Reprinted from Control ENGINEERING

Building Reliability Into Digital Process Control Systems

THE GIST: Nurtured by academic imagination on the one hand and the promise of handsome economic payout on the other, computing control has now attained acceptance by several users in the process industries. Just how much the (digital) computer must increase throughput, improve quality, and reduce operating costs to fulfill its promise depends on the process to be controlled. But none of these benefits can be obtained if a forced outage due to a failure occurs anywhere in the system—including the computer. Thus, the computer's own reliability and its effect on overall system reliability becomes of paramount importance in considering an integrated digital computer system.

Simple circuits and functional designs of computer sections, and selecting, testing, and derating components keep computer failures to a minimum. Should one occur, however, its effect on process operation is minimized by fail-safe circuits, output-range limits, and automatic transfer to manual control. Through such engineering features, the author maintains, a digital computer control system reduces the overall cost of process operation and keeps down its own maintenance costs.

WILLIAM S. AIKEN
The Thompson-Ramo-Wooldridge Co.

Anyone considering integrating a digital computer into a control system for an industrial process must ask several questions:

- Can the system be designed so that computer failure will neither damage nor upset the process?
- Will instrument failure mislead the computer into upsetting the process?
- What will be the effect of such an integrated control system on the maintenance costs of the process equipment?
- Can maintenance cost and downtime be held to a negligible amount?

Previous experience with data logging systems and digital computers in business applications may provoke skepticism about the basic reliability of computer-control systems. And the realization that these systems must operate on-line continuously may add to this skepticism. However, satisfactory answers to the above questions require appraisal of all aspects of the overall system, including special features that may ease reliability requirements.

The loss due to individual failures in a system varies widely, from the low cost of a vacuum tube and its replacement time to the high cost of repair of major process equipment, with the attendant loss of several weeks of operating time and process output. The overall annual cost C_f due to the failures of equipment anywhere in the system is expressed as the sum of the cost of individual failures times the frequency (per year) of their occurrence, plus the fixed annual cost C_m of the maintenance organization. C_m includes the costs of preventive maintenance schedules and investment in spare parts. Thus:

$$C_f = \Sigma \text{ (frequency of occurrence) (cost per occurrence)} + C_m.$$

A sound attack on the reliability problem must begin by reducing failure frequency to an absolute minimum, preferably to no failures at all, for to realize the anticipated earning power of the investment, a high-cost computing-control system must work well and continually. Preventive maintenance aims at holding down the cost of replacing a part. Such maintenance may actually increase the frequency of replacements (or failures, depending on one's definition) since parts are discarded before they have deteriorated sufficiently to cause an actual failure. Failures which are not or cannot be caught in this way should be minimized by fail-safe features.

Reliability of digital computer process control will be discussed with the typical system represented by Figure 1 in mind. Here, temperature, pressure, flow, level, and analytical-instrument measurements are fed continuously to the computer. Pneumatic

