PROVIDING AUTOMATED CONTROL FOR PBFA-II*

Victoria M. Italiano
Pulsed Power Operations Division
Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract

Four levels of control are available to the operator in the Particle Beam Fusion Accelerator II (PBFA-II) control/monitor system. At the lowest control level, remote manual, the operator is responsible for all accelerator control and coordination. He is also responsible for interpreting sensor and actuator values to determine the state of the accelerator. At the highest control level, auto-staging, the computer integrates the sensor and actuator values into reports it presents to the operator. The operator can control several accelerator subsystems with single auto-staging commands that the control/monitor system interprets into sequences of integrated functions. The control system is being implemented from the bottom up, from remote manual to auto-staging--but will not be completed until well into the characterization phase of the PBFA-II project. Control action tasks are being integrated now with no major changes to the control/monitor design. Once the control action tasks are completely implemented no more changes are expected in the design. The higher level control systems should be easily implemented. This paper is an overview of the control/monitor system and will discuss each control level of the system.

Introduction

The PBFA-II control/monitor system was designed to be operated in automatic mode. This approach to the design of the control system is a departure from the approach used in PBFA-I. The PBFA-I control system was originally designed to operate in manual mode; higher control levels were added on after the facility went into operation [1]. The disadvantage of using this bottom-up design philosophy is that the lower control level, remote manual, may not support the new higher control level, control action tasks. The possible solutions to this problem are to redesign and implement a new remote manual control system to support the control action tasks to be added or to limit the scope of the control action tasks to use existing remote manual constructs--the resulting control system may not work efficiently or acceptably.

Because PBFA-II was a new facility we used a different design philosophy based on experience gained from PBFA-I. A top-down design philosophy was used. We designed the automatic control mode to be the normal mode of operation. This does not mean no lower levels of control were designed and implemented. What it does mean is that we designed all the control levels and that the entire control system supports automated control.

Although we used a top-down design philosophy, we are implementing the control system from the bottom up. Remote manual, the lowest control level, has been implemented and is being used to test each accelerator subsystem as it is integrated into the accelerator facility. Control action tasks are being added for each subsystem that requires this level of control. Integrated functions and auto-staging will be added throughout the accelerator characterization phase of the project.

Bottom-up implementation is an efficient way to test both the accelerator subsystems and control software because only one element in the test is unknown. The remote manual software was tested fully using a simulator. Using a simulator was acceptable because remote manual is a straight forward implementation that uses and displays actual sensor values (that have been linearized to be displayed in the proper units). The operator manipulates the values of actuators, which can also be displayed. We are using remote manual to test accelerator subsystems as they are added to the facility. Once the accelerator subsystem has been tested, control action tasks can be added to the control system and tested.

Bottom-up testing forms a pyramid in the amount of testing to be done. Testing the accelerator subsystems using remote manual requires the most number of tests because all the sensor and actuator points must be tested. Control action tasks require fewer tests because only the coordination of the actuator commands and the reports that are generated must be tested. Integrated functions use control action tasks and auto-staging uses integrated functions. Since each new control level that is tested interfaces with the next lower control level, a control level that has been tested, fewer tests are required as higher control systems are implemented.

Control Philosophy

PBFA-II control philosophy was originally set down in the PBFA-II control system plan. This plan outlined a list of operation criteria that has been satisfied by software and by administrative control [2]. The basic philosophy is that the PBFA-II control system must allow safe operation of the facility but at the same time support operators with little or no computer experience. Stated simply, it must work but be user friendly. Making the control system work is met by designing and implementing at least one level of control--usually satisfied by remote manual. Making it user friendly is a reason for the higher control levels.

An overview of facility operation

The PBFA-II facility will operate in two modes: idle mode and shot mode [3]. Idle mode is the normal mode of operation. It supports system configuration, diagnostics and maintenance, and monitoring. The shot mode supports shot preparation and the high voltage system. The mode is determined administratively.

