Image Cover Sheet

CLASSIFICATION	SYSTEM NUMBER
UNCLASSIFIED	149685

TITLE

A SIMULATION-BASED APPROACH TO SPACECRAFT POWER SYSTEM FAULT DETECTION AND DIAGNOSIS

AN: 95-00553

System Number:

Patron Number:

Requester:

Notes:

DSIS Use only:

Deliver to: NL

A Simulation-Based Approach to Spacecraft Power System Fault Detection and Diagnosis

Peter Adamovits[1]
Canadian Space Agency
Communications Research Centre
3701 Carling Avenue
Ottawa, Ontario, Canada, K2H 8S2

Abstract

The paper describes the model-based Multiple Fault Diagnostic System (MFDS) that identifies and diagnoses faults that occur in a spacecraft Electrical Power System (EPS). The spacecraft on which the MFDS is demonstrated is large and complex. Communication opportunities are infrequent and short in duration. Effective management of the spacecraft is difficult for the human operators. High costs may result from operator error including loss of the spacecraft. The demand for increased reliability has resulted in the push toward increased automation. The MFDS attempts to assist the operator by monitoring the EPS identifying degraded or failed components.

In knowledge based systems, there is a distinct division between the knowledge and the mechanisms that operate on the knowledge. Here the knowledge component is further partitioned into the deep behavioral knowledge of the domain (the model) and the shallower knowledge of the reasoning elements. The reasoning elements are divided into 6 discrete steps, the Diagnostic Process. At each diagnostic process step, a shallow reasoning system is used to reason about the data, symptom or hypothesis set under study. The partitioned knowledge base is easier to create and maintain than the flat knowledge base that typically exists.

The model based reasoning approach used in the MFDS relies on a simulation for the model. Here the engineering details that system designers use to construct their simulation, test its accuracy and reliability in a variety of operational modes are also used in the diagnostic system model. The reliance on a simulation eliminates the time and cost associated with recoding the model in some other form (logic, rules, etc.).

The use of a simulation as the model, shallow reasoning elements and the diagnostic process has proven successful. The Multiple Fault Diagnostic System has successfully demonstrated the approach detecting and diagnosing several tens of faults at the same time with a high accuracy.

Introduction

Model-Based Artificial Intelligence (AI) software approaches to diagnosis require encoding a reasonable facsimile of the problem domain. This model is used as a reference for comparison with the data received from the domain being examined. Often, the model is distributed throughout the knowledge base violating one of Artificial Intelligence's tenets, that of the separation of the knowledge from the mechanism that manipulates the knowledge. In the work presented, the model is encoded as an object oriented simulation (continuous, linear) of the domain, a spacecraft electrical power system. The inferential elements of the system are kept independent and separate from the model, the fore mentioned simulation.

In this approach the fault detection and portions of the diagnostic reasoning system thus become comparitors between the expected behavior (that of the model) and the application domain under analysis. The diagnostic problem is partitioned into 6 discrete steps that include: fault detection, diagnosis and hypothesis generation, hypothesis space pruning, validation of the hypothesis, test case selection and verification of the diagnosis. The system performs a simplified form of learning by injecting known diagnosed faults into the model (compilation) to keep it consistent with the domain reducing further

[1]now at Bell Northern Research, P.O. Box 3511, Station C, Ottawa, Ontario, Canada, K1Y 4H7

unnecessary processing in the future. It has been demonstrated here that largely shallow reasoning systems performing a comparative analysis of the data is sufficient for a complex application.

The approach has been successfully demonstrated on a software simulation of the Space Based Radar Electrical Power System (EPS) breadboard now under development at the Canadian Department of National Defence. In terms of model based reasoning systems previously developed, the application domain is complex with more than 15,000 components and 35,000 sensor points.

The Application Domain

The US Air Force (USAF) with the Canadian Department of National Defence (DND) are together examining techniques for space based surveillance of North American airspace. That is to detect, localize and track aircraft from space. The Space Based Radar (SBR) program is intended to meet these needs through the use of a high power radar payload spacecraft at a highly inclined, low earth orbit. The Canadian SBR Research and Development (R&D) project will improve Canadian industries' understanding of the SBR concept and improve the technology base within Canada, so that Canada may contribute significantly to a collaborative SBR program [Eatock 1990]. As part of Canada's contribution, a hardware breadboard of the SBR spacecraft's Electrical Power System was designed and built by a team from CAL Corporation and Spar Aerospace [Moodie and Maskell 1989].

