IN-20
38699
p 11

NASA Contractor Report 187219
AIAA-91-3604

Space Engine Safety System

William A. Maul and Claudia M. Meyer
Sverdrup Technology, Inc.
Lewis Research Center Group
Brook Park, Ohio

September 1991

Prepared for
Lewis Research Center
Under Contract NAS3-25266

NASA
National Aeronautics and
Space Administration

SPACE ENGINE SAFETY SYSTEM

William A. Maul
and
Claudia M. Meyer
Sverdrup Technology, Inc.
Lewis Research Center Group
Brook Park, Ohio 44142

Abstract

A rocket engine safety system is designed to initiate control procedures which will minimize damage to the engine and vehicle or test stand in the event of an engine failure. This report describes the features and the implementation issues associated with rocket engine safety systems. Specific concerns of safety systems applied to a space-based engine and long duration space missions are discussed. Examples of safety system features and architectures are given from recent safety monitoring investigations conducted for the Space Shuttle Main Engine and for future liquid rocket engines. Also, a general design and implementation process for rocket engine safety systems is presented.

Introduction

The goal of every rocket engine design is to satisfy the mission performance requirements, while at the same time ensuring the safety of the engine and the vehicle or facility test stand. Due to the time, cost, and potential risks to human life involved in rocket engine operation, many investigations are currently underway to improve the current state of rocket engine safety monitoring. The rocket engine safety system should perform real-time, on-line detection and, when appropriate and possible, identification of failure modes, especially those that may lead to loss of crew, vehicle or mission. This paper outlines the features of safety systems and discusses the issues involved in their implementation.

This paper describes the current Space Shuttle Main Engine (SSME) safety system and recent activities in the area of advanced safety algorithms for the SSME. In addition, the safety system concepts proposed for future rocket engines are discussed. The impact of mission requirements and hardware limitations on safety systems are presented. Also discussed are the various implementation issues that must be addressed during the safety system design phase. Issues associated primarily with space engine applications of safety systems are discussed and a general safety system design process is proposed.

Background

Safety systems have been used throughout the history of rocket engine development. The systems implemented to date are based entirely on limit-checking algorithms; failure detection is achieved by comparing the sensor data to predetermined limits. Safety systems, currently in use, do limit-checking upon individual sensor signals. The SSME controller, for example, monitors six parameters during steady-state operation; four of the six are compared to absolute limits, while the fifth and sixth parameters are compared to limits that are a function of the operating state. If any of these limits is exceeded for three consecutive sampling intervals (a sampling interval is 20 milliseconds), a shutdown sequence is initiated.[1] In addition, start confirm criteria are applied to several parameters during startup to ensure that ignition has occurred.

One augmentation to the SSME safety system described above has been the Flight Accelerometer Safety Cutoff System (FASCOS). This system monitors the output from six accelerometers, three on each high pressure turbopump. FASCOS has been installed in ground test

firings and flights; however, physical connection to the main engine controller has never been made for flight due to a series of problems with faulty accelerometers.[2]

Other efforts are currently underway to improve SSME safety system performance.[3-10] Each effort provides the safety system with additional information about the current operation of the engine based on a selected sensor set. Although the techniques have been developed for the SSME, they could be readily applied to other rocket engines. All of these techniques are intended for real-time implementation.

The System for Anomaly and Failure Detection (SAFD) examines the time average of incoming sensor signals in order to filter out noise.[3-5] The filtering process allows limits which are tighter and more refined than for unfiltered signals. The data is averaged over a 200-millisecond window. This window size was chosen to permit the detection of rapidly occurring failures as well as failure modes that occur over long periods of time. SAFD analyzes a set of twenty-four parameters and indicates an anomaly when a predetermined number of sensors simultaneously exceed their limits.

Time series analysis was applied to SSME test stand data in two studies.[6,7] Both studies developed univariate time series (autoregressive) models and analyzed the residual information, actual sensor deviations from the models, to detect failure modes. The first study applied the autoregressive technique to nine parameters, while the latter study computed time series models for eighteen parameters. Although successful in detecting some failures, the time series technique requires the signal to be stationary over the entire period of engine operation to which it is being applied. SSME processes such as tank venting and repressurization, which occur during most steady power-level operations, cause non-stationary behavior. Therefore, the time series technique has limited applicability. The first study also investigated a detection technique that computed the average power of the signal with time. The Average Signal Power (ASP) technique was applied to eighteen SSME parameters. The technique requires the signal to be stationary only during each average signal computation window. A 2-second computation window was used to minimize the impact of non-stationary behavior.

