



CEBAF-TN-0193, Rev. A
September 17, 1990

**Description and Interfacing Guide
for the CEBAF Fast Shutdown System**

CONTENTS

- 1 Objectives**
- 2 System Structure**
- 3 Node Module**
- 4 System Integrity**
- 5 User's Guide to interfacing**

1. Objectives

The high energy beams in the CEBAF accelerator will carry enough power to burn through the vacuum walls very quickly—within an estimated 50 – 100 μ s. The objective of the fast shutdown (FSD) system is to detect a beam position fault, identify it, and shut down the beam before it can burn through, since a vacuum fault can be very destructive in the cryogenic, superconductive environment of the CEBAF linear accelerators. We have chosen our time limits by the following criteria:

- Assume 45 μ s burn through time.
- Note that 21 μ s of beam stored in the beam lines implies a maximum of 24 μ s for shut down.
- 4.2 μ s optical transit time leaves roughly 20 μ s for detection of a fault and transit of the signal through logic functions.
- We now partition this time into 10 μ s for detection functions, and 10 μ s for system logic functions.

This concept has now given two explicit components of the FSD: the detection component and the logic propagation component. Only the logic propagation component is discussed in detail here; thus only the 10 μ s limit is used for design of the logic modules.

2. System Structure

Two structural organizations were considered: a loop structure and a tree structure.

The loop was the initial basis for design due to its appealingly simple structure and topological similarity to CEBAF's accelerator configuration; however two problems with it quickly eliminated it from consideration. First, searching a loop is easy to do, but can be slow if many nodes are present and the fault is not conveniently located.

Second, and critical, technology puts a very intractable limit on the number of nodes, and therefore the number of fault inputs, available to the system. Our calculations put the limit at about 1000 inputs, which is little more than the already identified requirements.

A further consideration was that the loop is not a very adaptable structure; any changes would involve breaking the loop and finding a new route for the connections.

The tree, on the other hand (fig. 1), can give a vast number of inputs with few levels, since the number of possible inputs at each level is $k \times r^n$, where k is the number of inputs per node, r is the number of permission fan-ins per node, and n is the number of levels. For the CEBAF design, the limit is about 2.7×10^{14} inputs (k=7, r=7, n=16).

Finding a fault is fast and straightforward: the control system simply asks the first node in the fault chain who is not sending permission to run; then asks each node as it is indicated, until it reaches the fault detector that removed permission.

Finally, the tree is highly adaptable, permitting structures consistent with the system structure and permitting changes without breaking and rerouting connections.

The CEBAF FSD fault tree is organized around node modules with 8 fault inputs, 7 tree permission fan-in inputs, and one tree permission output per node. There are also some non-structural functions in each node module.

3. Node Module

There are five submodules in the node module: the CAMAC P1 line interface, the isolated electrical inputs, the fiber optic permission fan-in inputs, the watchdog timer, and the fault logic.

The CAMAC P1 line interface puts a 5 Mhz trapezoidal waveform on the CAMAC P1 user-available bus line and monitors it. If a fault module short-circuits the P1 line to ground, the FSD node module will detect this as a fault. However, if more than one fault detector is on the P1 line, the FSD node will not be able to determine which is the first to fault.

The isolated electrical inputs overcome this obstacle by requiring the fault module to generate its own 5Mhz permission. There are seven of these inputs, and the FSD node can determine to within about $1\mu s$ which was the first to fault.

The permission inputs are similar to the electrical inputs, but coupled with optical fibers; they are intended for structural fan-in use.

The watchdog timer counts down between control system scans, and if it reaches zero, generates a fault. Any valid control system access to the FSD node resets the timer.

The fault logic monitors all inputs and if a fault occurs determines which was the first to within about $1\mu s$. The first fault is held in the first fault register until the faults are reset. Any faults still existing are then latched in the first fault register. The fault logic also handles masking of inputs and propagation of permission to the next level.

4. System Integrity

The FSD system has been designed explicitly with failure tolerance in mind, by providing many inputs for redundancy, and designing so that almost all failures cause a spurious shutdown. A large number of beam loss radiation monitors provides a last resort of redundancy; most faults are backed up several times over by the beam loss monitors.

There are few components in the fault path, and those are lightly loaded devices; every level of the tree may be masked if necessary to continue running until maintenance is possible. The masking capability may be disabled by hardware switches on the node module for critical inputs which are considered too important to be masked.

Failures outside the fault path which might cause an inquiry error are not crippling, because the trace is backed up both above and below by other nodes in the fault tree; these failures will slow the fault trace but not make it impossible. They will not in any case interfere with the shutdown.

