PROTECTION INSTRUMENTATION FOR A LARGE SUPERCONDUCTING MAGNET

J.M. Reschovsky, P.C. Brown, W.R. Court, and W.E. Overstreet
General Electric Company, Schenectady, NY 12345

Abstract

Large superconducting magnets generally operate at very high currents and store large amounts of magnetic energy. These magnets need reliable protection against the occurrence of a quench, that is, an uncontrolled temperature rise of the magnet conductor resulting in a loss of superconductivity, a collapse of the magnetic field, and a potentially dangerous release of energy. This paper describes the protection instrumentation and controls for a large MHD magnet being built for the Department of Energy under subcontract from the Francis Bitter National Magnet Laboratory at MIT. This system is of particular interest because it has been configured with reduncancy and fault-tolerant features in a manner similar to the protection instrumentation required to insure the safety of nuclear facilities. The protection system includes a self-contained electronic instrument with customized circuitry and a microcomputer, associated remote sensors, and two large circuit breakers. It monitors for normal regions in the conductor, loss of cryostat vacuum, and other magnet faults during operation, and responds by automatically discharging the magnet. The magnet protect system is fault-tolerant in that it will respond to the most serious magnet faults despite one or more instrumentation malfunctions. Fault tolerance is accomplished by providing redundancy and automatic self-testing of all redundant paths. Redundancy is maintained throughout the system, from the remote sensors to the series connected circuit breakers that initiate rapid discharge. The microcomputer, although not a direct part of this protection process, provides self-testing capability. In accordance with a programmed strategy, the various redundant signal paths are tested and isolated from the system if found to be faulty. The fault-tolerant concepts applied to this design offer a unique alternative for instrumentation and control functions that require high reliability.

Introduction

General Electric has been contracted by the Francis Bitter National Magnet Laboratory to design, manufacture, install, and test a Superconducting Magnetohydrodynamic Magnet System for the Department of Energy's Component Development and Integration Facility (CDIF) in Butte, Montana. This paper describes the protection instrumentation designed for this magnet.

The magnet will be capable of storing 183×10^6 J of magnetic energy. Any uncontrolled discharge of this quantity of energy within the magnet could seriously damage the magnet. Consequently, very stringent reliability requirements have been placed on the instrumentation and control functions protecting the magnet. One can apply the fault-tolerant design principles in this system to magnet instrumentation for fusion research.

*This work was performed for the Francis Bitter National Laboratory as a part of Purchase Order ML65100, "Design, Manufacturing Installation and Test of a Superconducting Magnetohydrodynamic Magnet."

The magnet protect system is a self-contained electronic instrument with customized circuitry, a microcomputer, and associated sensors. It interfaces with the magnet power supply, two large circuit breakers, and a discharge resistor. The protect system design draws upon concepts previously applied to magnet protection,[1,2] expanding the use of protective redundancy and automatic self-testing to provide improved fault-tolerant operation.

This paper first describes the CDIF magnet and its instrumentation requirements, then reviews the principles of fault-tolerant design, and finally describes details of the magnet protect system and its operation.

The Magnet and Its Instrumentation Requirements

The magnet is a 45° rectangular saddle, pancake-wound, MHD dipole with graded field. The field and aperture axes are horizontal. Conductors are supported in grooved subplates stacked and bolted by a stainless steel superstructure. Liquid helium cools the conductors and the operating temperature of the windings is 4.5 K. The magnet incorporates a pair of 6200 A gas-cooled current leads which require the equivalent of 20 l/h of liquid helium for efficient cooling. The magnet produces an on-axis field of 6 T, operates at a current of 6130 A, and stores 183×10^6 J of energy. Table 1 presents a summary of the design characteristics of the CDIF Superconducting Magnet, and Figure 1 shows the magnet and its associated instrumentation. The magnet power supply provides the current necessary to operate the magnet through two series circuit breakers. The water-cooled discharge resistor connects in parallel with the magnet. The magnet protect system monitors for conditions that require discharge and opens the circuit breakers should it detect such a condition.