Several studies investigated the combination of various sensors in order to detect SSME failure modes.[7-9] Each study compared test stand data to nominal exemplar data sets developed from the SSME steady-state model or nominal test firings. The comparison resulted in a residual for each sensor. One approach involved a linear summation of the residuals; a failure was detected when the residual sum exceeded a predetermined nominal limit.[8,9] In another approach, the residual set at each time slice was correlated with an expected or nominal residual set; fault detection was based on the value of the correlation coefficient.[7,8]

The previous techniques were developed for use during steady-state operation of the SSME. Several techniques have been applied to non-steady-state operation on the SSME. One investigation involved the application of non-linear regression models to the startup and shutdown transients.[7] Neural network models have been developed for several parameters during startup.[10] In both cases, the deviations between the actual and model-predicted values are intended to be used as indicators of engine and/or sensor health. The use of SSME fleet-wide nominal performance envelopes during the various transient conditions has also been proposed.[9]

Figures 1a and 1b show the same typical SSME thrust profile. Figure 1a illustrates the current coverage of the SSME safety system, while Figure 1b illustrates the proposed coverage of the techniques described above. A larger number of sensors are employed for fault detection by the safety system described in Figure 1b. As can be seen, a collection of algorithms will be required in order to provide comprehensive coverage of the engine.

Several factors are involved in evaluating the performance of the safety system. These include the number of anomalies detected, the number of missed detections, and the number of false alarms.

In addition, the detection time buffer is extremely important. The detection time buffer is the time period between the detection of the failure mode and the time when the engine control cannot prevent significant damage to the engine or its surroundings. When applying an advanced safety algorithm to historical SSME failure data, the time buffer is defined as the time between detection of the failure mode by the safety algorithm and the time when the redline system initiated shutdown. Figure 2 illustrates the actual chamber pressure profile for SSME test firing 901-364. For this example, the time buffer is shown to be the difference between the SAFD detection time and the actual redline engine cutoff. This engine sustained significant damage which could have been reduced by an earlier shutdown.

Table 1 presents the results of applying several steady-state fault detection algorithms to five anomalous SSME ground test firings. Although the detection techniques were developed in these studies, the detection criteria need to be refined. Therefore, direct comparisons of the detection times between the various algorithms are inappropriate. The results do show that each algorithm provides improved detection times over the existing redline system; earlier detection times indicate larger time buffers. The algorithms take advantage of early failure indications in the data and hence permit earlier shutdown than the current redline system.

Space Engine Safety System Features

Rocket engine safety systems can exhibit a wide range of features which are dependent upon mission and engine requirements. Space engines are designed to perform in a space environment for long durations. Mission profiles require the space engine to be highly reliable (man-rated) and reusable, and perform during various mission phases such as orbit transfer and lander missions.[11] The safety system must have the flexibility to accommodate the multiple mission profiles anticipated for a space engine and to allow for changes during the development and production phases of the engine program. The design and operation of the safety system must also reflect the control capabilities of the rocket engine.

The primary requirement for any safety monitoring system is that it must perform in real time; the system must be able to collect, analyze and interpret sensor information. The safety system must take advantage of precursor failure indications in the data in order to minimize engine and vehicle damage and mission impact. As a minimum, the safety system should detect incipient failures early enough to give the controller sufficient time to shutdown the engine safely. Determination of "sufficient time" is based on either experience or on detailed knowledge of the failure mode, its rate of propagation and its effects. In cases where such knowledge is not available, system response to the failure mode should be initiated at the time of earliest detection.

