SLAC-PUB-4936
March 1989
(A)

Distributed Supervisory Protection Interlock System*

Helmut V. Walz, Romain C. Agostini, Loy Barker,
Raisa Cherkassky, Ted Constant, Russ Matheson

Stanford Linear Accelerator Center
Stanford University, Stanford, CA 94309

ABSTRACT

The Distributed Supervisory Protection Interlock System, DSPI, is under development at the Stanford Linear Accelerator Center for requirements in the areas of personnel protection, beam containment and equipment protection interlocks. The DSPI system [1], distributed over the application site, consists of segments with microprocessor-based controller and I/O modules, local area networks for communication, and a global supervisor computer.

Segments are implemented with commercially available controller and I/O modules arranged in local interlock clusters, and associated software. Segments provide local interlock data acquisition, processing and control. Local area networks provide the communication backbone between segments and a global supervisor processor. The supervisor processor monitors the overall system, reports detail status and provides human interfaces.

Details of an R&D test system, which will implement the requirements for personnel protection of 4 typical linear accelerator sectors, will be described.

1. GENERAL DSPI SYSTEM DESCRIPTION

To implement interlock requirements for personnel protection and similar applications at SLAC's accelerator and storage ring facilities, which extend over several kilometers, a distributed system architecture with local area network communication is under development. The global DSPI system architecture is shown in Figure 1. Data acquisition and control of interlocks in a system segment are handled locally by programmable logic controllers (PLCs). Global system supervision and operator interfaces are provided by the DSPI host computer located at the Main Control Center (MCC). Communication between segments and with the system host is implemented with dual redundant local area networks (LANs). Dedicated, counter-rotating fiber-optics ring networks provide redundant paths for high-security transmission of interlock faults and segment permissives, system control and status, and test and diagnostic functions. System response on a beam pulse-to-pulse basis for a maximum Linac repetition rate of 180 Hz is assured by LANs of at least 10 MBit/sec transmission rate. LAN protocols and fiber optic medium provide the very high levels of safety and tamper resistance important in Personnel Protection System (PPS) applications.

The DSPI system host computer at MCC provides global supervision and verification, LAN management, operator workstation interfaces for system control, status data logging, and handles a system database. It is also linked to the MCC VAX computer of the accelerator control system for exchange of status information . The host computer and distributed PLCs of each segment connect to the fiber-optics cables through LAN gateways.

* Work supported by the Department of Energy, contract DE-AC0376SF00515.

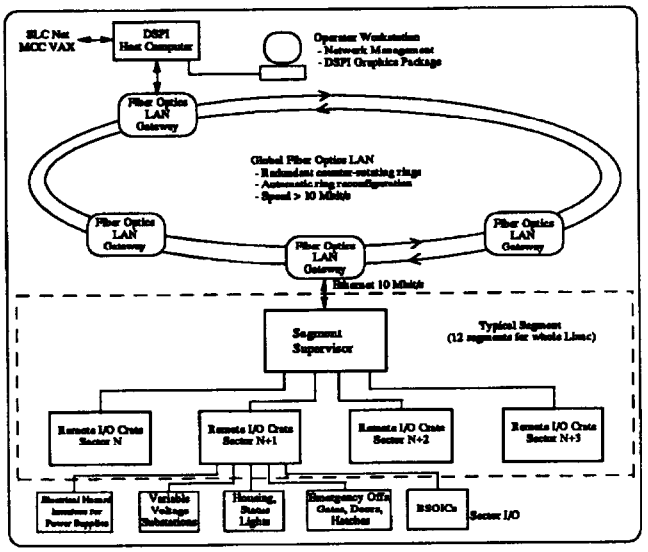

Figure 1: Global DSPI system architecture

At the segment level, a PLC system is utilized. A processor crate with CPU, memory, extension crate interface and LAN communication processor modules forms the segment supervisor. Peripheral I/O devices are connected to opto-isolated I/O modules which reside in remote I/O crates. These crates may be located several hundred meters from the processor crate. Each I/O crate forms a local interlock cluster with short connections for I/O channels. All sensitive interlock I/O is fully redundant. The PLC handles interlock data acquisition, processing of logic equations, control of interlock outputs, test-verify and output readback functions, and LAN communication with other segments and the system host computer. All software and interlock logic requirements are stored as firmware. Fail-safe interlock outputs and 'watch-dog' functions provide a safe shutdown in case of system failure.

Implementation of the DSPI system is based on extensive use of commercially available, fully modular hardware and software and standardized LANs.

2. DSPI SEGMENT DEVELOPMENT

To prototype typical PPS requirements for the Linac, we are implementing the PLC system for a DSPI segment.

2.1 Segment Programmable Logic Controller System

PLC hardware for a four sector Linac PPS segment is shown in Figure 2. A Siemens S5-150U system [2], consisting of a processor crate and four remote I/O crates, is used. One I/O crate will be installed in each sector; the processor crate will be mounted in one of the middle sectors resulting in a maximum interface bus cable length of approximately

220m to the most distant I/O crate. PPS peripheral input and output devices will be wired to the PLC I/O modules. Each sector I/O crate will have appr. 200 I/O channels installed for a total of 800 channels per segment.

