A FAULT DETECTION AND ISOLATION METHOD APPLIED TO LIQUID OXYGEN LOADING FOR THE SPACE SHUTTLE

Ethan A. Scarl
SCARL @ ECL
The Mitre Corporation
Bedford, MA 01730

John R. Jamieson
NASA, KSC, SE-FSD
Kennedy Space Center, FL 32899

Carl I. Delaune
NASA, KSC, SC-LPS-II
Kennedy Space Center, FL 32899

ABSTRACT

Process-monitoring and fault location techniques have been developed at the Kennedy Space Center in a domain of mixed media control in NASA's Space Shuttle Launch Processing System. An intuitively appealing diagnostic technique and representation of the system's structure and function were formulated in cooperation with system engineers. Functional relationships that determine the consistency of sensor measurements are represented by symbolic expressions embedded in frames. Functional relationships are stored in exactly one place, so they must be inverted to determine hypothetical values for possibly faulty objects. Propagating these hypothetical states to other sensors permits the location of faults. Standard symbolic inversion techniques have been extended to include conditional functions. A demonstration system is operating, and its evaluation will soon use live data from the firing rooms at KSC.

I INTRODUCTION

There is growing interest in the use of structure and function to assimilate observations of complex systems and deduce the causes of unexpected behavior. The LOX Expert System (LES) is an experimental system built to process sensor data to detect and locate faults in a system without feedback, and built from objects without state. Its diagnostic techniques and knowledge representation are designed to be transparent to system users (engineers). By symbolically inverting functional relationships, LES need store each relationship only once. We consider this necessary for maintaining large and complex knowledge bases.

Most previous work has been done in domains of electronic circuitry and digital logic (e.g., Davis, 1984; de Kleer, 1979; Genesereth, 1984), where there are relatively few sensors per active component but the unit under test may be readily taken out of service for diagnostic intervention. The method described here has been applied to a domain of discrete and analog devices with a mixture of electronic, pneumatic, hydraulic, and mechanical control. The domain is rich in sensors and it is LES' goal to determine whether a perceived fault makes it necessary to stop operations, by looking at presently available information.

The Space Shuttle's external tank is loaded with 140,000 gallons of liquid oxygen (LOX) from a million gallon storage tank (Figure 1) about 3.5 miles from controlling computers at the Launch Control Center. This critical operation begins six to eight hours before launch and must continue to within seconds of ignition. NASA's automated Launch Processing System controls this process and monitors sensor readings such as temperature, pressures, and valve positions, checking that they are each within some specified range. If anything goes wrong, a few experts must analyze the problem and determine whether to stop the process, leafing through 200 pages of schematics. A delay in troubleshooting could abort the Shuttle flight.

This is the first application of artificial intelligence sponsored by the Kennedy Space Center (KSC). An experimental system called LES (the LOX Expert System) has been constructed to aid in monitoring the LOX Loading process, and diagnosing faults. This domain, its history, and further details of its representation are described more fully elsewhere (Jamieson, 1984; Delaune, 1985). For more complete description of diagnosis methods, knowledge representation, and functional inversion techniques, see (Scarl, 1985).

II DEFINITIONS AND ASSUMPTIONS

First of all, it is assumed that: (a) Time between failures is long compared to diagnosis time, ruling out simultaneous failures (which

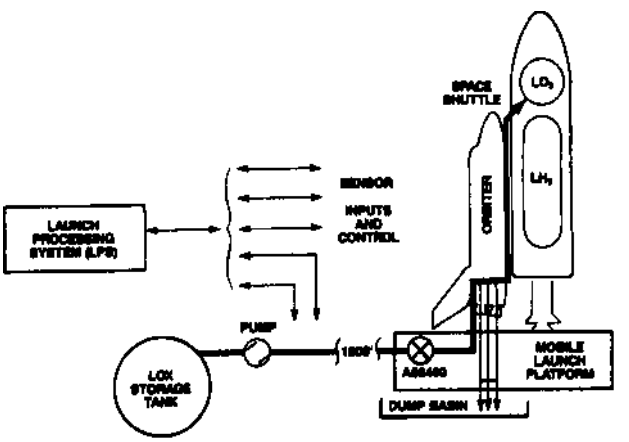

Figure 1. LOX TRANSFER AT KSC

historically do not happen in this domain). (b) Transient behaviors can be ignored by waiting for deliberate changes of state to stabilize. (c) Intermittent faults have cycle times longer than the diagnostic time.