Table 1

DESIGN CHARACTERISTICS OF THE CDIF SUPERCONDUCTING MAGNETOHYDRODYNAMIC MAGNET

Peak On-Axis Field	6 T
Active Field Length	3.00 m
Overall Length	6.452 m
Overall Diameter	4.110 m
Average Current Density (J)	0.183×10^8 A/M^2
Ampere Turns (NI)	14.22×10^6
Number of Turns (N)	2320
Operating Current (I)	6130 A
Total Helium Volume	10,000 l
Inductance	9.5 H
Stored Energy	183.1×10^6 J
Discharge Time Constant	1 min
Maximum Terminal Voltage	1000 V

Proceedings of the 8th Symposium on Engineering Problems of Fusion Research IEEE Pub. No. 79CH1441-5 NPS Vol. 1 pp 464 - 469.

Protecting the Magnet

In designing large superconducting magnets, a major concern is the possibility of developing a normal (nonsuperconducting) zone within the conductor during operation. Under some conditions the normal

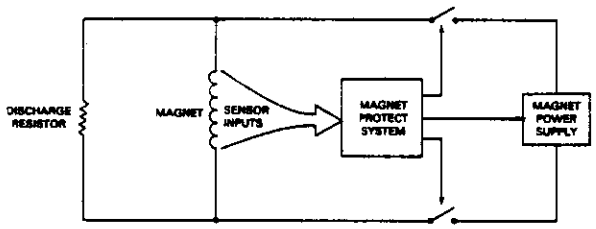

Figure 1. Magnet instrumentation

region will spread throughout the winding (a condition known as a quench) and cause the release of the stored magnetic energy in the winding. This may lead to high electrical and thermal stresses and, hence, damage to the magnet.

The CDIF Magnet Protect System's primary function is to automatically detect the magnet malfunctions that could damage the magnet, open the circuit breakers, and allow the magnet energy to dissipate in the discharge resistor. The magnet manfunctions that could result in normal zone spreading and therefore warrant a magnet discharge are

- Loss of vacuum
- Increased current lead temperature or voltage drop
- Resistive voltage drops across segments of the magnet coil

Additionally, failure of the protect system is considered severe enough to initiate magnet discharge.

A secondary protective action, implemented in the event of less critical malfunctions, is a gradual current ramp-down in which the magnet power supply transfers the stored energy to the ac power grid. The power supply is capable of a complete ramp-down from rated current in approximately two hours. The conditions requiring a ramp-down are

- Cryostat liquid helium level below specification
- Cryostat liquid nitrogen level below specification
- Discharge resistor water level below specification
- Loss of circuit breaker control power
- Marginal protect system capability (no redundancy)

The fundamental requirement of the protect system is that it must not permit a potentially damaging condition to exist in the magnet. The above conditions which result in a ramp-down are not in themselves damaging, but they are early indications of a potentially damaging condition. In contrast, the existence of those conditions which require magnet discharge is damaging if a rapid magnet discharge does not follow immediately. Therefore, the design of the protect system has emphasized the highly reliable performance of the magnet discharge function. The concepts of fault tolerance as defined below are applied to the portions of the system that provide this function. Portions of the system that provide the ramp-down and various annunciation functions are not fault-tolerant.

A failure of the magnet protect system to initiate a magnet discharge when required is the most serious type of system malfunction. A protect system malfunction that results in a magnet discharge when none is required also has a serious impact causing a disruption in the MHD test train run and a costly loss of cryogenic coolant. The protect system is implemented to minimize the chances of either of these types of malfunctions. However, design trade-offs that affect the relative probability of these two types of malfunctions are resolved so as to minimize the chances of a failure to implement protective action when required.

Principles of Fault-Tolerant Design

The serious consequences of a failure to initiate a magnet discharge when required impose rigid reliability requirements on the protection instrumentation. In response to these requirements, the magnet protect system has been designed to be fault-tolerant. This section reviews a few basic principles of fault-tolerant design and provides some justification for their use.

