

SMART MACHINE PROTECTION SYSTEM*

S. Clark, D. Nelson, A. Grillo, N. Spencer, D. Hutchinson, J. Olsen
D. Millsom, G. White, T. Gromme, S. Allison, K. Underwood, M. Zelazny, and H. Kang
Stanford Linear Accelerator Center, Stanford University, Stanford, CA 94309, USA

Abstract

A Machine Protection System implemented on the SLC automatically controls the beam repetition rates in the accelerator so that radiation or temperature faults slow the repetition rate to bring the fault within tolerance without shutting down the machine. This process allows the accelerator to aid in the fault diagnostic process, and the protection system automatically restores the beams back to normal rates when the fault is diagnosed and corrected.

The user interface includes facilities to monitor the performance of the system, and track rate limits, faults, and recoveries. There is an edit facility to define the devices to be included in the protection system, along with their set points, limits, and trip points. This set point and limit data is downloaded into the CAMAC modules, and the configuration data is compiled into a logical decision tree for the 68030 processor.

INTRODUCTION

The Stanford Linear Collider includes a number of safety systems that shut down the Collider when unsafe conditions arise. When the Collider shuts down, it becomes difficult to diagnose the cause of the problem. Often it becomes necessary to terminate the startup multiple times before the problem(s) are corrected and safe continuous operation can resume.

Substantially more effective operation would result from a safety system that would report the cause of the fault from the origin of the equipment trip, allowing safe, lower repetition-rate operation to continue, so that the machine can be used to diagnose itself. Automatic return to higher-rate operation after repairs speeds recovery and allows automatic handling of system glitches.

PROPOSED ENGINEERING SOLUTION

A new Machine Protection System (MPS) is being installed in the SLC that will improve machine protection and utilization. The new system will continue to detect unsafe conditions on a pulse-to-pulse basis; however, it will now rate-limit the machine to continue operation at safe levels for diagnostic purposes. This new system utilizes stand-alone array processors to scan the set of fault detectors (radiation, temperature, flows, etc.), making rate limit decisions based on the type and severity of any detected faults, using machine configuration and parameter limit tables developed by machine and radiation physicists.

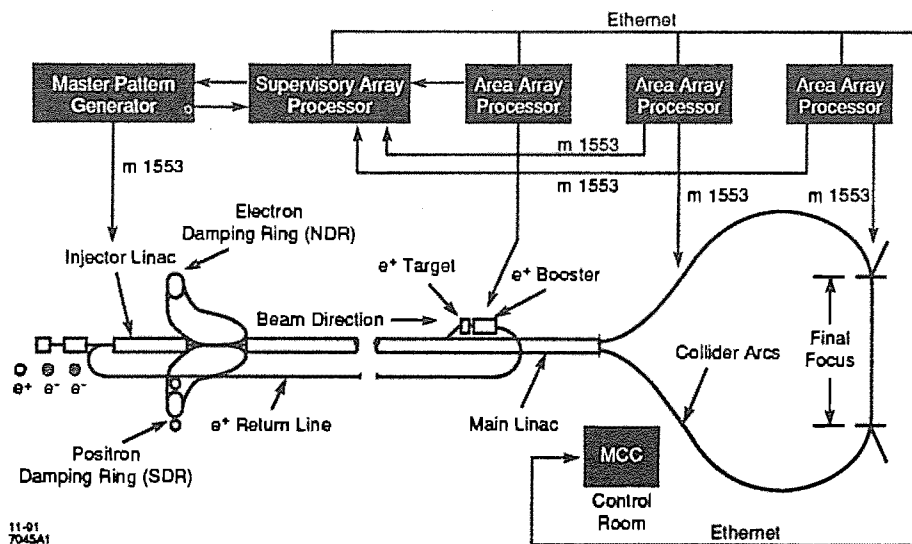
Facilities have been included to support logging of all machine state changes; the protection system forwards a message to the control room explaining which input signal faulted, and the nature of the fault. These processes allow operators to determine quickly and directly what the problem is/was and what remedial action is required, with a data trail available for later analysis or post-event review.