Finally, the control system will have a system integrity procedure that will search the entire tree for unsafe masks, faults, and node failures before each beam turn-on. The possibility of a continuously running system integrity procedure is also being discussed with the controls group. It is expected that these measures will offset the propensity of systems of this sort toward violations of the system's integrity for undisciplined maintenance efforts.

5. User's Guide to interfacing

The only output ports intended for use outside the FSD system are the P1 line, the watchdog timer output, and the auxiliary permission output. The external inputs are those on the J2 connector on back of the module, and the P1 line. The front optical inputs and outputs are intended for FSD system use only.

A. P1 Line (input and output)

The P1 line on the CAMAC connector is a CAMAC-defined bus line for use by CAMAC users. The FSD system uses this line as both an output and an input. Operation of the P1 line is based on the FSD permission signal: a 5 Mhz trapezoidal waveform is put on the line by the FSD node module. Users wishing to send a fast shutdown signal via the

P1 line should put a short circuit on the line through an open-collector TTL output. The SN7417 or equivalent is suggested as an output that works well. The FSD node modules themselves use a VN2010 MOSFET as the short circuit switch.

The switch used must be able to pull a signal to solid ground that originates as a 5 Mhz, 0V-5V square wave through a 200 ohm resistor.

The P1 line is also used as an output from the FSD node module, since if permission is lost from any unmasked input the node module itself shorts the signal to ground. Users wishing to monitor the FSD system may use the P1 line, since it duplicates the permission signal's presence or absence within about $1.5\mu s$. A suggested decoding circuit is presented in fig. 2; it is the same circuit used in the FSD node's permission decoders.

If a fault detector uses the external inputs (described later), it MUST NOT also use the P1 line, since the node module will not then be able to determine which input was first.

B. Watchdog timeout output

Every CAMAC crate connected to the accelerator control system will have a FSD node module to monitor system integrity; part of this monitoring is control system function. Every FSD node module has a watchdog timer whose time may be set by the I & C Group. If the watchdog times out, it will generate a FSD interrupt, and it will pull the WD OUT line on the J2 connector (fig. 3) from a TTL high to a TTL low. As long as the control system accesses the node module within the preset time limit, the WD OUT line will remain at a TTL high level. Interfacing to the WD OUT line is straightforward; a TTL input is all that is required.

C. Auxiliary permission output

The auxiliary permission output is an exact copy of the FSD system permission output. It is intended for users who may want to monitor fast faults in a local area for their own use. The auxiliary permission comes out on the AUX PERM output on the J2 connector. It is a 5 Mhz TTL waveform driven by 74LS125A bus drivers. The circuit of fig. 2 is also suggested for users needing to decode this output.

D. External Inputs

The external inputs are intended for users who need to send a fast shutdown signal to the system, and for whom the order of fault detection is important. The FSD node module will detect the first loss of permission within about $1\mu s$; faults closer together than this will be latched as simultaneous first faults.

Faults using the external inputs MUST NOT also use the P1 input, since the FSD node will not then be able to determine which fault was first.

The external inputs are optically isolated using 6N137 isolators. They are protected against reverse voltage, but there are no limiting resistors. It is important that users of these inputs conform closely to the input standard this section specifies.

