923

SIMULATION-BASED REASONING ABOUT THE PHYSICAL PROPAGATION OF FAULT EFFECTS*

Stefan Feyock
Dalu Li

Department of Computer Science
College of William & Mary
Williamsburg, VA 23185

*Supported by NASA/Langley Grant NCC-1-122

Abstract - The research described in this paper deals with the effects of faults on complex physical systems, with particular emphasis on aircraft and spacecraft systems. Given that a malfunction has occurred and been diagnosed, the goal is to determine how that fault will propagate to other subsystems, and what the effects will be on vehicle functionality. In particular, we describe the use of qualitative spatial simulation to determine the physical propagation of fault effects in three-dimensional space.

INTRODUCTION

The work described in this paper was performed in conjunction with the fault management research under way at the Vehicle Operations Research Branch of NASA/Langley Research Center. The goal of this research is to produce software that can serve as an in-flight pilot's aid to assist the flight crew when feasible. In particular, artificial intelligence (AI) techniques are being used to construct systems that will assist flight crews in dealing with in-flight malfunctions.

Any system malfunction raises three categories of questions: what has gone wrong (diagnosis), how will the system be affected (prognosis), and what should be done about it (recovery planning). Fault diagnosis is handled by an array of techniques including traditional rule-based systems, model-based monitoring (MONITAUR [Schutte]), and model-based reasoning from first principles (DRAPHYS [Abbott]). The research described in this paper is concerned chiefly with the prognosis of fault propagation, and takes as input the diagnoses produced by the DRAPHYS system. The physical propagation of fault effects is then simulated to determine possible effects on the air/spacecraft. It is also the case, however, that similar techniques can be run off-line to help construct the physical dependency net used by DRAPHYS. Since DRAPHYS plays a major role in this research, we begin by giving a brief description of this system.

THE *DRAPHYS* FAULT DIAGNOSIS SYSTEM

DRAPHYS reads in a database describing a set of components, predicates indicating which components are sensors and with which non-sensor components the sensors are associated, and predicates describing functional and physical dependencies among components. For example, the predicate *Sensor(N2B(CompressorB))* indicates that *N2B* is a sensor associated with jet turbine component *CompressorB.*

A component Y is deemed to be functionally dependent on another component X if a malfunction in X can affect the functioning of Y. A malfunction in CompressorB, for example, will affect the operation of CombustorB. Clearly any sensor associated with component X is functionally dependent on X. DRAPHYS uses such functional dependency information in its model of the physical system.

The other kind of dependency information utilized by DRAPHYS is physical dependency relationships. Component Y is deemed to be physically dependent on component X if a malfunction in X can physically damage Y. For example, examination of aircraft accident reports reveals that a disproportionate number of mishaps caused by physical component malfunction involves events such as turbine blades breaking loose and damaging nearby (and sometimes distant) components.

DRAPHYS makes its diagnosis by initially suspecting all components that could conceivably be implicated in the malfunction. Each of these fault hypotheses is then tested by determining whether, for every symptomatic sensor, there is a symptomatic path in the functional or physical dependency nets from the suspect component to the sensor. A symptomatic path is one that passes only through components that are either uninstrumented or have symptomatic sensors. DRAPHYS returns as output the set of suspect components that pass this test; the hoped-for result is that this set will be a singleton. It is worth noting that the set of suspects can be pruned dynamically as new symptoms arrive.

Since the functioning of aircraft and spacecraft systems is well-understood, it is generally straightforward (though tedious) to develop the database describing the functional dependency relations. Physical dependencies, however, are a different matter: the possible interactions among components are numerous and unpredictable. The expedient used in DRAPHYS has been to include the most obvious interactions (typically from the turbines and similar energy-bearing components to nearby components) and hope for the best. This approach is adequate for simple models, but becomes intractable for realistic cases. A more systematic approach was required.

Since we are operating on the assumption that the failed component has been diagnosed by DRAPHYS, we can use this information as starting point for the reasoning process. Beginning at the failed component, subsequent events are generated by means of a qualitative spatial simulation, in order to determine possible physical propagation paths. In the next section we describe the nature of this simulation process.

QUALITATIVE SIMULATION OF PHYSICAL FAULT PROPAGATION

We have found that a wide variety of malfunctions of physical systems can be characterized as *leaks*, i.e. the uncontrolled escape of a substance into the environment. Malfunctions such as burst hydraulic or gas lines are, of course, literally leaks. It has also proved useful, however, to treat short circuits as electrical leaks, fires as gas and thermal leaks, and mechanical malfunctions such as explosive decomposition or breakage as leaks of kinetic or potential energy. Our approach, then, is to use knowledge of the malfunction site and its nature, together with a database describing the 3-dimensional extent and composition of physical structures, to simulate the consequences of the leak in question.

