Sensor Data Qualification for Autonomous Operation of Space Systems

William A. Maul[1], Kevin J. Melcher[2], Amy K. Chicatelli[1] and T. Shane Sowers[1]

[1]Analex Corporation, [2] NASA Glenn Research Center
21000 Brookpark Road
Cleveland, OH 44135
William.A.Maul@NASA.Gov, Kevin.J.Melcher@NASA.Gov

Abstract

NASA's new Exploration initiative for both robotic and manned missions will require higher levels of reliability, autonomy and re-configuration capability to make the missions safe, successful and affordable. Future systems will require diagnostic reasoning to assess the health of the system in order to maintain the system's functionality. The diagnostic reasoning and assessment will involve data qualification, fault detection, fault isolation and remediation control. A team of researchers at the NASA Glenn Research Center is currently working on a Sensor Data Qualification (SDQ) system that will support these critical evaluation processes, for both automated and human-in-the-loop applications. Data qualification is required as a first step so that critical safety and operational decisions are based on "good" data. The SDQ system would monitor a network of related sensors to determine the health of individual sensors within that network. Various diagnostic systems such as the Caution and Warning System would then use the sensor health information with confidence. The proposed SDQ technology will be demonstrated on a variety of subsystems that are relevant to NASA's Exploration systems, which currently include an electrical power system (EPS) and a cryogenic fluid management system. The focus of this paper is the development and demonstration of a SDQ application for a prototype power distribution unit that is representative of a Crew Exploration Vehicle electrical power system; this provides a unique and relevant environment in which to demonstrate the feasibility of the SDQ technology.

Introduction

The President's *Vision for Space Exploration* set the stage for the United States to return to the moon, establishing an outpost that can be used as a staging area for human and robotic voyages to Mars and beyond. Charged with implementing this vision, NASA is developing an operational architecture that includes a new fleet of rocket-based vehicles and other advanced space systems. Autonomous operation and decision support, including diagnostic reasoning, will be required to meet the ambitious launch schedule, human-rating requirements, long quiescent periods, limited human access for repair or replacement, and long communication delays.

It is critical for any control or remediation responses to be made with the best information available. Therefore, all control and diagnostic functions require the sensor observations to be qualified by filtering or screening out faulty data information that is not representative of the current system. For real-time applications, this analysis must be performed on-line, on-board and as effectively and efficiently as possible.

For launch vehicles, currently applied data validation technologies use limit checks and hardware redundancy checks. Exceeding range or rate-of-change limits indicates that the sensor is experiencing a hard-failure, and the information from the sensor should be ignored. Hardware redundancy checks compare sensors measuring the same physical property. Redundancy checks can identify biases between sensors and out-of-family sensors when there are at least three redundant sensors available. While these technologies are efficient and perform well for each targeted failure mode, they have difficulty identifying subtle or soft sensor failures such as drifts.

One technology that could augment the current state-of-the-art is analytical redundancy, which uses a set of models to reconcile expected behaviors and actual outcomes (Bickford, Meyer, and Lee 2001; Lee 1994; Ibarguengoytia and Sucar 2001). Analytical redundancy utilizes relationships across a suite of sensors to build a network that is used to increase confidence in the traditional qualification checks and to allow monitoring of more subtle sensor failure modes. This paper presents a Sensor Data Qualification (SDQ) system based on analytical redundancy networks to extend the current state-of-the-art in identifying sensor failures. In addition to their usefulness in identifying sensor failures, validated predictions could be used to supplement or replace hardware redundancy.

This paper is organized in the following manner. An overview of the SDQ system is provided in the next section; this contains the baseline SDQ architecture, performance criteria and a description of the commercial software package used for the data validation. The third section of the paper describes the development of the SDQ technology for a Crew Exploration Vehicle (CEV) prototype Power Distribution Unit (PDU) in an electrical

power system (EPS) test bed. A description of the EPS test bed, the sensor failure modes addressed and the data acquisition system are presented. The fourth section contains the development of the SDQ system and the results from validation testing. The paper finishes with concluding remarks about this project and its influence on diagnostic system development, the acknowledgment of system domain experts and a list of references.

