



A Subsidiary of RGS Energy Group, Inc.

ROCHESTER GAS AND ELECTRIC CORPORATION • 89 EAST AVENUE, ROCHESTER, N.Y. 14649-0001 • 716 546-2700

www.rge.com

ROBERT C. MECREDDY  
Vice President  
Nuclear Operations

May 3, 2002

Mr. Robert L. Clark  
Office of Nuclear Regulatory Regulation  
U.S. Nuclear Regulatory Commission  
ATTN: Document Control Desk  
Washington, D.C. 20555-0001

Subject: Response to Request for Additional Information Associated with the Control Room Emergency Air Treatment System (CREATS) Actuation Instrumentation Rochester Gas and Electric Corporation R.E. Ginna Nuclear Power Plant Docket No. 50-244

References: (1) Letter from R.L. Clark, NRC, to R.C. Mecreddy, RG&E, Subject: *Request for Additional Information Regarding R.E. Ginna Nuclear Power Plant License Amendment Request Relating to the Control Room Emergency Air Treatment System Actuation Circuitry (TAC No. MB1887)*, dated January 28, 2002.

Dear Mr. Clark:

By the above reference, the NRC staff requested additional information regarding the Control Room Emergency Air Treatment System (CREATS) Actuation Instrumentation modification at the R. E. Ginna Nuclear Power Plant. Attachment 1 of this letter provides the requested information.

I declare under penalty of perjury under the laws of the United States of America that I am authorized by Rochester Gas and Electric Corporation to make this submittal and that the foregoing is true and correct.

If you should have any questions regarding this submittal, please contact Mr. Tom Harding, 585-771-3384.

Very truly yours,

Robert C. Mecreddy  
Vice President  
Nuclear Operations Group

1000466

1001

- Attachments: 1. Response to NRC Request for Additional Information (RAI) Dated January 28, 2002
2. Evaluation of Control Room Emergency Air Treatment System (CREATS), Conformance to IEEE Std 603 for Modifications Associated with License Amendment Request

xc: Mr. Robert Clark (Mail Stop O-8-C2)  
Project Directorate I  
Division of Licensing Project Management  
Office of Nuclear Reactor Regulation  
U.S. Nuclear Regulatory Commission  
11555 Rockville Pike  
Rockville, MD 20852

Regional Administrator, Region 1  
U.S. Nuclear Regulatory Commission  
475 Allendale Road  
King of Prussia, PA 19406

U.S. NRC Ginna Senior Resident Inspector

Mr. William M. Flynn, President  
New York State Energy, Research, and Development Authority  
Corporate Plaza West  
286 Washington Avenue Extension  
Albany, NY 12203-6399

Mr. Paul Eddy  
NYS Department of Public Service  
3 Empire Plaza  
Albany, NY 12223

## Attachment 1

### Response to NRC Request for Additional Information (RAI) Dated January 28, 2002

The response to the RAI will be structured as follows. The items in bold italics below are the questions provided by the NRC in the RAI dated January 28, 2002. A response to each item is then provided by RG&E. Several of the responses refer to a document contained in Attachment 2 titled "Evaluation of the Control Room Emergency Air Treatment System (CREATS), Conformance to IEEE Std 603 for Modifications Associated with License Amendment Request." The attached report provides an evaluation of the design of the CREATS modification with respect to the requirements of IEEE Std 603, and accompanying standard IEEE 7 - 4.3.2, to ensure that all applicable topics of review have been addressed.

A. **Responses to Questions Regarding the Proposed Design of the Class 1E CREATS Actuation System**

1. ***The licensee's submittal dated October 29, 2001, page 1, Section 1, Cable Separation/Isolation/Power Train Separation states that : "Separation of trains of internal wiring and devices in these cabinets (RMS2 and Auxiliary Bench board) will be maintained to the extent practicable..., " leads to the conclusion that in a few places, internal wiring separation between redundant trains or channels could not be maintained. If this is true, please justify how this is acceptable without compromising safety.***

Response: The proposed design was reviewed to identify the specific areas that separation of wiring did not meet the requirements of IEEE 384, "Criteria for Independence of Class 1E Equipment and Circuits". Section 5.6 of the attached IEEE 603 conformance report provides a description of where in the design physical requirements are not met, and the technical justification for those exceptions. In summary, separation is maintained at all points for cables that are specific to a single train. Where separation is not maintained due to the cross-train connection of devices, the justification is that no wiring failure can cause loss of the safety function of both trains at any point.

