ANL/IFR/CP--84087
Conf-950564--7

EBR-II ARGON COOLING SYSTEM RESTRICTED FUEL HANDLING I&C UPGRADE

by

Steven E. Start
Reed B. Carlson
Roger L. Gehrman

Argonne National Laboratory - West
Engineering Division
P.O. Box 2528
Idaho Falls, ID 83403-2528
(208) 533-7096

Submitted for Presentation at
The Ninth Power Plant Dynamics,
Control & Testing Symposium

May 24-26, 1995
Hyatt Regency Hotel, Knoxville, Tennessee

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

EBR-II ARGON COOLING SYSTEM RESTRICTED FUEL HANDLING I&C UPGRADE

Steven E. Start, Reed B. Carlson, Roger L. Gehrman
Engineering Division
Argonne National Laboratory - West
P.O. Box 2528
Idaho Falls, Idaho 83403-2528

ABSTRACT

The instrumentation and control of the Argon Cooling System (ACS) restricted fuel handling control system at Experimental Breeder Reactor II (EBR-II) is being upgraded from a system comprised of many discrete components and controllers to a computerized system with a graphical user interface (GUI). This paper describes the aspects of the upgrade including reasons for the upgrade, the old control system, upgrade goals, design decisions, philosophies and rationale, and the new control system hardware and software.

INTRODUCTION

System Description

The ACS circulates inert argon gas through fueled and non-fueled subassemblies during transfers from an interbuilding coffin (IBC) to the EBR-II reactor vessel, and vice-versa. This type of subassembly transfer is referred to as restricted fuel handling. The ACS consists of turbines, pipes, valves, instruments and a control system which serves to automatically maintain gas flow through a subassembly during a transfer. The ACS functions both as a heating system for components and individual subassemblies as they enter the reactor vessel and as a cooling system to remove decay heat from irradiated subassemblies as they are removed from the reactor vessel. Operation of the ACS, under normal conditions, is virtually automatic. The ACS control system directs inert argon gas flow through system piping by automatically controlling flow path valves in order to maintain subassembly heating or cooling. Some ACS flow path transitions are initiated by an operator at the ACS console. In the event of abnormal conditions, the ACS flow path may also be controlled manually. The Fuel Unloading Machine (FUM) is a manually operated subsystem of the ACS which is manipulated by a fuel handling operator to handle and transport a subassembly. The FUM consists of a shielded cask on a movable platform with a gripper mechanism for grasping subassemblies. The FUM moves back and forth along two rails in transporting a subassembly. FUM signals are carried via coiled cables which run from the movable FUM to one end of the FUM rails. The ACS and FUM have separate relay-based control systems which interact to accomplish all of the interlock and sequencing functions required for fuel handling. Figure 1 shows the ACS and FUM in relation to the reactor vessel and other fuel handling equipment.

System History

The ACS was designed and implemented using 1960's vintage components and used a complex network of relays and discrete components to perform control and readout functions. Operation and maintenance experience with the system in recent years has shown that much of the components and wiring are aged,

* Work supported by the U.S. Department of Energy, Reactor Research Technology under Contract No. W-31-109-ENG-38.

