THE RUN PERMIT PROTECTION SYSTEM FOR GTA *

W. H. Atkins and R. G. Jones
Los Alamos National Laboratory
P.O. Box 1663, Los Alamos NM 87545

Abstract

A Run Permit system has been designed for the Ground Test Accelerator (GTA). The system implements mode-dependent software interlocks to ensure proper operation of the accelerator, enabling the ion source extractor and RF systems when proper conditions are met. The system is implemented using the GTA control system, thus all information available to the control system is also available for use in interlock logic. The logic is defined in terms of control system channels, which reflect accelerator parameters such as actuator positions, power supply values, temperatures, etc. A mode switch in the control room selects the accelerator operating mode, for example 'injector only'. The Run Permit software selects interlock logic as appropriate to the operating mode. This implementation easily accommodates logic changes as requirements evolve. To ensure reliable operation of a software-based system, a special circuit with a watch-dog timer is employed to produce the system's output signals. The software must periodically address the circuit, or the output signals are forced to a disabled state. For additional protection, there are self-test provisions for detecting and reacting to failures of the control system.

The Role of Run Permit

The Run Permit system is one of several protection mechanisms utilized for GTA. These systems are complementary and are targeted to different needs.

Personnel safety is handled by a dedicated hardware-only system. Protection from beam spills and 'during-pulse' anomalies is handled by a system called Fast Protect, which can shut off beam within a few microseconds.

Run Permit fits in between. It does not address personnel safety, nor machine protection requiring fast response. It is designed for maximum flexibility and expandability. Its response time is moderate.

The Run Permit software is general enough to provide an interlock of any kind. The first implementation is to enable / disable beam. It is intended that the same scheme will later be used to enable / disable RF systems as well.

A Software-based System

The Run Permit implementation is primarily software-based, to achieve the flexibility and expandability desired. By utilizing the services of the GTA control system, any information known to the control system can be used by Run Permit. In addition to saving extra cabling, sensors, and instrumentation, a software-based system offers further advantages.

Through standard control system facilities, the status of any sensor or parameter involved in the interlock can be displayed to the operator through the usual workstation displays.

The interlock logic is defined in a file and can be easily re-configured. (It is important that this information be maintained under configuration control to protect the interlock integrity.)

The system can be maintained by personnel already familiar with the control system. Operators used to the control system already have a "feel" for Run Permit.

Interlocks may be bypassed at a number of levels. The bypassing function is available only to designated operators. All instances of changing the bypass status of an interlock are logged to disk with the date, time, and operator's initials.

At the operator's discretion, a change in status of the interlock is logged to disk with a time stamp.

Block Diagram

An overview of the Run Permit system is shown in Figure 1.

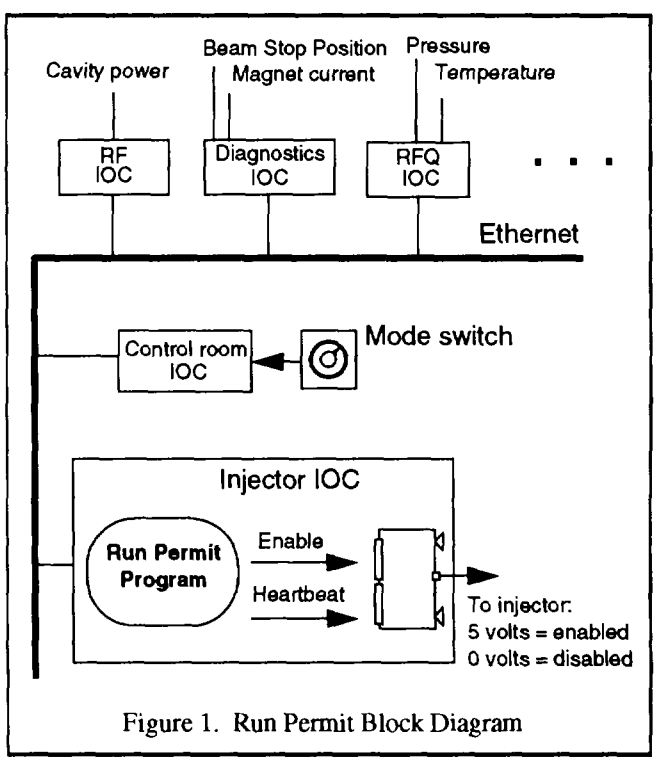

Figure 1. Run Permit Block Diagram

* Work supported and funded by the US Department of Defense, Army Strategic Defense Command, under the auspices of the US Department of Energy.