Each mode is divided into policies. A policy determines which commands and displays are available to the operator. It can also limit which control levels are available. The idle mode policies are unattended monitoring, offline operations, and maintenance operations. Unattended monitoring allows accelerator subsystems to be monitored when the control room is unattended and no shot preparation or

*This work is supported by the U.S. Dept. of Energy under contract DE-AC04-76DP00789

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 1985	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Providing Automated Control For PBFA-II	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Pulsed Power Operations Division Sandia National Laboratories Albuquerque, New Mexico 87185**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM002371. 2013 IEEE Pulsed Power Conference, Digest of Technical Papers 1976-2013, and Abstracts of the 2013 IEEE International Conference on Plasma Science. Held in San Francisco, CA on 16-21 June 2013. U.S. Government or Federal Purpose Rights License

14. ABSTRACT
Four levels of control are available to the operator in the Particle Beam Fusion Accelerator II (PBFA-II) control/monitor system. At the lowest control level, remote manual, the operator is responsible for all accelerator control and coordination. He is also responsible for interpreting sensor and actuator values to determine the state of the accelerator. At the highest control level, autostaging, the computer integrates the sensor and actuator values into reports it presents to the operator. The operator can control several accelerator subsystems with single auto-staging commands that the control/monitor system interprets into sequences of integrated functions. The control system is being implemented from the bottom up, from remote manual to auto-staging--but will not be completed until well into the characterization phase of the PBFA-II project.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT	b ABSTRACT	c THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**4**	

maintenance operations are running. Alarm reports, action reports, and accelerator subsystems states are recorded. Offline operations remove control and monitor capabilities from the system to allow reconfiguration, maintenance, and development activities. Maintenance operations provide routine maintenance and diagnostic functions. This will allow accelerator subsystems to be exercised using remote manual and control actions. Shot mode has two policies, shot preparation and high voltage. Shot preparation provides functions to prepare the facility for a high voltage shot but does not include high voltage charging. The high voltage policy provides high voltage charging, arming, and firing capabilities.

Overview of control system

All modes and policies are supported by the four basic control levels: remote manual, control action tasks, integrated functions, and auto-staging. All control levels use some or part of the control features that extract sensor values from the accelerator and manipulate actuators. The basic features of the control system include exception reporting of changes in sensor values, a report methodology to handle six types of reports including action reports, alarm reports, and milestone reports, a system to route reports to appropriate monitors, and monitors to display state information and provide the operator with a means to control the subsystem. How each control level uses these basic features and other features unique to a control level is discussed in detail in the following section.

Control Capabilities

The PBFA-II control/monitor system provides the operator with four levels of accelerator control. Each control level is defined by six features (of which three reference the operator and three reference the computer). The relationship of these features to each control level is displayed in Figure 1. These features are listed below:

- o the feedback information the operator requires to run an accelerator subsystem properly
- o the type of accelerator subsystem model the operator uses to successfully control the accelerator subsystem
- o what level of detail the operator must know about the equipment of an accelerator subsystem to coordinate its operation properly
- o the number of algorithms the computer provides for controlling an accelerator subsystem
- o the number of algorithms the computer provides for proper coordination of an accelerator subsystem and the accelerator facility
- o the type of feedback the computer provides to the operator so he can ascertain the status of an accelerator subsystem and the accelerator facility

Each level of control is described in this section using these features as baseline qualifications.

Remote manual

Remote manual is the lowest level of control provided by the control/monitor system. At this level of control the operator is responsible for all accelerator subsystem control and coordination. A process and instrumentation diagram (P&ID) is a good model of the accelerator subsystem to use because the operator must understand how the accelerator subsystem operates in great detail since he controls the subsystem by manipulating individual components within the subsystem. To determine the status of the subsystem the operator uses a set of linearized sensors displayed on a monitor.