A complex physical system is represented as a network of functional relationships. Any measurement that gives information about the state of the system is either consistent or discrepant. Consistent measurements agree with their adjacent network components, while discrepant measurements do not. The inputs to this network are commands, and the outputs are sensors. One may treat commands as constraints which propagate through the network to determine an expectation value that describes what an object's state be. Similarly, one may treat a sensor as a constraint which determines a hypothetical value that describes what the object's state is implied to be by that observation. In LES, hypothetical values are derived from both sensors and commands.

Given a sensor discrepancy, each object is:
(1) incapable of being the cause and so innocent,
(2) demonstrably the cause and thus the culprit,
(3) otherwise a suspect.

The OD (Original Discrepancy) is the first discrepancy noticed after a period of untroubled operation. A given sensor's siblings are those other sensors that depend in any way upon any of the commands that control it.

III LES

LES' knowledge base includes most of the LOX portion of the Launch Processing System at KSC. This domain includes analog and discrete commands and sensors, and other objects (transducers, relays, solenoids, valves, LOX pressures and temperatures, etc.) whose state the system is designed to control or sense. These are represented using the Frame Representation Language (FRL) (Roberts, 1977). A frame describes each replaceable component with its type, its value (for commands and sensors), and the units and tolerance of its output where appropriate.

Three slots (SOURCE, SOURCE-PATH and STATUS) express how the component is controlled: SOURCE points to the source of energy (e.g., a power bus or pressure line). The Boolean SOURCE-PATH expression determines whether the path from source to component is turned on or off. This is sufficient for discrete components, but an analog object also needs a STATUS to quantify its state when the SOURCE-PATH is on.

Figure 2 shows a simplified schematic for controlling an analog valve. The potentiometer (pot)'s STATUS expression simply points to the valve, since it should directly reflect the valve's position. The valve's SOURCE-PATH expression is true if the override closed switch is OFF and the analog command is ON. The valve's STATUS expression gives percentage open. The closed limit switch is discrete, and its SOURCE-PATH expression is (LESSP valve 7), meaning that this switch is

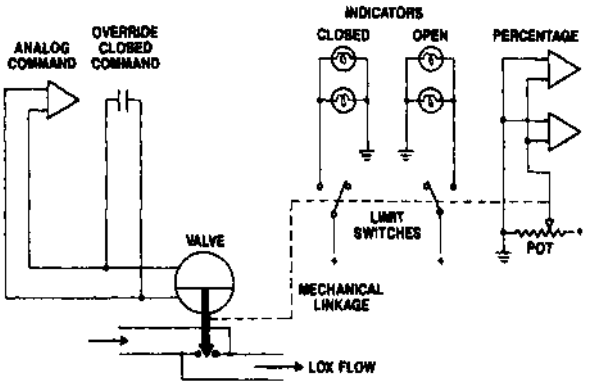

Figure 2. PART OF LPS CIRCUITRY FOR AN ANALOG VALVE

expected to be ON whenever the valve is less than 7 percent open.

Fault detection is invoked whenever a command or sensor value is received, whether from user input, a test file, or a port. If the received value is from a sensor, then the sensor s expectation value is computed by evaluating its SOURCE-PATH and STATUS expressions. Its controlling objects are evaluated recursively until objects are found bearing known values, which in LES are always commands. This expectation value is compared with the value received, and the sensor is marked consistent or discrepant accordingly.

If the received value resets a command, then all sensors affected by the command are tested against their expectations.

The suspects and relevant commands are the objects and commands visited while deriving the expectation value. This dynamic search produces the benefit (also enjoyed by (Genesereth, 1984)'s proof techniques) that when an object's controllers are "switched out," they and their related commands and sensors never appear and are implicitly cleared.

LES obtains considerable computational savings by storing expectation values in the frames, and resetting them only when commands are changed. This also gives LES a limited facility for handling components whose state depends upon history as well as current commands.

The current user interface is a "live" version of parts of NASA's electromechanical schematics. Most of these can be generated automatically from the database (New, 1985), and all can be generated as block diagrams. The user moves about by naming or mousing components. Sensors and commands display their current values with any discrepancies highlighted. Values can be moused for instructional or testing purposes, and several object types are animated to indicate their expectation values.

