UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

SUPPLEMENTAL SAFETY EVALUATION BY THE OFFICE OF NUCLEAR REACTOR REGULATION

GE SCOPE OF NSSS INSTRUMENTATION-PROTECTION AND

CONTROL SYSTEM INTERACTION

PENNSYLVANIA POWER AND LIGHT COMPANY

SUSQUEHANNA STEAM ELECTRIC STATION, UNITS 1 AND 2

DOCKET NOS. 50-387 AND 50-388

1.0 INTRODUCTION

An event on May 22, 1986, at the Susquehanna Steam Electric Station (SSES), involving the common computer input card for the four emergency diesel generators ground alarm circuits, raised common mode failure concerns in circuits where isolation devices are not provided between certain safety-related (Class 1E) and non-safety-related (non-Class 1E) instrumentation circuits. The instrumentation circuits of concern at SSES were provided by General Electric (GE) for the nuclear steam supply system (NSSS). In response to the staff concerns regarding these circuits, the Pennsylvania Power and Light Company (PP&L), the licensee of SSES, submitted an analysis performed by GE to address the electrical isolation requirements of IEEE Standard 279-1971 "Criteria for Protection Systems for Nuclear Power Generating Stations." Compliance with IEEE Standard 279-1971 is required in accordance with 10 CFR 50.55a(h) which is the licensing basis of the protection system design at SSES. A staff safety evaluation report (SER) dated June 28, 1991 (Reference 1), concluded that the GE analysis was not acceptable because the standard requires isolation devices. The position included in this SER neglected to state that NRC regulations would allow the staff to consider analysis justifying not installing isolation devices.

The staff determined in the June 28, 1991, SER that there was a potential generic issue involving GE NSSS circuit isolation in boiling water reactor (BWR) plants but, based on the low likelihood of fault propagation in these low voltage circuits, there was no immediate safety concern and action could be delayed pending further staff review of the generic issue. The staff thus requested that PP&L delay its response to the staff SER pending the results of the generic NRC review of the GE analysis. A subsequent staff review by the NRC Office of Research (RES) dated March 12, 1993 (Reference 2), determined that this issue was a compliance matter rather than a generic issue and should be addressed on a plant-specific basis. The RES review also determined that isolation devices in the GE circuits would not be necessary if tests or analyses demonstrate that the Class 1E circuits are not degraded below an acceptable level when postulating faults in non-Class 1E circuits that derive their signal from Class 1E circuits.

ENCLOSURE

Subsection 10 CFR 50.55a(3) allows applicants to propose alternatives to the specific design requirements of IEEE-279-1971 that demonstrate an acceptable level of quality and safety. Therefore, the SSES licensee by letter dated August 23, 1995 (Reference 3), submitted a new analysis of the GE instrumentation circuits and their power supplies for SSES Units 1 and 2 which demonstrated that a fault in a non-Class 1E component or its power supply does not degrade the Class 1E circuit below an acceptable level. In response to staff questions on this analysis, the licensee submitted revised analyses by letters dated June 27, 1996 (Reference 4), November 27, 1996 (Reference 5), February 3, 1997 (Reference 6), March 10, 1997 (Reference 7), June 25, 1997 (Reference 8), and September 5, 1997 (Reference 9). The staff reviewed the licensee's revised analyses to assure that faults in non-Class 1E circuits with no isolation devices do not degrade the Class 1E circuits below an acceptable level. The results of that review are described in this supplemental SER to the June 28, 1991, SER. This supplemental SER resolves the open issue identified is the June 28, 1991, SER.

2.0 BACKGROUND

The SSES Units 1 and 2 design, prior to May 22, 1986, allowed ground fault alarm circuits from all four emergency diesel generators (EDGs) to share a common computer input card with no electrical isolation provided at the interface between the safety-related EDG ground fault circuits and the non-safety-related computer input card. On May 22, 1986, while one of the four EDGs was being tested, a high voltage surge in the field circuit of the EDG under test caused a short circuit fault and a minor fire at the computer input card that resulted in a ground fault alarm on all four EDGs. The high voltage surge was not transmitted to the EDG protection and control circuits and the diesels remained fully functional. This event, however, raised the concern of the potential for a single fault in non-Class 1E circuits affecting redundant Class 1E circuits. The licensee performed an evaluation of all such circuits and removed computer inputs associated with the EDGs field. The licensee also confirmed that there were no other directly connected circuits which present the same risk of high voltage to redundant Class 1E circuits from a non-Class 1E circuit. Additionally, Section 8.1.6.1.q.7 of the SSES Final Safety Analysis Report (FSAR) documents that there are no potential transformer (PT) outputs directly connected to the computer and all current transformer (CT) outputs to the computer are through transducers that are designed to prevent secondary open circuit voltage of CTs from propagating to safety systems through the computer. The FSAR further documents that high voltage cables (480 volts and higher) are not potential voltage sources into the computer because these cables run in separate raceways from those for the computer input cables and do not come in contact with the computer cables.