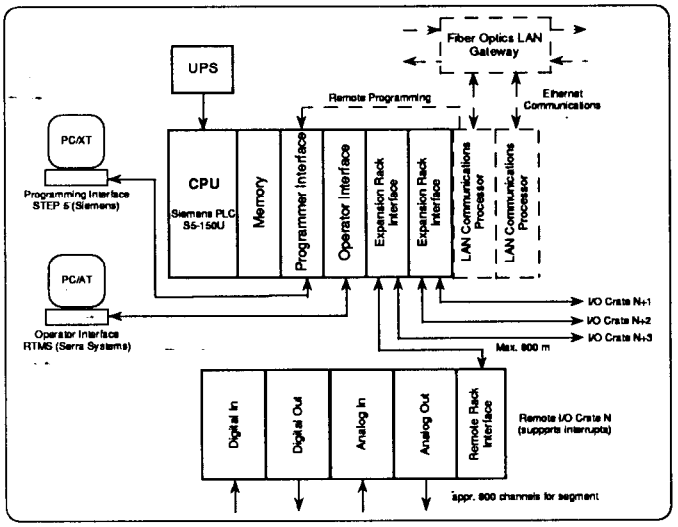

Figure 2: Hardware for a four sector Linac PPS segment

Initially, during prototype development and testing, no LAN connections will be implemented. Instead, two local PCs will provide programming and operator interfaces; also, the PLC system will be connected via I/O channels to the existing PPS system.

All PPS safety interlocks will be fully redundant from the peripheral I/O devices through the I/O module level. Additional I/O channels will be utilized to implement test-verify functions. Wiring of input signals will be fully tested; output signals will have read-back provisions. The user software, executed from non-volatile memory, will implement all local PPS interlock functions, background test-verify and communication functions. All I/O channels will be scanned in 2.2 ms maximum.

Development of this PPS prototype segment is planned in three stages. First, a computer simulation test will be performed. Instead of PPS peripheral I/O connections, I/O channels are connected to a second test PLC system which is also connected to the operator interface PC computer. The test PLC system will generate test vectors and acquire the associated interlock outputs. This simulation will provide an exhaustive test of segment PLC hardware and PPS applications software. The PC computer will evaluate stimuli and responses and will log test data.

After concluding this simulation test, approval and certification by the Radiation Safety Committee will be sought, to allow connection to the active PPS system. Finally, all PPS I/O connections will be installed and evaluation of the prototype segment as a 4 sector PPS system will start.

2.4 DSPI Software

The software consists of the following entities:

- S5-DOS operating system on an IBM PC compatible
- STEP 5 programming environment under S5-DOS
- STEP 5 runtime system (firmware) residing in the PLC
- STEP 5 user program (logic processing) running in the PLC
- RTMS runtime system on an IBM PC compatible
- RTMS user program (operator interface).

S5 and STEP 5 come from Siemens [3] and are used with their entire line of PLCs; RTMS is a generic operator-interface package for interfacing to a multitude of controllers [4].

2.4.1 S5-DOS/STEP 5 PLC Programming System

S5-DOS is an extension of the Personal CP/M-86 operating system; PCP/M-86 has to be installed on the PC in order to run this package. This means that a hard disk, controlled by MS-DOS, must first be partitioned and partially reformatted under PCP/M-86 before S5-DOS can be installed; about 5 MB of disk space are required.

STEP 5 is the proprietary Siemens programming language and environment for PLCs; it allows to edit logic blocks (create programs), handle files and control the PLC.

User programs can be written in three STEP 5 flavors: Control System Flowchart (CSF, boolean logic graphic symbols), Ladder Logic (LAD, schematic circuit diagrams graphic symbols), and Statement Lists (STL, similar to assembly language). If certain rules are followed, it is possible to transform user programs from one representation to another. STL, though, is the most powerful incarnation of STEP 5.

Dividing the overall program into self-contained modules ('blocks') leads to structural programming techniques allowing for easier debugging and standardization of commonly used sections (like functions and procedures in high-level languages). STEP 5 distinguishes between four major kinds of blocks: Organizational Blocks (OBs), Program Blocks (PBs), Functional Blocks (FBs) and Data Blocks (DBs).

OBs are only called by the runtime system; they determine the user program processing mode, cold and warm starts, and the handling of controller errors. OB1 typically contains only conditional and unconditional jumps to PBs and FBs. It is processed in an endless loop (*cyclic program processing*) like a main program. Several special OBs are called for PLC errors like time-outs, address error, illegal parameter substitution, etc. They may be regarded as exception handlers.

PBs are normally used for implementing logically self-contained software modules; they may in turn call other PBs and FBs. Nesting of blocks is allowed up to 18 levels. The main distinctions between PBs and FBs are that function blocks can only be programmed in STL (with an extended operation set) and can be assigned parameters.

Cyclic program processing is the 'normal' PLC operating mode. Another mode is *interrupt-driven processing* : cyclic processing may be interrupted by prioritized process (8) or user (4) events. OBs specific to the interrupts (comparable to interrupt service routines) are executed, and the processor returns to the point at which the cycle program was interrupted and continues normal processing. Cyclic processing can only be interrupted between blocks, and it can only resume after all pending interrupts have been serviced.