The ability of the safety system to provide these functions will depend upon the failure modes of the particular engine cycle as well as the type and location of sensors. Some failure modes propagate quickly, such as turbine blade cracking and duct rupture. These failures give little or no early failure indications in traditional performance sensors (temperatures, pressures, etc.) and may not be manageable without specialized sensors. Sensors can be divided into two classes: those that sense the primary effects of an anomalous condition and those that inferentially determine component conditions based upon secondary effects.[12] A bearing deflectometer is an example of the former; this sensor determines bearing wear by measuring the localized, cyclic deformations on the outer bearing race caused by the passage of the balls.[13] Alternatively, information from several inferential sensors can be fused and processed to provide fault detection capability. For example, bearing wear can result in turbopump performance degradation and can lead to changes in inlet and discharge pressures and temperatures, changes in fluid flowrate and/or changes in shaft speed. The difficulty in using inferential sensors for fault isolation arises in correlating a unique set of sensor responses to a particular failure mode. Critical failures which provide sufficient early failure indications in the available sensor suite should be the ones targeted by the safety system.

Additional features of a safety system are desirable to ensure mission success and to improve the operation of the safety system. Mission success may differ from engine safety in that the immediate shutdown of the engine may not be a preferred option given a particular mission profile. For example identification of the detected failure mode and its effects may indicate that the engine can operate safely at a reduced power level; this control option will allow more flexibility in the selection of engine command procedures based upon mission requirements. Features, such as sensor validation, fault accommodating control and automated diagnostics/prognostics will improve safety system performance by increasing the probability of mission success.

The space engine safety system should have the ability to validate sensor signals and to accommodate failed sensor measurements. On the SSME, sensors fail at a much higher rate than any other component. Several ground test firings have been shutdown erroneously due to failed measurements. In addition, an in-flight redlined temperature sensor failure caused an SSME to erroneously cut-off on flight STS-51F.[2] Sensor failures are either "hard failures" where the sensor completely discontinues functioning properly or "soft failures" where the sensor discrepancy is more difficult to ascertain, such as thermal drift. Sensor validation functions may include limit checks, built-in tests, voting logic for redundant sensors (three or more), and analytical redundancy techniques which provide a synthesized signal for comparison with an actual signal. Once sensor failures have been detected and isolated, they must be ignored by the fault detection algorithms to prevent false alarms. In some cases, it may be advantageous to use synthesized measurements for engine control or engine health assessment. The use of analytical redundancy for sensor fault detection, isolation and accommodation has been successfully demonstrated on aircraft engines.[14] Analytical redundancy techniques are currently being investigated for the SSME.[15] The availability of synthesized signals will be critical for space-based engine safety systems since some space-based engine studies have identified the entire engine as an Orbital Replaceable Unit;[16] therefore, individual sensors cannot be replaced.

The number and complexity of the functions that the safety system must support establish the computational requirements and therefore drive the hardware design. Throughput analysis assesses the processing and I/O requirements for these functions and provides an initial estimate of the hardware required. Each detection algorithm will have a specific set of computational requirements. Some detection algorithms may analyze the frequency information of the sensor signal and therefore require high sampling rates. Other algorithms may be designed specifically for sensors that supply large amounts of information, such as a spectrometer or optical pyrometer. The architecture must be designed to accommodate these throughput requirements. Furthermore, the architecture should be flexible to facilitate the evolution of the safety system as new sensors or fault detection and/or isolation techniques become available or mission requirements are altered.

One possible area of future evolution involves the use of real-time diagnostics for the purpose of fault accommodating control. Historically, rocket engine safety systems have been primarily used to initiate shutdown in the event of an engine anomaly. Fault accommodating control allows the safety system to respond based on engine health; an example is sensor fault accommodation. The reduction of mission risk is a primary driver in the development of fault accommodating control capabilities.[16] In addition, an advanced safety system could assess the probable risks associated with various control strategies in response to engine component degradations. For example, a possible response to an engine degradation would be to throttle back the engine to operate at a reduced power. Fault accommodating control requires real-time diagnostic and prognostic capabilities and will therefore be computationally intensive.

The final feature of the safety system for space-based engines involves its interaction with other systems, such as the engine controller and the vehicle or test stand. The controller can provide the safety system with the current engine operating point and the control process that is maintaining that point; the engine safety system supplies the controller with the current health of the engine and required action in the event of an anomaly. The engine safety system must also communicate

appropriate information to the vehicle so that mission and vehicle impacts can be assessed in addition to engine considerations. In a multi-engine configuration, for example, the vehicle safety system must perform all functions that require data from more than one engine. Thrust vectoring is an example of such a function. In all cases, the vehicle safety system and the crew must have the authority to override the commands from the engine safety system.