There are two fundamental approaches to achieving reliable systems. The traditional approach is "fault avoidance" (sometimes called fault intolerance).[3] One achieves high reliability by employing design and manufacturing practices that minimize the probability of the occurrence of faults. All resources allocated to achieving reliability are spent on perfecting the system prior to its use. Procedures such as use of the highest quality components, material screening, strict quality control, and derating of components all tend to minimize the chances that system faults might occur.

In contrast, the fault-tolerant approach accepts the inevitability that faults will occur and provides the facility for maintaining correct operation of a system despite the occurrence of a prescribed set of faults. One achieves fault tolerance through the use of redundancy and automatic self-testing techniques that provide for detection of faults and even reconfiguration of system architecture to recover from the fault's effects. These concepts are, of course, not new, but they have been applied more rigorously over the past decade, principally in computer systems. The applications of fault-tolerant designs have ranged from guidance computers in manned spacecraft to telephone switching networks.

Reliability

The reliability, R, of a system or element is defined as the probability that it will survive a time interval, 0 to t, without the occurrence of one of a prescribed set of faults. It is also meaningful to describe the unreliability, U=1-R, of the system or element as the probability of the occurrence of these faults over the same time interval. When it is possible to characterize the system or element by a constant failure rate, λ(fractional failures per unit time), then we may compute reliability.[4]

$$R = e^{-\lambda t} \quad (1)$$

It is also conventional to refer to the reciprocal of failure rate as the mean time between failures (MTBF).

We shall deal with the reliability (or unreliability) of modules which accept and process some form of input data, producing a single digital output (1 or 0). A fault will then result in an error in the state of this output. Faults may be classified as erroneous 1's (1 output when 0 is correct) and erroneous 0's (0 output when 1 is correct). The importance of this distinction is clear if we think of a module whose purpose is to monitor the condition of the magnet and change its output to a 1 if initiation of a protective action is warranted. Then, an erroneous 1 fault would cause an unwarranted protective action, whereas an erroneous 0 would result in a failure to initiate protective action.

Redundancy

The use of protective redundancy is essential to achieving fault tolerance. Hardware redundancy is provided in the magnet protect system at a modular level. That is, specific functional modules are duplicated or triplicated to increase reliability. Figure 2 shows a basic triple modular redundant (tmr) configuration. Three identical modules accept inputs from the same source and perform parallel functions, each providing a resultant output. Since only one output is ultimately required, the module outputs combine in a polling device. If no fault conditions exist, all three modules would produce identical results and the output state of the polling device is obvious. When faults do exist, these outputs may disagree and the polling device then makes a best decision based on a pre-established polling strategy. The most common polling strategy is the majority vote (two out of three) which will not produce an error until two of the three modules have failed. However, in cases where the impact of an erroneous 0 and an erroneous 1 are unequal, a logic OR (one out of three) or logic AND (three out of three) may be preferable.

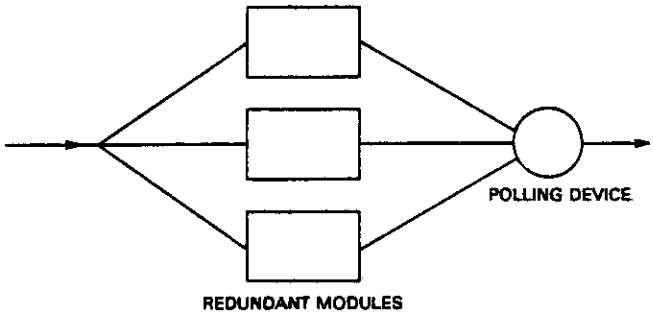

Figure 2. Triple modular redundant (tmr) configuration

Let us examine how the choice of a polling strategy effects the reliability of the triple modular redundant (tmr) configuration. We define U as unreliability of the polling device output and μ as the unreliability of individual modules in the configuration. These parameters are further classified by subscript, U_0 and U_1, corresponding to probabilities of erroneous 0's and erroneous 1's respectively. We shall at present assume a unity reliability for all polling devices.

