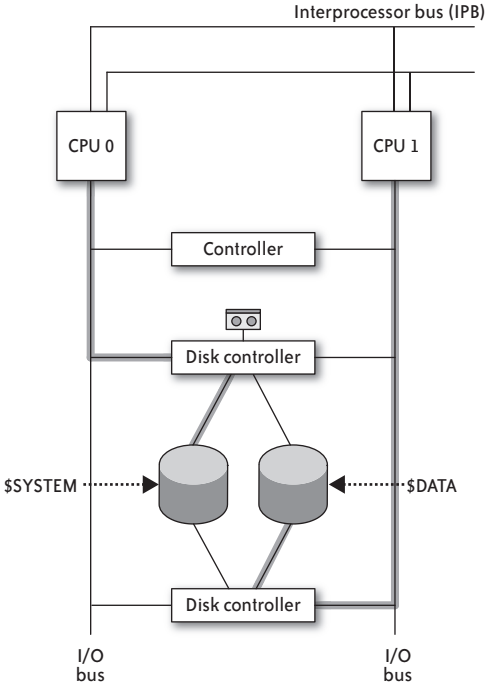

FIGURE 8-1. Mackie diagram

This could easily have led to at least doubling the cost of a system, as is the case with "hot standby" systems, where one component is only present in order to wait for the failure of its partner. Tandem chose a different approach for the more expensive components, such as CPUs. In the T/16, each CPU is active, and instead the operating system processes provide the hot standby function.

Diagnosis

The operating system needs to find out when a component fails. In many cases, there's not much doubt: if it fails catastrophically, it stops responding altogether. But in many cases, a failed component continues to run but generates incorrect results.

Tandem's solution to this problem is neither particularly elegant nor efficient. The software is designed to be paranoid, and at the first suggestion that something has gone wrong, the operating system stops the CPU—there's another to take over the load. If a disk controller returns an invalid status, it is taken offline—there's another to continue processing without interruption. But if the failure is subtle, it could go undetected, and on rare occasions this results in data corruption.