Sensor Data Qualification Overview

The following subsections describe the SDQ technology in terms of its architecture, performance criteria and data validation algorithm.

SDQ Architecture and Performance Criteria

The SDQ technology is intended to augment the current state-of-the-art in data qualification for launch vehicles, which applies threshold checks and hardware redundancy checks. The SDQ technology will utilize relationships, across a suite of sensors, to build an analytical redundancy network that is used to increase confidence in the traditional qualification checks. In addition, the monitoring and detection of more subtle sensor failures will be addressed, which will improve the existing methods. Figure 1 illustrates the proposed flow of information through the SDQ architecture.

The SDQ system will be validated in terms of fault diagnosis accuracy and speed. The following criteria will be used:

1. The unambiguous detection of failed sensors.
2. The number of measurement/data cycles to determine a sensor failure.
3. The sensitivity of the algorithm to failed sensor condition.

The first criterion will indicate if a correct diagnosis was made and no other functioning sensor implicated. The second criterion will determine if the diagnosis was made in a timely manner. Finally, the third criterion will gauge the robustness of the diagnosis, in terms of speed and accuracy, to the magnitude of the error signal.

SureSense® Software

The software selected to implement the SDQ technology is the SureSense Data Quality Validation Studio™ (DQVS), a commercial software product developed by Expert Microsystems in conjunction with NASA Glenn Research Center (GRC). SureSense automates the production of on-line signal data validation modules that detect sensor failures and other data anomalies by using analytic redundancy with Bayesian decision logic; it also provides a library of curve-fitting routines that allow the user to perform regression analysis upon the available system data. In addition, empirical relations derived using techniques such as statistical analysis, pattern recognition and neural networks can also be employed. For real-time applications, the SureSense development environment provides an autocode generator, which converts the sensor data validation modules into runtime modules for integration in control and monitoring systems. SureSense technology has been applied in the aerospace and nuclear industries (Bickford, Bickmore, and Caluori 1997; Bickford, et al. 1998; Bickford, et al. 1999; Herzog, Yue, and Bickford 1998; Hines and Davis 2004).

In the data validation model, a set of signals and a set of relations form a network of cross checks used to validate all signals. The difference between a signal's predicted