$$U_{0/OR} = \mu_0^3 \quad (2)$$

The probability of an erroneous 1 (i.e., an unwarranted action) for the logic OR strategy is the probability of exactly one, exactly two, or exactly three erroneous 1's on the module outputs.

$$U_{1/OR} = 3\mu_1(1-\mu_1)^2+3\mu_1^2(1-\mu_1)+\mu_1^3$$

$$= 3\mu_1-3\mu_1^2+\mu_1^3 \quad (3)$$

In contrast to the logic OR polling device which has very different reliabilities for erroneous 1 and erroneous 0 faults, the majority vote or von Neumann polling strategy has identical statistics for either type of fault. This configuration will fail when any two or all three modules produce identical faults. The classical formulation for this configuration[5] is

$$U_{MAJ} = \mu^3+3\mu^2(1-\mu)$$

$$= 3\mu^2-2\mu^3 \quad (4)$$

where the unreliability parameters may be subscripted either 1 or 0.

Figure 3 provides comparison of the formulations given above where all module unreliabilities are assumes equal ($\mu_1 = \mu_0 = \mu$). Equations 2, 3 and 4 are all compared to the nonredundant case ($\mu = U$). One can see that the configuration least likely to produce an erroneous 0 (fail to take action) is the logic OR, but this improvement is provided at a significant sacrifice in the reliability to erroneous 1 faults (unwarranted action). The majority vote strategy takes the middle ground, offering a modest reliability gain to both types of faults.

In all of the preceding discussion, the reliability of the polling device has been assumed to be unity. In real systems where polling circuits can fail, it is often desirable to provide redundant polling of the redundant modules.

Self-Testing

Redundancy can be configured to improve the reliability of fault-tolerant systems by requiring multiple faults before specific system functions are impaired. If the system has the facility to self-test various elements or modules within it and to take appropriate action when faults are detected, then reliability may be further improved. The appropriate action depends upon the system design and may or may not involve human intervention. One action might be to alert the operator that a fault has occurred and that maintenance is required. Other actions might include the automatic isolation of the failed portion of the system or even replacement by standby modules, a procedure called reconfiguration.

Self-testing as applied to the magnet protect system contributes to fault tolerance in two ways.