To address the staff concerns following the May 22, 1986 event, the licensee submitted several analyses, test results, and proposed modifications to the computer input and various instrumentation and control circuits involving Class 1E/non-Class 1E interfaces. The staff's June 28, 1991, SER found these analyses, test results, and modifications acceptable except for the analysis of NSSS instrumentation circuits in the GE scope of supply which did not

provide isolation devices between the Class 1E and non-Class 1E circuits. The GE analysis assumed that the non-Class 1E circuits are low energy and, therefore, a fault in these circuits despite their proximity or interconnection with Class 1E circuits does not affect the safety function of Class 1E circuits beyond an acceptable level. Notwithstanding the above analysis, the staff concluded in the June 28, 1991, SER that isolation devices were required in these circuits, per IEEE 279-1971. Furthermore, the staff disagreed with the GE determination that monitoring equipment is neither protection nor control. Therefore, the circuits within the GE scope of supply need to be isolated, per IEEE 279-1971.

The issue of isolation of Class 1E from non-Class 1E instrument circuits was determined by the staff to be generic and was incorporated in the staff evaluation of Generic Issue (GI) 161 "Associated Circuits." Associated circuits are non-Class 1E circuits that share power supplies, enclosures, or raceways with Class 1E circuits or are not physically separated or electrically isolated from Class 1E circuits by acceptable separation distance, barriers, or isolation device. GI 161 originated from licensing decisions on Nine Mile Point, Unit 2 (NMP-2), when the applicant for NMP-2 submitted a GE Failure Modes and Effect Analysis (FMEA) report for staff review. This report analyzed those circuits in the GE scope of supply for NMP-2 which did not have an isolation device in the Class 1E/non-Class 1E interface. GE stated in the FMEA that these low voltage monitoring circuits provided neither protection nor control functions and thus did not require isolation per IEEE 279-1971. Further, their low energy was insufficient to cause fault propagation from non-Class 1E to Class 1E equipment. GE also noted that the NMP-2 design was similar to other BWR plants, and this design approach had been accepted by the NRC staff during the licensing review of other BWR plants. The staff did not accept the FMEA for 111 of the 239 NMP-2 circuits involved and, as a result, the licensee provided 35 non-Class 1E components with qualified isolation devices while 76 non-Class 1E components were upgraded to Class 1E. Subsequently, the staff resolved GI 161 by concluding that it is a compliance matter to be addressed on a plant-specific basis rather than a generic concern. The staff resolution concluded that the lack of isolation between Class 1E and non-Class 1E circuits is acceptable if the associated circuits are analyzed or tested to demonstrate that the Class 1E circuits are not degraded below an acceptable level by faults in the non-Class 1E circuits. This resolution was documented in NUREG-0933 "A Prioritization of Generic Safety Issues," dated June 30, 1993.

3.0 EVALUATION

10 CFR 50.55a(a)(2) states, in part, that the protection systems of nuclear power reactors of all types must meet the requirements set forth in 10 CFR 50.55a(h), which endorses the requirements of the IEEE Standard 279-1971. The principle requirement of the standard for protection systems is the single failure criterion which states, in part, that any single failure within the protection system shall not prevent proper protective action at the system level when required. With regard to protection and control systems interaction, Section 4.7 of the standard states, in part, that:

> Any equipment that is used for both protective and control functions shall be classified as part of the protection system. The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements in the design bases.

Subsection 4.7.3 requires that:

> Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.

Also subsection 4.7.4 requires the plant design to provide alternate channels or equipment that are not subject to failure resulting from the same single event which causes a control system action that results in a plant condition requiring protective action and concurrently prevents protective action from multiple channels.

In order for these requirements to be met, when control circuits derive their input from protection circuits and their failure would cause a plant condition that requires protective action, isolation devices must be provided or the alternatives stated in 10 CFR 50.55a(a)(3) must be evaluated. The subject circuits addressed in this supplemental SER are not control circuits. Most of these circuits provide indication, some provide power supply and others are interconnecting cables between non-Class 1E and Class 1E components. Failure of these circuits could not cause a plant condition that will require a protective action. Therefore, a second postulated random failure will not cause a safety concern.

PP&L analyzed a total of 237 circuits for both SSES units within the GE NSSS scope of supply. These circuits are non-Class 1E and are identified in the SSES FSAR as "affiliated circuits." The licensee divided these circuits into the following five categories:

(1) Independent indication circuits (101 circuits).

(2) Indication circuits from redundant dual element thermocouples in the steam leak instrumentation circuits for automatic closure of containment isolation valves (66 circuits).

(3) Indication circuits from circuits whose failure or fault results in a fail safe condition of the protective system (42 circuits in the neutron and radiation monitoring systems).

