sensor was replaced by a sequence of white Gaussian random variables with zero mean and variance 1. The faulty sensor was detected and its information was discounted from the test process. As a result of losing the information from this sensor, the size of the ambiguity group increased from 3 to 5.

### *F. Estimation of Fault Severity*

**Example 12**: In this example, we replicated the scenario that was presented in example 9. We simulated the scenario with $30\%$ , $40\%$, $50\%$, $60\%$, and $70\%$ blockages in the left fuel line of the engine L2D. The respective estimates for these cases are $34.424\%$, $44.951\%$, $54.597\%$, $63.165\%$, and $70.845\%$. When the severity of the blockage is in the range of $30\%$ to $80\%$, the estimates are within $\pm 5\%$ of the actual value.

**Example 13**: In this example, engine R1U was fired at $t = 7$ seconds . A leakage in the fuel-helium tank occurred at $t = 11$ seconds, and the engine stopped firing at $t = 12$ seconds. We simulated the scenario for holes of sizes $0.4\text{in}^2$, $0.6\text{in}^2$, $0.8\text{in}^2$, $1\text{in}^2$, $1.2\text{in}^2$, $1.4\text{in}^2$, $1.6\text{in}^2$, and $1.8\text{in}^2$. The estimated hole sizes for these cases are $0.675\text{in}^2$, $0.813\text{in}^2$, $0.998\text{in}^2$, $1.179\text{in}^2$, $1.354\text{in}^2$, $1.521\text{in}^2$, $1.706\text{in}^2$, and $1.892\text{in}^2$, respectively.

## VII. Conclusion

A data-driven FDI scheme was developed for the aft section of the NT-OMS/RCS which is capable of detecting and uniquely isolating many of its faults; those faults which cannot be uniquely isolated by the scheme can often be resolved into small ambiguity groups. While the basic approach can clearly be applied to other FDI problems for which a complete mathematical model of the system is not available, the proposed scheme is still system specific. Future work will focus on the development of a generic data-driven FDI methodology that will allow for easy extension to other FDI problems for which model-based diagnosis is not possible.

## Acknowledgment

This work was supported by NASA-ARC under contract #NAG2-1635. We would like to thank Olivier Rumbout and Bill Othon for their assistance in running the TRICK® simulator.

## References

[1] D. Huit, "Non-Toxic Upgrade for the Orbital Maneveuring System (OMS) for the NASA Space Shuttle", Propulsition Engineering Research Center, 2001.

[2] R. Patton, P. M. Frank, and R. N. Clark, *Issues of fault diagnosis for dynamic systems*, Springer Verlag publishers, 2000.

[3] M. J. Steele, G. Rabadi, and G. Cates, "Generic Simulation Models of Reusable Launch Vehicles", Proceedings, Winter Simulation Conference, 2002.

[4] K. Vetter, *The Trick User's Guide Trick 2003.2*, LicCom Corp., NASA, JSC Automation, Robotics, and Simulation Division, 2003.

[5] S. Deb, K. R. Pattipati, V. Raghavan, M. Shakeri, and R. Shrestha, "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] M. Basseville and I. V. Nikiforov, *Detection of Abrupt Changes: Theory and Application*, Prentice Hall Information and System Sciences Series, NJ, USA, 1993.

[7] I. Daubechies, "The wavelet transform, time-frequency localization and signal analysis", *IEEE Trans. Inf. Theory*, vol. 36, pp. 961-1005, 1990.

[8] A. M. Reza, *From Fourier Transform to Wavelet Transform: Basic Concepts* White Paper, Spire Lab, UWM, Oct. 1999.

[9] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S. N. Kavuri, "A review of process fault detection and diagnosis: Part I: Quantitative model-based methods" *Computers & Chemical Engineering*, vol. 27, pp. 293-311, 2003.

[10] S. Simani, C. Fantuzzi and R. J. Patton, *Model-based fault diagnosis in dynamic systems using identification techniques*, Springer Verlag publishers, 2003.

[11] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - a survey and some new result", *Automatica*, Vol. 26, No. 3, pp. 459-474, 1990.

[12] V. Krishnaswami, G.-C. Luh, and G. Rizzoni, "Nonlinear parity equation based residual generation for diagnosis of automotive engine faults", *Control Eng. Practice*, Vol. 3, No. 10, pp. 1385-1392, 1995.

[13] J. J. Gertler and R. Monajmey, "Generating directional residuals with dynamic parity relations" *Automatica*, Vol. 33, No. 4, pp. 627-635, 1995.

[14] V. Krishnaswami, G.-C. Luh, and G. Rizzoni, "Nonlinear parity equation based residual generation for diagnosis of automotive engine faults", *Control Eng. Practice*, vol. 3, No. 10, pp. 1385-1392, 1995.

[15] J . Luo, F. Tu, M. Azam, K. Pattipati, P. K. Willett, L. Qiao, M. Kawamoto, "Intelligent Model-based Diagnostics for Vehicle Health Management", SPIE Conference on Fault Diagnosis, Prognosis and System Health Management, Orlando, Florida, April 2003.

[16] Qualtech System's website: http://teamqsi.com/publications.htm