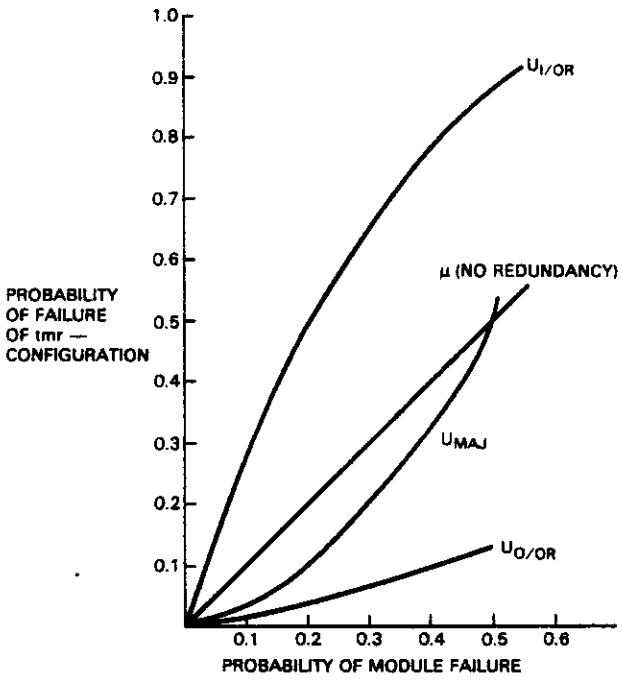

Figure 3. Unreliability of tmr Configurations

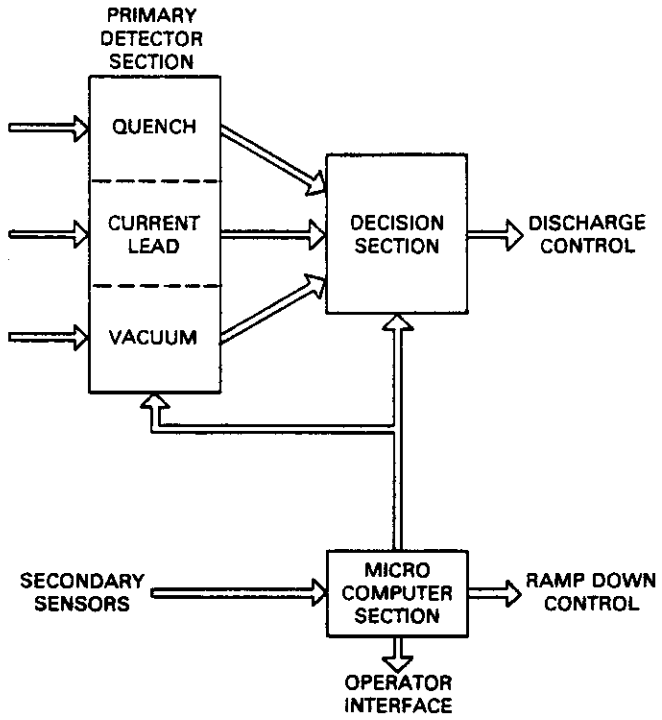

Figure 4. Magnet protect system

First, by sequentially self-testing each module in its redundant configurations, the system provides operators with a constantly updated status of the instrumentation's health, and initiates a magnet ramp-down if the system capability is sufficiently impaired. Secondly, self-testing has a direct impact on the reliability gain achievable from redundant configurations. An example best explains this point.

Three or more redundant sensors and detectors are provided in the protect instrumentation for each magnet condition requiring magnet discharge. These redundant paths are combined using a logic OR strategy, thus minimizing the probability of a failure to detect the condition (Equation 2). Without self-testing, this choice would increase the chances of unwarranted protective action (Equation 3). However, when 1 appears at the logic OR output, protective action is momentarily delayed, allowing the system time to self-test those detectors indicating discharge condition. If they fail the test, they are disabled (isolated) and unwarranted action is averted. If they pass, and the detected condition persists, protective action is initiated. Thus, one uses a self-testing strategy to reduce the probability of erroneous 1 faults causing unwarranted discharge.

System Description

As previously outlined the magnet protect system initiates magnet discharge upon the detection of specified magnet malfunctions. The system also initiates a ramp-down of magnet current upon detection of less severe malfunctions. The system architecture shown in Figure 4 implements the magnet discharge function in fault-tolerant hardware, and the ramp-down function in a nonfault-tolerant microcomputer.

The microcomputer also provides the operator interface and enhances the fault tolerance of the magnet discharge hardware by self-testing the circuitry.

The detector section incorporates 18 magnet sensors and their associated signal conditioning. These sensors provide redundant detection of normal regions in the magnet winding, current lead malfunctions, and a loss of cryostat vacuum, as summarized in Table 2. Each of the 18 detectors has a digital output indicating the presence of a magnet condition requiring a discharge. These outputs combine in the decision section, an expanded redundant polling device that determines if a magnet discharge is warranted.

Table 2

SUMMARY OF MAGNET DETECTORS

Magnet Condition	Total Number of Detectors	Number of Redundant Measurements	Detector Type	Criteria for Discharge
Normal Region	7	3	Bridge	>50 mv imbalance
Vacuum	3	3	Cold Cathode Vacuum Gage	$>10^{-3}$ torr
Current Lead Malfunction	4 (each lead)	2 (each lead)	Voltage	>300 mv across current lead
		2 (each lead)	Temperature	>300-400 K (copper temperature)

The microcomputer is an 8080-based processor interfaced with a CRT display and front panel controls. The system interface to the microcomputer is provided

through TTL I/O logic and analog inputs. The microcomputer interace to fault-tolerant portions of the system is gated by a watchdog circuit which isolates the computer in the event of a computer malfunction.