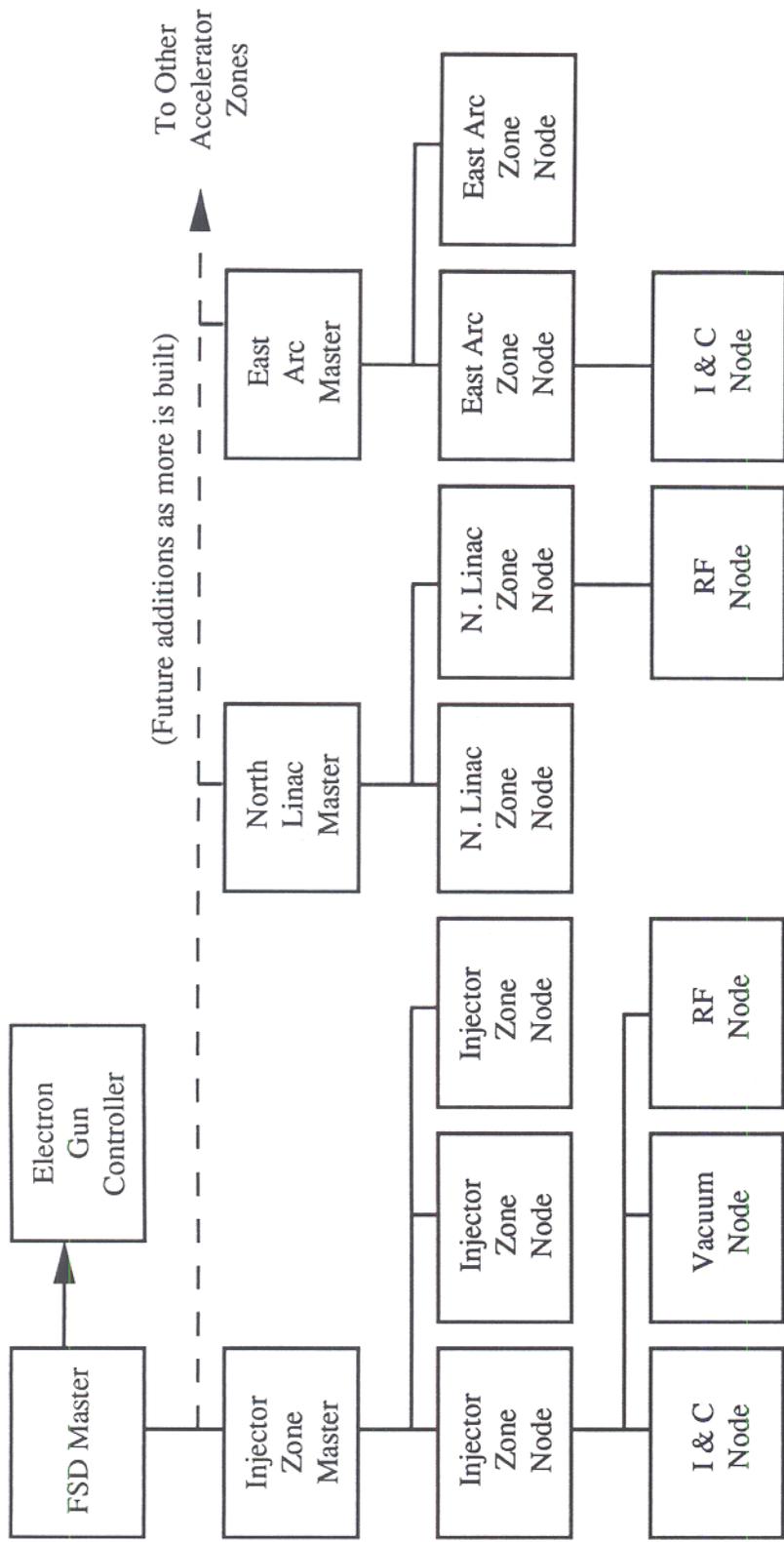
Signal parameters to these inputs must be:

- $5Mhz \pm 10\%$
- 45% - 55% duty cycle rectangular current waveform
- $I_{low} \leq 0.5ma$
- $10ma \leq I_{high} \leq 30ma$

A suggested circuit that meets these criteria is presented in fig. 4. We emphasize that

ordinary logic circuits cannot meet this standard; bus drivers are the minimum level of output capability required. The required cable for this system is fully shielded twisted pair, *properly terminated* and grounded. Coax should not be used, as there is no requirement for constant impedance, and properly used shielded twisted pair has both lower transmission and lower pickup of interference. An excellent exposition of shielding technique is given in chapter 4 of *Grounding and Shielding Techniques In Instrumentation* by Ralph Morrison (Wiley & Sons, NY, 1986).