Beam rate control will be hard wired into the Master Pattern Generator (MPG) and the Injector interlocks used to control the accelerator, so that the machine can be shut down if the expected rates are not properly executed. Failures of sensors or communications failures in sensor processors are treated as if the associated device or included devices were in a worst case failure mode, and appropriate action is taken.

HARDWARE IMPLEMENTATION

The new system will be implemented as a loosely coupled element of the SLC control system, with common facilities on the CAMAC side, new elements built into VME systems, and integrated SLC user interface and applications facilities. As shown in Fig. 1, the system will

Figure 1.
MPS system architecture.



*Work supported by Department of Energy contract DE-AC03-76SF00515.

Content from this work may be used under the terms of the CC BY 4.0 licence (© 1992/2024). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

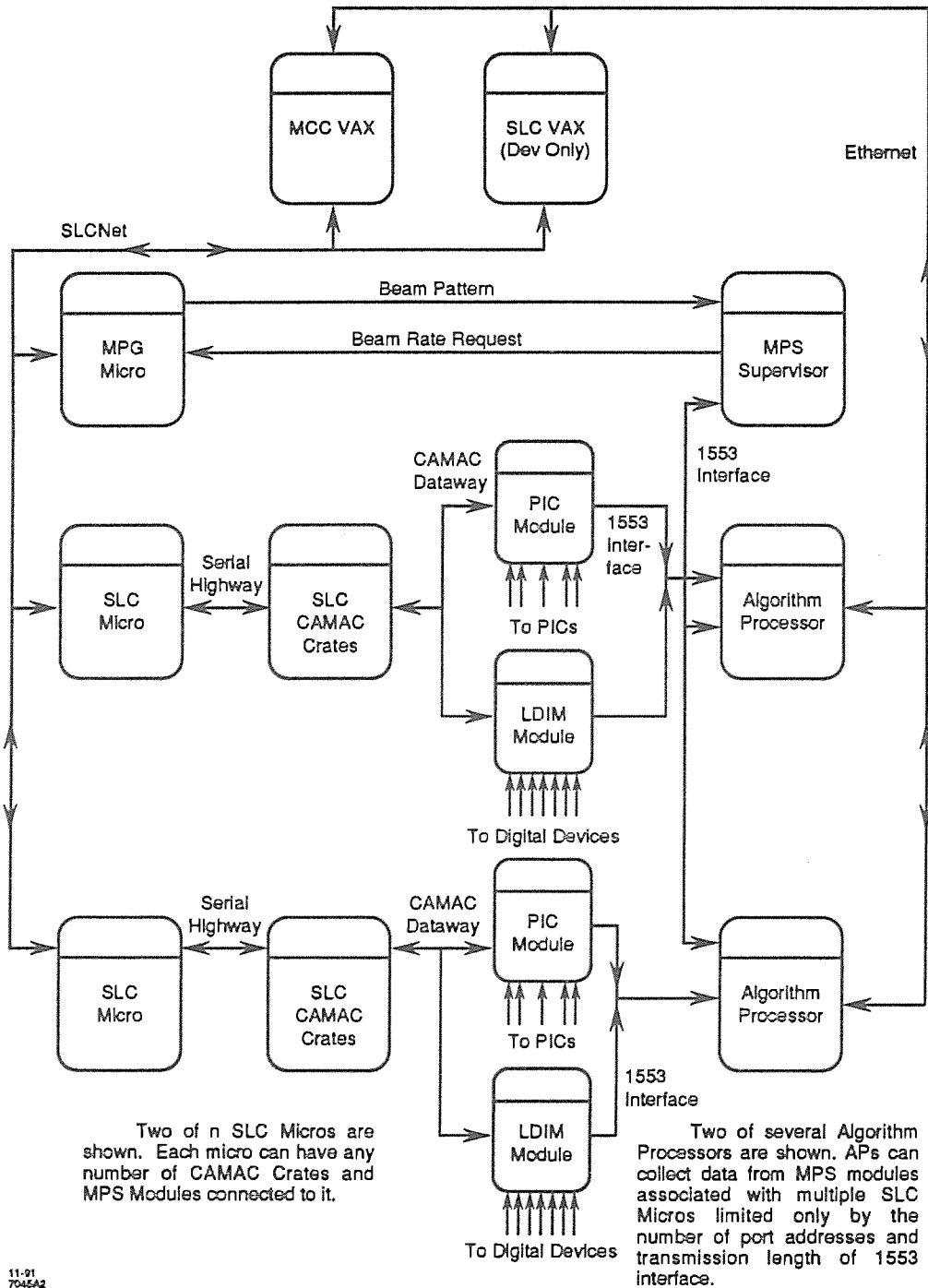


Figure 2. MPS computers and network.

Content from this work may be used under the terms of the CC BY 4.0 licence (© 1992/2024). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

Content from this work may be used under the terms of the CC BY 4.0 licence (© 1992/2024). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI

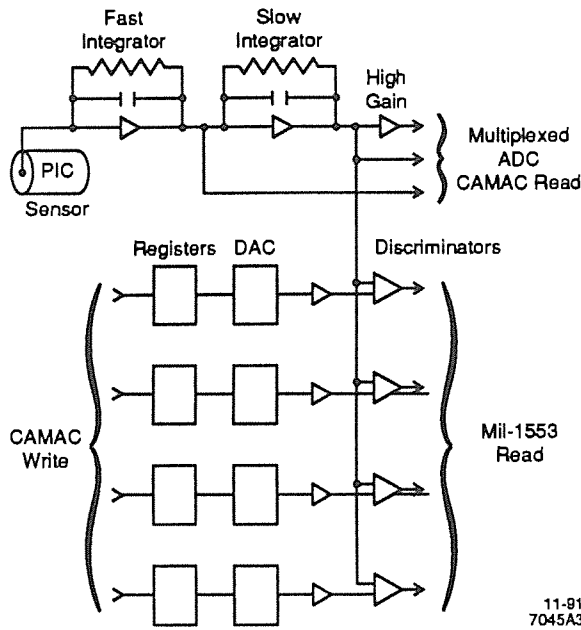


Figure 3. PIC Electronics.

be implemented in clusters structured around functional elements of the accelerator (Linac, Arcs, Final Focus, etc), or around subsystems (injector, positron system, etc.) as appropriate. A modular approach allows new systems to be phased into the overall machine protection system on an incremental basis.

The architecture is modular and consists of CAMAC sensor cards that condition sensor signals and generate go-nogo signals to an Array Processor, which scans these signals and passes on its own summary go-nogo signal to the next level supervisory array processor. The summary process leads to the MPG (see Fig. 2), which sequences the accelerator.

The system is being implemented first in the positron production system, supporting Protection Ion Chambers (PIC's). These Ion Chambers use custom CAMAC modules which interface the radiation sensor and implement the severity level measurements driving the go or no-go signal to the Array processor. Limit levels for the various machine repetition rates are loaded into the PIC from the SLC control system, and scale the acceptable radiation at each beam rate with some hysteresis for stability and automatic return to higher beam rates after the faults are resolved. A facility has been provided via the SLC control system to recover analog measurements from the PIC's for comparison or correlation.

These analog data channels originate in fast and slow integrators in the CAMAC electronics (see Fig. 3), which also drive presetable discriminators that provide the level control signals monitored by the array processors. The system also provides facilities for providing secure changes to level setpoints, and deliberate trips on these control signals to confirm the functionality of the full system and the correctness of the protection system logic.