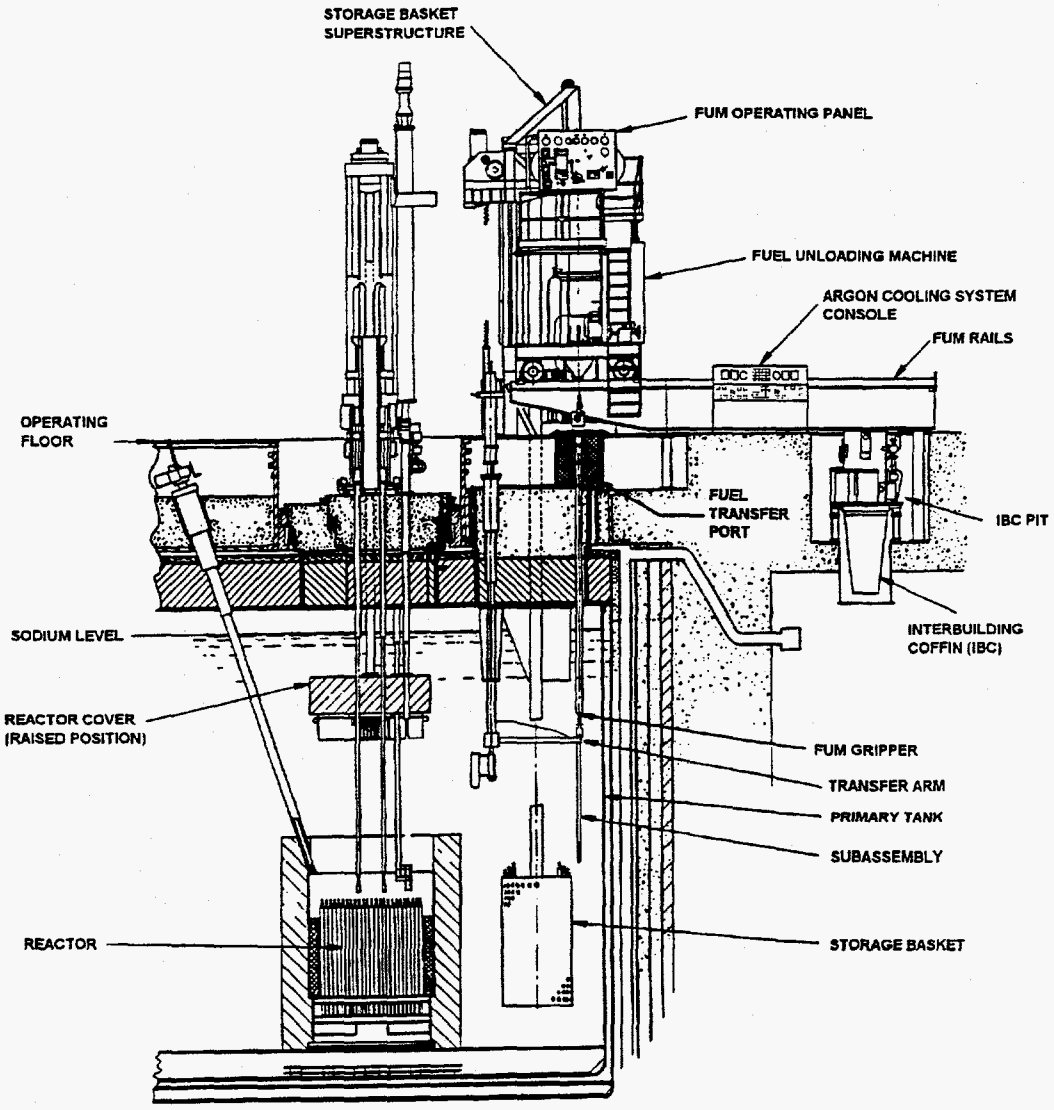


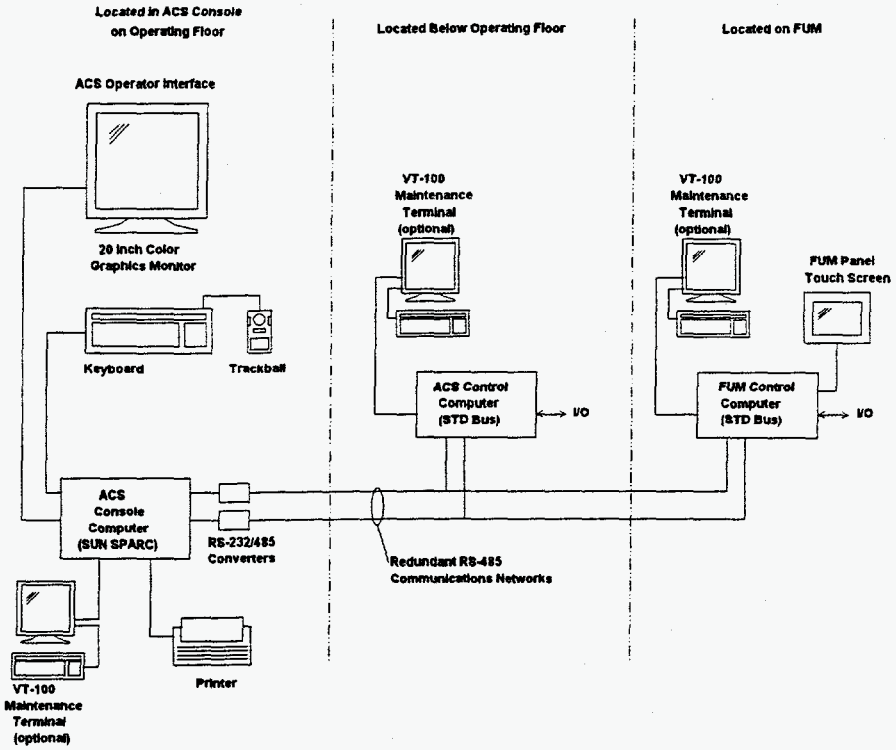
Figure 1: EBR-II Reactor Vessel and Fuel Handling Equipment

subject to failure and obsolete. Broken wiring and relay failures periodically cause the control system to malfunction. In addition, the complexity of the wiring and relay-based control logic have made troubleshooting both time consuming and difficult.

The Control System Upgrade

The FUM-ACS control system is in the final design stages of an upgrade to be installed in the summer of 1995. Computerized control and indication replaces most of the existing relay control and discrete indication. The upgrade utilizes three computers: a SUN SPARCstation and two smaller control (STD Bus) computers. The SUN SPARCstation, referred to as the ACS console computer, resides in the ACS operator console on the main operating floor of the reactor building. It drives the CRT based operator interface and provides system-wide diagnostic and smart alarm functions. The operator interface provides graphics that show the entire FUM and ACS. The two smaller STD bus computers, referred to as the ACS and FUM control computers, reside in separate hardware termination cabinets. These two computers

replace most of the system's relay-based control logic with computerized logic. They perform all of the real-time input/output (I/O) functions for the system. An overall view of the computers used in the upgrade is shown in figure 2.



The upgrade improves the ACS console and FUM panel operator interfaces by replacing the existing designs with new ergonomic designs that use modern components. Old and obsolete instruments throughout the system are replaced with modern units.

