Reactor On-Line Computer Applications

Kris L. Gimmy

Abstract

Thirty-five years ago, most people were just becoming aware of the digital computer, in the form of large IBM machines. But, there was another kind of computer called the "on-line computer" just starting to be used for industrial automation. These computers looked promising as a way to improve productivity and safety at the Savannah River Site (SRS). Four technical support groups worked together to apply on-line computers to the operation of SRS reactors. The reactors were chosen because each reactor had over 3500 instrument signals that had to be monitored for proper operation.

The 20-year "computerization" effort went hand-in-glove with the effort to raise reactor powers and to produce a variety of different products. The first ten years saw computer application move from data processing, to monitoring the hydraulic limits on each reactor element, to computer control of reactor power operation. The second ten years saw newer, faster computers used as the primary safety system for reactor emergency shutdown. On-line computers were also used to automatically diagnose plant alarms and to display corrective action to the reactor operator.

Computerization was an integral part of safe operation as the reactors were upgraded to operate at seven times their original output!

Introduction

On-line computers are rugged industrial computers that are wired in to a plant process. They are there to make something run better or safer. On-line computers accomplish this by reading signals from plant instruments and running software that can operate plant controls and alarm panels. They can also do data processing and display the results to the plant operators. The on-line computers are not, however, general purpose computers, like the PC on your desk. The user cannot load new programs or alter the software designed for the specific installation (see Figure 1).

A good example of an on-line computer is the "on-board" computer in your new car. It reads about 30 signals from the engine and the environment. It adjusts for existing conditions, such as temperature and altitude, so there is no stumbling or hesitation upon startup. As you drive, it continually fine-tunes the engine, which now gives twice the gas mileage of 1950s' cars. The onboard computer improves safety in emergency conditions by controlling the brakes to avoid skidding (anti-lock brakes). It alerts you to problems with dashboard alarms. Finally, if the car needs service, it saves data that helps the technician diagnose the problem.

In like manner, the productivity and safety of the nuclear reactors at the Savannah River Site (SRS) were improved by the addition of on-line computers in an aggressive program that started 35 years ago!

1964—Data Processing and Alarms for Plant Operators

The first application of an on-line computer for SRS reactors was to do data processing and to alert operators to bad instrument signals and other minor process problems. While this sounds like a straightforward computer task, there were three major hurdles to overcome.

- A production reactor had over 3000 instrument signals that the computer would have to read.