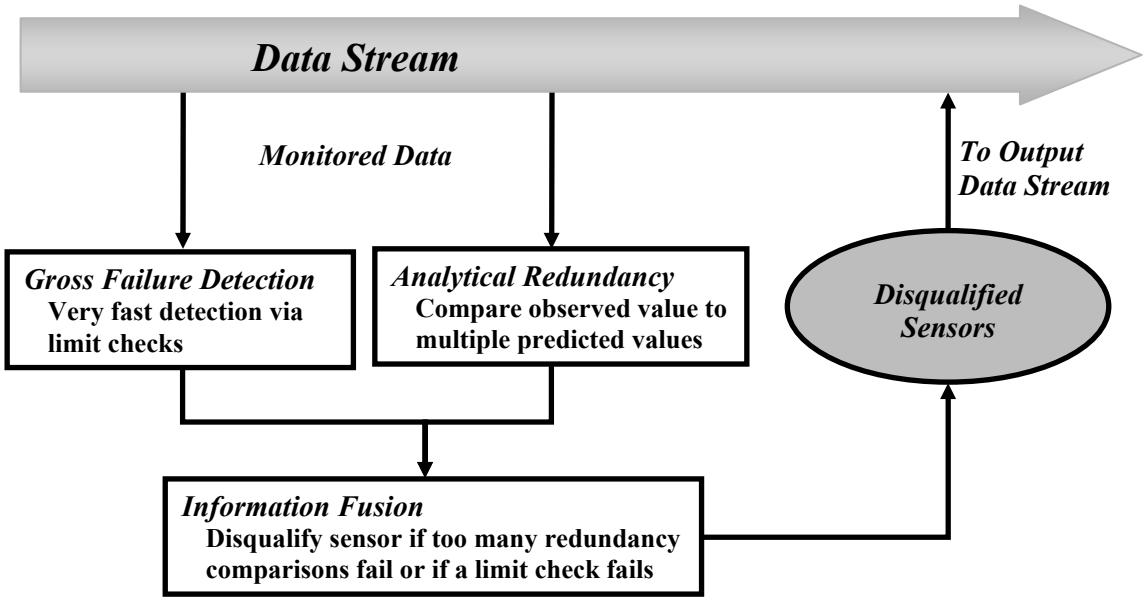

Figure 1. Information flow through proposed SDQ architecture

value and its directly sensed value is termed a residual. Threshold values for the relation residuals are pre-computed using nominal system operating data. Threshold values can be adjusted for normal run-to-run variations in the process signals using a procedure termed relation biasing. Biasing is accomplished during a short user-defined interval at the start of each new monitoring phase. The software automatically computes bias offsets for signal validation relations over this short interval using a bias-period threshold and bias limiting logic in order to prevent faulted signal characteristics from being "learned" by the biasing algorithm.

Once the redundancy relationships and validation requirements are defined in the data validation model, the production of the data validation model is automated. The verification procedure tests the comprehensiveness of the model. Using Bayesian probability theory, the voting table generation procedure creates a runtime voting table and a decision confidence table. The runtime voting table describes how many of a signal's relationships must fail before a failure is declared. The decision confidence table determines the probability of a signal being valid given the number of relations that validate a signal, and the number of relations that currently hold. User-provided inputs and sensor design information enable the system to develop an acceptable level of projected performance for both of these tables, and thereby estimate the performance of the data qualification network.

CEV EPS Test Bed

The SDQ software was applied to a prototype PDU as a means of demonstrating its ability to diagnose sensor failures in an EPS. The following sections provide a description of the EPS test bed, the sensor failure modes that will be investigated and the control and data acquisition system used to operate the test bed.

Description

The prototype PDU is designed to be representative of a portion of the CEV EPS. The test bed contains one power supply, the prototype PDU, three load banks, and a LabVIEW®-based data acquisition and control system. A schematic of the test bed is shown in Figure 2. The reader should note that, although the test bed configuration is representative of a space power system, the components are not generally qualified for space flight.

The primary test bed component is the PDU shown in Figure 3. It is composed of a power bus, three input relays, three output relays, and controller cards for each of the relays. Power can be supplied from a variety of sources (e.g., batteries, solar cells, fuel cells). Turning on a given input relay allows power to flow from the associated supply to the power bus. For the tests described in this paper, a single programmable power supply is connected to one of the input relays. The other input relays are inactive. In addition to the three input relays, the three output relays are also connected to the power bus. The state of a given output relay determines whether power supplied to the bus is delivered to the associated load. The relays used in this