UPGRADE GOALS

At the onset of the project, it was important to set goals for the upgrade that would influence project design decisions. The overall project goal was to improve the safety, reliability and availability of the ACS and FUM. In addition, the upgraded system was to:

- meet or exceed all established safety requirements,
- provide an improved operator interface using a computer CRT,
- provide computer based diagnostics to better pin-point problems and reduce troubleshooting time,
- utilize improved components to increase system reliability, availability and functionality,
- provide smart alarms to recognize abnormal states while avoiding nuisance alarms,
- be completely prefabricated, mocked-up and tested prior to installation to:
    (1) allow hands-on operator training prior to installation,
    (2) reduce installation,
    (3) minimize post-installation testing.

ANALYSIS AND DESIGN

The following subsections discuss some of the major and significant areas where analysis influenced the upgrade design.

Technical Specifications

EBR-II technical specifications for the ACS were analyzed to ensure that the upgrade would not introduce a failure mode that would increase the chances of violating the technical specifications. There was only one specification that had the potential to be impacted by the upgrade. The requirement pertained to a minimum acceptable cooling flow rate while transferring an irradiated subassembly. A fault tree, shown in figure 3, was constructed to show the circumstances that could cause the specification to be violated.

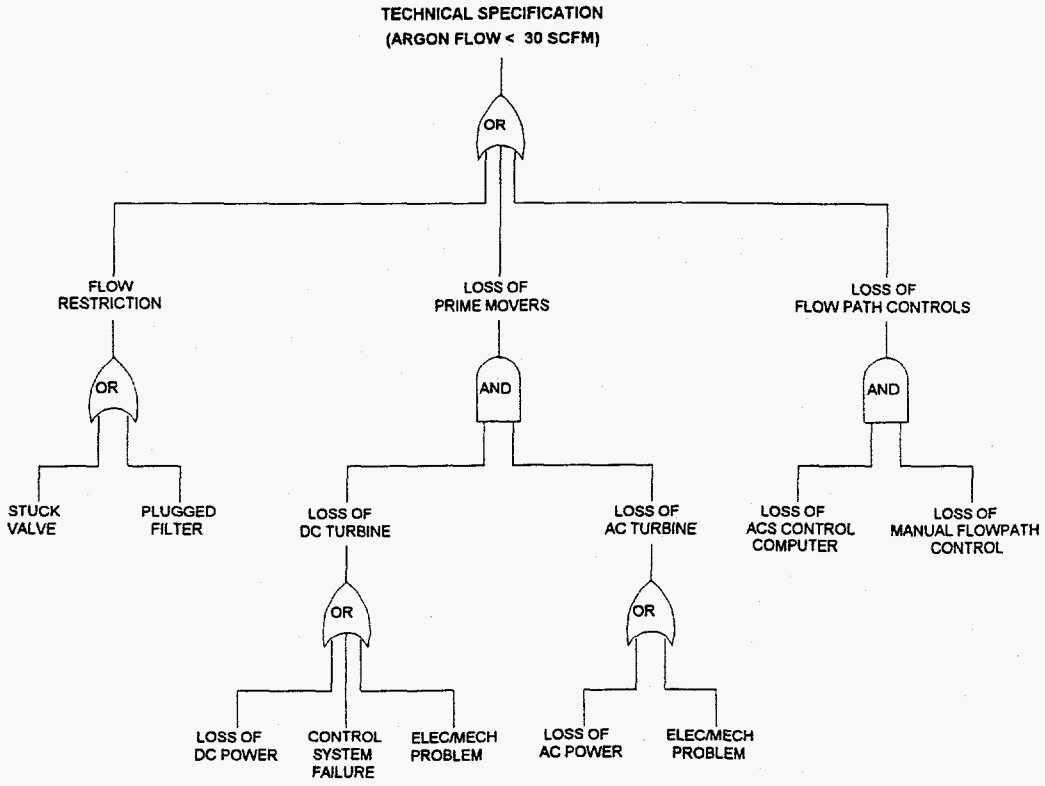


Figure 3: ACS Technical Specification Fault Tree

Flow could drop below the technical specification minimum if there was a flow restriction, if both turbines failed, or if the flow could not be directed through the correct flow path. The consequence for violating the technical specification is that the subassembly must be placed in a secure location and fuel handling must be terminated until the problem is corrected. While the old system also had a manual operating mode, the fault tree illustrated the need for independent manual controls and separate flow indication and alarms apart from those available through the computers.

Items retained as discrete controls, indicators, and alarms on the new ACS console were identified on the basis of a design philosophy that failure of any or all computers in the system will not constitute a violation of technical specifications. That is, manual control capability and display status for all essential ACS functions would be retained as a backup means of operating the ACS in the event of a control computer failure.

Failure Modes and Effects Analysis (FMEA)

Key system components, especially those related to computerization of the control systems, were analyzed to determine if there was a significant consequence of failure. If it was determined that a significant consequence existed, a simultaneous failure of more than one item would be required in order to cause the undesirable consequence. For example, the FUM control computer drives a digital output which picks up the FUM carriage clutch which moves the FUM along its rails. There are undesirable consequences if the FUM carriage moves when it is supposed to remain stationary. A FMEA showed that a control system failure and an operator error must occur together in order for the FUM carriage to move inadvertently as shown in figure 4. In this case, no design changes to the original system design were required.