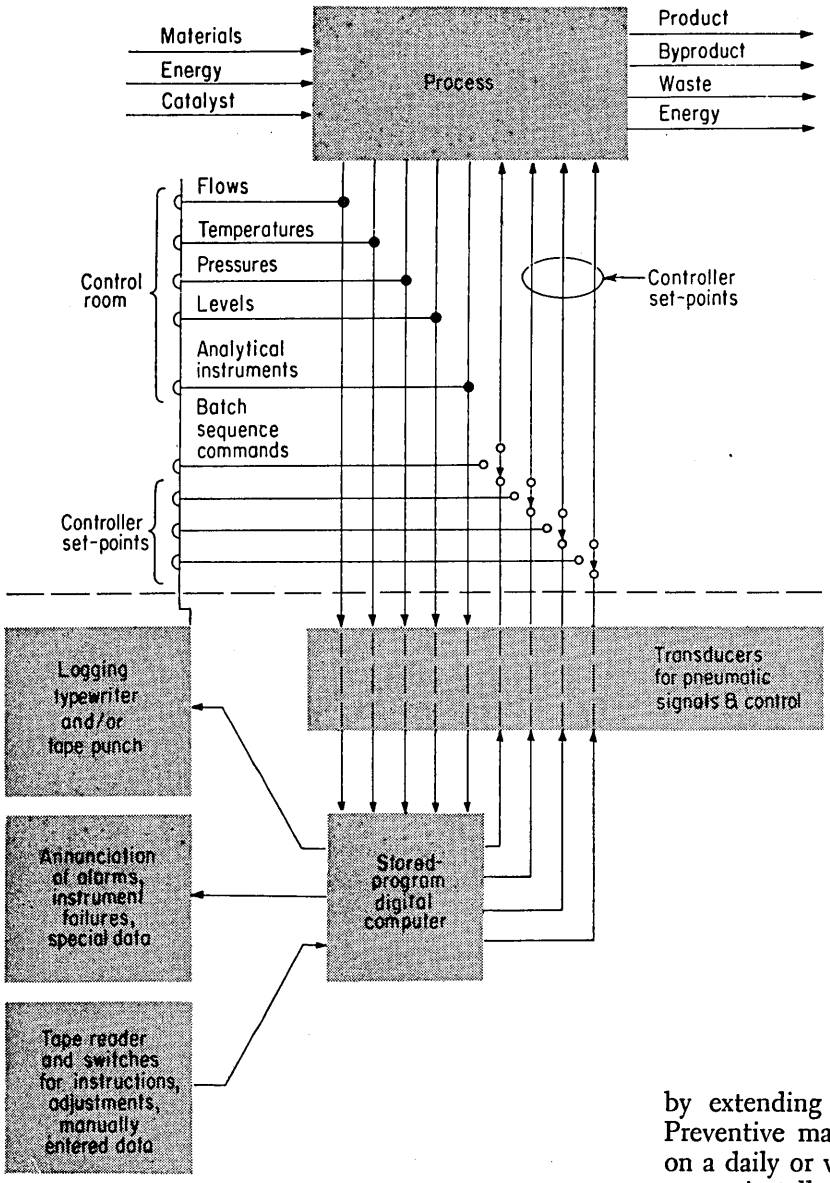

FIG. 1. The typical integrated process control system using a digital computer consists of the process and instrumentation, above the dashed line, and the digital computer and transducers, below.

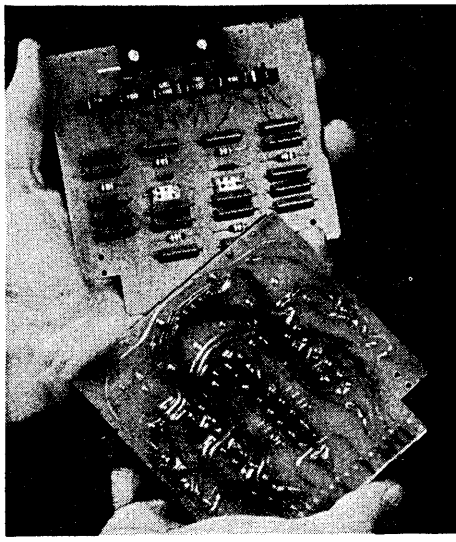

FIG. 2. Etched wiring and permanent components improve system reliability.

signals are transduced to electrical signals for compatibility. Periodically, the computer performs appropriate calculations, based on programs stored in its memory section, and readjusts its electrical outputs to modify the set-points of conventional controllers. The computer's memory has room for many instructions and constants which can be changed either by a human programmer or by the stored program. The memory also stores raw data and intermediate and final results of processed data.

The system of Figure 1 consists of three main sections: the computer, the process, and the associated instrumentation and control equipment. The system's cost of maintenance may be evaluated by estimating the probable cost of failures in these individual sections.

Computer reliability

The reliability of a continuously-operated process control computer must surpass that of the business or scientific machine by a substantial factor, for it will not be possible to make up lost working time by extending a 24-hour operation into overtime. Preventive maintenance, including chassis rotating, on a daily or weekly basis would be unacceptable in many installations. Therefore, emphasis must be less on detecting and correcting failures and more on preventing failures from occurring at all.

Computer reliability is achieved principally in two ways: by functional design and by selecting, testing, and applying individual components. Functional design, of primary importance to both the computer manufacturer and user, involves compromises between equipment simplicity on the one hand and operation speed, capacity, and flexibility on the other. For instance, the computer's control and arithmetic sections may be kept simple by limiting the number of individual instructions the computer must recognize in its program. This would mean more work for the programmer of a scientific computer, for it would require that he write additional steps into its constantly changing programs. In a process control computer, however, such reprogramming will be relatively infrequent and a simple instruction system may be adequate.