(4) Diverse protective function circuits (26 circuits in the reactor water cleanup (RWCU) system).

(5) Indication circuits from circuits whose failure or fault affects a subsystem (2 circuits controlling the reactor coolant isolation cooling (RCIC) condensate pump).

An FMEA for each of these groups of circuits was performed following the format of IEEE-352-1975, "General Principles of Reliability Analysis of Nuclear Power Generating Station Protection System." The FMEA evaluated the effects of an open or short circuit in the non-Class 1E component and an unlikely fault voltage of 250 VDC (288VDC max) on the cable connecting the non-Class 1E component to Class 1E circuits. The FMEA determined that the design of the above circuits was acceptable by demonstrating that a random channel failure will not prevent the remaining channels from performing their intended protective function. The FMEA also determined that a random division failure will not prevent a redundant division or a back-up protection system from performing its protective function. This determination is described further below.

(1) Independent indication circuits

These circuits do not share a signal with the protection system because they are connected to separate loops on dedicated instrument taps. Therefore, any failure of these circuits could not affect the protection circuits which are connected to separate taps.

Seven of the 101 indication circuits are used to provide indication following a station blackout event as indicated in the Station Blackout Emergency Operating Procedures in conformance with the guidelines of Regulatory Guide (RG) 1.155 "Station Blackout." The remaining indication circuits, if lost due to an open circuit, short circuit or impressed voltage will have no effect on plant safety since none of those indications are required for post-accident monitoring purposes per the guidance of RG 1.97 "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following An Accident" or by emergency operating procedures. The licensee further determined that the loss of power supplies to these circuits does not adversely affect any protective system except the high pressure coolant injection (HPCI) controller. The loss of power supply to the HPCI controller results in the loss of HPCI. However, in the event of loss of HPCI, the redundant automatic depressurization system (ADS) will provide the required safety functions as a backup to the HPCI system consistent with the FMEA acceptance criteria. Based on the above evaluation, the staff finds that these indication circuits meet the requirements of IEEE Standard 279-1971 for protection of Class 1E circuits from faults in non-Class 1E circuits.

(2) Indication circuits from circuits with dual element thermocouples

Redundant dual element thermocouples are installed in various equipment areas and in the inlet and outlet ventilation ducts in the residual heat removal (RHR), HPCI, RCIC, and RWCU systems to provide isolation on high ambient and differential temperature indication. These thermocouples initiate automatic closure of containment isolation valves in the event of steam leaks in the associated equipment area. One element of both thermocouples in each division initiates a signal to operate a temperature switch in the associated containment isolation logic while the second element of both thermocouples in one redundant train is connected to a non-Class 1E recorder. An open or short circuit on the recorder or connecting cable has no effect on the element providing the protective isolation actuation function because of the separation of the elements. The thermocouple wires conducting the protective signal have a minimum of 300 volts withstand rating to prevent migration of impressed voltage (max 288 VDC) from the indication circuit to the protection system initiation logic. Even if the impressed voltage migrates to the element providing the protective function, the associated temperature switch will fail in the safe mode (actuation occurs). Nevertheless, PP&L analyzed hypothetical scenarios of the thermocouple protective element being affected by a fault or failure in the non-Class 1E component or cables with the consequential loss of the HPCI and RCIC systems and inadvertent closure of the RWCU and RHR system valves. The licensee determined that the acceptance criteria of the FMEA was met because required containment isolation actuation protective functions were available. Based on the above evaluation, the staff finds that these dual element thermocouple circuits meet the requirements of IEEE Standard 279-1971 for protection of Class 1E circuits from faults in non-Class 1E circuits.

(3) Indication circuits from circuits where faults and failure result in a fail safe condition

Under this category, the license analyzed the following protective system Class 1E/non-Class 1E interfaces:

(a) Neutron Monitoring System
(b) Area Radiation Monitoring System

The neutron monitoring system channels trip modules provide trip signals through an operational amplifier to the reactor protection system (RPS). A voltage output to the non-Class 1E instrument is developed through the voltage divider circuit of an operational amplifier. An open or short circuit or maximum impressed voltage on the non-Class 1E instrument or connecting cables is cleared by the fuses on the Class 1E circuit boards. If the fuses and the back-up voltage divider circuits fail to isolate the fault, the high voltage will cause the operational amplifier output circuit to fail open (fail safe mode) and initiate a reactor scram.

In a similar manner, the area radiation monitoring instrumentation initiates a signal to the standby gas treatment system "LOCA Trip and Reset Logic" and provides voltage output to non-Class 1E recorders through a voltage divider circuit. If the voltage divider fails to isolate the impressed voltage on the non-Class 1E recorder or the connecting cable, the area radiation monitoring system fails in a safe mode by actuating the standby gas treatment system. Based on the above evaluation, the staff finds that the neutron monitoring and area radiation monitoring circuits meet the requirements of IEEE Standard 279-1971 for protection of Class 1E circuits from faults in non-Class 1E circuits.