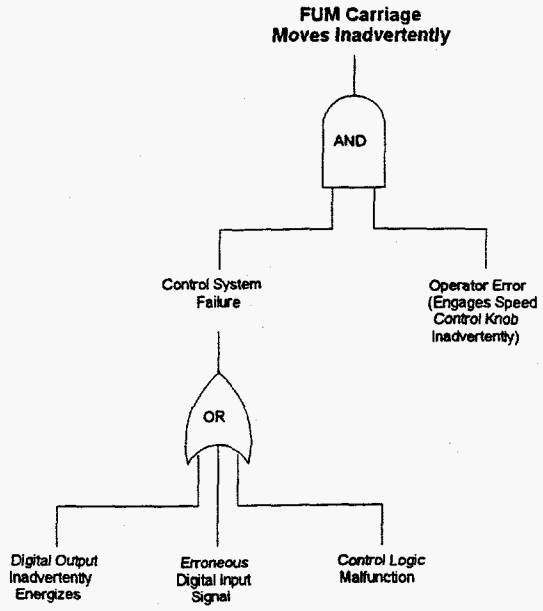


Figure 4: FUM Carriage Failure Modes and Effects Analysis Logic

In the process of doing the FMEA for the FUM and ACS, two areas were identified as having potential for adverse consequences not accounted for in the original system design. As a result, additional design features were introduced that require multiple failures to occur in order for the adverse consequence to occur.

System Weaknesses

Maintenance and operating experience with the ACS revealed design weaknesses in the system that could be corrected as part of the upgrade. For example, coiled cables that carry signal and power to the FUM had been subject to failure. The result was that most coiled cords were eliminated and I/O signals to and from the FUM were carried via redundant communications networks by means of a new festooned cable.

The system was also analyzed for single point failures that could have a significant impact on system operation. As a result, a single point failure was discovered in some power circuitry and was correctable as part of the upgrade.

Recommendations and Observations

First hand observation of fuel handling revealed other areas where the design could be improved. Many incandescent lights were used throughout the ACS and FUM operator interfaces and were subject to frequent burn out. Burned out bulbs caused fuel handling operations to be suspended while the suspect bulb was tested and changed. To correct this, all indicators used in the upgrade are light emitting diodes (LEDs) which should operate well beyond the life expectancy of the system.

In addition, it was observed that a fuel handling operator on the FUM operating platform frequently had to obtain an indication or reading from the ACS console down below him. A video touch screen terminal was added to the FUM panel to provide him with the information he required while on the FUM. Limited space on the FUM operating platform as well as improved usability made a touch screen more suitable than a keyboard or mouse driven terminal.

In the old system, all but one of the FUM and ACS alarms were located on the ACS console annunciator panel. The one alarm was located on the FUM operating platform which meant that an operator had to climb the FUM ladder to the operating platform to acknowledge this alarm. This alarm was relocated to the ACS console on the main operating floor.

Human Factors Guideline Summary

In redesigning the operator interfaces, consideration was given to several human factors resources. A summary of human factors guidelines was generated containing information that would be applicable to the upgrade. A list of the guidelines consulted is given in the references section of this paper[1][2][3]. Utilized with common sense and an understanding of how the system is operated, these provided helpful information in redesigning the ACS console, FUM panel and the graphics screens. Concerning the panel layout, EPRI's NUREG 0700 states the following:

> *"The layout of panels is a compromise among a number of considerations. In some instances various human factors principles will conflict, not only with each other but also with other design requirements. Because it is difficult to rate the conflicting considerations for importance, final decisions must be based on careful evaluation and sound judgement." - NUREG 0700, Guideline 6.8.2.1*

Recognition of this is especially important when redesigning or upgrading an existing operator interface. Constraints on the scope of a modification can make "verbatim compliance" both cost and schedule prohibitive. For instance, since this upgrade focused primarily on I&C portions of the system, major mechanical changes to the FUM panel such as redesigning its size or location, were not considered. The new ACS console and FUM panel were designed in cooperation with an EBR-II fuel handling specialist and with comments and feedback from fuel handling operators.

ASPECTS OF THE UPGRADE

Computerized Control System

The upgrade is built around a UNIX-based computer workstation and two I/O front-end micro-computers. The workstation provides a graphical CRT-based operator interface for the ACS and FUM. The I/O front-end computers perform all real-time control tasks for the system. The computer system is designed so that failure of the least reliable computer, the ACS console computer, has minimal impact on restricted fuel handling. To minimize the consequences of the ACS console computer/graphics screen failing during fuel handling, the FUM and ACS items controllable from the ACS console graphics screen were limited to non-critical or seldom used functions such as heater setpoint changes.

Computer Communications

To minimize the number of conductors run between the FUM and ACS and to minimize the communications demand between the three computers, a half-duplex multi-drop serial communications scheme is used. This is referred to as RS-485. The ACS console computer, ACS control computer, and FUM control computer are all connected to the RS-485 network. This allows the console computer to get all required information from the control computers without the control computers explicitly sending messages to the console computer. Message efficiency and reliability is further increased through the use of a binary protocol that utilizes a CRC-16 checksum. To increase the reliability of the communications between the computers, a second pair of wires is added for a backup or redundant communications link. Should a cable be damaged, the communications will automatically switch to the second link.

The UNIX Workstation Computer

A UNIX based computer was needed to provide the high resolution graphics on the ACS console. The graphics development and run-time tool used as a standard in EBR-II for sophisticated color graphical operator interfaces[4] is DataViews by V.I. Corporation. This tool is designed to run on UNIX platforms.