Space Based Radar-Electrical Power System

The SBR spacecraft is expected to have a total electrical power demand on the order of 40K watts. To reduce the power carrying capacity requirements for the individual electrical components and increase reliability, the EPS is divided into 10 parallel EPS strings. Each string is identical and provides $1/10^{th}$ of the power requirements of the spacecraft.

The EPS breadboard now under development implements one EPS string and includes the EPS elements: solar panels, batteries, power distribution conductors, power conditioning and regulation components and loads. The breadboard also includes control electronics and computing elements to manage and control the EPS. Each string includes some 1548 electrical components (Fig.1) each of which has a variety of failure modes. The health and effectiveness of the EPS and health of the components is monitored through sensors located at points of interest. There are some 3500 sensors that measure voltage, current, temperature, power (electrical or RF) and logical (status) values in the base line breadboard design of one SBR-EPS string. The sensor values are available from the breadboard *on demand* and are available through a simulated telemetry stream. (It is expected that sufficient bandwidth will not be available on the telemetry channel to transmit this data continuously.)

While the breadboard EPS design has some level of fault isolation through circuit breakers and fuses, the system does not reason about the causality of the symptom nor the specific component that caused the symptom to appear. The Canadian Space Agency (CSA) Research Branch has considerable experience in developing Knowledge Based Reasoning Systems to address that address fault detection, diagnosis and scheduling / planning. As part of ongoing research in *model based reasoning* as applied to fault detection and diagnosis the CSA has been working cooperatively with DND, CAL and Spar to develop a system to address the SBR-EPS.

The Multiple Fault Diagnostic System (MFDS) described in this paper is intended to assist the spacecraft operator in monitoring the spacecraft EPS operation, detect the existence of faults, identify the component causing the fault and if possible prescribe actions that will either provide an alternate configuration or isolate the fault.

Model Based Diagnosis

Model based reasoning has generated considerable interest in the research community particularly as applied to diagnosis. Systems have been developed by several noted researchers [Davis 1984; Genesereth 1984; deKleer and Williams 1987; Hamscher 1991 and Reiter 1987].

In model based reasoning systems, the model is used as a reference to which the observed behavior of the domain system is compared. These models are based on theories or experimental data from the domain. *The model is not based on experiential data from the domain but a deeper understanding.* To be effective, the model must accurately describe the underlying *science* of the domain. Models may be constructed (encoded) in a variety of forms (logic, frames, rules, procedural code and others). The models operate either in a quantitative or qualitative

domain [Kuippers 1986]. Rothenberg [Rothenberg 1989] (page 75) defines modeling in the following general terms:

> *"Modeling in its broadest sense is the cost effective use of something in place of something else for some cognitive purpose. It allows us to use something that is simpler, safer, cheaper than reality, instead of reality for some purpose."*

Modeling or model based reasoning however are not sufficient to ensure the above results. Brittleness of the reasoning process is the breakdown of the reasoning process due to: a lack of sufficient understanding of the underlying mechanisms that exist in the domain; the use of an inappropriate or insufficiently expressive language, tool or technique and others. It is the belief of this author that through the use of object oriented modeling and programming techniques significant gains can be realized.

Object oriented techniques are ideally suited to modeling elements of a system where the boundary values and describing equations or relationships of the component are well known. For example: The SBR-EPS contains several power regulation and conversion components with known operational voltages, currents and operational efficiencies.

For the solar panel the first order behavioral model is based on a piece wise continuos equation that describes the voltage / current characteristic of the photo voltaic arrays:

voltage volts	current amps
170	0
160	25
0	30

Describing equations:
voltage = 170 - ((10/25)*current) for 0<current<25
voltage = 160 - ((160/5)*current) for 25<current<30

The above relationship is in fact encoded in a Smalltalk class that defines the voltage-current characteristics of solar panel in the model. It should be noted that the granularity of the model is limited by the level that sensor data is available from the EPS. The EPS does not contain sensors at individual cells or groups of cells in the solar panel. Diagnosis a level below the complete solar panel is thus not possible. Modeling at this lower level will have little or no benefit in this case.

The EPS model is constructed by connecting instances of models of the individual components that comprise the EPS. While each string of the EPS contains some 1548 component, there exist only 9 unique components within the EPS. These are: solar panel, primary power conditioner, battery cells, cell packs and battery assembly, intermediate conditioners, transmit receive conditioners, auxiliary conditioners and radar loads. Once the connectivity of the components has been established, the various components of the EPS model are updated by performing a power (energy) balance across the network. This is accomplished by propagating the power demand from the loads through the intermediate components to the source components and then performing a power balance (using Kirchoffs laws) at the source components (solar panel and batteries). (The above discussion was based on material drawn from Adamovits [Adamovits 1992]).