Space Engine Safety System Design and Implementation Issues

The design of the safety system is strongly influenced by the engine design and mission requirements. This section proposes a rocket engine safety system design process that satisfies the features and requirements described in the previous section. The proposed methodology assumes that the safety and engine system designs are highly interactive and that they are conducted concurrently.

Initially a Failure Modes and Effects Analysis (FMEA) is performed on the current engine design to identify potential failure modes and the probable effects of the modes. The failure modes are then prioritized based on mission impact and probability of occurrence. A sensor set is selected to allow detection and possible identification of the prioritized failure modes. The sensor set is then introduced back into the engine design where implementation issues, such as any effects on engine operation and engine structural integrity due to sensor placement, are addressed. Several iterations may be required in order to achieve an acceptable sensor set for both the engine and the safety system. For example, an optimization procedure used by the Rocket Engine Condition Monitoring System (RECMS) program for the National Launch System, was based on life cycle cost.[12]

Once the optimum sensor set is selected, analytical tools must be chosen to process the sensor data and to detect the prioritized failure modes. These tools may be selected from previous safety system applications or they may require development due to new sensor technologies or unique requirements. The refinement of the detection tools to the particular engine may be achieved through engine models and component test rigs, until the engine development is complete.

Based on the detection capabilities and the controllability of the engine system, the safety system designer determines the extent of the diagnostic and prognostic capability required of the safety system. Results from the FMEAs and Failure Information Propagation Models, expert knowledge and qualitative models will generate the diagnostic tools needed to isolate and identify the failure process occurring. The prognostic tools will supply the system with the propagation of the failure mode with time, including limited component life prediction. Also, available control strategies, such as reduction in thrust or change in mixture ratio, are developed in response to anomalous engine conditions. During operation, the safety system will supply the proper control action based on the identified failure mode, the prognosis for that mode and the current mission requirements.

After the analytical tools for the safety system are defined, the system framework or architecture can be devised. The architecture must optimize mass, throughput and reliability. The architecture must also allow for modifications of the safety system due to changes in the engine or the safety system algorithmic tools, and for the verification and validation (V&V) of the safety system. Several architectures for a real-time monitoring and control system for rocket engines have been considered.[17] The two main categories of architectures are centralized and de-centralized. In the centralized system, all of the algorithmic tools are dynamically allocated on multi-processor boards in order to utilize computer resources efficiently and minimize response time. The de-centralized system features the organization of the tools onto discrete processors or sets of processors by some criteria. Algorithmic tool functionality and engine component breakdown are two de-centralized system architectures; other de-centralized architectures might include, algorithmic tools that utilize common signal inputs or are scheduled to be applied during the same mission phase. Centralized system architectures require less hardware, while offering maximized utilization of all resources. De-centralization of the system architecture will allow for the greatest ease in modifying the safety system and in performing a thorough application of V&V techniques.

V&V must be an important consideration in the development of the safety system. The software framework must allow for V&V hooks, so that each algorithm can be checked out independently. Finally the total safety system package, both hardware and software must be tested to ensure that all components interact properly and efficiently. The testing process for the safety system should be thorough in order to provide reliable safety system operation.

Concluding Remarks

This paper presented the issues involved in the development of a space engine safety system. A space engine safety system must be able to supply reliable, real-time protection to the engine and vehicle or facility test stand. Experience with the SSME indicates that a collection of algorithms is required in order to provide complete and comprehensive coverage of the engine. The safety system features are dependent on the anticipated mission profiles and the design and controllability of the engine. The engine design establishes the failure modes, while the engine controllability and mission profiles will define the real-time responses available to the safety system. The failure modes and the available responses may suggest the need for fault accommodating control, which will in turn require real-time diagnostic and prognostic capabilities.

The safety system design process presented emphasizes that the safety system should be designed concurrently with the engine. The selection of sensors and algorithmic tools, and the system framework are heavily influenced by the engine design. At the same time, the engine design and performance are effected by selection of the sensor suite and their locations. The safety system framework should be selected based on throughput and reliability considerations, as well as ease in V&V and overall system modification and expansion. Thorough evaluation of the safety system features presented in this paper, with the mission and engine requirements and proper system design will provide a safety system that enhances engine safety and reliability.

