January 1975 B74-10279

NASA TECH BRIEF

NASA Pasadena Office

Automated Maintenance for Complex Hybrid Systems

An extensive study has been undertaken of the requirements for implementing the fully automatic maintenance of complex hybrid systems. The study has also resulted in unified criteria for determining when and how such automatic maintenance should be used.

Automatic maintenance is defined as the automatic detection of and recovery from system failures. Recovery is accomplished by the use of replacement subsystems. The state of the art of the automatic maintenance of electronic data processing systems is still undeveloped. Only a few computer systems have been produced to date which provide any significant degree of protective redundancy.Furthermore, there are as yet no agreed-upon figures of merit or design criteria as to how to provide protective redundancy for any given system.

The automatic maintenance of complex systems other than computers is even less advanced. There is no doubt, however, of the increasing need (and number of applications) for the automatic maintenance of complex systems in a wide variety of disciplines, including the fields of transportation, medicine, business, education, process control, communications, and engineering. As systems continue to become larger, faster, more complex, more expensive, and more depended upon, it becomes increasingly difficult in many cases to obtain the correct manual response to system failures in a time short enough to preclude unacceptable loss of information, system unavailability, damage to property or equipment, or injury to personnel.

Automatic maintenance should be employed whenever system failure modes exist which cannot be corrected manually in time to preclude an unacceptable result. Results may be unacceptable for economic, safety, or political reasons. It is, first of all, necessary to determine what failure modes exist in a specific system and the time that will be required to detect each potential failure and to bring about system recovery without the aid of automatic maintenance. The impact of these potential failures on the total system function must then be evaluated in the context of the system objectives to determine if the results are acceptable or not. The practical implementation of automatic checkout and the continuous maintenance of entire systems imposes additional requirements on the system designers.

From the very beginning, the design of the systems must be influenced by the concept of automatic maintenance, including the interface with the computer. The design of each system must allow for algorithmically-defined evaluation procedures by which all failures can be detected. Furthermore, each system must be organized into efficiently-sized replaceable units. Evaluation procedures must be capable of isolating detected failures to one of these units and then effecting the replacement of the failed unit. The replacement of a failed unit does not necessarily mean that the unit will be physically replaced by a spare or identical unit. Replacement as used here may also be accomplished by functional redundancy, which means that the function of the failed unit can be accomplished by some alternate method. Functional redundancy includes the assumption of the function by the computer itself.

At the heart of the replacement system is the Control Computer Subsystem (CCS), which is a digital computer possessing a high degree of fault tolerance. The CCS embodies the concepts of self-test and repair which have been developed during a 10-year research effort. It is capable of monitoring its own performance and of identifying and replacing with a standby spare any of its units that fail. This

(continued overleaf)

fault-tolerant environment of the CCS is extended to the other system subsystems, including their interface with the computer. The CCS then becomes the monitor and automatic repair facility for the entire system. The performance parameters of the subsystems are instrumented with engineering sensors. Diagnostic routines within the computer utilize the outputs of these sensors to evaluate the performance of the subsystem.

Systems such as high-speed trains, giant-sized airplanes, automated intensive care wards in hospitals, large time-sharing data processing centers, automated telephone exchanges, command and control centers, and complex spacecraft are potential candidates for the application of automatic maintenance.

Note:

Requests for further information may be directed to:

Technology Utilization Officer
NASA Pasadena Office
4800 Oak Grove Drive
Pasadena, California 91103
Reference: TSP74-10279

Patent status:

NASA has decided not to apply for a patent.

Source: George C. Gilley of
Caltech/JPL
under contract to
NASA Pasadena Office
(NPO-13143)