A Sun SPARCstation was chosen over other manufacturer's computers primarily because the Sun UNIX operating system, Solaris 2.X, which has soft real-time enhancements that are needed to satisfy RS-485 communications timing requirements. The STD bus computers, being hard-real-time computers running without an operating system, could guarantee communications response in an allotted time frame. Solaris 2.X was able to meet the timing requirement and fit within project budget constraints

The ACS console computer runs two primary tasks, an operator interface task and a communications task. The operator interface task handles the diagnostic and alarm processing, DataViews based graphical screen displays, and any operator input related to those displays. The communications task handles the communications links with the FUM and ACS control computers. The two tasks exchange data through shared memory.

The STD Bus Computers

The FUM and ACS control computers perform the real-time control and data acquisition functions for the system. The RS-485 communications link between the two computers is used to provide control information that each needs from the other and to provide status information to the ACS console computer. The RS-485 networks replaced several coiled cords which were used to send signals between the FUM and ACS relay control systems.

Since the old control logic for the FUM and ACS consists primarily of relays, programmable logic controllers (PLCs) were considered for use as the real-time control computers in this upgrade. While the real-time control functions for the FUM and ACS could be implemented using PLCs, general purpose STD bus computers were selected instead of PLCs for this upgrade for several reasons:

- Cost of STD bus systems is less than PLCs,
- FUM and ACS control logic is relatively small and simple as compared with the Fuel Handling Console [5],
- Communications details between a PLC and the SUN SPARCstation were unknown and unavailable because high speed PLC communications links use proprietary protocols,
- Development, maintenance and operating experience with STD bus systems was available within EBR-II and software from previous STD bus projects was available to be reused in the upgrade.

The FUM and ACS control computers each run two tasks, a hard-real-time interrupt driven foreground task and a background task. Each system's foreground task handles real-time I/O, control logic, and communications message processing. The background task handles the VT-100 and touch screens interfaces. This design methodology has been used for several years in EBR-II embedded systems [6].

The ACS Console

Utilization of a graphics screen on the ACS console allows many displays, controls and alarms that were on the old ACS console to be eliminated. Discrete displays, controls and an alarm panel are still necessary on the new ACS console in order to provide sufficient system control and information to an operator in case one or more computers in the system fail. The new console layout is shown in figure 5.

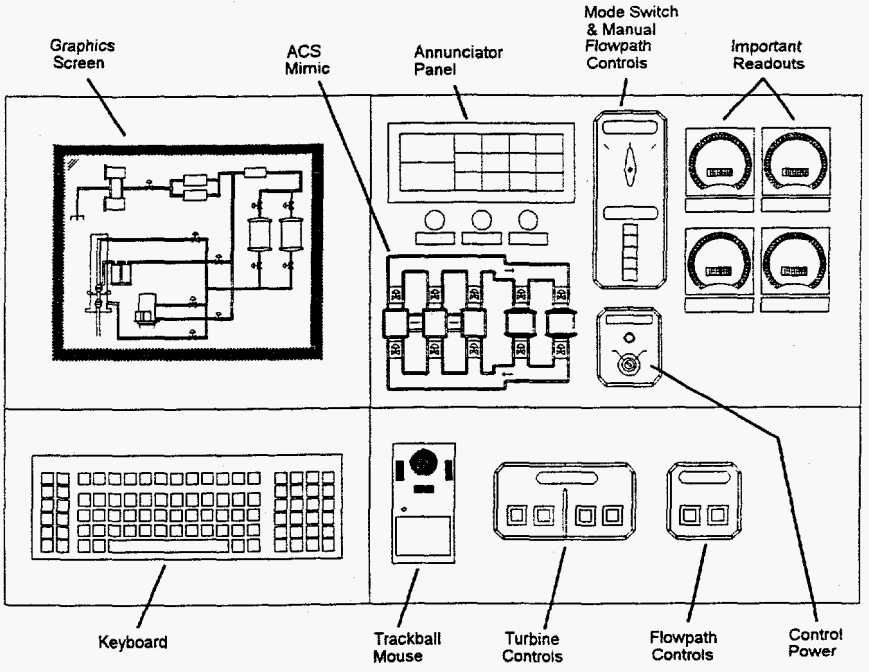


Figure 5: The Upgraded ACS Console

The graphics screen, keyboard and trackball were located on the left side of the console. During typical operation, the keyboard is not used but is stored underneath a cover on the keyboard shelf. The trackball normally occupies a space on the keyboard cover. Ample space was provided on the console compartment to the immediate right of the keyboard shelf to permit the trackball and keyboard to be used together under certain circumstances. The turbine and IBC flow controls are used frequently and are therefore placed on the horizontal control surface. The annunciator panel was placed in the upper middle part of the ACS console to provide good visibility of alarm conditions and because it is used with the graphics screen when alarms occur. The two alarms in the left-most annunciator section, "ACS LOW FLOW" and "ACS LOW-LOW FLOW" occupy larger annunciator windows than the rest of the alarms because of their importance as related to ACS technical specifications. The five alarms in the center annunciator section are needed to provide notification of conditions related to subassembly cooling or temperature, or conditions which could adversely affect systems connected to the ACS during transfers. The right-most annunciator section provides notifications of computer failures and alarm conditions detected by the ACS console computer. Valve indicating lights and flow and pressure readouts were positioned on the ACS

console for good visibility. The ACS control power keyswitch, the operating mode selector switch and the manual flowpath controls were positioned on the vertical portion of the ACS console because they are operated less frequently and also to minimize the chances for accidental operation during fuel handling. Lines of demarcation and component spacing were used to aid in separating functional control groups and components.