At the present stage of research we have implemented the capability to simulate fluid leaks, and have a partial implementation of kinetic energy leaks. (An example of such an energy leak is provided by the turbine disintegration that caused the recent crash of United 231 by propagating to the hydraulic control lines.) We have found that a limited set of principles and constructs has emerged that has allowed the systematic and expeditious creation of qualitative spatial simulations, as well as their extension to new malfunction categories. These constructs are described in the next section.

The Simulation

The qualitative simulation of fault propagation in 3-space (and time) requires the spatial representation of physical structures. This requirement raises problems that are more typical of graphics applications than classical simulation programs. In particular, two broad categories of spatial representation exist: volumetric and boundary representations [Requicha]. Volumetric representations describe an object by systematically subdividing space and describing the content of each subdivision. Boundary representation techniques describe solids in terms of their enclosing surfaces.

The best-known volumetric representation technique is probably oct-trees [Jackins]; boundary representations are more commonly found in applications such as CAD/CAM systems. The current implementation uses a boundary representation technique, since the computations required to perform the simulation are more efficient in this representation. Alternate representations are, however, still under active consideration.

To describe a physical object such as an aircraft or spacecraft, the user enters sets of (coplanar) points in 3-space into the database; each such point determines the vertex of a planar plate. The present system constrains the point sets to be convex polyhedra; the planes defined by such point sets are thus more accurately described as convex polyhedral plates in 3-space. These plates form the surfaces of the volumes to be represented. Furthermore, the user may specify points and volumes that represent ***components***, i.e. entities and subsystems that can fail. Malfunctions occur at/in components, and propagate from component to component, either physically or functionally.

Our simulation system is based on a package of procedures for performing a basic set of geometric computations on the representation of 3-dimensional objects described above. These procedures include algorithms to compute the intersection of two or more planes, the intersection of lines and planes, the gradient (downward direction) at a point in the plane, and similar computations. These procedures, in turn, are based on more fundamental routines that find the equation of a plane, given the defining vertices, that determine whether a point is in a plane (i.e. within the polygon defining the planar plate), and similar auxiliary functions. As indicated above, the function library we have developed, while of moderate size, appears to be powerful enough to support an extensive variety of 3-space simulations. We will describe the simulation of the propagation of faults resulting from fluid leaks in some detail, and end by indicating how additional categories of leaks can be represented.

Simulation of Fluid Leaks

As stated previously, a wide variety of malfunctions can be conceptualized as leaks of some type of substance or entity. It was deemed reasonable to begin our investigation by attempting a qualitative simulation of fluid leaks. While such malfunctions are more likely to cause problems via functional rather than physical propagation, fluid leaks can propagate physically by shorting out accessible electrical components, corrosion, and a wide variety of other types of spoilage. A more important consideration, however, was the expectation (justified, as it happens) that the algorithms developed in the process of implementing a qualitative simulation of fluid leakage would form a basis for simulating other kinds of faults as well. By way of example, propagation from gas leaks can be simulated by running the fluid leak simulation twice, the second time with the direction of gravity reversed.

Recall that DRAPHYS produces as output the identity of the initial failed component. Since malfunctions can occur only in components, and since the physical location and extent of each component is stored in the database, we will assume that the exact location of the leak is known. This is in fact a simplifying assumption for the purposes of this discussion, since in most cases the sort of components that can leak fluid will be pipes, which typically extend for considerable distances. A description of each component can be stored in the database, so that the nature of the leak (fluid type, pressure) can be retrieved. For aircraft the leaking fluid will usually be hydraulic fluid or fuel. We make the additional simplifying assumption that the fluid is not under high pressure (else techniques more appropriate to energy leaks become appropriate), that there are no complications such as phase changes or leakage into slipstreams, and that the leaking fluid remains inside the air/spacecraft (we cannot simulate "blue ice" at this stage of the game).

We thus have a fluid leaking into the vehicle interior from a known

Simulation-based reasoning of the sort described in the present paper, as well as the work of [Taylor] and [Gardin], represent explorations in reasoning techniques based on analogical representations.