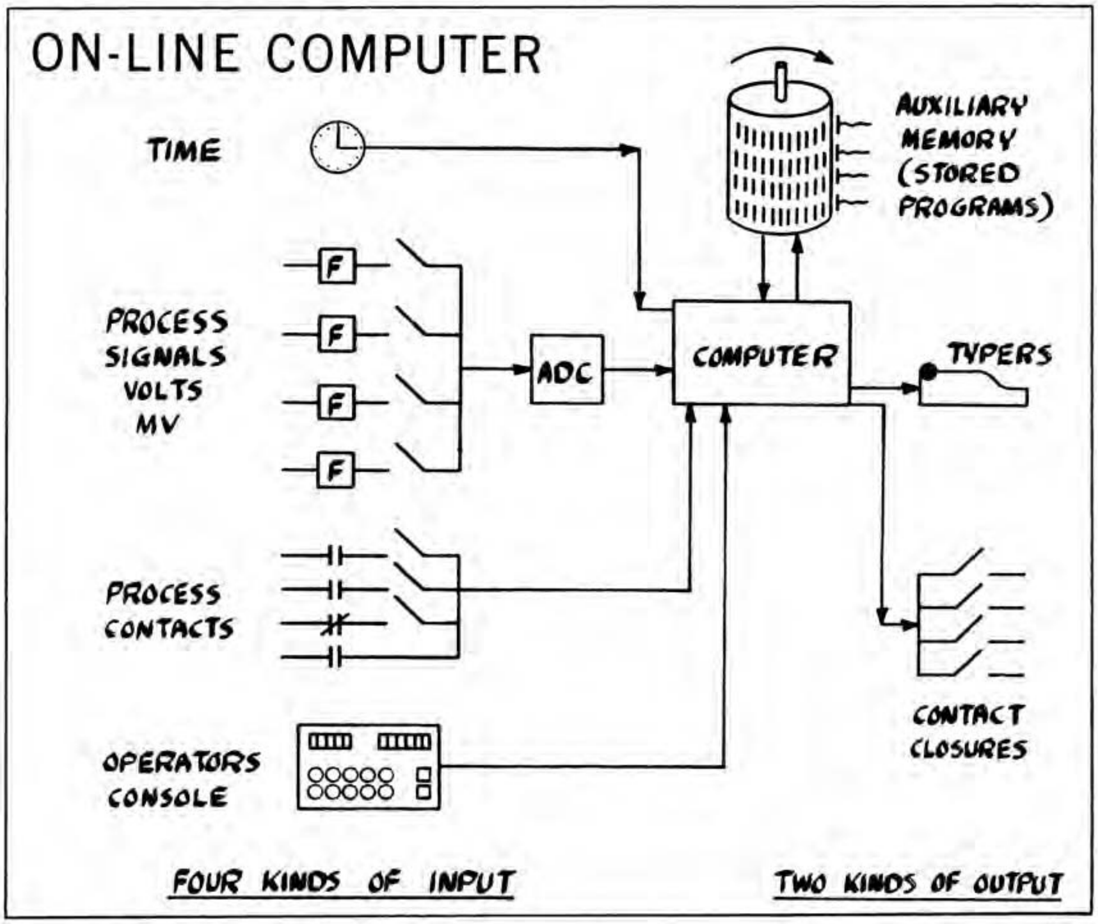


Figure 1. On-line computer

- An operator interface would have to be developed that the reactor operators could use and that would be consistent with plant procedures.

- The on-line computer system would have to be reliable and repairable by plant instrument people.

These challenges were met by four SRS departments closely working together.

The Equipment Engineering Group developed a switching matrix that would preselect reactor signals in groups of 30, which the computer could then read at 10 inputs per second. This yielded a 5-minute scan of the entire reactor process—a major improvement over the 2-4 hours it took to manually read data from recorders and the plug-in jack panel.

The Plant Project Group designed the installation of the computer (five cabinets each the size of a refrigerator) and the wiring requirements and blueprints to connect the thousands of plant signals.

The Plant Instrument Group did the wiring during scheduled reactor shutdowns without disrupting the existing analog instruments. This group also set up training and spare parts so they could repair the computers.

The Reactor Technology Group worked with the vendor (General Electric) to design a simple panel that the operators could use. Remember, this was 20 years before the Macintosh computer introduced the graphical interface we all use today. The panel specified enabled the operator to call for programs, or enter data, by using rotary switches (0-9). Two printers were also installed in the control room, one for requested data and one dedicated to alarm messages.

With the design firm and installation underway, the Reactor Technology Group took training to prepare the reactor software in the Assembler Language used by the GE computers. By the time the installations were completed, there were about 10 programs to print reactor data and display the power distribution within the reactor. The favorite program of the reactor operators was the "Histogram" program used to fine-tune the temperatures of the fuel elements surrounding the 61 control rod groups in the core. This program sorted the 1464 temperatures and generated a bar chart that showed which control clusters were hot and which were cool. It had been an onerous job that took the operators eight hours to do at the jack-panel with paper and colored pencils. The on-line computer did the job in five minutes, if you set the "Program" knobs to "08". By the end of 1964, the prototype installation at K Reactor was scanning more signals than any computer in America (including those at NASA).

