Space Shuttle Main Engine Failure Detection

Harry A. Cikanek, III

ABSTRACT: The problem of how to improve recognition of anomalous behavior in the Space Shuttle Main Engine is currently under study. The effort is planned to lead to an advanced real-time failure detection system for test stand application. This paper addresses motivation for the study, engine characteristics, failure detection problems, and the technical issues that are involved.

Introduction

Failure detection is a major arena of research and development in control systems engineering. The results of recent theoretical and experimental efforts have opened the possibility for solution of practical failure detection problems. This paper presents such a problem. It will address a current study of improvements to Space Shuttle Main Engine (SSME) failure detection concentrating on engine characteristics, engine history, failure characteristics, the system concept, and technical issues. To conclude, a brief preview of approaches to solving the problem will be presented.

During Space Shuttle Main Engine ground testing, there have been 27 major failures resulting in substantial engine hardware damage and loss. The failures have occurred despite an extensive conventional failure detection system for both control and plant component failures. After each failure, detailed analyses were conducted to determine the most probable cause and the steps necessary to prevent recurrence. One task in each investigation was to correlate failure events with anomaly symptoms that were reflected in engine performance data.

A review of the failure event correlations showed that, in many cases, anomaly symptoms were evident well before a shutdown command was given by the current failure detection system. In addition, the anomaly symptoms were usually evident in more than one measurement. The failure data also indicated that, in most failures, damage was progressive. Therefore, if in future failures more symptoms are recognized, failure detection and response can be accomplished earlier and the magnitude of damage due to engine failures can be reduced.

A literature review was undertaken to identify possible methods for detecting failure signatures in performance data. Merrill [1] surveyed detection literature concerning aircraft engine sensor failures. Success was reported for detecting various sensor failures primarily with filtering/estimation methods under simulated conditions. Willsky [2] discussed failure detection in a broader sense and gave mathematical insight into many of the filtering methods. At the time of that paper, most results were theoretical only. Later, Loparo and Buchner [3] gave estimation and pattern recognition as two possible approaches to detecting failures in process systems. Pau [4] presented failure detection as a subset of the condition-monitoring problem. These and some general texts on pattern recognition [5], [6] indicated that methods to advance engine failure detection performance were available. With the ever-increasing economies in computational power and the possible approaches available, improving engine failure detection appeared feasible with reasonable cost. Once the study was initiated, the first efforts undertaken were to identify engine system characteristics that would impact a detection system.

Engine System Characteristics

The Space Shuttle Main Engine is the first reusable staged combustion cycle rocket engine (a schematic with typical operating parameters is shown in Fig. 1). It is also the most complex and highest performance propulsion system ever built. System operation and vehicle constraints require careful monitoring and very precise control. The extremely high power density, reusability, and the highly stressed nature of the engine are characteristics that can magnify the effect of any shortcomings in engine materials, design, workmanship, or other category of anomaly. Extensive precautions are therefore taken with each engine in every stage of design, development, and testing to assure successful operation. Even so, the potential for a major failure always exists.

During testing and flight, the engine normally operates in three modes: start, mainstage, and shutdown. Closed-loop controls on main combustion chamber pressure and mixture ratio are utilized throughout the normal operating range (approximately 65–109 percent of rated power level). Open-loop valve sequences control the low-power-level portions of start and shutdown. Engine start lasts approximately 5 sec and engine shutdown lasts approximately 3.5 sec. Shutdown may be entered at any time after engine start initiation. Other engine operating modes are available to provide various levels of fail-operate and fail-safe redundancy.

To command the engine, the avionics system (depicted in Fig. 2) includes two identical cross-strapped engine-mounted computers, input and output electronics, and timers. The avionics are designed to eliminate single point failures. This package, known as the controller, interfaces with the vehicle or test stand to receive commands and transmit 128 standard on board measurements in the Vehicle Data Table.

The input electronics condition signals for a turbine flowmeter, shaft speed detectors, thermistors, pressure transducers, both rotary and linear variable differential transformers, and other minor instrumentation. Output electronics condition commands for valves, spark ignitors, servo-switches, and the backup pneumatic shutdown system. Software implements the control laws and threshold engine protection logic (redlines). Adjustments to control and redline parameters which tailor controls to a particular test and engine are made through adaptation data in the software.

Tests are supervised by a digital computer unit (also depicted in Fig. 2) in the blockhouse called the Command and Data Simulator. In addition to communicating with the engine, the Command and Data Simulator unit displays the Vehicle Data Table for human controllers, helps supervise prestart and post-shutdown procedures, and can interface with added test electronics. Typically, about 250 additional standard measurements are recorded during a test by a facility computing and data storage system.