Detector Section

Although there are different types of sensors for detection of different magnet conditions, all detectors share the common architecture, shown in Figure 5. In addition to detecting a magnet malfunction, each detector provides for complete self-testing while in service. The signal conditioner converts the sensor input to a signal proportional to the measured quantity, and works under microprocessor control to test the detector circuit operation and to check the continuity through the sensor and its associated wiring. The comparitor output indicates that the measured quantity exceeds a preset threshold. The disable circuit, under microcomputer control, isolates the detector output temporarily during circuit test and permanently should a fault be detected.

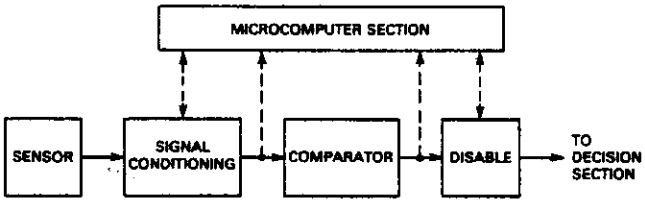

Figure 5. Detector architecture

Triply redundant detection of normal regions in the magnet windings is achieved using seven quench detectors in the configuration shown in Figure 6. Because of the presence of large inductive voltages, bridge circuits are used to compare magnet sections to detect resistive voltage drops from normal regions. Bridge A compares the two halves of the magnet, bridges B1 and B2 compare magnet quarters, and bridges C1, C2, C3, and C4 compare magnet eighths. Most normal regions are simultaneously sensed by three quench detectors. Normal regions that propagate symmetrically about the center of any bridge are sensed by only two detectors. The quench detectors circuit is configured to maintain a constant normal region voltage threshold despite any inductive dissymmetry between the magnet sections used in the bridge.

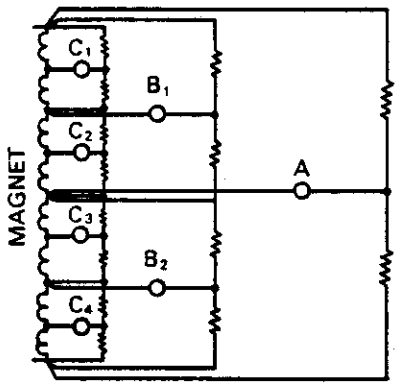

Figure 6. Quench detector bridge configuration

Redundant measurement of the cryostat vacuum is made with three independent cold cathode vacuum gages and associated circuitry. Current lead protection for each lead is provided by doubly redundant measurements of both the temperature of the lead at the point of entrance into the cryostat and the voltage drop across the lead. The integrity of each of these sensors and voltage taps is verifiable through microcomputer-controlled self-testing.

Decision Section

The architecture of the decision section is a logical outgrowth of the fault-tolerant principles outlined previously. Its function is to poll the detector outputs and to initiate a magnet discharge if any of the magnet malfunctions is present for at least one second. In addition, a magnet discharge will result if, through self-testing, the system establishes that it is unable to detect and act upon any of these malfunctions.

As Figure 7 shows, a triply redundant logic OR polling strategy is used to combine the detector outputs. Each of these OR outputs drives a one second integrating delay timer. Since the delay timer allows complete self-testing before initiating a magnet discharge, the OR strategy provides the minimum probability of a failure to detect a magnet malfunction without increasing the probability of an unwarranted discharge.

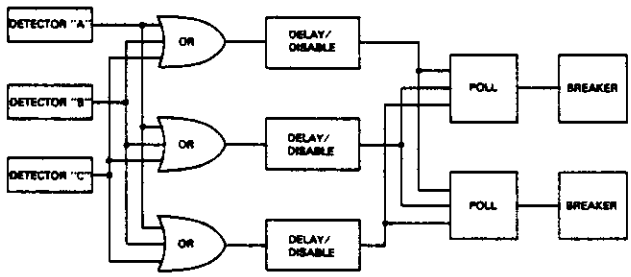

Figure 7. Decision section discharge function

With the addition of a disable circuit just after the delay, one can also test the delay timers without initiating a magnet discharge. The three output signals finally combine in two redundant polling devices, each controlling one of the two redundant circuit breakers. These polling devices normally use a majority vote strategy. However, if one or more of the delay timers is disabled as a result of self-testing, the strategy is reconfigured to be a logic OR combination of the remaining inputs.