1968—Automatic Monitoring of Hydraulic Limits

From day one, the SRS reactors were operated under strict, written limits to ensure there would be time for the automatic shutdown mechanisms to work if there were a process upset or equipment failure. This safety margin was monitored manually by plugging into the signals for the hottest fuel assemblies and watching the continuous traces. But, the simple temperature limits of early operation became more complex as engineering changes were made to each reactor to increase productivity. One of the major justifications for the on-line computers was to provide automatic calculation and monitoring of the hydraulic limits specified for each reactor load. Reliable monitoring of the hydraulic limits had to go hand in hand with engineering changes that eventually led to a sevenfold increase in reactor productivity. (See "Reactor Program for Increased Production Capability" by James M. Morrison in this proceeding.)

One of the most complex limits, needed at high power densities, was to provide a Burnout Safety Factor. You can visualize this phenomenon of heat flux burnout by imagining an aluminum pan filled with water, sitting on a burner on your stove. As you turn up the heat, small bubbles of steam form on the bottom of the pan, then rise toward the surface. If you turn up the heat more, the bubbles get bigger. If the heat on the pan is increased enough, the bubbles will join and form a blanket of steam on the bottom of the pan. The bottom of the pan will melt, even though the pan is still full of water.

The Burnout Safety Factor guarded against a power density high enough to cause film boiling on the aluminum cladding used on SRP fuel assemblies. Monitoring the safety factor was a complex calculation that determined the power profile along the length of each reactor fuel assembly. The formulas used data on temperature, flow, pressure, and in-core flux profiles. When done by hand, the calculation took a desk calculator and a worksheet that looked like an IRS tax form (see Figure 2). But, by 1968 (just as power was increased enough to need this limit), it was being calculated automatically by the on-line computer.

The Limits program was set to run automatically every five minutes and could not be turned off. If any parameter exceeded its limit, there was an alarm message issued. If the limit was exceeded by more than one degree, the computer closed a relay to cause a power setback of about 2%. Every hour, a summary of the margin from all of the hydraulic limits was printed automatically as a record of reactor operation.