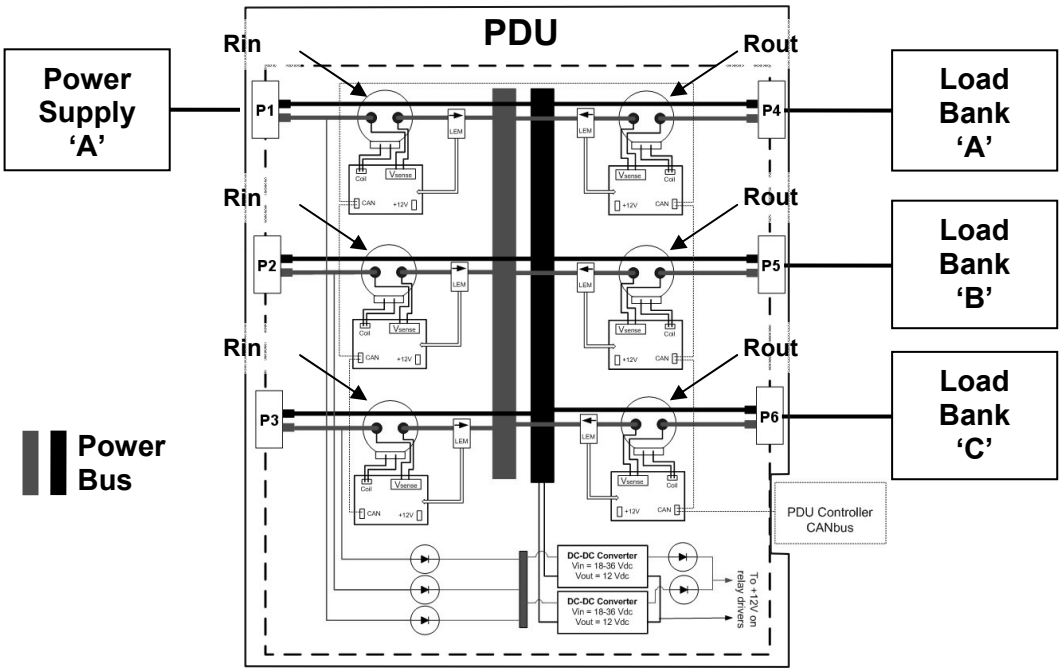

Figure 2. Schematic for the EPS test bed

test bed have an operating limit of 200 A. Relay operation was limited to ±100 A and 0 to 50 V during tests described in this paper. A custom controller board is used to activate each relay and to measure the current flow through and voltage at that relay. Each controller board also includes a CAN (Controller Area Network) bus that provides for communication between the controller card and the data acquisition and control system.

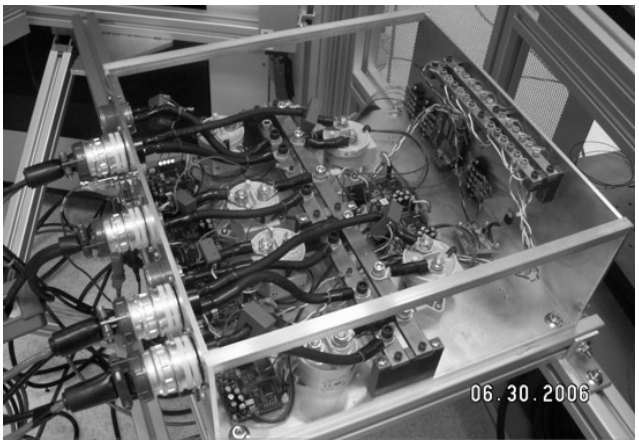

Figure 3. PDU within open enclosure showing components

Sensors and Failure Modes

The prototype PDU contains eighteen sensors. Twelve sensors represent measurements directly associated with the six relays – one current and one voltage measurement for each relay. There are six additional voltage sensors; one at each point where a relay connects to the power bus. The output of each sensor is available for data qualification. During nominal operation, the voltage across a given relay and the associated voltage measurement at the power bus are essentially identical due to high reliability and negligible losses between the two measurement points. This results in hardware redundancy within the sensor network. Additional information on the system state is also available for data qualification. This information includes the six relay states (on/off) and the three load states (high/low).

With input from the domain experts that developed the EPS test bed, sensor fault scenarios were identified for testing the SDQ system. These scenarios represent some of the potential sensor faults that would be encountered in a real application. The fault scenarios were taken from three basic groups: hard faults, intermittent faults and signal drifts; these are listed in Table 1.