Microcomputer Section

The microcomputer section, consisting of the microcomputer and its associated circuitry, performs the self-test, ramp-down, and operator interface functions in the magnet protect system. Although well-suited to these tasks, the microcomputer does not, due to its inherent complexity, have the high reliability associated with the system's fault-tolerant sections. Therefore, its interface to these portions of the system is controlled by a watchdog circuit that monitors the microcomputer operation. If any of the microcomputer power supplies are out of tolerance or if the microcomputer fails to reset a timer within a specified time period, the watchdog circuit will isolate the microcomputer from the rest of the system.

The microcomputer automatically self-tests all the magnet discharge hardware, including the circuit

breakers, before the power supply may start. While the magnet is in service, periodic testing is performed on all hardware that may be tested without initiating discharge. Each portion is in turn disabled and tested by injecting test signals under microcomputer control. If the system responses to these test signals meet the programmed pass/fail criteria, the circuit under test is enabled again. Otherwise, the circuit is left disabled and an alarm is annunciated to make the operator aware of the need for system maintenance. If a condition requiring a magnet discharge is detected, all portions of the system indicating the presence of the condition are tested during the one second delay period.

The ramp-down function, in contrast to the magnet discharge function, is much less critical and is implemented in the microcomputer. If any of the conditions requiring a ramp-down are present, the microcomputer transmits a signal to the power supply to initiate the ramp-down.

Since the protect system operation is fully automatic, the operator interface to the system is primarily an information display function. The CRT continuously displays the status of all portions of the system, including self-test results and alarm conditions. Other operator controls and indicators provide manual control of the breakers and an indication of the existence of alarm conditions.

Conclusions

Equipment protection in large experimental cryogenic facilities, whether for fusion or MHD research, is a critical function. Protect instrumentation must be extremely reliable and its operation and maintenance must not place significant demands upon facility personnel. The protect system for the CDIF Superconducting Magnet meets these objectives. The use of fault-tolerant architecture in conjunction with a microcomputer provides fully automatic operation and virtually eliminates concern about magnet quench.

In designing fault-tolerant instrumentation, it is important to analyze all possible faults and their impact on operation. System design must reflect trade-offs such as those between the impact of a failure to discharge and the impact of an unwarranted discharge. It is also important to recognize that faults are more likely to occur in sensors and in cabling than in the electronic circuitry. Sensor redundancy and self-testing must therefore be implemented accordingly.

References

1. R.F. DiGesare and M.J. Hennessy, "A Microprocessor Based Superconducting Magnet Protection System," 1978 Applied Superconductivity Conference, September 25-28, 1978, Pittsburgh, Pa., IEEE Transactions on Magnetics (MAG-15 Number 1).
2. R. Stiening, R. Flora, R, Lauckner, and G. Tool, "A Superconducting Synchrotron Power Supply and Quench Protection Scheme," 1978 Applied Superconductivity Conference, September 25-28, 1978, Pittsburgh, Pa., IEEE Transactions on Magnetics (MAG-15 Number 1).
3. R.G. Bennetts, "Designing Reliable Computer Systems," Electronics and Power, November/December 1978.
4. I. Bazovsky, Reliability Theory and Practice, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1961.
5. W.G. Bouricus, W.C. Carter, D.C. Jessup, P.R. Schneider, and A.B. Wadia, "Fault Tolerant Computer Modeling," IEEE Transactions on Computers, November 1971.

Acknowledgment

The authors acknowledge the many individuals within the General Electric Company who made contributions to the design of the Magnet Protect System. Particular appreciation is expressed to Dr. A.K. Khalafallah for his contributions and encouragement in the preparation of this paper.