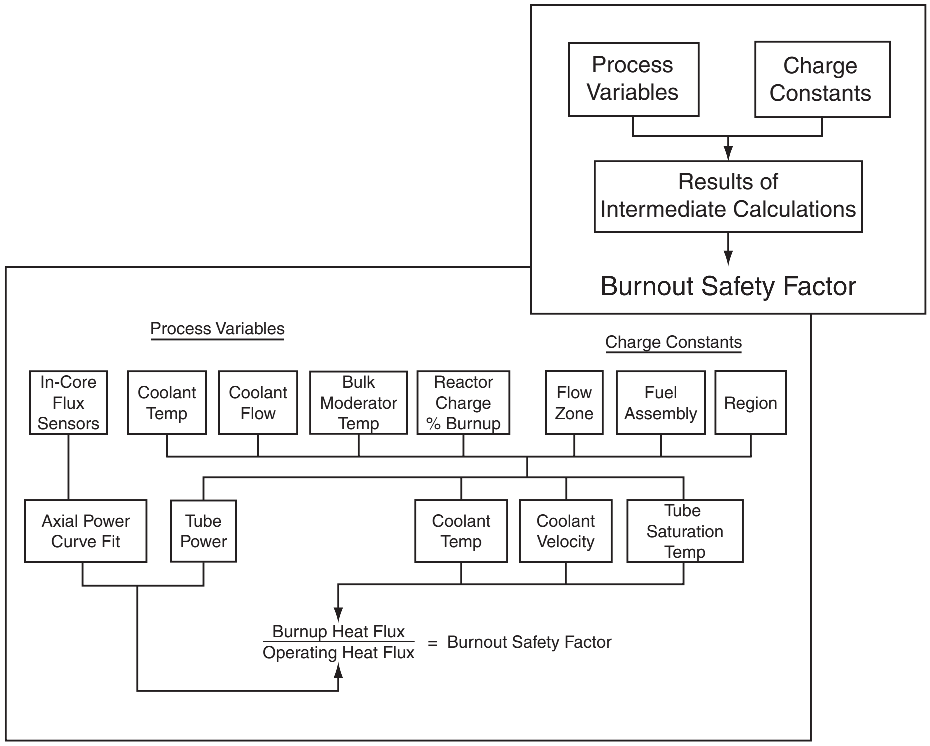


Figure 2. Burnout Safety Factor calculation

1970—Closed-Loop Control of Reactor Power

Closed-loop control of reactor operation was accomplished by adding stepping motors to the six control units used by the operators to move the three gangs of full-length control rods and the three gangs of partial-length control rods. The full rods controlled the power across the radius of the reactor, and the partial rods were shuttled up and down to control the axial distribution of reactor power.

Once again the SRS Equipment Engineering Department designed an electronic interface so a computer command could move control rods a specified number of steps. They also provided a "control panel" so the operator could select three states of automatic control (see Figure 3):

HOLD = maintain the current power level

ACTION = change power (up or down) to a new level specified by the operator

OFF = no computer control (both software and the stepping motors were disabled).

Thus, the computer control was designed to be very much like the automatic pilot found on commercial airplanes. The computer could not do a startup (takeoff) or a shutdown (landing), but it could fly straight and level, and it could ascend or descend to a new level. The benefit to the production reactors was that every control action was made in such a way as to equalize the power distribution within the reactor core since the data to do this was at hand. This ensured the most productivity (within the hydraulic limits) and the most uniform product. Computer control had the additional benefit that it checked all of the requirements for safety circuits and hydraulic limits before it would raise power. Closed-loop computer control was used for about 90% of a reactor production cycle and proved to be a most diligent "operator".