A hard failure represents a complete loss of sensor signal, typically via an open circuit (failure to zero) or a short circuit (failure to maximum voltage). An intermittent failure represents an unreliable connection of the wiring to the sensor. The intermittent faults were further divided into either a random binary output or a filtered output. The binary output represents a partial failure where the sensor signal is interrupted for short random periods of time. A cracked solder point within the sensor would generate this type of signature where at times the sensor signal is valid and then go to a low or zero value. The filtered output represents the case where the sensor data qualification system is not located on the local sensor processing board. The local processor would gather data samples over some period of time, average and then pass that averaged value up to a higher level data qualification system. These filtered values of data in the presence of an intermittent binary fault, would be some partial value between zero and the true signal. The signal drift faults represent a subtle change in the current sensor signals due to thermal impact on the sensor resistive element. Based on analysis, only a 2% of full scale drift was anticipated. Therefore, 2% full scale drifts were inserted into the sensor signal at three distinct rates (4.3 mA/sec, 6.7 mA/sec and 16.7 mA/sec) to examine the impact on the SDQ system's performance.

Table 1. Sensor Faults

Group	Description
1	Hard Low
	Hard High
2	Intermittent - Binary Mode
	Intermittent - Filtered Mode
3	Drift -Low Rate
	Drift -Med Rate
	Drift -High Rate

Operation and Data Acquisition

LabVIEW was used to create a user interface to facilitate use of the test bed. This interface allows the test operator to manually control the configuration of the test bed by changing the status of the input and output relays and to initiate data acquisition. The interface can also run pre-programmed test sequences defined by the test operator. Once data is acquired, it can be saved for further analysis. Besides control and data acquisition, this interface provides a mechanism for injecting simulated faults into the test data. Fault injection is accomplished by layering sensor faults on top of the nominal operating data during data acquisition. Data from both nominal operation and data containing simulated sensor faults were used to develop and evaluate the SDQ system presented in this paper.

The data were sampled locally at each relay controller board at 500 Hz. These raw data were processed and passed on to the data acquisition system at 25 Hz. The resolution of the analog-to-digital converter (ADC) was 62 mA for the current sensors and 62 mV for the voltage sensors. It is anticipated that signal noise will be smaller than the resolution for the sensor signals generated by the PDU system.

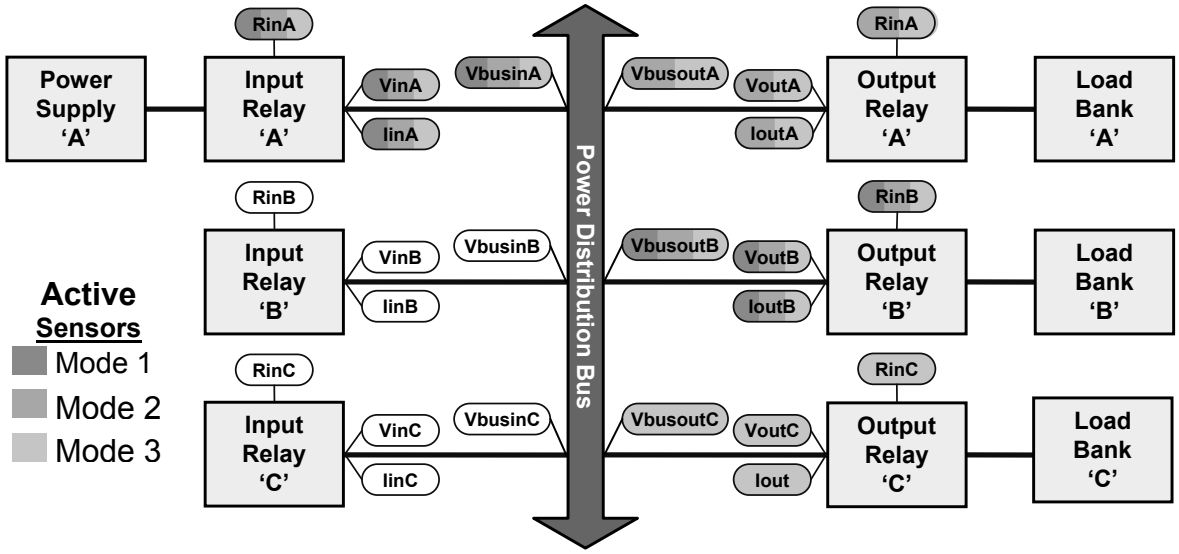

Figure 4. Diagram showing active relays and sensor for each test bed operating mode.