REFERENCES

Abbott, K. H. (1988), Robust Operative Diagnosis as Problem Solving in a Hypothesis Space, *Proceedings of the 7th National AAAI Conference on Artificial Intelligence.*

Gardin, F, et al. (1986), The Analogical Representation of Liquids in Naive Physics, *Proceedings of the 7th European Conference on Artificial Intelligence, (ECAI-86), Brighton, U.K.*

Jackins, C. L., and S. L. Tanimoto (1980), Oct-Trees and Their Use in Representing Three-Dimensional Objects, *Computer Graphics and Image Processing , Vol 14, 249 -270.*

Requicha, A. (1980), Representations of Solids: Theory, Methods, and Systems, *Computing Surveys, Vol. 12, No. 4.*

Schutte, Paul C. (1989), Real-time Fault Monitoring for Aircraft Applications using Quantitative Simulation and Expert Systems, *Proceedings of the AIAA Computers in Aerospace VII Conference.*

Sloman, A. (1986), Why we need Many Knowledge Representation Formalisms, *British Computer Society Expert Systems Conference.*

Taylor, Hadley C. (1986), Studi sulla Modellazione Computazionale nella Fisica Naive, *M.S. Thesis, University of Milan.*

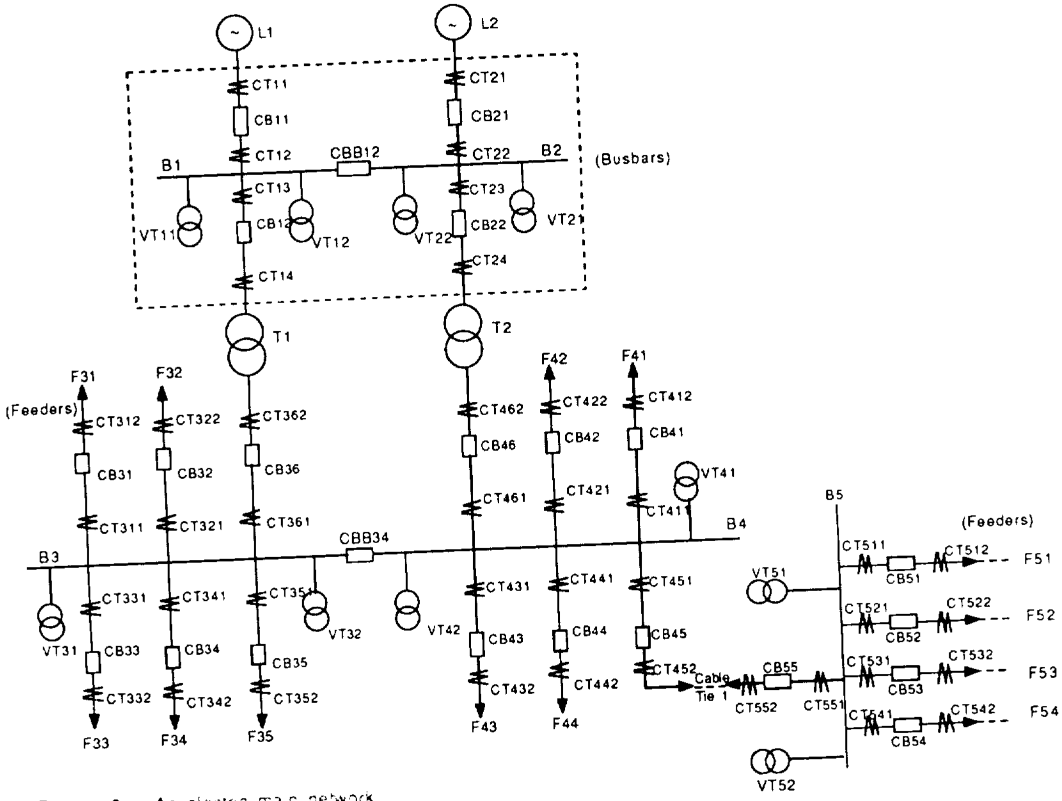


Figure 2. An electric main network

A. The power system is treated as a multi-level and hierarchical diagnosed system,

B. The diagnosed system is divided into separated subsystems at each hierarchical level,

C. A subsystem consists of one or several diagnosed components which have some kinds of characteristic relations,

D. An abnormal or faulted component to be diagnosed is a subsystem at the lowest level.

For example, assuming that the part enclosed with a dotted line in Fig. 2 is live, a description of the HSM is as shown in Figure 3.