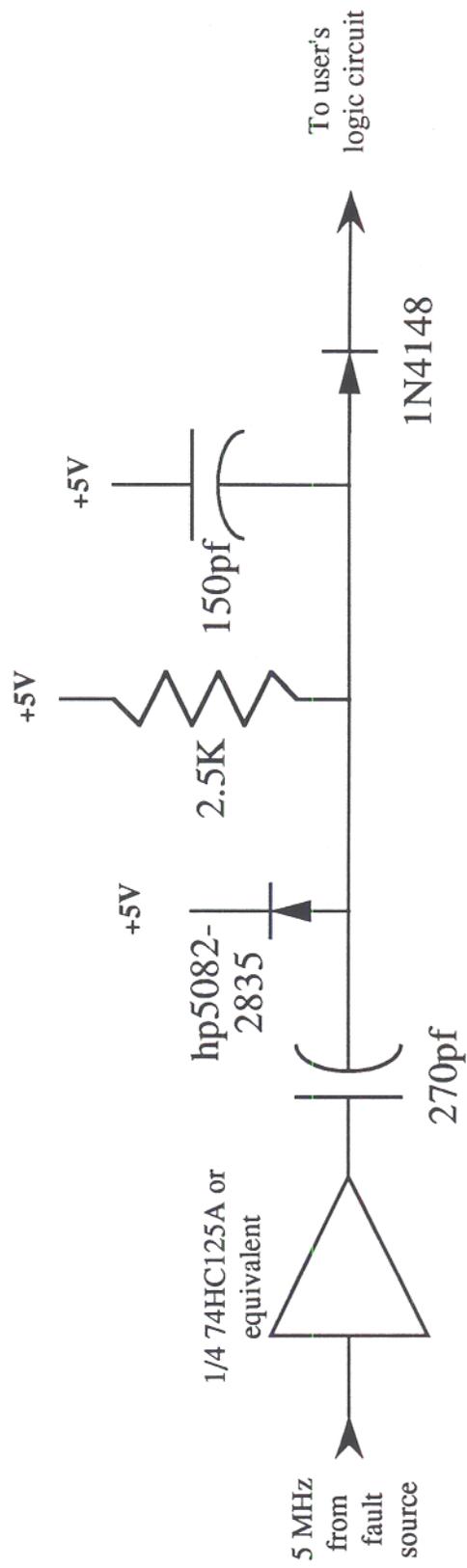
In testing you will note that the cable waveform will not appear as one would expect (see fig. 5); this is in fact normal and has no effect on circuit performance. Note that this is a current waveform driving a very nonlinear load in parallel with a relatively large cable capacitance. In particular, the cable should not be switched directly to ground or to Vcc, since the increased voltage charging times will severely degrade circuit performance.



Current implementation of system

Fast Shutdown Tree Structure

Figure 1

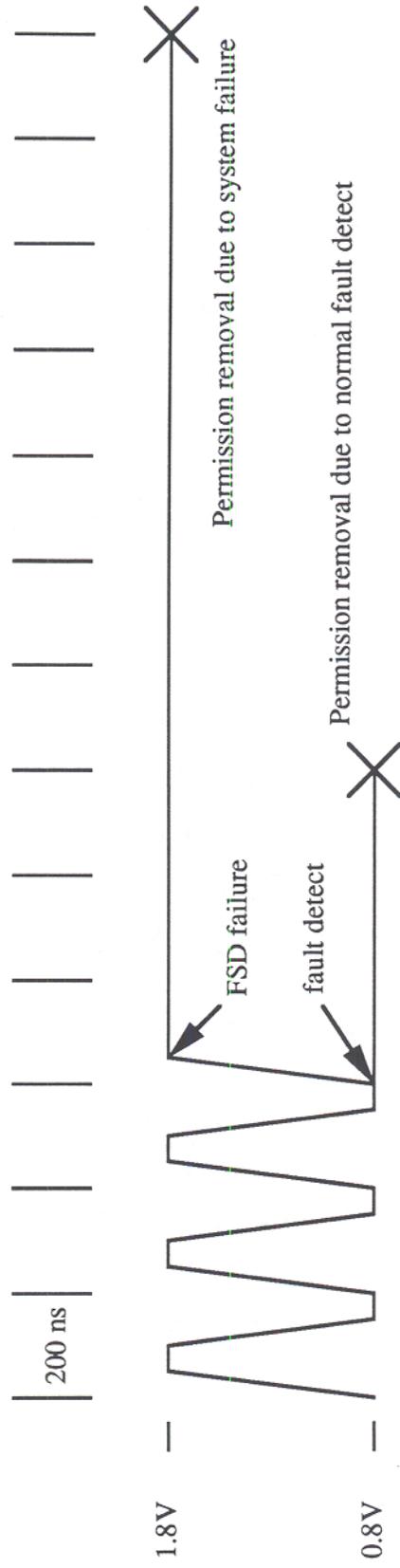


FSD permission signal decoder

Figure 2

...Signal Name...	SIDE A	Position	SIDE B	...Signal Name...
EXT 0 SIG	A	1	B	EXT 0 RET
GND	A	2	B	GND
EXT 1 SIG	A	3	B	EXT 1 RET
GND	A	4	B	GND
EXT 2 SIG	A	5	B	EXT 2 RET
GND	A	6	B	GND
EXT 3 SIG	A	7	B	EXT 3 RET
GND	A	8	B	GND
EXT 4 SIG	A	9	B	EXT 4 RET
GND	A	10	B	GND
EXT 5 SIG	A	11	B	EXT 5 RET
GND	A	12	B	GND
EXT 6 SIG	A	13	B	EXT 6 RET
GND	A	14	B	GND
WD OUT SIG	A	15	B	WD OUT RET
GND	A	16	B	GND
AUX PERM SIG	A	17	B	AUX PERM RET
GND	A	18	B	GND

Fig. 3-J2 connector signal definitions



FSD Permission Signal--normal fault is current OFF

Figure 5