2. ***The licensee's submittal does not address Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) qualification of the proposed design change. Please confirm that CREATS instrumentation will not be susceptible to EMI/RFI, will not become a source for conducted and/or radiated EMI/RFI for other safety-related circuits, and that the EMI/RFI specifications for the CREATS instrumentation envelope the design limits specified in EPRI TR-102323. In addition, other environmental qualifications such as temperature, humidity, pressure, radiation, and seismic withstand capability should be discussed.***

Response: The radiation monitoring equipment being installed for this modification was procured from Inovision Radiation Measurements and has been qualified to the requirements of EPRI TR-102323-R1. This qualification confirms that the instrumentation will not be susceptible to levels of EMI/RFI, nor will it become a source for conducted and/or radiated EMI/RFI for other safety-related circuits. Other environmental qualifications are addressed in Section 5.4 of the attached IEEE 603 conformance report, stating that the equipment was procured and installed to meet the requirement for performing their safety functions for environmental conditions listed in the UFSAR for both normal and accident conditions.

3. ***Unless your in-house setpoint calculation methodology for safety-related instrumentation was previously reviewed and approved by the staff, please confirm that your Procedures EP-3-S-0505, "Instrument Setpoint/Loop Accuracy Calculation Methodology," and CH-RETS-RMS, "RMS Monitor Setpoint Determination", are based on the staff approved industry standards.***

Response: The setpoint calculation methodology used in preparing the final setpoint analysis has been performed as follows. Procedure EP-3-S-0505, "Instrument Setpoint/Loop Accuracy Calculation Methodology" contains the setpoint calculation methodology used at Ginna Station which was created in accordance with ANSI/ISA 67.04 and NRC Regulatory Guide 1.105. Procedure CH-RETS-RMS, "RMS Monitor Setpoint Determination" has been deleted and superseded by IP-DES-4, "Setpoint Change Process". IP-DES-4 requires setpoint changes to be performed in accordance with EP-3-S-0505, which contains the setpoint control methodology. EP-3-S-0505 was used to create Engineering Design Analysis DA-EE-2000-009 to determine the actual setpoints.

4. ***From the submittals, it was not evident to the staff if the licensee has performed failure modes and effects analysis for the new Class 1E CREATS instrumentation system. Please explain how the CREATS actuation circuitry is protected from a potential common cause failure which could cause both radiation protection channels to fail in a non-conservative direction (i.e., instrument output loop fails low).***

Response: A simplified failure modes and effects analysis (FMEA) was performed for the new CREATS instrumentation system. The reliability of the system is addressed in section 4.9 of the attached IEEE 603 conformance report, which focuses on defense in depth through redundancy and testing. Section 4.9 contains both a qualitative and quantitative review of the system design to demonstrate the design strategy is sufficient to minimize the likelihood and consequences of failures on the system, and to conclude that the design has an acceptable level of defense against a failure of safety function performance. Section 5.1 of the attached IEEE

603 conformance report addresses single failure criterion, again discussing the defense in depth approach that ensures performance of the safety functions when required. No common cause failures of the system configuration or logic were identified. Testing throughout the process has been planned and verified to further reduce the probability of an unexpected failure. The vendor has a qualified test program that is reviewed by Ginna before acceptance. Additional bench testing has been performed at Ginna as part of receipt inspection and preliminary bench calibrations. Finally, post-modification testing and instrumentation calibration is performed in the field in the as-installed configuration to demonstrate operability of each individual component required to perform the system's safety function. The post-modification test plan is designed to isolate individual components to test independently, followed by a full functional test to ensure compatibility of all components as installed. After installation, periodic testing and calibration will be scheduled and performed as specified in the Technical Specification request to ensure on-going operability is demonstrated.

5. ***If the toxic gas monitors, actuation logic and associated wiring are to be non-Class 1E circuits, please confirm that physical separation and electrical (signal) isolation will be maintained for Class 1E circuits.***

Response: Separation of non-1E toxic gas from 1E CREATS has been demonstrated in Section 5.6.3.1 of the attached IEEE 603 conformance report. This section describes that fuses are used to isolate power and contact signals of the non-safety related equipment from the safety related portion of the actuation circuit. In addition, Class 1E isolators provide isolation between non-class 1E Plant Process Computer System (PPCS) computer inputs and safety-related ratemeters.

Physical separation has been maintained between toxic gas equipment and safety related CREATS and Radiation Monitoring equipment. All of the toxic gas electrical equipment is installed in dedicated panels in the Turbine Building, and on a dedicated mounting plate on the wall next to the air intake duct in the Turbine Building. The toxic gas detector probes are mounted in the same air intake duct as the Radiation Monitor detectors, with adequate physical separation maintained so that there is no interference between the two systems for any plant conditions. Conduits were routed in the Turbine Building so no failure could result in damage to the safety related components.

6. ***In your response to our request for additional information, please include a statement verifying that the proposed CREATS actuation circuitry design meets all previous commitments regarding NRC regulations and industry standards for safety-related systems.***

Response: The proposed CREATS actuation circuitry design was performed to meet all previous commitments regarding NRC regulations and industry standards for safety-related systems as listed in our Technical Specifications and UFSAR.