The Multiple Fault Diagnostic System

The Multiple Fault Diagnostic System (MFDS) is a model based reasoning system that detects diagnoses and verifies EPS components' faults. [Adamovits 1992, Adamovits and Pagurek 1993] It is capable of identifying multiple concurrent faults that may have either interacting or independent symptoms as reflected in the sensory data. The MFDS relies on a model of the EPS that is in the form of a software simulation containing both continuous and discrete elements. The majority of the MFDS was implemented in Smalltalk [Digitalk 1988] an object oriented language. The Prolog language [Clocksin and Mellish 1982] with a few changes to control the backtracking was used as a simple rule base interpreter for the inferential reasoning components of the MFDS. All rules used in this system are shallow in nature. That is, the rules do not contain a deep understanding of the underlying behavior of the components of the EPS but instead have a shallow understanding of the differences between the expected and observed behavior. These shallow rules bases conclude possible hypotheses based on the observed behavior.

While the rule bases contain largely shallow rule structures, the MFDS is capable of addressing the multiple fault application through the use of the deep knowledge contained within the model.

Diagnostic process

In the Multiple Fault Diagnostic System (MFDS) the fault detection/diagnosis through to hypothesis

testing on the spacecraft EPS is broken down into several discrete steps. These are referred to here as the *Diagnostic Process*. The Diagnostic Process is the activity of identifying the underlying causes for unexpected changes in a system's behavior. It includes several key reasoning steps that must be completed along the way. For the purposes of this paper the Diagnostic Process is defined to include the steps:

- data acquisition,
- fault detection,
- diagnosis and hypothesis generation,
- hypothesis space pruning,
- hypothesis validation (testing) on a model of the system,
- test case selection,
- hypothesis verification (testing) on the EPS.

The Diagnostic Process is illustrated in Fig.2 and is further described in the following sections paragraphs [Adamovits and Pagurek 1993]:

Data acquisition - The MFDS implements the data acquisition system as a data buffer that samples and holds the data resulting from the model and the spacecraft EPS[2]. These data sets are maintained until a new sample command is issued. The sample and hold approach ensures that the data sets remain consistent through all remaining steps of the diagnostic process. (This approach is also consistent with the expected mode of operation of the spacecraft as sensor data is only expected to be available on request.)

Fault detection - Present day space industry approaches to fault detection typically involve comparing the received data against fixed (with respect to time) upper and lower set points. That is limit checking. A fault is detected when the telemetry data deviates from the range defined by the limits specified. These limits are typically set manually on an infrequent basis by the spacecraft operator. On occasions when transients are expected to occur, the limits are set quite wide to reduce the possibility of false alarms. Widely set limits however serve little no value in monitoring the rates of change in the data. This can only be accomplished by other means. Fault detection performed in this way is effective for largely static data only.

The SBR-EPS experiences high power transients as the radar payload switches on and off. In this dynamic environment, static limits are ineffective. To meet the needs of the SBR-EPS, fault detection is accomplished through two parallel reasoning components performing qualitative and quantitative fault detection respectively. In both cases these components perform a comparison between the expected data from the model with that received from the domain.

The quantitative fault detection component performs this as a numeric (or logical) comparison between the two data sources (domain and model). If the difference exceeds some threshold, a fault is postulated. This is analogous to the limit checking approach of the typical spacecraft operations center. In this case however, the simulation capability of the model presents state varying data that is used to establish state varying limits. The range of these limits upper and lower limits is established to suit the individual data element (figure 3).

Qualitative fault detection is accomplished by qualitatively interpreting the quantitative data from both the domain and the model. The qualitative values (decreasing, no change and increasing; {- 0 +}) are then compared to determine if the *direction of change* of the domain data is that predicted by the model. If not, a qualitative fault is indicated. (The pairs {(- -) (0 0) (+ +)} indicate no qualitative fault. All others indicate a fault that is dependent on the context of the EPS and the component being examined). This qualitative fault detection approach is similar to the qualitative reasoning systems of Kuippers [Kuippers 1986] and others.