Most on board and facility data are digitized at a rate of 50 samples per second prior to recording. Vibration data generated by engine-mounted accelerometers is the major exception to digitizing. It is handled separately from the other data systems, and maintained as wide-band analog data. Facility measurements include many measurements.


June 1986 0272-1708/86/0600-0013 $01.00 © 1986 IEEE
similar to those taken onboard, plus data streams from devices such as thermocouples and strain gages. The majority of the engine and facility data concerns performance and, thus, has potential employment in failure detection.

Current controller failure detection methods include electronic self-tests and interrupts to take advantage of the cross-strapped design. One interesting self-test example is an electronic valve actuator dynamic model. The model output is compared with actuator-sensed position and a tolerance test is made to determine if proper operation is achieved. (A valve out of tolerance with its model has produced two launch pad engine shutdowns.)

On board plant failure detection consists of about ten redline parameters that must fall within specified upper and/or lower limits at various times during a firing. On board response to failure includes either switching to redundant hardware or shutdown-sequence initiation.

Current ground failure detection includes Command and Data Simulator simulation of vehicle major component failure logic (for loss of redundancy) and monitoring of other critical conditions that will shut the engine down prior to simulated solid rocket booster ignition. A facility computer is utilized to monitor itself, and facility redlines. Human observers are typically utilized to oversee high-pressure pump operation, Command and Data Simulator operation, make video and visual observations of the exhaust plume and engine, and monitor fuel low-level indications. The observers are also utilized to control pre- and post-test conditions. Shutdown-sequence initiation is the only response available to facility indications of engine failure.

Engine testing began in 1975. To date there have been over 1000 hot fire tests conducted on three single engine stands and one cluster stand (for Shuttle vehicle simulation). The types of testing include flight operations testing (consisting of acceptance and certification firings), and development testing (consisting of design improvement, analysis verification, endurance limit determination, life definition, life extension, and performance improvement). A third type of testing (planned to begin in 1988) will be a test bed project utilizing higher levels of instrumentation to increase understanding of internal engine processes and to test higher risk advanced hardware concepts. The risk of major failures is lowest in the flight engine program, and is increased in the development and test bed programs.

Engine tests usually have multiple objectives (3 to 10) and, since major components are line-replaceable, engine builds may vary from test to test. Test duration may also vary. A typical burn simulating a flight throttle profile would be 520 sec predominantly at the 104 percent power level with throttling early in the burn to around 67 percent for 30 of the 520 sec. Yet tests may run from 1.5 sec for start-sequence development to over 800 sec for endurance testing.

The engine system characteristics noted here point out the extreme complexity and interrelatedness of the engine, its controls, and the test facility. They also underline the tremendous volume and variety of information available for failure detection and the speed with which it must be processed. This
Space Shuttle Main Engine and Ground Test History

Early in the design of the engine control system, a decision was made to require that the flight and test stand engine control systems be identical except for individual adaptation data. This philosophy eliminated many potential problems with verification, cost overruns, and safety for the avionics. The same philosophy requires that a new detection system should not alter the current engine and its control system.

During the course of testing, experience has guided engineering judgment as to where and when to place redline limits on engine measurements. Some have been in place from the beginning of the engine program and others have been implemented in response to failures. Some are stationary from test to test, while others are altered periodically due to hardware changes or new findings. The vibration redlines, for example, are set on a statistical basis and may vary from test to test. Similar flexibility must be built into an advanced failure detection system.

Redlines, the primary plant failure detection method, have shutdown from a high of 46 percent of all engine firings in 1978 to a low of 7.8 percent in 1981. In the last four years, the percentage of premature shutdowns per test has stabilized at around 10 percent. The reasons for crossing a redline can be extremely varied and the measurement that exceeds a redline may be a very indirect symptom of the anomaly occurring. This limits the response of a redline detection system. For instance, turbine over-temperature shutdowns have been caused by a flowmeter being out of calibration, an abnormal start transient, hydrogen leaking through nozzle coolant tube splits, and massive turbine blade failure. In each case, maximum temperature boundaries were not the first indication of the anomaly.

Another limitation of redlines is that they are only implemented in a stand-alone fashion on individual measurements. A shutdown indication due to high turbine temperature is not confirmed by a speed or pressure excursion. Thus, false alarms occur when a sensor fails and the plant is normal. In summary, while redlines indicate many failures rapidly, there are a number of instances when impending major failures were not detected as soon as possible.