The FUM Panel

Utilization of a touch screen on the FUM panel allowed some discrete meters and indicators to be eliminated while providing better overall system information. Unlike the ACS, the FUM is operated manually and therefore requires several groups of manual controls on the FUM panel. Items needing to be retained as discrete items on the new FUM panel were identified and relocated into sequentially operated functional groups as shown in figure 6.

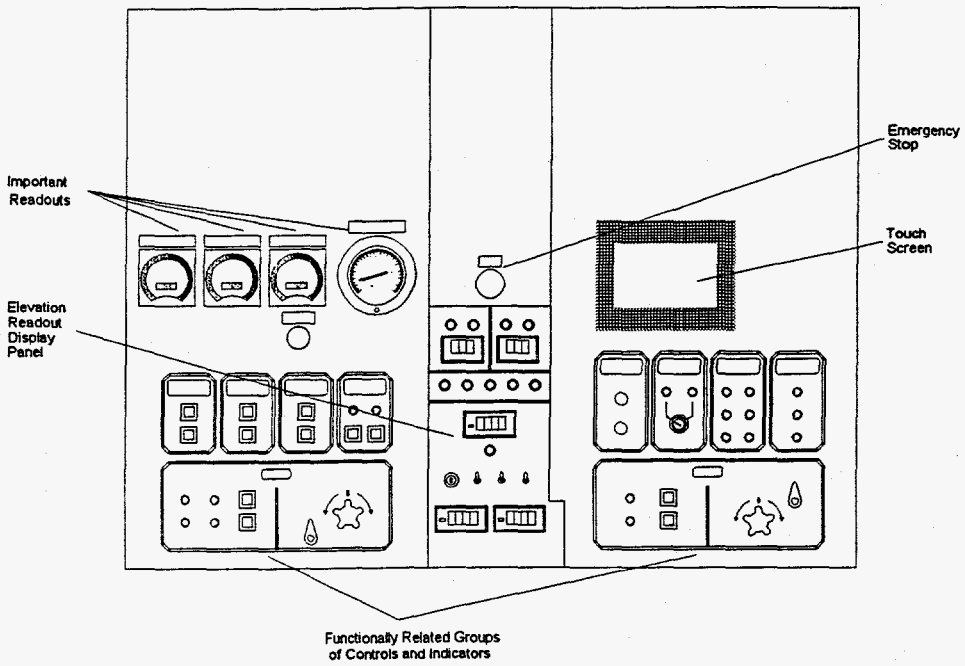


Figure 6: The Upgraded FUM Panel

Improvements to the FUM panel were possible due to the elimination of unnecessary items from the FUM panel, the computerization of the FUM and ACS, the addition of a touch screen, and by selecting better components. The layout reflects an attempt to make the panel more aesthetically pleasing. Because there is limited space for moving around on the FUM, all controls and displays remained positioned on the vertical panel. In general, the controls and displays were lowered to a more accessible level. Lines of demarcation and component spacing were used to aid in separating functional groups and components. To the largest degree possible, functional groups were arranged sequentially, according to their order of use. Within the functional groups, pushbutton controls that operate equipment that moves up and down were arranged vertically. Both sides of the panel were arranged to give the panel symmetry. The touch screen provides information useful when operating the controls on either side of the FUM panel so it is positioned near the center of the panel. The emergency stop pushbutton is located in the center of the panel and functions to physically removes electrical power from all of the FUM motors.

ACS Console Graphics Screen

The operator at the ACS console normally interacts with the ACS through graphical screens on the SPARCstation 20 inch color graphics monitor. A typical screen is shown in figure 7. The graphical screens allow the operator to monitor restricted fuel handing operations as they occur, to view complete systems or subsystems, and to change setpoints and respond to alarms. The screens show system details down to the individual control computer inputs and outputs.

The graphics screen consists of seven areas called viewports. Viewports are rectangular areas on the screen where graphics or text can be displayed. Figure 7 shows all seven viewports. At the upper left is the select main view viewport; across the top are the alarm indication viewport, the date/time viewport, and the communications status viewport; below these viewports is the message viewport; below the message viewport is the main view viewport; and at the lower left is the manual valve operation viewport. The main view viewport, which comprises most of the screen, shows any one of eighteen views of the FUM and ACS. The other viewports do not change except to show pushbutton, alarm status, date and time, communications status, message, or manual valve operation changes. For example, figure 8 shows the results of selecting another main view. Note that the left and upper viewports appear basically the same as in figure 7.

The eighteen views are setup; FUM elevation; ACS view; turbines; vapor trap and molecular sieve; fuel transfer port and interbuilding coffin; FUM; valve status; FUM gripper elevation status; FUM gripper status; FUM carriage status; FUM locator pins status; FUM shield and seal status; rotating ports status; interbuilding coffin status; turbine, pressure, and heater status; power status; and miscellaneous status. The FUM elevation and ACS view are shown in figures 7 and 8. The last eleven status views are more text based and show the status of items down to individual control computer I/O level. The first seven screens are more graphical object based and show the FUM and ACS from a system and subsystem level. All of the views, whether text or graphical object based, use color, text, number, move, fill, graph, or visibility dynamics to show the changing status of the items being displayed. These dynamics are updated every 250 milliseconds to reflect real-time changes to the FUM and ACS.