Another compromise involves the computer memory's writing characteristics. Such permanently stored information as programs for control computations, data logging, alarm scanning, and other service work occupy most of the memory and need

not be varied during normal operation. The input and output variables, their accumulated averages, variable parameters, and "scratch pad" areas—the changing data—generally occupy less than one-fourth of the total memory. Therefore, if the computer is designed so that only a limited area of its memory accommodates changes in normal operation, the permanent program can be safeguarded automatically against accidental erasure or writing.

Functional design for reliability also means not using equipment that can be troublesome. About 90 percent of the malfunctions encountered in business and scientific computers arise in mechanical input and output equipment, printers, and magnetic and paper tape and punched card handlers. These failures can be avoided in the process control digital computer system by direct transfer of signals from

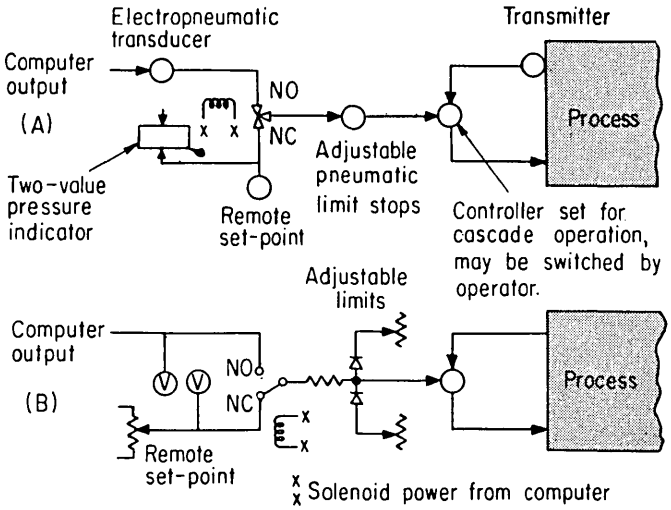

FIG. 3. The computer automatically determines the set-point for the conventional controller. Adjustable limit stops restrict the range to safe desired values, and the solenoid operated valve (or switch) enables the operator to take over manual control at will or at failure of computer power.

the process to the computer's memory and from the memory to the process, i.e., with no moving parts other than those in the conventional instrumentation and transducers and in sealed relays.

This direct transfer often is a major argument for using a special-purpose computer on-line to control a process. System inputs through a card or tape reader can be held to an absolute minimum, and then only for loading the initial program, informing the computer of startup or shutdown, changing a limit of a variable, or making an incremental change in loading of a pump. The alternative to on-line computing, sharing a general-purpose computer with nonprocess activities, requires transmitting information from a data logger in tape or card form, and transmitting printed control signals from the computer to the control board.

The computer's many individual components are the subject of an even more detailed reliability study. Much work has already been done in guided missile and other military programs to relate the overall reliability of a system to the number of its components and the reliability of individual components to testing methods and environmental conditions. Such experience can be adapted to a digital computer for process control, which might have 6,000 active parts, including transistors, diodes, resistors, condensers, and transformers. For this computer to average one month of continuous operation between failures, the individual components themselves must average one failure in 6,000 months, or 500 years of continuous operation! This imposing demand for reliability can be met only by high-quality, well-sealed, permanent components, and by minimizing the number of nonpermanent components.

Flush-etched wiring on epoxy-resin boards, Figure 2, and new types of solderless connection (for conventional wiring) answer these requirements. So do hermetically sealed relays with mercury-wetted contacts and proper arc suppression across the contacts, for these are guaranteed for 1 billion operations (and have been known to reach 3 billion operations with no sign of failure after the initial burn-in period). Other safeguards: premium-type vacuum tubes conservatively derated for long life, and stabilized circuits for satisfactory operation over a wide range of component values. Finally, in recognition of the burn-in characteristics of many components, factory checkout of the computer, including the control and logging programs, should be planned so as to exercise components for several hundred hours.

It must not be assumed that because care has been exerted in the design, manufacture, and checkout of a process control system, permanent and random nonrecurring failures will not occur. Fail-safe philosophy as it applies to a computer control system design has two principal objectives:

1. Wherever possible, to detect failures before they have any effect on the process and determine effective remedial action.
2. To minimize the effect on the process of failures that cannot be preceded by a warning.