The fault detection system (qualitative and quantitative fault detection components combined) returns a set of plausible faults based on a shallow analysis of the available data. That is, only a symptom based analysis of comparing the sensor data from the model and domain is performed. This approach however, includes the deep knowledge aspects of the domain by including the dynamically changing behavior of the EPS model in the symptom based analysis.

Diagnosis and hypothesis generation - Based on the results of the fault detection system, the diagnostic system identifies combinations of symptoms (detected faults) that indicate specific component failures.

[2]During the development of the MFDS the SBR-EPS breadboard was not complete. To provide representative spacecraft data, another instance of the model was created and used to represent the spacecraft.

Many of the faults identified by the fault detection system are in fact the propagation of symptoms from lower level components. For example:

> If a component (e.g. load 1) is drawing more power than anticipated then, the power source components (e.g. IntCond22 and TRCond1) for this failed component will also be likely drawing more power than predicted by the model. A failure however does not exist in these other components.

The diagnosis and hypothesis generation system attempts to reduce the number of incorrectly detected faults and prevent their further propagation to later steps in the diagnostic process. While the analysis here is also shallow in nature, a certain degree of deep knowledge is also contained within the diagnosis and hypothesis generation knowledge base. This deep knowledge is in the form of knowledge of component connectivity and knowledge of how components may pass symptoms when they are not in fact at fault.

The output of the diagnosis and hypothesis generation system is a set of plausible diagnosis hypotheses. Each plausible hypotheses is supported by some subset of the detected faults or sensor and model data from the data interface system, *the hypothesis is locally consistent with the data.*

A few poorly supported and incorrect diagnoses will remain however. By poorly supported it is implied that the hypothesis is inconsistent with other hypotheses that have been identified. That is: *the poorly supported hypotheses are globally inconsistent with each other when a deep analysis is performed.* The removal of inconsistent or poorly supported hypotheses is performed in the next step in the diagnostic process.

Hypothesis space pruning - The set of hypotheses resulting from the hypothesis generation step are examined discarding those that are not strongly supported or are contrary to the expected based on other believed hypotheses. Hypotheses may be rejected based on a variety of criteria (known operational state of the spacecraft, solar conditions, etc.).

The MFDS implements a hypothesis space pruning step that is based on the knowledge of how symptoms propagate from electrical source components to lower level electrical components. For example, if the set of hypotheses from the diagnosis and hypothesis generation system includes the hypotheses {... (load1 to load4 open circuit) ... (transmit receive conditioner open circuit)...} then we may assume that if these components are related electrically, then the load1 to load4 open circuit hypothesis is poorly supported. This is based on the fact that if the load has no source electrical power then it can expect to also have the hypothesis of open circuit. The load open circuit hypotheses are thus further symptoms of the higher level (electrically a source component) component's fault.

The result of the pruning step is a *minimal ordered list* of plausible supported hypotheses. These become the basis of the hypothesis validation step.

Hypothesis validation (with the model) - In an effort to diagnose the fault and resolve the problem, several competing hypotheses may remain on the pruned hypothesis list. The most likely of these is selected for further detailed examination.

The MFDS performs the hypothesis validation step through the use of the EPS model before proceeding. First, the most likely hypothesis is selected from the set of pruned and ordered hypotheses. To verify this candidate, the *model* is first altered to represent the fault identified in the hypothesis (e.g. if a component is hypothesized to have an open circuit, then the component model will be changed to represent the open circuit). At this point, the data acquisition, fault detection, diagnosis and hypothesis generation and hypothesis space pruning steps are repeated.

During the process of propagating the revised model data through the reasoning systems, a meta-level reasoning system monitors the progress. If following the examination of the new model data, the selected hypothesis is no longer in the set of pruned and ordered hypotheses, then the selected hypothesis is a plausible representation of the identified fault. At this point the selected hypothesis can be considered to be validated. If this is not the case, the hypothesis will be rejected and another hypothesis will be selected by the meta-level reasoner and the process is repeated. This will be continued until at least one valid hypothesis can be identified.

It should be noted that the identification of a plausible hypothesis is not sufficient. Several fault hypotheses may identify identical symptoms (e.g. a tripped circuit breaker and an open circuit within the same component). The resolution of these can often only be performed by further testing in the domain (e.g. resetting the circuit breaker). This further step is completed during hypothesis verification.

Test case selection - Once a hypothesis has been validated and identified as a plausible representation

of the problem situation, a test is selected to provide either further supporting or refuting evidence when applied in the domain. In situations where component degradation and failure modes are known, these tests can be recorded and stored in a library of accepted cases. In situations that are new and unanticipated, a test case must be devised as necessary.