SDQ Application for the EPS Test Bed

Using data from the previously described EPS test bed and the SureSense software, a SDQ system was developed. The development and validation of that system is described in the sections that follow.

Sensor Network

A sensor qualification network was established for the EPS test bed described previously. Switch indicators were provided from the test bed to indicate which relays were closed. For this initial test phase, the current loads when accessed each had two operating points, minimum amperage of 15 and maximum amperage of 20. Also, the initial tests had three distinct operational modes as pictured in Figure 4. An operational mode is defined by the combination of closed relays. For example, Mode 2 had the input relay A and output relays A and B closed. The operational modes were further subdivided by the output current loads. Current output load status was inferred by input and output current measurements. This allowed the relationships to more refined.

The data qualification network was developed by defining constraints (i.e. relationships) between the system parameters. The first group of applied constraints utilized the physical redundancy of the voltage measurements. Due to the configuration of the electrical circuit, the voltage measurements were essentially identical (e.g. VinA = VbusInA). Conservation of charge was used to constrain the input current to the sum of the output currents, and the relationships between the voltages and currents were included into the network of constraints. Each operational mode had a different number of active sensors and relationships as shown in Table 2.

Table 2. Operating Modes

Mode	Active Sensors	Relationships
1	6	15
2	9	27
3	12	49

The initial networks developed for this test bed, attempted to utilize the SureSense software curve-fitting routines to establish the relationships. Due to the electrical circuit size and limited operating points, there were little variances in the voltage measurements. Therefore, the automated regression routines performed poorly in fitting the data, and the initial testing resulted in false alarms. The resolution to this problem was to instantiate the regression coefficients based on a clear understanding of the system design. If the design knowledge is available, then direct instantiation of the relationships is preferable rather than having the software perform regression analysis to establish those values.

Results

For this test series, the network required a minimum of 5 relationships to fail before issuing an alarm for a sensor and three consecutive alarms to actually fail the sensor. Once a sensor was declared failed, all relationships involving that sensor within the network were removed. Then, the network would perform an internal check to determine if enough relationships remained in the network to continue qualification or to suspend the process. Both of these requirements for detecting and declaring the sensor failed are selected by the network based on sensor design

information and user-provided system requirements for missed detections and false alarms.

Tables 3 through 5 show the results for the SDQ system testing. There are 13 sensor fault scenarios for each operating mode; they are defined by the "Fault Type" listed in column two and the "Sensor Failed" listed in column three. (Refer to Figure 4 for the active sensors and relays for each test mode.) A "Pass" in the "Failure Isolated" column indicates that the SDQ system correctly isolated the fault.

As can be seen in the results, the network demonstrated the ability to detect both hard and soft faults in the sensor data. For the hard faults, all declaration times occurred within approximately 0.08 seconds of fault occurrence. The sample rate of the test bed is 25 Hz; therefore the detection is immediate and consistently within the time constraint of the required three consecutive data cycles. A conventional hard-limit detection system with limits at the sensor range would perform no better given the same requirement of three consecutive data cycles. Therefore, the SDQ system results are comparable to the current state-of-the-art.

The intermittent sensor results were similar to those of the hard faults; they are detected within 0.08 seconds. It is important to note here that the intermittent-binary mode faults basically behave the same as the hard faults for the same initial time period. However, the intermittent-filtered mode faults do not. Since they output partial signal values, these faults would not necessarily be detected using a conventional hard-limit detection system.