References

(1). Roth, P. *Computer Program Contract End Item, Flight 4C Configuration, Space Shuttle Main Engine Controller Operational Program, Part 1.* CP406R0001, Revision F, Rockwell International/Rocketdyne Division, November 1988.

(2). Wong, K. *Space Shuttle Sensor Assessment,* Vitro Corporation, April 1990, Internal NASA HQ Report.

(3). Taniguchi, M.H. *Failure Control Techniques for the SSME, Phase I, Final Report.* NASA CR-179224, 1986.

(4). Taniguchi, M.H. *Failure Control Techniques for the SSME, Phase II, Final Report.* NASA CR-179231, 1987.

(5). Panossian, H.V.; Kemp, V.R. and Eckerling, S.J. *Real-Time Failure Control (SAFD), Final Report.* NASA CR-184025, 1990.

(6). Meyer, C.M. and Zakrajsek, J.F. *Rocket Engine Failure Detection Using System Identification Techniques.* AIAA Paper 90-1993, July 1990.

(7). Hawman, M.H.; Galinaitis, W.S.; Tulpule, S., and Mattedi, A. *Framework for a Space Shuttle Main Engine Health Monitoring System, Final Report.* NASA CR-185224, May 1990.

(8). Maul, W.A. *Multi-sensor Analysis Techniques for SSME Safety Monitoring.* AIAA Paper 90-1990, July 1990.

(9). Nemeth, E. *Health Management System for Rocket Engines, Final Report.* NASA CR-185223, June 1990.

(10). Meyer, C.M. and Maul, W.A. *The Application of Neural Networks to the SSME Startup Transient.* AIAA Paper 91-2530, June 1991.

(11.) Millis, M. G. and Binder M. P., *Integrated Controls and Health Monitoring for Chemical Transfer Propulsion.* AIAA Paper 90-2751, July 1990.

(12.) Carter, R.D. and Denny, S.K. *Rocket Engine Condition Monitoring System Phase I Technical Report, Volume 1.* AFAL CDRL 3012, 1990.

(13.) MacGregor, C.A. *Reusable Rocket Engine Maintenance Study, Final Report.* NASA CR-165569, 1982.

(14.) Merrill, W.C.; DeLaat, J.C. and Abdelwahab, M. *Turbofan Engine Demonstration of Sensor Failure Detection.* Journal of Guidance, Control, and Dynamics, Vol. 14, No. 2, 1991, pp. 337-349.

(15.) Makel, D.K.; Flaspohler, W.H. and Bickmore, T.W. *Sensor Data Validation and Reconstruction, Phase 1: System Architecture Study.* NASA CR-187124, 1991.

(16.) Bickford, R.L., Collamore, M.L.; Gage, M.L.; Morgan, D.B. and Thomas, E.R. *Orbit Transfer Rocket Engine Integrated Control and Health Monitoring System Technology Readiness Assessment, Final Report Task E.7.* NASA CR-187122, 1991.

(17.) Binder, M.P. and Millis, M.G. *A Candidate Architecture for Monitoring and Control in Chemical Transfer Propulsion Systems.* AIAA Paper 90-1882, July 1990.

SSME Test Firing	SAFD Ref. 5	Time Series		ASP Ref. 6	Linear Sum		Correlation		Redline Cutoff Ref. 3
		Ref. 6	Ref. 7		Ref. 9	Ref. 8	Ref. 7	Ref. 8	
901-307			9.0		43.5	15.6	8.6	15.6	75.0
901-340	19.8	291.0	12.2	21.0		279.2	405.5	290.2	405.5
901-364	205.7	154.0	210.0	387.0		45.2	42.7	38.0	392.2
901-436		369.0	70.0	48.0		325.9	302.4	141.0	611.1
902-249		398.0	160.0	398.0	329.6	158.8	5.2	20.9	450.6

Table 1. Available detection times by proposed steady-state detection techniques on five catastrophic SSME test firings.