Colors, object shape, and messages are used to convey status changes, function, and information to the operator. Blinking red signifies a component or input in an abnormal condition that requires, at least an operator acknowledge. Steady red signifies a component or input that is abnormal whose condition as been noted and acknowledged by the operator. Rectangular green objects function like an indicating light telling the operator of the normal status of an item. Rectangular red objects tell the operator that an item is abnormal. Objects that are shaped like buttons can be clicked on with the trackball button to make selections. Button objects that appear depressed show selections that have been made.

In the main view viewport system operational changes are shown by objects changing position and/or colors. For example, in the FUM elevation view, the FUM moves back and forth on the FUM rail; the FUM gripper moves up and down; a subassembly object is shown on the FUM gripper; the rotating and sliding ports rotate and move; timer indication bars unfill; and components, valves, and pipes change color or fill to show that they are open and have gas flow.

The screen layouts, colors, and dynamics are consistent with similar control systems in the EBR-II plant. This was done to provide the same look and feel to the operators. This ensures that there is a minimum of confusion when going from one control system operator interface to another and, as a result, minimizes the chances of an operator error or misinterpretation.

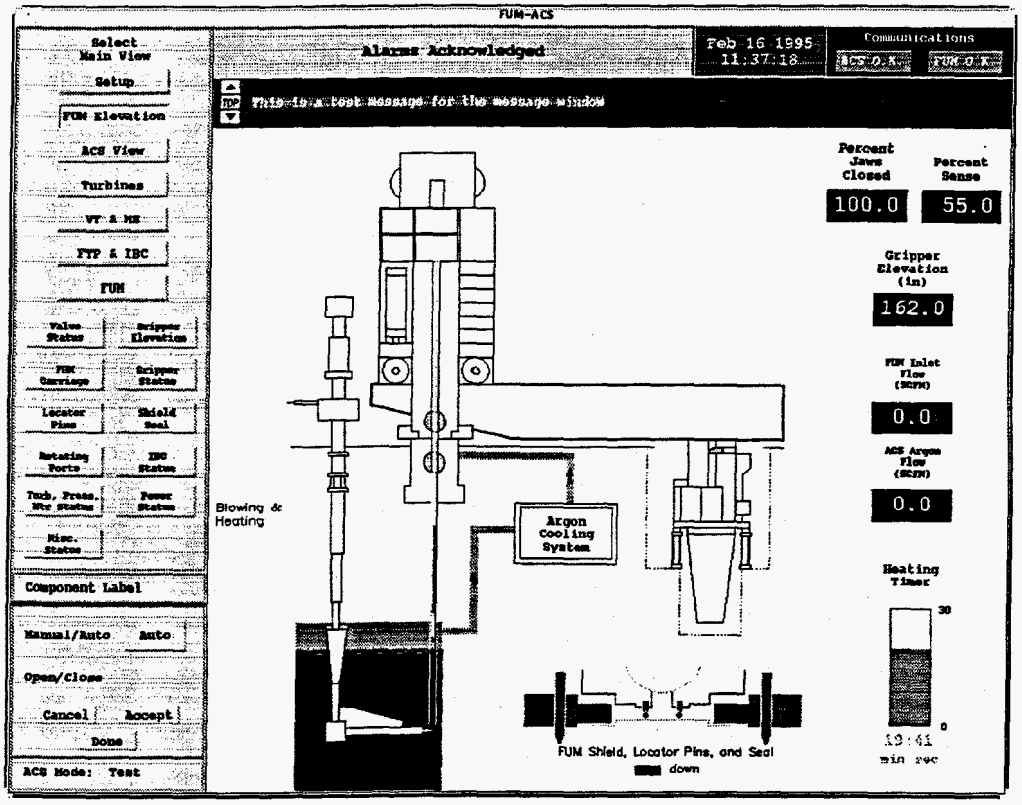


Figure 7: SUN SPARCstation Graphics Screen - FUM Elevation View

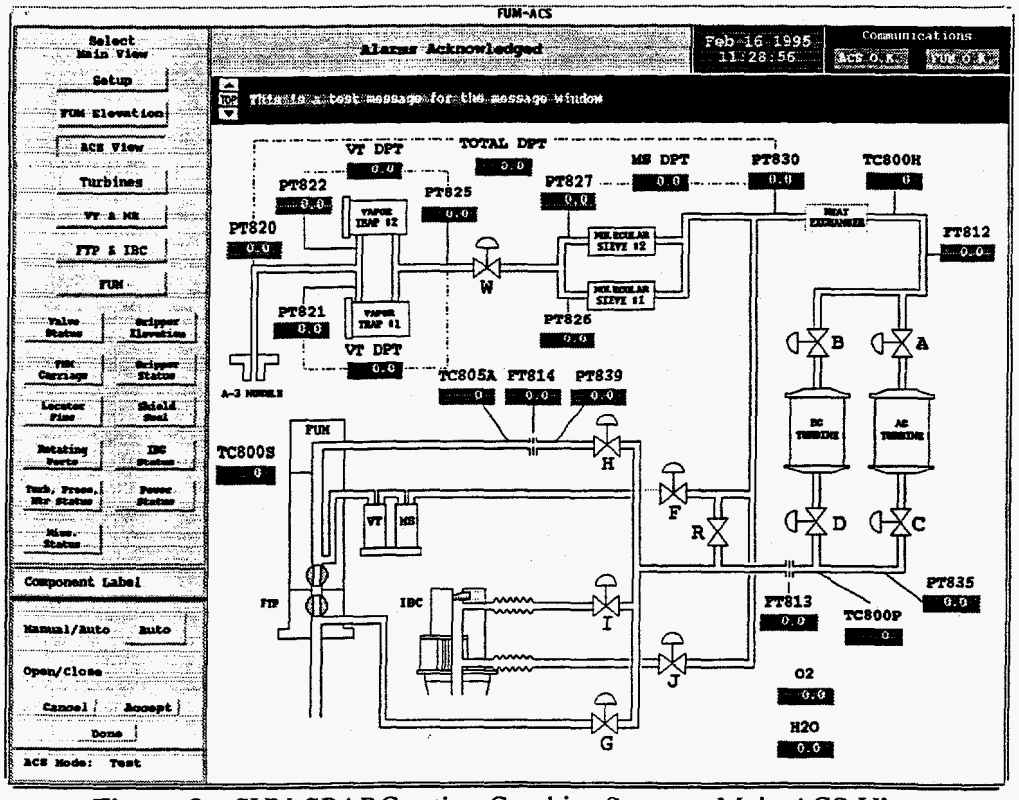


Figure 8: SUN SPARCstation Graphics Screen - Main ACS View

SOFTWARE DEVELOPMENT AND SIMULATION

Software development for this upgrade uses a structured engineering approach involving conceptual, preliminary, final and code implementation phases. The software is designed and prototyped through the conceptual and preliminary engineering phases and final code was developed through the final and implementation phases. Reviews are held for each of the phases with code walkthroughs at intermediate points.

All code development is initially done on a workstation. The code is written in C for portability. During development, the console and control computer code are implemented as three separate tasks that are subsequently integrated to allow the entire system to be simulated and tested at this level. The code for the control computers is written using compiler directives so the same code could be used on the target system hardware. Code is written to simulate the system I/O. During simulation, the actual touch screen and VT-100 maintenance terminals are connected to workstation serial ports to allow interaction with the screen software in the same manner as in the final system. This approach to software development and testing allows realistic operation of the control software and operator interface for demonstration, training and operator feedback purposes.

The code for each control computer is moved to a personal computer where it is downloaded to the target STD bus systems. The target code is debugged and tested on the target system using a remote debugger. At this point, the software and prefabricated system hardware are integrated and tested to verify proper cabinet wiring, software I/O and display operation.