Future hardware developments will include latched digital status inputs (LDIM), RTD temperature inputs, and Long ion chamber (PLIC). These devices will be set by the SLC control system, and communicate with the array processors via the 1553 bus as do the current PIC's.

System control and data connections are implemented using standard hardware and communication protocols. The real-time control connections between the sensors, the array processors, and the MPG are implemented using MIL STD 1553 as a secure, low-overhead, multidrop communication link (with technology borrowed from Fermilab and CERN). The separate Ethernet link, employing TCP/IP, is used for downloading configuration files, and provides the control room message link for passing the location and nature of any system faults. Both of these links are well-characterized standards, which offer flexibility, reliability, and convenience.

Array Processors (AP) are essentially programmable logic arrays implemented in firmware. These scanners are built from VME 68030 processors running C code on top of a real-time executive. These devices scan the various binary sensor inputs, and evaluate the significance of the signals based on configuration and response tables down-loaded from the VAX via Ethernet. These tables come from a special configuration editor and compiler resident on the VAX. Special security facilities control the integrity of the table transfers, and periodically confirm that no unauthorized or uncommanded changes have occurred in the AP database.

Supervisory Array Processors (SAP) are essentially AP's which combine the outputs of the AP's in the cluster, signal the MPG for beam rate control, and monitor the MPG's responses. This hierarchical model provides for flexibility in grouping MPS sensors, and provides rapid evaluation response by distributing the scan task. A SAP can interrupt the MPG's pipe-lined beam control sequence in 2-3 pulses before accelerator damage can occur. A SAP also has hard-wired access to the injector interlock system should it be necessary to override the MPG.

SOFTWARE IMPLEMENTATION

A configuration editor has been developed so that devices can quickly and accurately be added to the configuration files, using the appropriate boolean operators. This facility provides for the loading of action set-points, device limit parameter, normal device status, and accelerator operation configuration. These files are then compiled into the database for the array processor. The configuration editor then downloads data to the AP's via the Ethernet, and provides a change history and a verification facility to insure system integrity. There is a secure copy of an original or "gold" version of the configuration file which is maintained separately as a global check against all subsequent modifications.

There is a security facility that records equipment bypass actions as they are initiated, and requires that they be reauthorized by senior machine operators at the start of every shift. These listings serve as both a reminder of machine condition and a log of corrective actions yet to be accomplished.

Self-test software is being developed which allows the VAX to test the entire MPS network for continuity, as well as for the correctness of the trip logic. The VAX can initiate trip signals to any selected sensor module and channel, which will be acted upon by the array processors. The test demonstrates a closed loop in the system, and the type of response (limit or shut-down) demonstrates that the logic, limits, and response severity are as specified in the configuration database.

The communication networks were selected for their convenience and for conformance to accepted industry standards. The 1553 bus offers a fast, secure, low-overhead, and multidrop channel for communication between signal conditioning CAMAC cards and the various levels of array processors.

Ethernet with TCP/IP was selected for the message and data links since the messages can be long and there is no requirement for a real-time deterministic type of facility. This tied in nicely with the Ethernet remote debugger purchased with the development environment.

USER INTERFACE

The Control Room User Interface includes facilities to monitor the performance of the system, and track rate limits, faults, and recoveries. Touch panels are used for control, and a series of X-window screens indicate status, faults, and the analysis data from the various applications packages.

SOFTWARE DEVELOPMENT ENVIRONMENT

The MPS Application Software and array processor firmware were developed on the SLC VAX cluster. All software and firmware were developed in Ansi C, and commercially available development tools (such as remote network debuggers, real-time kernel facilities, and standard networks) were used extensively. The microprocessor firmware was developed in a cross-compilation environment and run on the pSOS kernel (Software Components Group).

Content from this work may be used under the terms of the CC BY 4.0 licence (© 1992/2024). Any distribution of this work must maintain attribution to the author(s), title of the work, publisher, and DOI