***B. Questions Regarding the Process for Dedicating Commercial Grade Digital Equipment***

The digital ratemeter instrumentation being procured for this change is not being procured commercial grade and then being dedicated by RG&E for use in a safety related application. Ginna Station is purchasing this equipment from Inovision (formerly Victoreen), a qualified Appendix B supplier, as equipment qualified as safety related under all of the requirements of both the Inovision and the Ginna Station QA programs. Ginna procurement specification EE-171 requires that the equipment be safety related and shall be supplied in accordance with the requirements of 10CFR50, Appendix B. RG&E relies on the Quality Assurance programs and the auditing mechanisms built into the industry NUPIC, and our own source surveillances, to provide assurance that all equipment supplied by Inovision that is qualified as safety related meets nuclear industry standards for qualified equipment. Due to the procurement and qualification method being used, RG&E did not follow the process for dedicating commercial grade digital equipment. Answers to the RAI questions follow to the extent that the information is relevant for components procured qualified as safety related.

***1. What are the types of equipment, manufacturer and model? What documentation is available on the dedication process?***

Response: The system manufactured by Inovision Radiation Measurements is a Model 955A Geiger-Mueller tube Area Monitor, which includes a Model 956A-201 Universal Digital Ratemeter (UDR) and a Model 897A-210 GM detector. The digital ratemeter uses the P/N 94095603 EPROM. The detector operates over the range of  $10E-2$  to  $10E3$  mR/h. The Model 956A UDR provides display, control, and annunciation functions. The basic functions of the UDR are to convert the input pulses from the detector into a digital value, and to compare this value with the setpoint. Analog outputs are provided for connection to the Ginna Plant Process Computer System. Alarm setpoints are programmed through front panel pushbuttons. The equipment is being supplied by Inovision as safety related per the requirements of 10CFR50, Appendix B, and their QA records document the dedication of this equipment.

***2. What type of digital device is used, i.e. microprocessor, PLC, or Application-Specific Integrated Circuits (ASICs)? Which device is it?***

Response: The Model 956A UDR is a microprocessor based device, whose operation is controlled by the installed firmware. The microprocessor is a 8 bit Motorola 6802.

**3. *How many of these are in use at other sites, nuclear and non-nuclear?***

Response: The Victoreen 94X series digital ratemeters were originally designed in 1984. The same basic algorithms are also used in the 956A type devices. The UDR has been installed in over 2,000 process and area radiation channels since then. This series of monitoring systems has been provided to fourteen nuclear sites, totaling over 100 channels. At four of the sites, Inovision (Victoreen) provided them as qualified units. Ginna Station has 25 units installed that have the 94X series of ratemeters installed with the same or earlier revisions of the same software.

**4. *Is there a failure history available, and if so, how accurate is it?***

Response: The NUPIC audit referenced in the IEEE 603 conformance report (Ref. 2.10) contains a section that “verifies that measures are established and implemented to assure that the software errors and failures from both internal and external sources are identified, documented, resolved, evaluated, assessed for impact on past and present applications, and resolved.” The report then refers to the vendor QA programs that provide documentation that an adequate process is in place.

A customer complaint data base is maintained for each product. Customer Complaints are logged and tracked in this system. No complaints have been filed for the 956A product. The Victoreen / Inovision Customer Service Repair Department tracks equipment returned for repair. Since 1987, of the 200+ 956A units shipped, approximately twenty have been returned. All but five of the units were returned for recalibration. Of the five units not returned for calibration, four were sales demonstration units and one was incorrectly classified as a repair. This data accurately reflects the field proven reliability of the unit as there is no adverse failure history related to misoperation of the software / firmware.

RG&E has performed a search of the nuclear OE database, and found no history of failures of Inovision or Victoreen radiation monitoring equipment that would be applicable to our installation.

**5. *What type and how much memory is in each device?***

Response: The microprocessor uses standard 54LS logic for timing and system interfaces. Program storage is provided on 32Kb ultraviolet erasable, programmable, read-only memory (EPROM). 8KB random access memory (RAM) is provided for data storage, stack, and operating parameters. A 64 byte electrically erasable, programmable, read-only memory (EEPROM) is provided for long term parameter storage (i.e., set points).

The memory is not user-accessible. The only changes that can be made to the programming are the user-programmable functions on the front pushbuttons. The setpoints are set through those pushbuttons, and those activities are controlled by Ginna operating and modification procedures so that they cannot be changed without following the change-control process.

6. ***Is the code in the device accessible to the end-user? How many lines of code are there?***

Response: The code is not accessible to the end-user.

There are approximately 8,000 lines of code in 31 software modules.

7. ***What programming language was the code written in? What tools were used during software development?***

Response: The code was originally developed on a Hewlett-Packard 64000 microprocessor development system, and is written in Motorola 6802 Assembly Language. The software development system has since been transferred to an ASCII text editor on a DOS based PC. The American Arium (formerly American Automation) Development System's assembler and linker are used to generate the absolute executable source files.