The GTA control system [1] is distributed between many VME-based Input / Output Controllers (IOCs) connected by Ethernet. Each IOC interfaces with a set of accelerator parameters and maintains a local database with information about the parameter. Any parameter is available to any program on the network via standard control system services.

The Run Permit program resides in the injector IOC. It receives pertinent data from other IOCs over the network, sums the values of these parameters and produces an interlock value. This value is written to a special VME interface which produces the hardware signal actually wired to the injector.

Mode Switch

There are many different operating configurations of the accelerator, identified by operational modes, for example, 'injector only'. A mode switch in the GTA control room selects the desired operational mode. The mode setting is read by an IOC and is monitored by the Run Permit program. The interlock chain appropriate for enabling the injector differs from one mode to the next, so Run Permit selects the parameters for the interlock based on the mode setting.

Fail Safe Features

To offset potential drawbacks of a software-based system, Run Permit incorporates a number of features to ensure fail-safe performance.

The 'enable' signal to the injector is a positive voltage. If the driving electronics fail or the cable is disconnected, the extractor is disabled

If the Run Permit program itself fails, a watch-dog timer on the VME interface will not receive a 'heartbeat' and the output signal is disabled.

If another IOC which is reporting parameter values to the Run Permit program fails, the Run Permit program will detect a missing 'heartbeat' from the IOC and disable the output signal. This heartbeat mechanism will also detect network failures.

Each accelerator parameter monitored has an associated status which indicates whether the parameter is valid. An invalid status causes the Run Permit program to disable the output signal.

The integrity of each IOC is monitored along with accelerator parameters. Each IOC is checked for adequate available memory, available processing time, stack overflows, and suspended or missing tasks.

Operator Interface

The status of Run Permit can be displayed on any workstation normally used for accelerator operation. A number of color graphic screens display the interlock chains and the status of each component. The "top-level" screen for Run Permit is shown in Figure 2.

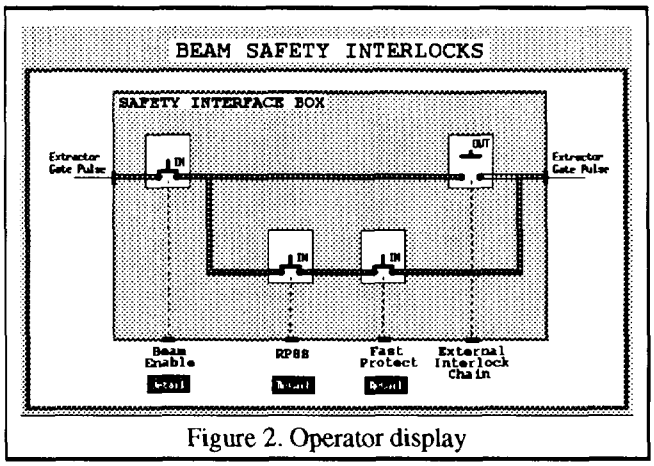

Figure 2. Operator display

The screen shows a partial schematic of the wiring of the extractor pulse from the timing system to the injector. The Run Permit system operates one of the switches which interrupts the pulse (the one labelled Beam Enable). If Run Permit is presently enabling the injector, this screen will show the switch closed, as in the figure. If Run Permit issues a disable signal, the switch appears open.

If the operator clicks on the "Detail" button under Beam Enable, a screen is activated which shows more details of the interlock chain. This screen is shown in Figure 3.