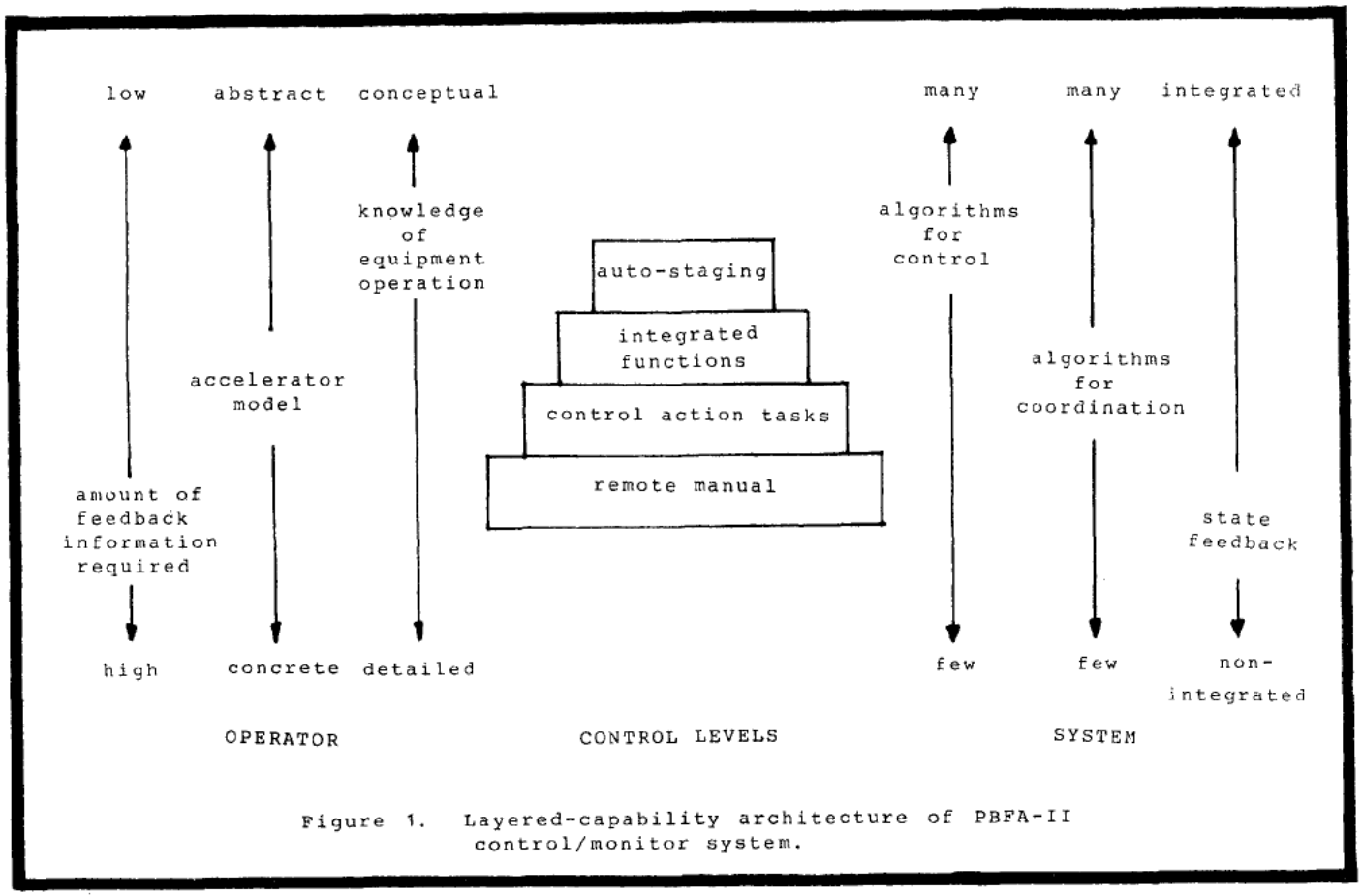

Figure 1. Layered-capability architecture of PBFA-II control/monitor system.