The following excerpt from a correspondence with Inovision provides additional detail on the system software operation:

The software (firmware) is programmed in assembly language, and does not contain an embedded operating system. Upon start up, an initialization routine is run. Once completed, the main program loop, which performs all functions, executes. The main loop calls function specific subroutines, (e.g. counts, alarms, analog output, check source, calibration, RS232 communications, display, setpoint entry, etc. ) to run each cycle. The system is timed by the Non-Maskable Interrupt (NMI), which is generated from a 4Mhz crystal clock. Four NMI events are generated each second. A hardware watchdog timer is provided. If the watchdog timer is permitted to time out (i.e. the main loop does not complete its cycle and provide a reset output), a MPU Fail condition will occur, causing the FAIL relay to change state and the front panel FAIL LED to illuminate. The Fail relay is wired into the CRHVAC Isolation circuitry so that a FAIL alarm will initiate a Control Room Isolation. The functional operation of the specific monitor functions may be easily verified in the monitor factory acceptance test (FAT).

The NUPIC Audit referred to in this response provides a description of the document controls utilized by Inovision for software development, control, and testing.

**8. *How was the code verified and tested? Are those records available?***

Response: The code was developed prior to the application of a formal validation and verification program. The code was manually verified and tested by the developer. Those records are not available. Operating experience of units in the field combined with factory testing and change control processes are used to validate the use of the existing software in these devices. The Inovision QA program, as reviewed by NUPIC, provides assurance that the testing and record keeping are appropriate for application in the industry. Code testing is performed using factory functional testing of the equipment for a complete range of operating conditions. The test plan identifies critical functions, and verifies that the equipment operates as expected, enveloping the code functions.

IEEE 7-4.3.2 Annex D provides guidance on addressing qualification of computers that were not developed per this standard. The objective of this qualification is to determine, with reasonable assurance, that the item being qualified satisfies the requirements necessary to accomplish the safety function. This involves identifying the safety functions that the computer must perform, identifying the characteristics the computer must possess in order to accomplish the safety functions, and demonstrating that the characteristics are acceptably implemented. The documentation that provides that assurance is provided on the Product Information Bulletin. In summary, the combination of actual operating experience in commercial and nuclear facilities, control of the firmware and changes, and functional testing that replicates the actual conditions and safety functions that must be performed, combine to provide adequate evidence that the unit will perform as designed.

**9. *How was the hardware tested? Are those records available? Was a written and verified test plan used?***

Response: Final hardware testing is the Loop Test LT956A/897A-21X included in the System Manual issued with the equipment. This procedure tests the entire channel using operating firmware and a multi-rate portable radiation source to trip alarms, drive analog outputs, verify over/under and loss of count modes. Additional tests for UDR hardware and memory using diagnostic firmware, and factory multi-point range calibration of the GM detector for linearity have been provided to Ginna. Additional contract-specific testing is documented in Qualification Report 950.366. These tests include energy dependency, detector

stability over contract temperature range requirements, tube plateau and repeatability. Consistent with IEEE 7-4.3.2, this testing was performed with the computer functioning with software and diagnostics that are representative of those used in actual operation, and all portions of the computer necessary to accomplish the safety function were exercised during testing.

This testing of the hardware was performed by Inovision as part of the procurement process, and has been submitted to Ginna as part of the qualification documentation in the Operators Instruction Manual, RG&E Purchase Order 4500008671. These documents have been transmitted to RG&E, and have been reviewed for acceptance by engineering. A written test plan was used and reviewed by RG&E for acceptability.

**10. *What in the device is user modifiable? How will this be controlled?***

Response: The device can be modified by the user in three areas:

1. The device contains jumpers that can be moved to select different operating modes for output functions. These jumpers and their functions are described in the vendor manual. All of these functions were reviewed and selected appropriately for the output functions desired for this design and incorporated into the design change package, which receives engineering independent review and verification. Changes to these jumpers cannot be made without following the appropriate design change process, per Ginna procedure IP-DES-2, "Plant Change Process".
2. Setpoints for high and alarm limits are selected through front panel pushbuttons. Changes to those setpoints are controlled by the Ginna design change procedure IP-DES-4 "Setpoint Change Process". Physical changes to the ratemeter to change the setpoint is controlled by calibration procedures.
3. Calibration changes can be made by qualified technicians by varying a potentiometer. That process is per vendor manual instructions that are contained in Ginna controlled calibration procedures.

**11. *What configuration control does the vendor have? If Ginna decides to buy a replacement device in 5 years, what assurance do they have that the new device will be the same as the old device? If it is different, how will Ginna know what the differences are?***

Response: The Inovision Document Control System maintains part number and revision level control of all documents. This includes the master source files used to program the EPROM. Changes to source code must be identified, and are also controlled via our Document Control System. The specific EPROM part number

and, if necessary, the revision originally supplied may be reproduced from our controlled source files.

The firmware/software is defined as a document per their process EI001, change control is in place and can be verified during the procurement process for replacement components by Ginna.