The network also correctly detected all simulated drift failures. Again, it is important to note that these faults would not necessarily be detected using a conventional hard-limit detection system. The detection time was dependent upon the fault progression rate applied, as expected. If the time required by the network to detect one or more sensor faults is unacceptable, then other relational characteristic analyses may need to be employed.

Table 3. Sensor Data Qualification Results – Mode 1

Scenario	Fault Type	Sensor Failed	Failure Isolated	Detection Time (seconds)
Fault 1	Intermittent - Binary Mode	VoutB	Pass	0.08
Fault 2	Intermittent - Binary Mode	IoutB	Pass	0.08
Fault 3	Intermittent - Binary Mode	IinA	Pass	0.08
Fault 4	Intermittent - Filtered Mode	VoutB	Pass	0.08
Fault 5	Intermittent - Filtered Mode	IoutB	Pass	0.08
Fault 6	Intermittent - Filtered Mode	IinA	Pass	0.08
Fault 7	Hard Low	VoutB	Pass	0.08
Fault 8	Hard Low	IoutB	Pass	0.08
Fault 9	Hard High	VinA	Pass	0.08
Fault 10	Hard Low	IinA	Pass	0.08
Fault 11	Drift -Low Rate	IoutB	Pass	254.96
Fault 12	Drift -Med Rate	IoutB	Pass	156.70
Fault 13	Drift -High Rate	IoutB	Pass	63.29

Table 4. Sensor Data Qualification Results – Mode 2

Scenario	Fault Type	Sensor Failed	Failure Isolated	Detection Time (seconds)
Fault 1	Intermittent - Binary Mode	VoutB	Pass	0.08
Fault 2	Intermittent - Binary Mode	IoutB	Pass	0.08
Fault 3	Intermittent - Binary Mode	IinA	Pass	0.08
Fault 4	Intermittent - Filtered Mode	VoutB	Pass	0.08
Fault 5	Intermittent - Filtered Mode	IoutB	Pass	0.08
Fault 6	Intermittent - Filtered Mode	IinA	Pass	0.08
Fault 7	Hard Low	VoutB	Pass	0.08
Fault 8	Hard Low	IoutA	Pass	0.08
Fault 9	Hard High	VinA	Pass	0.08
Fault 10	Hard Low	IinA	Pass	0.08
Fault 11	Drift -Low Rate	IinA	Pass	475.26
Fault 12	Drift -Med Rate	IinA	Pass	298.07
Fault 13	Drift -High Rate	IinA	Pass	118.09

Table 5. Sensor Data Qualification Results – Mode 3

Scenario	Fault Type	Sensor Failed	Failure Isolated	Detection Time (seconds)
Fault 1	Intermittent - Binary Mode	VoutB	Pass	0.08
Fault 2	Intermittent - Binary Mode	IoutB	Pass	0.08
Fault 3	Intermittent - Binary Mode	IinA	Pass	0.08
Fault 4	Intermittent - Filtered Mode	VoutB	Pass	0.08
Fault 5	Intermittent - Filtered Mode	IoutB	Pass	0.08
Fault 6	Intermittent - Filtered Mode	IinA	Pass	0.08
Fault 7	Hard Low	VoutC	Pass	0.08
Fault 8	Hard Low	IoutC	Pass	0.08
Fault 9	Hard High	VinA	Pass	0.08
Fault 10	Hard Low	IinA	Pass	0.08
Fault 11	Drift -Low Rate	IoutA	Pass	438.90
Fault 12	Drift -Med Rate	IoutA	Pass	284.97
Fault 13	Drift -High Rate	IoutA	Pass	111.44