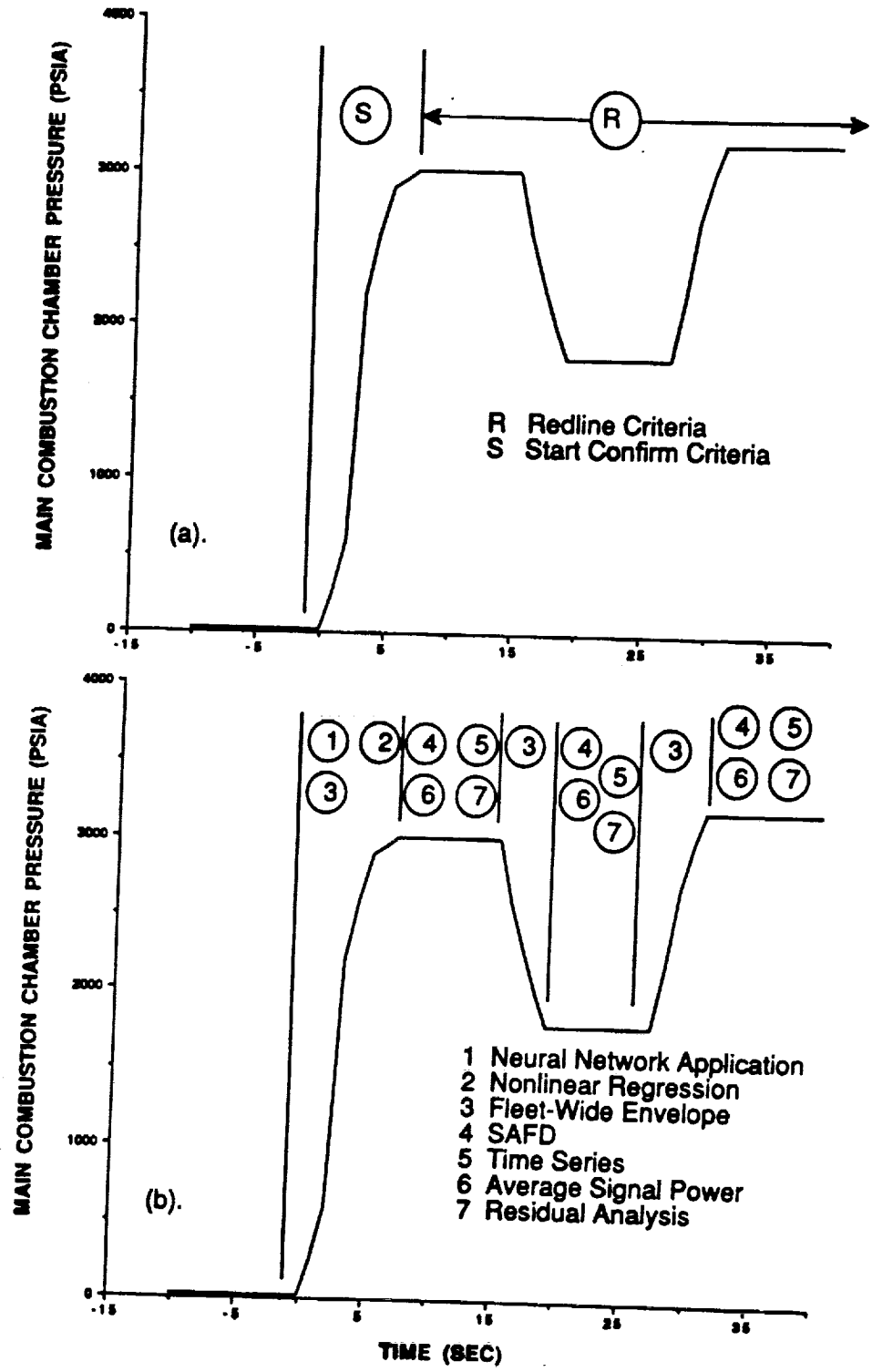

Figure 1. The anomaly detection coverage of a typical SSME thrust profile for (a) the current safety system and (b) a proposed set of safety detection algorithms.