Evaluation of Control Room Emergency Air Treatment System (CREATS)

Conformance to IEEE Std 603 for Modifications  
Associated with License Amendment Request

April 26, 2002

Prepared By: Paul M. Smith 4/26/02

Reviewed By: Thomas J. Hardy 4/26/02

Approved By: John J. Smith 4/26/02

## 1. Purpose

Ginna plant modification PCR 99-004 is being installed to upgrade the radiation monitoring system associated with the Control Room Emergency Air Treatment System (CREATS). The design of this PCR will change the method of detection, measurement, alarm levels and output functions of the Radiation Monitoring equipment. Actuation logic of the CREATS system, including manual and automatic initiation signals, has also been modified. This document will provide an evaluation of the design of the CREATS modification with respect to the requirements of IEEE Std 603, and accompanying standard IEEE Standard 7- 4.3.2, to ensure that all applicable topics of review have been addressed.

## 2. References

- 2.1 PCR 99-004, "Control Room Radiation Monitor Skid Replacement"
- 2.2 Ginna Station UFSAR
- 2.3 10 CFR 50, Appendix A, GDC 19 - Control Room
- 2.4 Design Analysis, DA-EE-2001-047, "Instrument Bus Electrical System Evaluation", Rev. 0.
- 2.5 Design Analysis, DA-EE-2000-009, "Instrument Loop Performance Evaluation and Setpoint Verification, Instrument Loop Number RMS R45/R46, Rev.0"
- 2.6 Design Analysis, DA-EE-2001-009, "Electrical Factors Analysis for PCR 99-004"
- 2.7 Design Analysis, DA-EE-2001-013, "Control Room Radiation Monitors Analytical Limit Calculation, Rev. 0"
- 2.8 Ginna Electrical Specification, EE-100, "Technical Specification for Fuse Requirements", Rev. 10.
- 2.9 Ginna Electrical Specification, EE-171, "Control Room Radiation Monitor Specification", Rev. 1.
- 2.10 NUPIC Audit Number 17889, NUPIC Joint Audit of Invision Radiation Measurements, Aug. 30, 2001.
- 2.11 ANSI/ISA-67.04.01 "Setpoints for Nuclear Safety-Related Instrumentation"
- 2.12 EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants"

- 2.13 IEEE Std 338, “ IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems”
- 2.14 IEEE Std 344, “IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations”
- 2.15 IEEE Std 384, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits”
- 2.16 IEEE Std. 379, “ Application of the Single-Failure Criterion to Nuclear Power Generating Safety Systems”
- 2.17 IEEE Std 497, “ IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations”
- 2.18 IEEE Std 603-1991, “Criteria for Safety Systems for Nuclear Power Generating Stations”
- 2.19 IEEE Std 7-4.3.2, “Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”
- 2.20 ISA-RP67.04.02, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.”
- 2.21 Regulatory Guide 1.53, “Application of Single-Failure Criterion to Nuclear Power Plant Protection Systems”
- 2.22 PSAER 2002-0009, “PSA Evaluation Request”, PCR 99-004, 3/29/02.

### **3. Modification Description (PCR 99-004)**

- 3.1 The existing CREATS system has a single train of logic to initiate an automatic isolation of the Control Room HVAC system. Radiation is monitored by a single sensing skid that has three detectors - noble gas, particulate, and iodine. A single pump draws an air sample through tubing from the Control Room air intake duct. Each detector has a single high alarm output contact. These contacts are connected in series in a single train of initiation logic so that any single detector will activate a Control Room isolation. Loss of power to any component in the system will cause an automatic isolation - all components are configured in a “fail-safe” arrangement. There is also a single manual isolation pushbutton located in the Control Room Auxiliary Bench Board (ABB), which operators can use to manually initiate an isolation signal.
- 3.2 The modification will replace the existing single train with two redundant systems. The radiation monitoring portion of the system will consist of duplicate radiation detectors, ratemeters (designated R-45 and R-46), and power supplies. The sensors are mounted in the Control Room air intake duct, directly in the intake air flow, so no air sample needs to be drawn off for

monitoring. The sensors will measure total counts of radiation versus the separate components of the existing system. The count signals will be converted into mR/hr dose rates in the ratemeters, with displays in the Control Room and on the Plant Process Computer System (PPCS). The ratemeters and isolators will be mounted in the Control Room in the Radiation Monitoring System (RMS) racks (R-45 will be in rack Incore 5 (IC5) directly next to rack RMS 3, so it will be considered and referred to as one of the RMS racks in this document). High alarm values will be set in the ratemeters to provide an isolation output signal when values reach the proposed setpoint limits. A Main Control Board Annunciator and PPCS alarm will come in when the alarm level is reached and an isolation initiated. Warning alarm levels will be set in the ratemeters and on PPCS to provide indication of levels increasing before reaching alarm level. A FAIL signal in the ratemeter, which is initiated by a loss of signal from the detector, loss of power or anti-jam trip, will also initiate the isolation signal. Ratemeter outputs will also be displayed on chart recorders already mounted in the RMS racks to provide trend data to the operators for reference.