After the control computers are installed in the system, individual sensors are read in and each actuator is activated to verify that the wiring from the ACS system to the cabinet terminal strips is correct. Minor software changes are made at this point as necessary and verified for correctness before the final software is programmed into flash PROMs and the system is operated in its final configuration.

This software development and checkout method provides a hierarchical approach to a final computer control system. Each step completes, debugs, and verifies correct operation of some level of the software. The workstation step completes the higher level control and screen software; the remote debugging step completes hardware specific setup, driver, and interrupt handling software; the STD bus I/O cabinets remote debug step completes and verifies software and hardware out to terminal strip interfaces; and, after installation in the system, the final step completes and verifies hardware from the terminal strips out to the sensors and actuators. This approach localizes checkout and debugging to appropriate levels of the hierarchy; items that are further up the hierarchy having already been checked and verified, would not be the location of problems that appear at a lower level.

CONCLUSION

The ACS upgrade utilizes modern computing and I&C technologies to correct original system design deficiencies and improve the reliability, availability, operability, maintainability, and safety of the system. Selection of modern instruments, computers and components with high mean-time-to-failure reliability data increases system availability. Computerization of the control system provides more comprehensive and understandable information to the fuel handling operators via a graphical user interface. Maintenance is simplified by modern instrumentation, by digitizing analog I/O signals and standardization. Safety is improved by understanding the types of failures that can occur, the effects of those failures, and making design decisions that mitigate consequences of failures, as well as prevent them. The analysis process used in this upgrade was useful in establishing high-level design philosophies based on system needs that

may not have otherwise been perceived. While it is virtually impossible to design and implement a perfect system, this upgrade, because it is centered in computer technology, will allow future design enhancements, such as advanced system diagnostics, that could not have been implemented with the old system.

REFERENCES

1. "Guidelines for Control Room Design Reviews," *U.S. Nuclear Regulatory Commission*, NUREG 0700, September 1981.

2. J. L. Seminara, "Effective Plant Labeling and Coding," *Electric Power Research Institute*, EPRI NP-6209, December 1988.

3. W. E. Woodson et al., Human Factors Design Handbook, McGraw-Hill, Inc., New York, NY, Second Edition (1992)

4. G. G. Peters, D. D. Wiege, and L. J. Christensen, "EBR-II Fuel Handling Console Digital Upgrade", Proceedings of the 9th Power Plant Dynamics, Control & Testing Symposium, Knoxville, TN, (1995).

5. J. D. Staffon and G. G. Peters, "EBR-II Cover Gas Cleanup System (CGCS) Upgrade Graphical Interface Design", Proceedings of the 8th Power Plant Dynamics, Control & Testing Symposium, Knoxville, TN, (1992).

6. R. B. Carlson and S. E. Start, "Embedded Systems for Control Applications in EBR-II" *Proceedings of the Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies*, Oak Ridge, TN, (1995).

DISCLAIMER