The test case selection system of the MFDS uses the verified hypothesis as an index into the case library of generic component test cases. The selected case is altered to include information of the component identified by the validated hypothesis. The test case is applied in the next step in the diagnostic process.

Hypothesis Verification (testing on the domain system) - Once a hypothesis has been selected and validated the spacecraft configuration is modified through the application of the test scenario. The test case may require resetting circuit breakers, turning components on or off etc. The intent is to either resolve the problem (fault recovery) or to provide further supporting or refuting evidence to be examined in an effort to improve the belief in the hypothesis describing the fault.

Hypothesis verification is accomplished by sending commands and observing the results in the telemetry data. As in the previous steps, the MFDS performs this in a fully automated way[3]. During verification, both the model and domain are altered in *identical ways*. That is, actions to acquire additional data from the domain are also applied to the model. If the predicted hypothesis is correct then the actions performed to the model and domain should indicate some expected behavior. As part of the verification step, the data acquisition, fault detection, diagnosis and hypothesis generation and pruning steps are repeated. The results from these systems are examined to determine the success in recovering from the hypothesized fault or providing further supporting or refuting evidence of its accuracy.

Discussion

The MFDS was constructed and successfully demonstrated against a software simulated SBR-EPS[4]. In this software simulated environment the MFDS operated to the extent of the knowledge contained within the knowledge base (solar panel, primary power conditioner and battery components were not diagnosed.) The remaining components that were diagnosed represent 1540 of the 1548 components that comprise the EPS (i.e. 99.5% of the total). The inclusion of these other components was not an indication of the limitation of the approach but rather a limitation on the available resources (i.e. time).

Model based reasoning has shown great promise for diagnostic systems. However, considerable computational cost is often associated with the approach. This cost is due largely to the cost of updating the model and maintaining it consistent with the domain. In the approach demonstrated, a very efficient model was created using object oriented techniques. It is believed that through the appropriate techniques such as a object oriented simulation that model based reasoning can be very effective in the diagnosis realm.

When compared to typical diagnostic systems, the MFDS has several benefits. These are:

- The model is constructed using objects that represent physical components as building blocks. These component models describe well known behaviors of the components and are well defined.
- The model contains the majority of the deep knowledge that describes the domain
- Monolithic knowledge bases, difficult to maintain, are avoided and are replaced by the knowledge bases identified in the Diagnostic Process. The reasoning systems contain largely shallow knowledge and are very small specific in nature.
- The system learns by adapting to changes in the behavior in the domain system (in this case the SBR-EPS) by altering the model to represent the changes in operational characteristics of the components. This learning process saves future computations by accurately modeling the already recognized faults.

Conclusion

The Multiple Fault Diagnostic System has been shown to be an acceptable approach to diagnosis in large scale problem domains (1500 elements, 3500 data points). An object oriented simulation has been

[3]During transition to full automation, the MFDS will be expected to operate in an advisory capacity only. As the diagnostic sysetm accuracy and reliability becomes better known, closed loop operation as described will likely be used.

[4]The SBR-EPS breadboard was not complete at time of testing

demonstrated to be an appropriate approach to modeling. It is expected that the simulation/model based reasoning approach and the Diagnostic Process will find application in any domain where the behavioral parameters can be modeled with some accuracy.

References

Adamovits, Peter J. 1992. "Model Based Reasoning Applied to the Diagnosis of Spacecraft Electrical Power System Faults", masters thesis, Mechanical and Aerospace Engineering, Carleton University, 175 pages.

Adamovits, Peter J. and Bernard Pagurek, 1993, "Simulation (Model) Based Fault Detection and Diagnosis of a Spacecraft Electrical Power System", 9th Conference on Artificial Intelligence Applications, IEEE, 3-5 May, Orlando, Florida.

Clocksin, W.F. and Mellish, C.S. 1982. "Programming in Prolog", Springer-Verlag, 279 pages.

Davis, Randal. 1984. "Diagnostic Reasoning Based on Structure and Behavior" Artificial Intelligence, Elsevier Science Publishers, Volume 24, Pages 347-410.

Digitalk. 1988. "Smalltalk/V 286 Tutorial and Programming Handbook", Digitalk Inc., 561 pages.

Eatock, Brian C. 1990. "Progress on DND's Space-based Radar R&D Project", Sixth CASI Conference on Astronautics, Ottawa, November, Pages 452-463.