- 3.3 The CREATS isolation logic is also being upgraded to provide redundant strings for isolation initiation. Redundant relays will initiate isolation in a one out of two logic. Each ratemeter supplies an isolation contact to both logic trains. Redundant manual pushbuttons are set up so that pushing either button sends an initiation signal to both isolation relays. Upon initiation of an isolation from any signal (automatic or manual), the system will seal-in to the isolation position so that it cannot return to normal configuration without Operator action to depress a manual reset pushbutton. The logic trains are supplied by train-separate Class 1E control power sources (120 VAC from Instrument Buses). The failure mode for loss of power or signal of any component is to fail to the isolation configuration. Attachment 1 illustrates the redundant features and the cross-train connection of initiation signals that provide additional assurance of an isolation initiation.

#### **4.0 Design Basis - IEEE 603 Sections 4.1 - 4.12**

- 4.1 The design basis events applicable to the operation of this equipment are the events that are evaluated in the Chapter 15 of the Ginna UFSAR. The modified system has been designed to function for the following events and resulting operating conditions: Large Break Loss-of-Coolant Accident, Small Break Loss-of-Coolant Accident, Rod Ejection Accident, Steam Generator Tube Rupture Accident, Steam Line Break Accident, Fuel Handling Accident, and Tornado Missile in Spent Fuel Pool. Environmental and operating conditions used as design requirements are based on the most limiting conditions for the area that the equipment is located in as described in UFSAR Table 3.11-1. For all of these events, the functional requirements for the new system are the same - to maintain an ability to isolate the Control Room upon an increase in radiation levels in the air intake duct. The modified system operates independently of other ESFAS systems, so this equipment will respond and perform its safety functions irrespective of the operation, or failure to operate, of other plant systems. Each component has been analyzed or qualified to operate throughout the range of most limiting conditions, and the installation has been reviewed to ensure that the qualification to maintain that ability has not

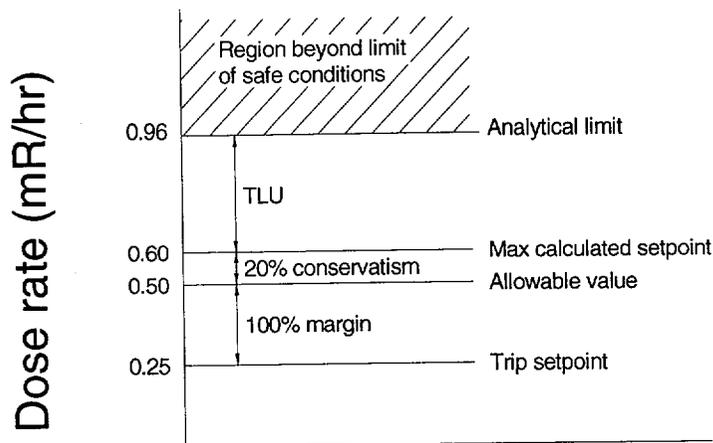
been degraded.

- 4.2 For all design basis events referenced in 4.1, the safety functions and corresponding protective actions of the execute features remain the same. The new radiation monitoring systems' functions are:
- detect radiation in the air intake duct airflow before it enters the Control Room environment
  - measure the radiation counts and calculate an equivalent mR/hr total dose rate
  - display the dose rate value to the operators
  - initiate a Control Room isolation signal to the isolation logic when pre-set radiation alarm limits are reached, which are based on the limits prescribed in GDC 19. This is a maximum of 5 rem whole body dose or its equivalent to any part of the body, with a 30 day weighted average dose rate of less than 15 mr/hr. The selected setpoint will ensure that these limits are not exceeded.
  - the modified isolation logic will operate to send a signal to all of the isolation devices to go to the isolation position (dampers travel to their isolation position, charcoal filter fan starts), and remain in that isolation position until the condition clears and operators take deliberate manual action to restore the CREATS to normal configuration.
  - the logic will also go to isolation upon a manual isolation initiation performed by the Operator
  - the logic will initiate a Control Room isolation on loss of power to any individual relay, power supply, ratemeter, or to the complete system
  - the logic will initiate a Control Room isolation upon failure of the detector or on over range signal received at the ratemeter
- 4.3 The bypass capability available is two individual maintenance bypass switches, one for each radiation monitor, that operate independently to disable the trip function of one train. This function was incorporated to allow system maintenance or testing of a single channel while the redundant channel could still perform the required safety functions without having to perform an unnecessary actuation of the safety system. The bypass switch, when put in the bypass position, closes a contact around the output isolation initiation contacts of the ratemeter, effectively inactivating the isolating capability of that individual ratemeter. Each ratemeter has a switch independent of the other unit, so bypass of one unit does not impact the isolating capability of the redundant ratemeter. When a single unit is in bypass, the unit is declared inoperable, and the plant enters an LCO and a time limit is placed on restoration of the unit. If restoration is not achieved within the time limit, a manual isolation signal will be initiated to place the Control Room in the isolation mode. Operation of the bypass switches is procedurally controlled. There is red-green light indication of the switch status. The switches and lights are prominently visible to the operators at all times on the front of the RMS racks in the Control Room, so inadvertent actuation of the bypass switches is unlikely, and if it occurred, would be detectable. Additionally, the panels are checked during shift routine operations checks. There is no bypass switch that can operationally bypass the system. If both maintenance bypass switches are put into the bypass position coincidentally (though procedurally prohibited), the automatic initiation signal would be blocked from both trains, but the manual isolation pushbuttons would still allow the isolation function to be performed. The PPCS would still be displaying the radiation level

and would alarm if high level was exceeded.