The history of major failures is somewhat different than that of premature shutdowns (see Fig. 3). The number of major failures was fairly constant from early in the test program through the beginning of the operational engine testing with the exception of peaks during 1978 and 1981. Most of the failures during the peak times were attributed to design deficiencies that were shaken out during development testing to raise engine thrust.

Major failures have been quite random in cause. Many of the major engine components have been the point of failure initiation at some time during the program. These include ducts, valves, injectors, and turbopumps. Other failures were initiated by experimental instrumentation or through improper handling, quality control, or manufacturing. The wide range of initiators and causes implies that a new detection system should be adaptable, modular, and take into account as many measurements as possible. Also, even

June 1986
though design deficiencies have been resolved, future programs (for example, the test bed) demand that a new detection system be sensitive to the older failure signatures.

**Failure Characteristics**

In Fig. 4, a plot of parameter amplitude versus time gives a generic trace of many failures typical of liquid rockets. This plot assumes that the sensor is operating properly. On this plot we can define three amplitudes of importance to failure detection. These amplitudes delineate the four states of operation listed in the figure. Volkov et al. [7] defined similar parameters. In normal operation, the parameter indicates as expected. In degraded operation, the parameter indicates a problem that is not serious enough to warrant action by the controls. In emergency operation, the parameter indicates that a major failure will occur if no corrective action is taken. The failed state indicates extensive damage is occurring and engine operation can no longer be maintained.

A measure of failure detection potential can be defined by utilizing the time difference between the emergency and failure states. This measure, called the *failure response time*, is: $T_R = T_F - T_E$. For Space Shuttle Main Engine purposes, $T_R$ will be defined as the time the engine shutdown sequence began. In reviewing engine failure history, it was observed that a 0.5–1.0-sec improvement in shutdown initiation response would substantially reduce the extent of failure damage for the failures with $T_R \geq 1$ sec. This result is due to the engine shutdown sequence providing a greater than 60 percent power-level reduction within the first second of shutdown-sequence initiation.

How many failures had $T_R \geq 1$ sec and multiple indications? Of 17 failures reviewed in detail, 16 had multiple indications before shutdown was signaled. Eleven had response times of greater than 1.0 sec. Therefore, there is ample opportunity for reducing the number and magnitude of major failures.

Organizing failure characteristics is another problem. There are two natural categories of failures: control system and plant. Control system failures have the potential for inducing engine damage through either misapplication of controls or inability to monitor critical functions. The data signatures of control system failure can be classified in three types. The first type is hard failure, usually

![Figure 3](image-url)  
**Fig. 3.** Space Shuttle Main Engine shutdown and failure history.
characterized by a jump in the parameter. Figure 5a illustrates a jump due to a sensor purge port failure. A second type involves noise and erratic behavior, and the third involves drift and bias.

Plant failures are not likely to lead to noisy signatures but can include jumps, drift, bias, and also exhibit some unique characteristics. To illustrate, bias could be indicative of a miscalibration or shift in calibration of the fuel flowmeter, which could cause a high mixture ratio and resultant high turbine temperatures. An alternative type of bias is that which must be taken into account because of different radial locations for turbine discharge temperature sensors. Radially separated sensor locations could cause a 50-degree temperature difference in the sensed flow environment. The former condition is an example of a sensor anomaly which could lead to failure, and the latter is a plant condition due to the nature of the unevenly distributed flow field and is not indicative of a dangerous condition.

Special signal characteristics such as exponential growth, lag in response, humps, or dips in the data stream could be indicative of very dangerous conditions. Exponential growth in turbine temperature could signify degrading turbomachinery efficiency leading to an unbalanced engine operating point (Fig. 5b). A hump or dip in a pressure measurement, as shown in Fig. 5c, could indicate blockage or a leak path. A lag in a fuel flow response to outside changes, as shown in Fig. 5d (such as a commanded thrust variation), could signify a duct blockage.

Vibration measurements present another set of special signatures different from those found in the low-frequency performance data. They are also very difficult to characterize and interpret; taking substantial computational effort and expert analysis. Therefore, root-mean-square (RMS), vibration-level threshold cutoffs for redlines are expected to be very difficult to improve upon. As a result, this study will concentrate on improving detection of other performance parameter indications. This factor and those presented previously lead to the concept presented next.

**Concept and Technical Issues**

The failure detection system concept (shown in Fig. 6) centers around a stand-alone computing system, which will tap data from current devices, perform a detection analysis, and send continue/shutdown indications to the engine all in real time. The efforts to develop the system concept will first require detailed characterization of the failure modes and their reflection on current engine performance data. Then, methods to detect each mode must be developed and applied. Finally, an architecture must be developed to enable the system to perform under a set of constraints and goals. Of course, these are not discrete tasks; there will be interplays and trades made between each aspect of system development.