A third operating mode is *time-controlled processing*. Signals from an internal clock cause the processor in the controller to interrupt normal cyclic processing and to execute specific OBs.

The STEP 5 operations are similar to those of a microprocessor and include instructions for binary logic, timer and counter operations (start, reset, increment, decrement), load and transfer operations, comparison functions, block calls, jump operations (unconditional, conditional on zero, negative, positive, overflow), shift operations, etc.

2.4.2 The STEP 5 User Program

The I/O is processed locally in every segment, and only values or results from logic operations needed by other segments are transmitted on the network. After having executed a set of logic equations, the PLC system evaluates the local system in order to detect any integrity problems or hardware failures. If problems are detected, flag bits are set, alarms are given on operator interfaces and panels, and the system is shut down if the problem detected requires so.

Segments check their neighbors regularly and see whether they are still alive. If this check fails or an interlock violation is detected, an interrupt is generated, and a shutoff message is sent on the LAN to all segments.

In order to guarantee an acceptable interrupt latency, the DSPI software will be partitioned into logical modules and implemented in blocks of such a length that a maximum specified processing time per block will not be exceeded.

2.4.3 The Operator Interface Software

The man-machine interface for the DSPI R&D test system will be implemented with the Real-Time Monitoring/Control System (RTMS) on a PC/AT clone. It will consist of several color graphics pages showing the system state and allowing manipulation of the process (operator commands).

The package allows definition of up to 36 graphics screens ('windows'). Each item in a window can have several attributes, such as foreground/background color, blinking, etc. RTMS includes a special set of extended graphics characters which can be used for designing a window. Items created may be moved, duplicated and resized.

Upon system start, a 'startup' window is displayed; it is the entry point for the custom interface and normally represents a general system overview. Windows can be password-protected, either for viewing or for full access (allowing process command input).

Dynamic items in a window or whole windows may pop up on the screen, change color, start to blink or display a message as a reaction to a process event or user request. Numeric fields can be displayed as a number string or as an animated bar graph. Additionally, alarms can be logged with a specific message and a time stamp to a printer.

3. Global LAN development

The PLC system can be equipped with an Ethernet interface and related networking software (provided by Siemens) allowing the controllers to communicate with each other. Unfortunately, Ethernet has some limitations which make it inadequate for our use:

- limited cable lengths
- costly bridges if several Ethernet segments need to be connected together
- increasing number of collisions in a large system
- non-deterministic behavior

Most of those short-comings can be eliminated if a network based on fiber-optics is used. One way to achieve this in our case is to use Ethernet-to-fiber gateways. These devices, including all network- and protocol-related software, are readily available from a number of companies and have an Ethernet interface on the PLC side. If several Ethernet devices are directly hooked up to such a gateway, collisions are limited to the local traffic going to the gateway. If only one device is hooked up to the gateway, collisions are totally eliminated. On the fiber side, those gateways typically run a token-ring protocol (often at a speed well above the Ethernet speed of 10 MBit/sec) which eliminates collision problems right away. The only non-deterministic behavior of such a system is local to the Ethernet side of the gateways.

For redundancy and fault-tolerance purposes, two fiber-optics rings will be run in a counter-rotating fashion. That way, intelligent gateways can isolate faulty nodes and reach all remaining nodes even when one of the fibers is broken.

The LAN will be used for a variety of purposes:

- Intelligent, high-security and fast system-wide shutoff mechanism
- Reciprocal test messages between segments
- Compressed data collection for operator displays
- Hookup of remote diagnostic tools

In order to achieve the fastest possible shutdown broadcast message, the existing Ethernet access protocol will have to be altered in such a way that a transmission channel with minimal access time is achieved.

4. Development Plan

An upgrade of the Linac PPS system is being planned with several milestones. The simulation test of a DSPI prototype segment is expected by 9/89. Approval and installation as a four sector PPS system is planned by 11/89. A parallel effort to install and develop the fiber optic LAN will result in implementation of the first two LAN nodes by 1/90. Now the global DSPI LAN will be used to connect the prototype PPS segment to the operator interface PC computer, which will be relocated in MCC. To test network and system software required to support multiple DSPI segments, a second segment will be installed by 3/90.

Finally, the complete upgrade of the Linac PPS system with the installation of ten additional PPS segments and a final host computer and operator workstations is proposed to start by mid 1990. The final completion date will depend on funding, scheduling and manpower constraints.

5. References

[1] H. V. Walz, *Conceptual Design Report Distributed Supervisory Protection Interlock System DSPI*, Electronics Department Internal Report, SLAC, July 1987.

[2] Siemens Energy & Automation, Inc., Programmable Controller Division, Peabody, MA 01960.

[3] Hans Berger, *Programming of Control Systems in STEP 5*, Vol. 1 and 3, Siemens Aktiengesellschaft, Munich 1980.

[4] Serra Systems, *Real-Time Monitoring/Control System - User's Manual and Overview*, Serra Systems, Healdsburg, CA, 1988.