Concluding Remarks

The primary goal of the SDQ system is the validation of sensor data and the accurate detection and isolation of failed sensors. All diagnostic systems rely on the fact that data presented to them represent the true state of the system. Therefore, it is critical that none of the diagnostic processes use "bad" data when determining the state of the system. The results of the SDQ system testing demonstrated that the detection and isolation of failed sensors can be achieved accurately. In particular, the SDQ system was successful in meeting the performance criteria described in the preceding sections of this report. It should be noted that the sensor failure modes for the intermittent-filtered outputs and the drifts probably would not have been detected by conventional methods and relying on those types of sensor validation systems would most likely have resulted in missed detections. The results from the demonstration indicated the number of data cycles required to disqualify a sensor; however, no formal timing studies have been conducted that would benchmark the processing time required for qualification. Likewise, the sensitivity of the validation algorithm to a failed sensor condition was demonstrated in a limited manner using one type of sensor fault (drift) and needs to be further investigated.

The success of this study leads to other areas of research that need to be considered, such as

- Multiple sensor failures
- Real-time implementation issues
- System component failures
- Sensor failures within a closed-loop control system

In addition, to demonstrate the scalability of the SDQ system to other applications, benchmark timing studies need to be conducted with larger data qualification networks in order to determine the impact on real-time operation and CPU and memory requirements. This is important, because the data validation system will share computational resources with other functions that are already present for the diagnostic system.

In the future, the SDQ technology will be implemented in other environments in order to demonstrate its feasibility, operation and application to a variety of subsystems, and the team at GRC is actively pursuing other applications that are realistic and relevant to NASA's Exploration goals. Currently these include two cryogenic fluid management experiments at GRC and a reaction control system at the White Sands Test Facility that includes the propulsion feed system and engines.

Acknowledgements

The authors would like to thank the members of the GRC Advanced Electrical Systems Branch, Robert Button, Marcelo Gonzalez and Adolfo Torres, for providing their domain expertise and for the development and operation of the EPS test bed. In addition, Expert Microsystems is recognized for their guidance and support in using their SureSense software package.

References

Bickford, R.L., Bickmore, T.W., and Caluori, V.A. 1997. Real-time sensor validation for autonomous flight control. AIAA-1997-2901. AIAA/ASME/SAE/ASEE 33rd Joint Propulsion Conference and Exhibit.

Bickford, R.L., Bickmore, T.W., Meyer, C.M., and Zakrajsek, J.F. 1998. Real-time sensor validation for propulsion systems. Collection of Technical Papers (A98-45901 12-66) AIAA-1998-5184. AIAA Defense and Civil Space Programs Conference and Exhibit.

Bickford, R.L., Bickmore, T.W., Meyer, C.M., and Zakrajsek, J.F. 1999. Real-time sensor data validation for Space Shuttle Main Engine telemetry monitoring.

AIAA-1999-2531. AIAA/ASME/SAE/ASEE 35th Joint Propulsion Conference and Exhibit.

Bickford, R., Meyer, C., and Lee, V. 2001. Online Signal Validation for Assured Data Quality. In Proceedings of the 47th International Instrumentation Symposium, 107-110. Denver, Colorado: The Instrument Society of America.

Hines, J., and Davis, E. 2004. Lessons Learned from the U.S. Nuclear Power Plant On-Line Monitoring Programs. *Progress in Nuclear Energy*. Forthcoming

Herzog, J. P., Yue, Y. Y., and Bickford, R. L. 1998. Dynamics sensor validation for reusable launch vehicle propulsion. AIAA-1998-3604. AIAA/ASME/SAE/ASEE 34th Joint Propulsion Conference and Exhibit.

Ibarguengoytia, P. and Sucar, L. 2001. Real Time Intelligent Sensor Validation. *IEEE Transactions on Power Systems*, 16(4):770-775.

Lee, S.C. 1994. Sensor Value Validation Based on Systematic Exploration of the Sensor Redundancy for Fault Diagnosis KBS. *IEEE Transactions on Systems, Man and Cybernetics*, 24(4):594-605.