Remote manual uses a generic 22-line monitor to present information to the operator. The operator requests the sensor points he wishes displayed when the monitor is brought up. This monitor lists the sensor points by name and gives the current value, the point engineering units, and the time the report was posted. This information is used to determine the state of the accelerator subsystem. Actuator points can be manipulated using this monitor and the current actuator values are also displayed.

The control/monitor system is responsible for providing the operator with current point values and responding to actuator commands. At this level of control, the computer does not provide any algorithms for control nor coordination. It cannot prohibit or initiate any action.

Because remote manual requires the operator to process a lot of feedback information, to ascertain the accelerator subsystem status and provide a lot of actuator commands to coordinate the subsystem, it is to be used primarily for diagnostics and maintenance. Since the computer cannot prohibit any action, it does not provide any form of protection for the safety of personnel or accelerator subsystem equipment. Only the operator provides this protection. Few operators will be allowed to operate an accelerator subsystem at this level.

This is an example of a control sequence to fill the water tank to a specified level. An operator has to open a series of valves between the storage tanks and the accelerator tank plus bring a set of pumps up to speed to start filling the tank. He would have to monitor sensor points to determine the level of the water in the tank. Once the tank has reached the target level, the operator would have to close the valves and shutdown the pumps to stop filling the tank.

Control Action Tasks

Control action tasks is the next level of control available on PBFA-II. At this level the operator is responsible for accelerator subsystem coordination but the control action tasks provide control. A PID is too detailed to use as a model at this level. The operator needs more of a flow chart for a model to outline the sequence of tasks for proper coordination.

Related groups of control action tasks are presented on a custom-designed display monitor. The monitor has a group of touch buttons that are used to input operator commands. Commands are presented as tasks; fill the water tank, fill the oil tank, charge the Marx generators. The control system translates the operator command into a sequence of actuator commands to control the accelerator subsystem. Subsystem status is displayed on a monitor for the operator along with messages that announce the state of the control action task. Subsystem state information can be displayed either in reports or in graphic form, such as bar graphs that display the relationship between target state and the current state. Because the information is viewed graphically, the operator does not have to be concerned with actual sensor values.

An example of a control action task in the water transfer subsystem is filling the water tank. The operator specifies the level the water tank should be filled to and then commands the system to fill the tank. The control action task sequences the actuator commands to open valves and bring pumps up to speed. It monitors the water level in the tank until the target level is reached, then it shuts down the pumps and closes valves to stop the water flow into the tank.

Integrated Functions

The next level of control is integrated functions. At this level of control the operator and the computer share the responsibility for coordination but the computer is responsible for control. The same type of model can be used as that used for control action tasks because integrated functions are much the same as control action tasks. But there is one important difference. An integrated function can prevent the operator from initiating a command. It contains a set of permissive state variables (status points from the same accelerator subsystem and other related subsystems) that must be satisfied before an operator request will be initiated. If these values are satisfied the computer will process the command as described in the previous section on control action tasks. If these variables are not satisfied, the computer will not initiate the command. The accelerator subsystem is in a state that does not support the operator request. The operator will be told the reason the command was rejected.

Integrated functions use the same type of monitor as the control actions tasks, but this monitor intercepts the operator request to check the permissive state variables. If the permissives are met the monitor will initiate a control action task. These functions can prohibit actions but cannot initiate any unsolicited actions.

Auto-staging

Auto-staging is the highest level of control available to the operator and should be considered the normal mode of operation. At this level of control the computer provides both coordination and control. Auto-staging is a control level that allows the operator to manipulate a group of accelerator subsystems by initiating a single command. A useful accelerator model is a flow chart in which each block contains integrated functions from several accelerator subsystems--as opposed to control action tasks that involve only one accelerator subsystem in control and coordination and integrated functions that involve one accelerator subsystem in control and many in coordination.