III. CAUSE EFFECT RELATION (CERM).

In order to efficiently perform diagnostic reasoning, some experimental and heuristic diagnosis knowledge is integrated into the KB to speed up the failure search. The CERM employs a semantic network approach (Toransso, et al.,1987) coupled with the search for failure by using indirect relationships between failure and symptoms. In addition, CERM bridges the gap between electric symptoms and failures in non- electric parts.

COMBINATORY DIAGNOSIS PRINCIPLES IN KBIMD.

To achieve a speedy and accurate implementation of diagnostic reasoning in the ES suggested for KBIMD, a combinatory diagnosis KB scheme is developed. The functions are discussed in four different subsystems below.

1. DIAGNOSIS BASED ON FIRST PRINCIPLES (DBFP).

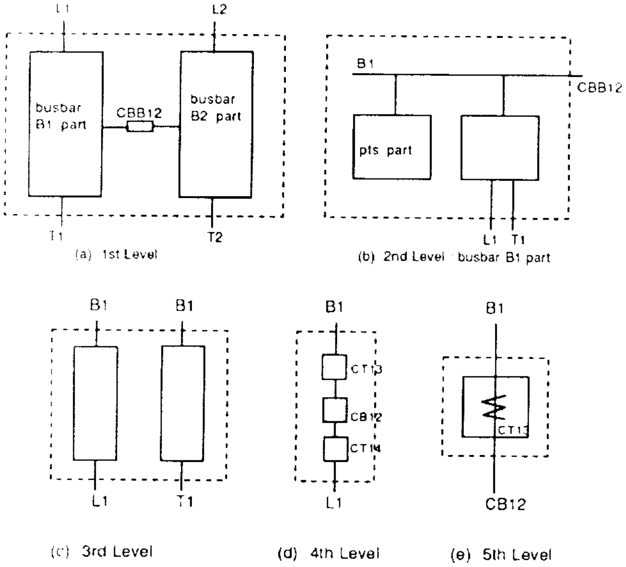
The DBFP subsystem obtains information from structural description of diagnosed objects quantities and behaviors. This subsystem employs a validation check on physical laws to pinpoint the existence of failures.

For example, in Figure 2, the sum of primary currents at CT1 or CT2, CT21 or CT22, CT14 or CT13, CT24 or CT23 are checked on the same phase conductors and checked for zero measurements at normal conditions. If non-zero values are obtained, a failure signal is flagged.

2. DIAGNOSIS BASED ON STRUCTURE (DBSK)

The diagnosis is based on the multilevel and hierarchical structure (HSM) of the electric power subsystem. It begins with the highest level of the HSM and moves to the lower level in the model. As in previous levels, it employs first principle and experimental knowledge as tools for its diagnostic reasoning. This (DBSK) is capable of narrowing down possible failure to a low level within a small region. The application of this structure-based diagnosis scheme is demonstrated for failure of CT13 in Figure 2.

The sequence of diagnostic reasoning in a multilevel sequence is shown in Fig 3. It illustrates the failure search pattern from level I to level V.



(a) 1st Level

(b) 2nd Level busbar B1 part

(c) 3rd Level

(d) 4th Level

(e) 5th Level

Figure 3 A HSM example discription

III. DIAGNOSIS BASED ON FUNCTION KNOWLEDGE (DBFK).

The function-based diagnosis is employed only when failure search has been narrowed to a suspected component. It is the functional relation and model of diagnosed component. The DBFK identifies suspected failures or eliminates a suspicion. In the latter, this suspicion is recorded as a failure disturbance. The recorded components are available for subsequent diagnosis.

IV. DIAGNOSIS BASED ON EXPERIENTIAL KNOWLEDGE (DBEK).

Experiential knowledge of human experts is based on their diagnostic practice over a lengthen period of time. This allows them to diagnose failure faster, accurately and efficiently. The DBEK employs the following different strategies to construct the knowledge bases.

(a). Identification Based on Comparison.

This involves cross comparison between a given component of the same type with same input. If one of them is faulty, the observation will yield different results. The second is the self-comparison approval which compares the components with current observation on a component with its historical record. The difference is used to verify the possibility of a fault. The third approach removes a component part of the HSM system and checks if it leads to a failure-free system, and then recommendation of the fault situation is suggested.

(b). Determination of Diagnostic Ordering.

When diagnostic reasoning is exhausted, further diagnostic reasoning is needed to execute the experience of failure probability. The diagnostic ordering scheme identifies components guaranteed to fail.

(c). Discrimination Based on Historical Record.

When recent historical records on components manifest repeated "failure disturbance." It is certain that a fault exist in the component.

(d). Discrimination Based on the CERM.