Consider first the steps taken within the computer program toward accomplishing these objectives. Most failures in the computer itself can be detected in time by requiring the computer to perform a test problem immediately before computing a new output value. The test problem exercises all computer instruction codes and portions of the memory. The computer may be programmed so that failure of this test idles it and warns the operator to take over control of the process. Meanwhile, all outputs can maintain their last calculated values.

A digital computer's process-control functions lend themselves readily to a reasonableness check. Usually, the computer measures process variables and periodically repeats a set of calculations. A simple check,

to guard against a random nonrecurring failure that could affect the calculation of any individual output, consists of specifying for each output the maximum increment by which a new calculated value differs from its previous value. When this increment is exceeded the output is left at its present value until the calculation has been repeated and checked, either immediately or on the next programmed pass through the calculation. A variation of this approach is to allow the output to change by a small increment: if the change is due to a random error the value of the variable is reestablished properly on the next pass. This second approach is superior, in some situations, in that it also sets a maximum limit on control-point change, smoothing the normal control action for the process.

Failure of a component in the final stage of an output or loss of power by the computer may take immediate effect, with no warning to the operator. To understand how these effects may be minimized, consider how the computer is connected to the process control points. In Figure 1, the instrumentation and set-point controllers above the dashed line comprise an independent conventional process control system which may be used during periods of computer maintenance, program modification, system startup and shutdown, and, of course, as a standby control system.

Figure 3 details the way the computer controls the process by adjusting the set-point of individual control loops. (The computer could replace the controller by measuring the variable directly and adjusting the valve or output control point, but in many cases this would represent an impractical and uneconomic use of an expensive mechanism.) The first step in minimizing the effect of any sudden local computer failure is to limit the output control range to the minimum necessary for satisfactory control of the process. This is done by means of the inherent scale limits of the transducer or controller hardware, or more conveniently by setting the continuous analog limit stops, Figure 3, so that they restrict the computer's control to that needed for startup, shutdown, or other infrequent modes.

In the event of sudden total failure, such as loss of power in the computer, control of all outputs must be automatically transferred to the standby system. This transfer is actuated by removing the power from the computer to the solenoids, Figure 3, for all control loops. The system must be designed so that the operator can operate any solenoid at will and thereby obtain control of any output set-point or return control of any variable to the computer. To minimize bumping the process, each variable is provided with a two-pointer indicator which continuously displays the computer output and manually-set reference point in a convenient form for comparison.

Pneumatic control systems may be arranged so that the removal of power from the solenoid valve in Figure 3A holds the control pressure at its present value, allowing the operator to manually match reference points and complete the transfer of each output without bumping. With this arrangement, daily tracking of the computer's outputs by the operator is not necessary; however, all equipment and operating personnel in the standby system must be drilled often enough to retain operating efficiency.

Instrumentation reliability

A digital computer will probably have only a secondary influence on the frequency of related instrument failures. But it can aid instrument maintenance by giving early warning of any failures that do occur. It can watch for hardover conditions, for readings that do not fluctuate when they should, and for excessive drift in calibrations.

The effect on the process of instrument failures would be far greater than in conventional systems if the computer blindly followed instrument readings without discriminating between valid and invalid data. The input system (through the selection of data ranges) and the program should be organized so that the computer not only recognizes and announces instrument faults but also makes suitable allowances for them in executing its control equations. Then, instead of using faulty data, the computer may refer to a secondary source of data, to the last value of data, to an arbitrary constant, or to data derived from other variables. These provisions add to the bulk of the computer's program, but they are the necessary price of the full integration of a complex control system.

Process reliability

In many installations reductions in process maintenance will outweigh additional computer maintenance. Maintenance scheduling of process equipment may benefit by having the computer perform periodic checks on such items as heat exchanger and pump efficiencies and catalyst poisoning. Maintenance checks can be permanently stored in the computer's memory or loaded in from permanent tapes each time they are needed, sharing space with such other infrequently used programs as computer maintenance and process startup and shutdown.

The digital computer control system provides, as a by-product of process control, improvement of process reliability. It acts as a sophisticated limit-checking alarm system, warning of dangerous or near-dangerous conditions. It can be programmed to take appropriate control action, following an alarm, through its regular control output or through specially assigned relay outputs. It detects such conditions not only by standard limit-checking but also by checking the deviation of variables from calculated set-points, by extrapolating trends to predict impending limit excursions, by testing correlation between different variables to detect obstructions, and by making material and energy balances to detect leaks and loss of process efficiency.