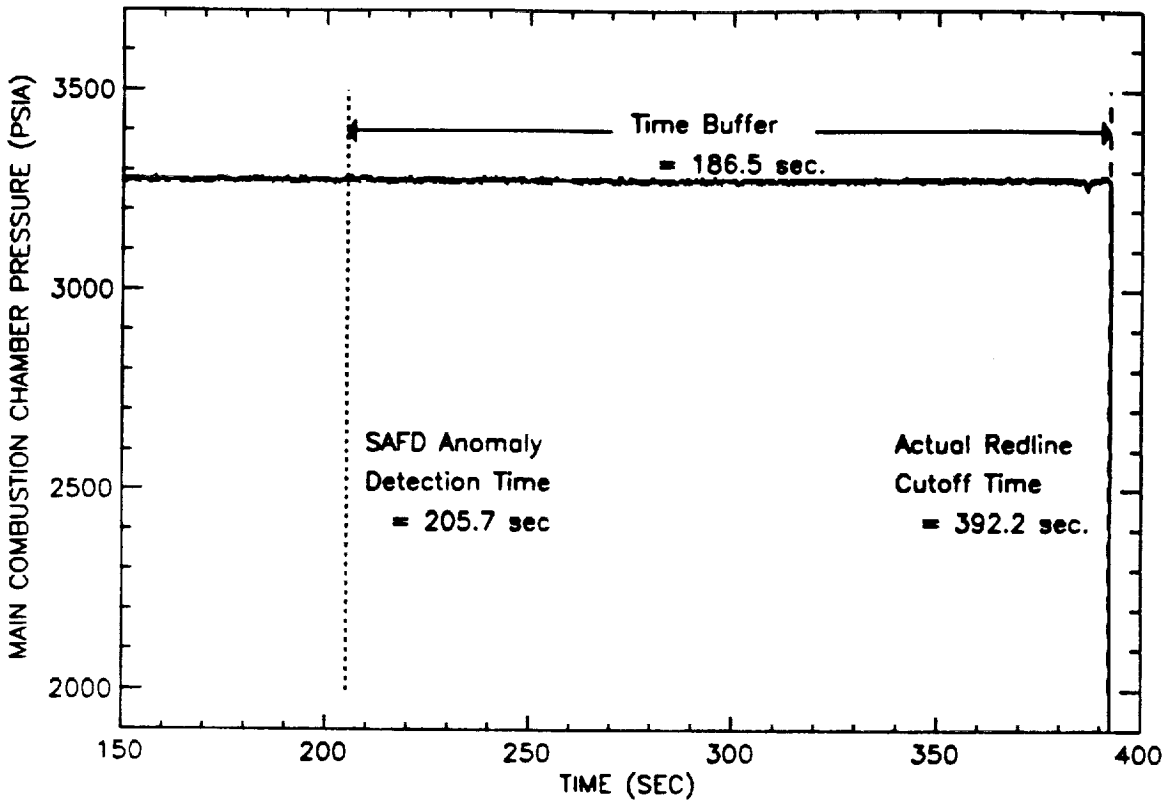

Figure 2. The time buffer for the SAFD detection algorithm applied to SSME test firing 901-364.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1991	Final Contractor Report

4. TITLE AND SUBTITLE

Space Engine Safety System

5. FUNDING NUMBERS

WU-590-21-41
C-NAS3-25266

6. AUTHOR(S)

William A. Maul and Claudia M. Meyer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Sverdrup Technologies, Inc.
Lewis Research Center Group
2001 Aerospace Parkway
Brook Park, Ohio 44142

8. PERFORMING ORGANIZATION REPORT NUMBER

E-6565

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Lewis Research Center
Cleveland, Ohio 44135-3191

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA CR-187219
AIAA-91-3604

11. SUPPLEMENTARY NOTES

Project Manager, Larry P. Cooper, Space Propulsion Technology Division, NASA Lewis Research Center, (216) 433-8089. Prepared for the Conference on Advanced Space Exploration Initiative Technologies cosponsored by AIAA, NASA, and OAI, Cleveland, Ohio, September 4-6, 1991.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Categories 15 and 20

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

A rocket engine safety system is designed to initiate control procedures which will minimize damage to the engine and vehicle or test stand in the event of an engine failure. This report describes the features and the implementation issues associated with rocket engine safety systems. Specific concerns of safety systems applied to a space-based engine and long duration space missions are discussed. Examples of safety system features and architectures are given from recent safety monitoring investigations conducted for the Space Shuttle Main Engine and for future liquid rocket engines. Also, a general design and implementation process for rocket engine safety systems is presented.

14. SUBJECT TERMS

Warning systems; Spacecraft propulsion; Aerospace safety; Rocket engines

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	