Genesereth, Michael R. 1984. "The Use of Design Descriptions in Automated Diagnosis" Artificial Intelligence 24, pages 411-436.

Hamscher, Walter C. 1991. "Modeling Digital Circuits for Troubleshooting", Artificial Intelligence 51, Elsevier Science Publishers, Pages 223-271.

deKleer, J. and Williams B.C. 1987. "Diagnosing Multiple Faults". Artificial Intelligence 32(1), Elsevier Science Publishers, Volume 32, Pages 97-130.

Kuipers, Benjamin. 1986. "Qualitative Simulation" Artificial Intelligence Volume 29 Elsevier Science Publishers, pages 289-338.

Moodie, M.H. and Maskell, C.A. 1989. "Electrical Power Distribution on Space based Radar Satellites" IEEE AES Magazine, November.

Reiter, Raymond. 1987. "A Theory of Diagnosis from First Principles", Artificial Intelligence 32(1) Elsevier Science Publishers, Pages 57-95.

Rothenberg, Jeff. 1989. "The Nature of Modelling", Artificial Intelligence, Simulation and Modeling, Widman, Lawrence E.; Loparo, Kenneth A. and Nielsen, Norman R. editors, John Wiley and Sons, pages 47-74.

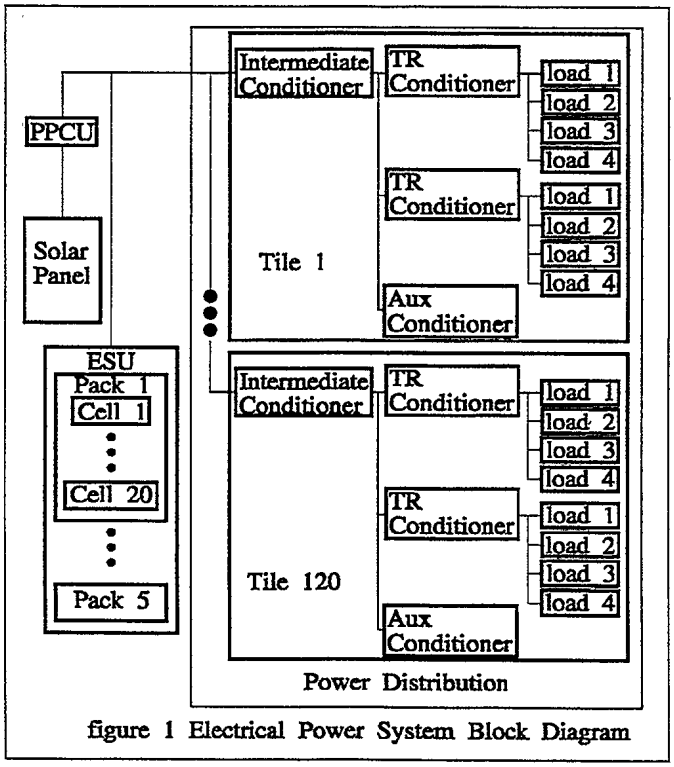

figure 1 Electrical Power System Block Diagram

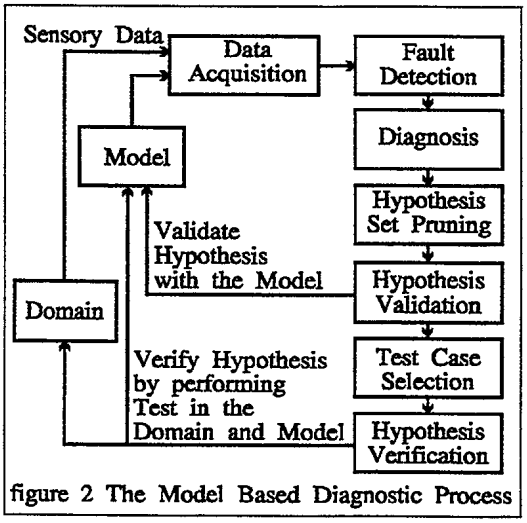

figure 2 The Model Based Diagnostic Process

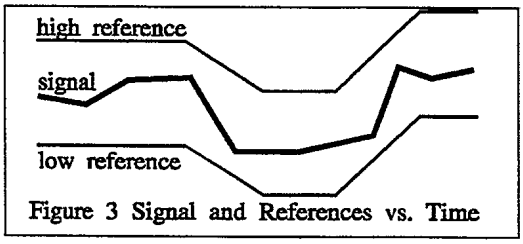

Figure 3 Signal and References vs. Time