LES resides primarily in a dedicated Symbolics 3600 which lives in the Launch Control Center at KSC. Test data now comes from an adjacent PC, but

will soon come from a "Common Data Buffer" containing the control system's most complete and current status. Software in the Firing Room will filter the data, sending only data exhibiting "significant" change (any change for discrete measurements, and a few percent for analogs). It is anticipated that a 9600 baud serial port can handle such filtered data. By summer of 1985, LES should have begun active testing during simulated and actual Shuttle launches. Diagnoses now take 10-40 seconds.

IV THE DIAGNOSTIC METHOD

The diagnoser is invoked when a discrepancy (the 0D) has been noticed. Suspects, commands, and siblings of the OD are located. An attempt is now made to derive a hypothetical value for each suspect from the OD. A suspect is innocent if any one of the following four criteria is true:

1. The suspect controls the OD only through objects known to be innocent.
2. No hypothetical value can be established for the suspect because the functional dependency of OD upon suspect cannot be inverted.
3. The suspect's hypothetical value agrees with its expectation value.
4. The assumption that the suspect actually has its hypothetical value does not cause all sensors to become consistent.

These criteria are listed in order of application, but 4 is the core of the algorithm.

Computing a hypothetical value means understanding what the OD's measurement is telling us about the state of one of the suspects. Such information is implicit in the SOURCE-PATH/STATUS dependence of sensor upon suspect, but, believing it important to represent such relationships uniquely, we do not store these reverse dependencies explicitly. Instead, we have automated the inversion of sensor-upon-suspect dependencies.

Arithmetic functions present no special problems, but LES' STATUS/SOURCE-PATH expressions may include conditional operators like MAX, OR, AND, IF or even COND, which are not invertible in the standard sense. Nevertheless, it is possible to invert them using conditional tests. For example, if the status of x is (AND (STATUS z) (STATUS y)), then LES in effect solves for y as

```
y - (COND ((STATUS z) (STATUS x))
          (T '*INNOCENT*)).
```

The token *INNOCENT* is passed back to the diagnoser telling it to declare y innocent (by criterion 2, above).

V REMARKS

The first application domain for the method described here is a good fit with the assumptions listed in Section II.

LES' representation scheme for structural and functional relationships seems to have advantages in compactness, perspicuity, and in suppressing unneeded detail. This could be important to an engineer attempting to analyze the network's functionality under stressful conditions. LES* methods are now being considered for experimental development in other prelaunch activities at KSC, some of which have proven more expensively troublesome than LOX loading, if not so critical in the final countdown.

ACKNOWLEDGMENTS

This work is funded by the Advanced Project Office of theKennedy Space Center. The authors wish to thank Dona Lethbridge, Richard Brown, Caroline Wardle, Judy Clapp, and Skip Saunders for their helpful comments.

REFERENCES

[1] Davis, R. "Diagnostic Reasoning Based on Structure and Behavior." Artificial Intelligence 24:1-3, 1984, 347-410.

(2) de Kleer, J. "Causal and Teleological Reasoning in Circuit Recognition," TR-529, Artificial Intelligence Laboratory, MIT, Cambridge, MA, 1979.

[3] Delaune, C. I., E. A. Scarl, and J. R. Jamieson "A Monitor and Diagnosis Program for the Shuttle Liquid Oxygen Loading Operation." Proc. First Annual Workshop on Robotics and Expert Systems, Johnson Space Center, Houston, TX, June 1985.

[4] Genesereth, M. R. "The Use of Design Descriptions in Automate Diagnosis." Artificial Intelligence 24:1-3, 1984, 411-436.

[5] Jamieson, J. R., E. A. Scarl, and C. I.Delaune "NASA's LOX Expert System." Proc. Am. Inst, of Aeronautics and Astronautics, Computers in Aerospace V, New Orleans, LA, 1984.

[6] New, E. "Schematic Generation for NASA's LOX Expert System." Proc. First Annual Workshop on Robotics and Expert Systems, Johnson Space Center, Houston, TX, June 1985.

[7] Roberts, R. B., and I. P. Goldstein "The FRL Manual," Artificial Intelligence Laboratory, Memo 409, MIT, Cambridge, MA, September 1977.

[8] Scarl, E. A., J. R. Jamieson, and C. I. Delaune, "Process Monitoring and Fault Location at the Kennedy Space Center." SIGART Newsletter, in press, 1985.