during a loss of power. The NM-1000 has self-diagnostic circuits and also has a watchdog timer circuit which places the NM-1000 in a tripped condition and scrams the reactor if power fluctuations prevent the software from operating properly. The NM-1000 Software Functional Specification and Software Verification Program (March 1989) describes the tests performed on the NM-1000 to verify that the system returns to proper operation after the power is restored. The staff finds this acceptable.

7.4.1.4 Failure Modes and Effects

The applicant performed a scram circuit safety analysis to identify the various ways in which the reactor safety system could fail. These include the following:

- (1) Physical system failure (wire breaks, shorts, ground fault circuits)
- (2) Limiting safety system setting failure (failure to detect)
- (3) System operable failure (loss of monitoring)
- (4) Computer/manual control failure (automatic and manual scram)

The applicant performed this analysis using fault trees to predict a failure to scram for various failure modes. The applicant concluded that a failure of all safety systems and therefore, failure to scram was extremely unlikely. The applicant evaluated all failures attributable to the unique failure modes of the software of the NM-1000. The staff has reviewed the applicant's analysis of the failure modes and effects of the new system and finds this acceptable.

7.4.1.5 Independence, Redundancy, and Diversity

The staff reviewed the data link between the safety channels and the nonsafety systems. The safety channels provide hard-wired scram inputs and are also wired directly to independent indicators on the control console. The operators receive information from both the analog NP-1000 and NPP-1000 power monitors and the digital NM-1000 monitor. The information is displayed on both direct wired bar graphs and on a graphic CRT. The safety channels also provide inputs to the non-class IE data acquisition computer (DAC) through isolators. The isolators used have not been tested for the maximum credible faults that the staff requires for isolators used in power plants. However, the manufacturer has tested them to standard commercial criteria. The staff concludes that the use of isolators tested to standard commercial criteria is. acceptable for the UT TRIGA reactor. The DAC is then connected through redundant high speed serial data trunks to the non-class IE control system computer (CSC) which interfaces with the operator by controls, a keyboard, and CRT displays. The CSC would not meet the independence requirements of a power plant because the CSC does interface with the safety channels. However, the staff concluded that this independence was not necessary for the current application at UT.

The scram circuit has a fail safe design using automatic and manual contacts which open to remove power to the control rod magnets. Redundant fuel temperature inputs are provided to the scram circuit at the UT facility. Redundant power level inputs (NP-1000, NPP-1000) to the scram circuit are also provided.

9301280279 930121 PDR ADUCK 05000602 P PDR