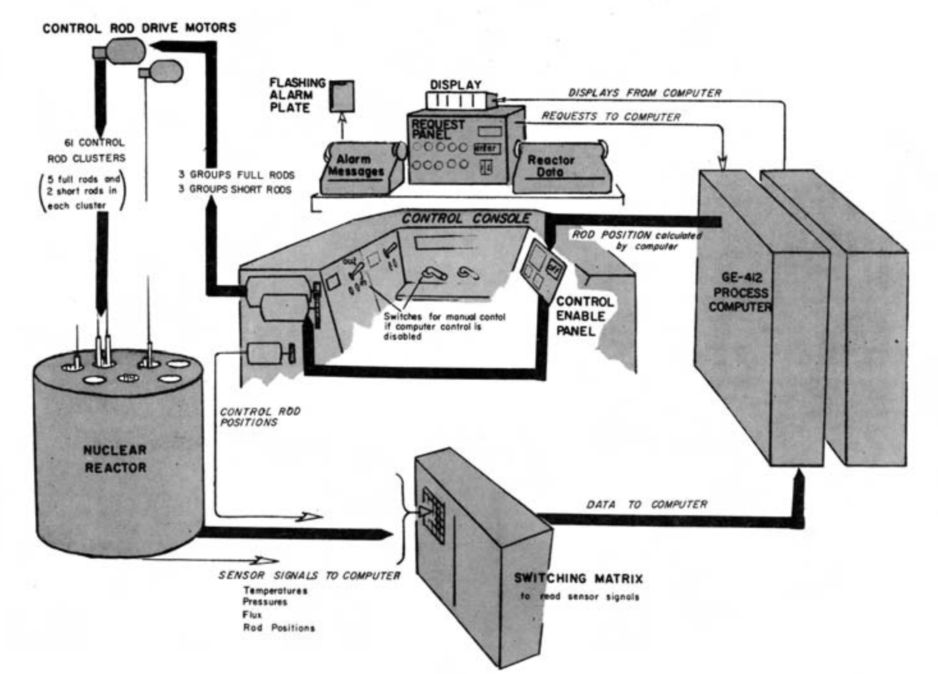


Figure 3. Automatic control of a nuclear reactor using a computer

1974—Dual Safety Computers

Ten years after the initial installation, on-line computers were much smaller and much cheaper. The installation at each SRP reactor was upgraded to a four-computer system. Two computers took over reactor control functions; these computers were essentially unchanged, but with one serving as a backup, yielding an availability of 99% of the time. The other pair was called safety computers and replaced the original mechanical safety circuits, which had hundreds of individual adjustments on one wall of the control room. Each computer monitored the flow signals from half of the 600 reactor assemblies and the temperatures signals from the other half of the assemblies. This arrangement provided either flow or temperature monitoring for the coolant to each reactor position, even if one computer was off-line. They were programmed by the Reactor Technology Group to be a safety circuit, capable of shutting down the reactor in one second if the safety limits on flow or temperature were exceeded.

1980—Automatic Backup for Fast Shutdowns

There had always been a concern that the safety rods of the fast shutdown system might fail to drop into the reactor for certain highly unlikely circumstances. For example, a severe earthquake might displace the reactor core or distort the safety rod guide tubes. A backup shutdown system was installed that could inject a liquid neutron absorber under high pressure. The system was manually activated by the control room operator. But by 1980, the safety computers had proven to be reliable enough to serve as a backup for operator action. The logic for the software was simple. The safety computers would monitor all circuits that could initiate a fast shutdown. If a fast shutdown was called for, and if reactor power didn't decrease by at least half in a few seconds, the safety computers would fire explosive valves to inject the backup system liquid into the reactor core. The plumbing for this system was made redundant, to ensure full effectiveness even if only one safety computer was operating.

1982—Automatic Diagnosis of Multiple Alarms

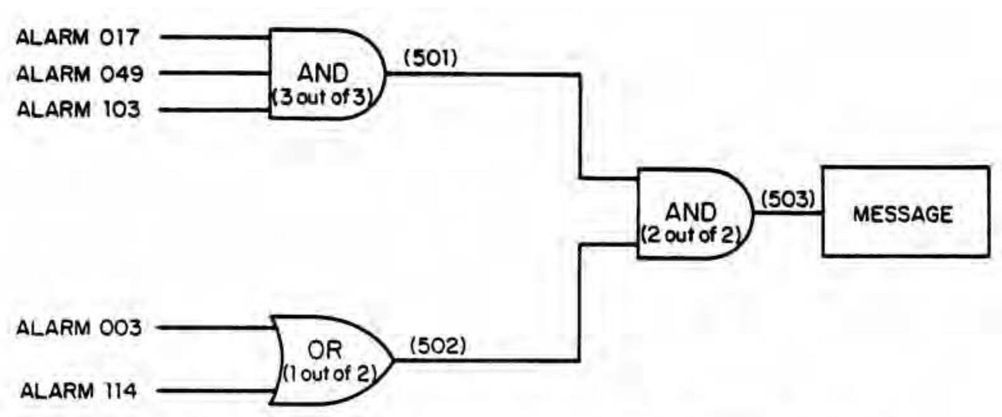
If the previous application was a simple extension of existing technology, the diagnosis of the plant alarms definitely was not. Our review of the reactor accident at Three Mile Island (TMI) led to some new research, which in turn led to a system to diagnose multiple alarms. It was called the DMA system and was installed at all SRP reactors.

The main finding of the TMI accident study was that the plant operators got so many alarms that they were overwhelmed mentally. They got over 100 alarms in the first 5 minutes of the accident. Some indicated minor problems, some simply reported a change of state, and some were very important. By the time the important ones came on, they were buried in the confusion.

SRP also had procedures to deal with individual alarms and combinations, but not 100 alarms in 5 minutes, which we concluded was also possible at our reactors. We decided to take the diagnostic steps in all those procedures and put them into "fault trees"—the same type of fault trees that General Motors was starting to use in their automotive shop manuals. This was a one-year task. Then we worked out a new way to store these fault trees in a computer in "tabular form" (see Figure 4).