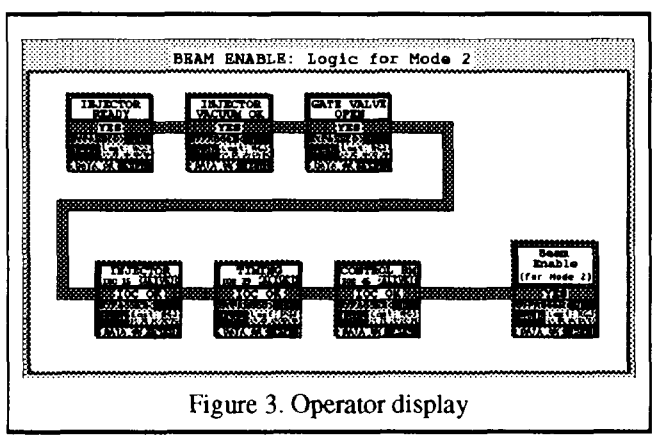

Figure 3. Operator display

The screen represents the interlock chain as a series of boxes connected with a line or bar. The box at the lower right is labelled 'Beam Enable' and represents the output signal from Run Permit. If all the interlock components are "ok", the bar is colored green and the Beam Enable box is marked "YES". If one or more of the components is not in the appropriate state for enabling the beam, the green bar is not visible, the component boxes in question are labelled "NO", and the Beam Enable box is marked "NO".

Figure 4 shows a component box in more detail.

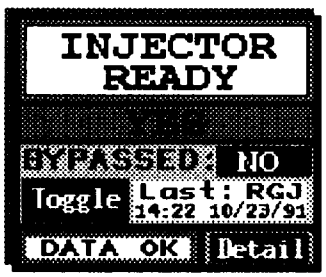

Figure 4. Interlock Component Box

The first two fields are the title of the component and the status. The component title is always formulated so that a status of YES or NO makes sense, for example a good title is "Beam Stop In" rather than "Beam Stop Position". In addition to the labels YES or NO, the status field is colored green for YES and black for NO.

Below the status field is a field indicating whether or not the component is bypassed. This is also designated by color and with YES or NO. An operator may bypass or un-bypass a component by clicking on the field labelled "Toggle". This activates another screen which requires entering a password. If this is completed, the component is bypassed or restored, the field next to the Toggle field will display the operator's initials and time and date when the interlock bypass was toggled.

At the lower left of the component box is a field which displays DATA OK or DATA BAD. This reflects the validity of the component value. If a remote IOC cannot determine the position of the beam stop, it is reflected here.

The last field is a button labelled "Detail". Clicking on this field activates another screen which gives further details, e.g. a more detailed interlock chain which makes up this component. In this case, the detailed screen would show the components which comprise "Injector Ready". These chains may be nested to whatever depth makes sense.

With this type of hierarchy, it is simple and intuitive for the operator to continue to ask for details of failed interlock components until the smallest piece is identified.

Performance

The performance characteristic of most interest is the time it takes for the beam to shut off after some parameter wanders out of tolerance. This is a function of the sensor and electronics monitoring the parameter, the time for the control system to transmit the information over the Ethernet to the Run Permit program, the time for the Run Permit program to send a disable signal, and the time for the beam to go away after loss of the extractor pulse. The dominant delays in this scheme are the sensor time and network transmission time.

Many accelerator parameters are monitored by slow, asynchronous instruments. For instance, temperatures and pressures are typically polled every 2 seconds. Therefore, an out-of-range temperature can not shut off the beam with any quicker average response. Other measurements, such as the beam position are measured each beam pulse and this information is available in a few milliseconds.

The time between sensor information being available to the computer and Run Permit issuing a disable signal is typically within 50 milliseconds. It is difficult to specify a worst-case time, due to the nature of Ethernet. Testing shows that in over 98% of the tested cases, the response is less than 50 milliseconds.

Other types of failures have different response times depending on the method of detection. For example, a failure of the network is detected by a missing heartbeat signal from an IOC to the Run Permit program. The heartbeat period is 1 second, so 1 second can elapse before this condition is discovered. A failure analysis identifies failure types and response times. From this, design choices can be made to ensure that system response is commensurate with potential damage or loss of beam time.

References

[1] L.R. Dalesio, et al, "EPICS Architecture", Proceedings of the International Conference on Accelerators and Large Experimental Physics Control Systems, Tsukuba, Japan, Nov. 11-15, 1991.