Engine characteristics will affect how the system is developed in the following ways. The variation in normal engine operation due to reusability and line-replaceable-unit design coupled with the adaptation data approach in the control software suggest that failure detection algorithms will require some sort of adaptation to current conditions. The extensive amount and wide variety of data indicate that careful selections and/or combinations must be made and a variety of detection approaches might be required. The engine control system design eliminates single point failures and gives extensive electronic redundancy so that the scope of this effort can be limited to mechanical control components and the plant.

The closed-loop controls, the general complexity, and the coupled nature of the engine must be taken into account when trading detection sensitivity and false alarm robustness. Single indication will probably not be reliable enough. A final engine system factor is that due to the harsh environment; much engine data will have semipredictable drifts and biases during normal engine operation. Therefore some detection methods might re-
quire a form of qualitative rather than quantitative analysis.

Space Shuttle Main Engine history also has affects on detection system development. Since all current engine operations and hardware have been through extensive qualification and certification, any attempt to alter the current engine system would be extremely costly. Limiting the scope of the failure detection system by not allowing changes in the current engine testing practices will eliminate the cost penalties with relatively few attendant restrictions on the failure detection system. Chief among these restrictions is that data rates will be limited to 50 Hz. This restriction is not as severe as it seems. All data from past failures were taken at 50 Hz, so there are no reliable means for characterizing higher frequency effects. Also, response will be limited to initiating engine shutdown. Predicting engine response is difficult and requires empirical data even when engine performance is nominal. Therefore, for this study, it is not practical to attempt a response to failure other than shut down. One impact of such a limitation is that the detection system need be operable only during start and mainstage.

Finally, the failure characteristics will have the driving influence on how the detection system will be formulated. Some of the failure response times will be too short to tackle. Catastrophic structural failures having millisecond response times are the dominant short-response examples. However, for those failures with response times long enough to perform useful detection, the wide range of signatures and the multiple indications will give an opportunity to apply a range of techniques and redundancy in the logic. This multiplicity of techniques will probably lead to parallel and/or distributed architecture for the system.

Solution Approaches

Detecting failures will generally consist of three major approaches: filtering, pattern recognition, and intuitive methods. Each of these overlaps to some degree, and it is expected that the detection system developed in this study will draw from each method. Filtering may be best applied to sensor failure signatures or to signatures like those of sensor failures. Pattern recognition may be employed to sense broad deviations in the internal state vector of the engine or of a major component. Intuitive methods can imply utilizing combinations of parameters like efficiency for static balance comparison, or broader use of concepts such as the valve actuator model.

To find the best approach, experiments will be conducted to trade the performance of each detection method on each of the failure signatures. Then good performers will be combined into an integrated system. One possible approach is to form a layered architecture that would move data through successively more complex algorithms. Other approaches may be envisioned that are equally likely possibilities. In general, it will be desirable to organize the system with modularity, adaptability, and minimum requirements for human supervision to keep costs low and performance high.

Conclusion

Many factors led to the formulation of a study to develop a breadboard advanced failure detection system for Space Shuttle Main Engine operation during hot fire ground testing. Among the factors were the test history, current detection system limitations, and increased computing capability. The current detection system includes: avionics system failure detection with interrupts, self-tests, and hardware redundancy management; and engine/test stand system detection with red-line logic and human monitoring.

How the engine works and how it is operated will place demands and constraints on any new detection system. Among the demands and constraints are the volume of data, the very fast response times necessary, the requirement for minimum alteration of current systems, and the variability of engine operation.

Data available for failure detection include the low-frequency digital, wide-band vibration, and facility digital data. Definition of nominal engine operation versus degraded and dangerous operation will be an early major task in the study. Test history shows that there are many classifications of failure signatures and a wide range of measurements in which the signatures may be found. The three major approaches to robust failure detection that will be applied include filtering, pattern recognition, and model comparison. Experimentation will determine what approaches are promising and how they will be integrated to gain the most performance at reasonable cost.

References


Harry A. Cikanek, III, is an Aerospace Engineer in the Control Systems Division of the Systems Dynamics Laboratory, NASA/George C. Marshall Space Flight Center, where he has worked for over two years. He received his bachelor's and master's degrees in mechanical engineering from the Georgia Institute of Technology. His current work includes modeling, simulation, control, failure detection, and condition monitoring of pump-fed, large liquid rocket engines. He is a Member of the Energy Systems and Control Panel of the ASME Dynamic Systems and Control Division, and a Member of the AIAA Alabama-Mississippi Section Board of Directors.