(4) Diverse protective function circuits in the RWCU system

The following diverse signals are provided to detect pipe breaks in the RWCU system and to initiate signals for an automatic closure of RWCU containment isolation valves:

- RWCU System High Differential Flow
- Redundant High Equipment Room Ambient Temperature
- Redundant High RWCU Inlet - Outlet Differential Temperature
- Redundant High Differential Pressure
- Redundant Reactor Water Level

The RWCU instrumentation for RWCU high differential flow, high equipment room ambient temperature and RWCU inlet-outlet differential temperature safety function is provided to initiate automatic closure of containment isolation valves in the event of a pipe break in the RWCU system. An open circuit in the non-Class 1E instrument or connecting cable results only in the loss of indication which is not required to be available in a LOCA or other design basis accident condition. A loss of non-Class 1E power to the instrumentation loop results in an automatic closure of RWCU containment isolation valves, which is the safety function of this system. The closure of these valves does not initiate an inadvertent actuation of a safety system. A short circuit or an impressed voltage on the non-Class 1E instrument or connecting cable results in the loss of trip signals to the containment isolation logic. For this unlikely event, containment isolation would be initiated by the high differential pressure and reactor water level instrumentation channels which do not have non-Class 1E instrumentation connected to their loops. Based on the above evaluation, the staff finds that the above circuits meet the requirements of IEEE Standard 279-1971 for protection of Class 1E circuits from faults in non-Class 1E circuits.

(5) Indication circuits from circuits where failure or fault results in a loss of a subsystem

In this category of instrumentation circuits, the non-Class 1E instrument (level switch) initiates starting of the RCIC condensate pump on a high level in the "Barometric Condenser Tank." An open circuit or an impressed voltage on the non-Class 1E instrument or connecting cable prevents the start of the condensate pump while a short circuit on these components may spuriously start the pump. However, the RCIC Barometric

Condenser Tank Subsystem is not required in order for the RCIC system to perform its safety function of providing make-up water to the reactor vessel following a reactor isolation due to loss of coolant flow from the feedwater system. The RCIC system is not required to respond to a loss-of-coolant accident or other design basis event, and no credit is taken for RCIC injection in the SSES safety analysis. Thus, failure of the non-Class 1E RCIC system level instrument circuit has no effect on safety.

In addition to the single random failure analyses, the PP&L FMEA also included a common mode failure analysis where open circuit, short circuit, and impressed voltage were postulated to affect all cables in the raceways containing the cables of the GE-affiliated instrumentation circuits. Based on the common mode failure analysis, the licensee determined that the failure of all cables in one raceway may cause the loss of one division of a Class 1E instrumentation system. However, the redundant division of the Class 1E system will be available to perform the required safety function. It was also noted that the one-out-of-two taken twice reactor protection system is not affected by failures in GE-affiliated cables as the reactor protection system cables of each channel are routed in separate conduits from the GE non-Class 1E circuits. Based on the above evaluation, the staff finds that the SSES circuits within the GE scope of supply meet the requirements of IEEE Standard 279-1971 for protection of Class 1E circuits from faults in non-Class 1E circuits.

4.0 CONCLUSION

The staff has evaluated PP&L's submittals addressing the open item from the June 28, 1991, staff SER concerning the effects of failures in non-Class 1E GE supplied instrumentation and finds that the GE-affiliated circuits at SSES are in compliance with the requirements of 10 CFR 50.55a(h) in that a lack of channel independence, physical separation and isolation, as required by IEEE-279-1971, does not degrade the performance of Class 1E protection systems below an acceptable level. The results of the licensee's FMEA shows that credible failures and faults in the non-Class 1E GE-affiliated circuits concurrent with a random failure (fault) in the raceway system does not prevent the required safety-related protective action at the system level when required. The staff, therefore, concludes that the SSES Units 1 and 2 instrumentation meets the requirements of 10 CFR 50.55a(h) for protection of the Class 1E/non-Class 1E interface from faults in the non-Class 1E circuits.

Principal Contributor: I. Ahmed

Date: November 5, 1997

5.0 REFERENCES

1. NRC Letter, W. Butler to PP&L, H. W. Keiser, dated June 28, 1991

2. Office of Research Letter, E. S. Beckjord to T. E. Murley, NRR, dated March 12, 1993

3. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated August 23, 1995

4. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated June 27, 1996

5. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated November 27, 1996

6. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated February 3, 1997

7. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated March 10, 1997

8. PP&L Letter, R. G. Byram to NRC, Document Control Desk, dated June 25, 1997

9. PP&L Letter, G. T. Jones to NRC, Document Control Desk, dated September 5, 1997