This was the breakthrough needed, for now we could use ONE computer program to do all of the fault trees as each new alarm signal came in. The computer could easily keep up, and it could determine which fault tree had gone the farthest and identify the source of the trouble (see Figure 5). This was important stuff. The online computers would automatically diagnose what was wrong and tell the operators in plain English.

The concept of having a computer do a diagnosis based on symptoms and stored knowledge was known as an expert system. Many research groups were working on expert systems, but ours was the first that converted the logic trees to tabular form. This simplified programming and gave a simple way (using checksums) to validate any changes to the stored knowledge. After all, if you were going to let a computer diagnose something, you wanted to be sure it was right.



Decision	Number of Inputs	Number Required	Input Identification	Message
501	3	3	017, 049, 103	NO
502	2	1	003, 114	NO
503	2	2	501, 502	YES

Figure 4. Sample alarm logic tree and decision table

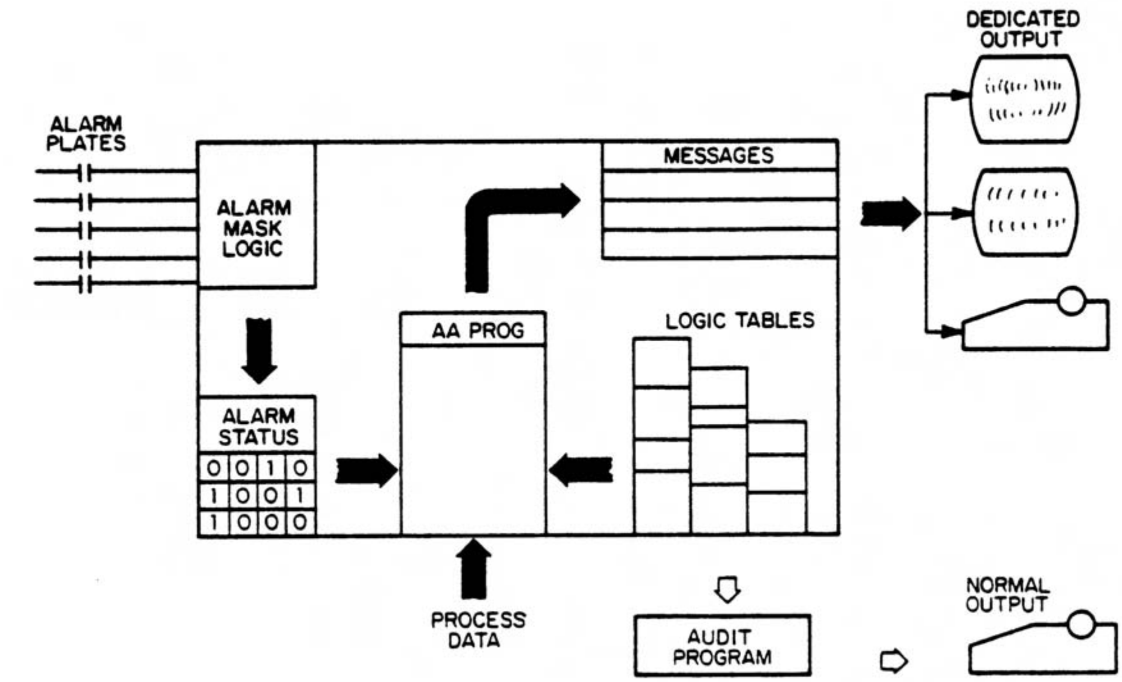


Figure 5. Data flow for alarm analysis

Biography

Kris L. Gimmy is a chemical engineer from Washington University in St. Louis, Missouri. During a 33-year career with Du Pont, he worked in all three divisions associated with nuclear reactors at SRS. He worked as a shift supervisor in Reactor Operation, as technical support in Reactor Technology, and in reactor safety research at Savannah River Laboratory. He also served as a consultant to the U.S. Nuclear Regulatory Commission.

Intentionally left blank