- 4.4 IEEE 603 section 4.4 requires establishing a basis for the setpoints of the instrumentation that will initiate the safety functions required. The setpoints applicable to this section are the high radiation alarm settings in the ratemeters that will, when exceeded, automatically initiate the safety function. Design Analysis DA-EE-2001-013 is a setpoint calculation that describes the basis for determining what the safety limits are, and determines an appropriate setpoint to ensure that the system analytical limit for isolation initiation will maintain an environment below absolute dose limits required by GDC 19. DA-EE-2001-013 results are incorporated into DA-EE-2000-009, which is the instrument total uncertainty analysis that calculates the actual setpoint values that will ensure that the analytical limit is not exceeded. An Allowable Value of 0.96 mR/hr was calculated to be the maximum dose rate that would be acceptable without being able to reach the 30 day exposure limit of 5 Rem specified in GDC 19, leading to a conservative alarm trip setpoint value of 0.25 mR/hr. Figure 1 illustrates the relationship between the nominal safety system setpoints and limits of safe conditions. The analytical safety limit, setpoint allowable value, and trip setpoint of the ratemeters are shown, which also shows the calculated margins for all equipment uncertainties and allowable equipment drifts. The calculation methodology used in developing uncertainty analysis DA-EE-2000-009 was developed using Ginna procedure EP-3-S-505, "Instrument Setpoint/Loop Accuracy Calculation Methodology", which is based on industry standards, as referenced in IEEE-603. The standards used in developing the methodology used are ANSI/ISA-67.04.01 "Setpoints for Nuclear Safety-Related Instrumentation", utilizing the recommended practice of ISA-RP67.04.02 "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation. The determination of the values and the relationship between them shown in Figure 1 below follows the methodology of ISA-RP67.04.02 section 7 Figure 6.

<i>Limit Label</i>	<i>Dose Rate (mR/hr)</i>
<i>Analytical Limit</i>	<i>0.96</i>
<i>Maximum Calculated Setpoint</i>	<i>0.60</i>
<i>Setpoint Allowable Value</i>	<i>0.50</i>
<i>Trip Setpoint (nominal)</i>	<i>0.25</i>



Constant for all events

**Figure 1  
Setpoint Limits Graph**

4.4.1 Monitored Variables

4.4.1.1 The variable being monitored is the radiation dose rate detected in the airstream passing through the air intake duct to the Control Room. The range of the instrumentation is 0.01 - 1000 mR/Hr. The value detected in normal conditions (background radiation) is 0.01 - 0.05 mR/hr, based on actual measured values at the air intake duct. During accident conditions, the maximum value detected at the sensor location for the DBA cloud is 5.63 mR/hr, per analysis DA-EE-2001-013. These values are within the operating range of the monitoring system. The rate of change of the radiation level in the duct has been assumed to range from the minimum gradual ramp up rate of increase up to an instant step change from 0 to the maximum DBA cloud dose rate.

4.4.1.2 The most limiting rate of change is the step change, and that has been analyzed with respect to the response time of the new equipment in section 7.3.1 of DA-EE-2001-013, as follows:

The total response time of the system to a step change in the radiation value is 60 seconds, which is the total averaging time of the detector due to the pulse counting algorithm. The DBA cloud would have a concentration of noble gas that would result in an in-duct reading of 5.63 mr/hr (from DA-EE-2001-013), as described above. At time zero, the 60 second rolling average is at 0 mr/hr. When the most severe design basis cloud reaches the detectors with an instantaneous equivalent dose of 5.63 mr/hr cloud, it would take 11 seconds to reach an

averaged reading at the ratemeter of 0.96 mr/hr. Two factors make that delay in reaching the analytical limit insignificant. First, the transit time for the air to get from the in-duct detector location to the Control Room isolation dampers is greater than 30 seconds, so the cloud will not have reached the Control Room in that time period. Secondly, if the transit time is not considered and it is assumed that the cloud is dumping into the Control Room for the complete 11 seconds, that air is diluted into the total Control Room volume, dramatically reducing the cloud concentration and hence effective dose. Mathematically, 11 seconds of air at 2,000 cfm (existing HVAC capacity) is 367 cu. ft., diluted into the Control Room volume of 36,000 cu. ft (measured volume of CR). The resulting concentration of noble gas in the Control Room is approximately 1% of the DBA concentration, or less than 0.9 mr/hr actual Control Room dose which is insignificant when compared to the GDC 19 limit 30 day dose rate of 15 mr/hr.