The operator uses commands to prepare the support systems, charge and fire the accelerator, and shutdown the facility. He does not need to know how individual accelerator subsystems work; he needs to understand how the facility operates. The computer provides integrated feedback in the form of action reports that explain what actions the auto-staging sequence has initiated and milestone reports that describe the accelerator target states that have been reached. This information is integrated by the computer to decrease the amount of information presented to the operator. Although he is provided few reports, the reports have a lot of meaning.

This level of control is very powerful. A single operator command can initiate several accelerator integrated functions, either together or in sequence. This is the only control level in which the computer can initiate integrated functions unsolicited by the operator. The single auto-staging command begins a sequence of integrated functions. Some at the time the auto-staging command is initiated and others when specific accelerator states are reached.

Each integrated function (as described in the section on integrated functions) must satisfy its own

set of permissive variables before it initiates the control action task. While the integrated function is running, the auto-staging sequence is monitoring a set of continuation state variables (a set of accelerator state variables that must be satisfied continually while an integrated function is running). If these variables are not completely satisfied the auto-staging function will generate an alarm report. The computer will suggest a course of action the operator can take to correct the alarm condition. If enough information about the failure is anticipated, the computer could automatically initiate the corrective integrated function. If it does this, it will inform the operator of the action it took.

Auto-staging has the most complex type of monitors because accelerator coordination is involved. The monitors contain segments to check permissive state variables for integrated functions, segments to coordinate groups of integrated functions, segments to check continuation state variables, and segments to handle alarm conditions when the continuation state variables are not met. This monitor may respond to accelerator alarm conditions by informing the operator of its actions or by handing coordination back to the operator.

Mechanisms of Control

The control/monitor system contains a three-tier hierarchy of computers that partition the functions of control and feedback. The lowest level computer, the I/O processor, is responsible for providing reports of changes in sensor values and to implement changes to actuator values. For sensor values, the operator can specify the amount of change that must occur before a sensor point value is reported (threshold) and he can specify the limits of acceptable value (values outside these limits are considered alarms).

While the lowest level computer is dedicated to point-by-point control and feedback, the second level computer, the subsystem control unit, is concerned with implementing control action tasks and packaging reports. The control action task is run at this level because the bottom two computers communicate quickly (they are located in the same chassis) and because it unloads some of the responsibility from the host computer (the highest level). The control action tasks require a tight feedback loop to safely control an accelerator subsystem. Packaging reports is a task that resulted from the characteristics of the communications link between this computer and the host.

The host computer is the highest level computer. It contains all responsibility for coordination and operator interface (providing monitors). Commands to control action tasks are generated at this level by integrated and auto-staging functions. The monitors are updated using a data base, maintained in the host, that contains the current sensor values. This data base also contains information that characterizes each sensor point. Another data base is used to store the accelerator parameters that are used as target states in the control action tasks.

Conclusion

Some or all standard control mechanisms support each control level. Remote manual has been implemented and control action tasks are being implemented now. The implementation and integration of these control levels into the system is on schedule. The major effort in the design of the control action tasks has been specifying how the each task should be coordinated. No mechanisms of control have been redesigned to support these control tasks. Implementing the higher control levels should follow the same pattern; emphasis should be placed on characterizing the coordination of the accelerator facility and no control mechanisms should have to be redesigned.

Acknowledgements

The PBFA-II control/monitor system design is the result of work by members of the control/monitor design team. The design team is made up of members of Sandia National Laboratories and EG&G WASC, Albuquerque.

References

1. J. L. Spiller, "Implementation of Automated Control on PBFA-I," 5th IEEE Pulsed Power Conference, June 1983, Arlington, Virginia.

2. S. Y. Goldsmith, S. A. Goldstein, and M. T. Butler, "PBFA-II Control/Monitor System Plan--Priority 1 System", Unpublished Sandia Internal Report, June 1983.

3. Control/Monitor Team, "PBFA-II Control/Monitor System Initial Design", Unpublished Sandia Internal Report, March 1984.