- 4.4.1.3 The event that would result in the longest total response time would be a fractional event that resulted in a cloud that had a dose rate that exactly matched the setpoint of 0.25 mR/hr. This event would take the complete 60 seconds (60 data samples) to bring the average value up to the 0.25 setpoint. Again, without taking credit for the transit time in the duct, the 60 seconds of cloud traveling into the Control Room at 2,000 cfm is diluted into the 36,000 cu. ft. Control Room volume will result in a dose rate 18 times (36,000 cfm / 2000 cfm) smaller than the measured setpoint. No credit was taken for this dilution factor in the setpoint analyses, so the resulting isolation at this limiting condition would be a factor of 18 times below the 30 day dose rate.
- 4.4.2 Design analysis DA-EE-2001-013 calculates the safety limits using required limits specified in GDC 19. In summary, the setpoint limits are based on maintaining the Control Room at a dose rate level that, if sustained, would not result in an Operator accumulating a whole body dose greater than the GDC 19 thirty day limit of 5 Rem whole body. A mR/hr maximum dose rate has been calculated taking into account the exposure time expected over thirty days, Control Room geometry, and intake duct (sensor location) geometry. Conservative assumptions have been made in considering all of these variables, as described in the analysis. The calculated analytical safety limit is 0.96 mR/hr. This value is illustrated in Figure 1.
- 4.4.3 Design Analysis DA-EE-2000-009 calculates the total instrument loop uncertainty to develop actual required setpoint values to ensure that the analytical safety limit determined above is not exceeded. The analysis considers all appropriate variables and uncertainties listed below in calculating the maximum setpoint and in recommending a final setpoint to include additional margin for actual operation of the system. The basic equation used in calculating the maximum setpoint, as taken from DA-EE-2000-009 Section 7.8 is:

## TLU Alarm

$$TLU_A = \pm (TLU_1 + M\&TEU^2 + DU^2 + REU^2 + TU^2)^{1/2}$$

Where:

- TLU<sub>1</sub> = The Total Loop Uncertainty Indication
- TLU<sub>A</sub> = The Total Loop Uncertainty Alarm
- REU = Rack Equipment Uncertainty
- SU = Sensor Uncertainty
- DU = Drift Uncertainty
- TU = Tolerance Uncertainty
- IU = Indication Uncertainty
- M&TEU= Measurement and Test Equipment Uncertainty

Figure 1 illustrates the relationship between the setpoint calculation values. The setpoint analytical safety limit is 0.96 mR/hr, the maximum calculated setpoint is the Analytical Limit minus Total Loop Uncertainty which equals 0.60 mR/hr, and the conservative value to be used as maximum allowable value in the Tech Specs is  $\leq 0.50$  mR/hr. The actual setpoint value is conservatively recommended to be one half of the Tech Spec allowable value, so it is set nominally at 0.25 mR/hr.

- 4.4.4 The multiple layers of conservatism that drive the actual setpoint much lower than the analytical limit is acceptable because the consequences of inadvertent operation of the system to perform its safety function does not impact the safe operation of any other plant equipment. A false trip initiates a Control Room isolation. That condition does not impair the operators from performing any other control activities. The Control Room can remain in isolation indefinitely from an operating perspective. The restoration of the system to normal after clearing the false signal is a one step process of pushing a manual reset pushbutton, so there is no excessive efforts required to recover from a false alarm. In addition, this conservative setpoint was evaluated for the risk of experiencing a false initiation with respect to the normal radiation levels measured at the sensor location. The nominal setpoint is approximately ten times the normal background value, so inadvertent actuation due to normal conditions or slight perturbations of normal conditions is unlikely.
- 4.5 The CREATS isolation system is designed so that the system goes to the isolation position automatically when alarm limits are reached with no manual actions required of the Operators. Limits are set at levels so that an isolation will occur before radiation levels in the Control Room have reached a point that would put them in a condition where a Manual initiation of the system would be required. Each ratemeter in the Control Room has a very visible LCD readout indicating the mR/hr dose rate measured by the detectors. Both channels are constantly reading and updating, so a radiation excursion would be evident to Operators monitoring these racks, and the Operator has the discretion to take manual action for any off-normal condition. The measured radiation values are also connected to the PPCS, with alarm levels set to alert operators if the ratemeter level goes above the setpoint level. Manual initiation of a CREATS isolation is one of

the system's design functions. Redundant manual pushbuttons are on the Control Room Auxiliary Bench Board. Pushing either pushbutton will result in an isolation signal to both trains of logic. An Operator can, at any time, manually initiate a Control Room isolation with either of these pushbuttons. There are no other interlocks. A manual initiation will not impact any other systems or degrade the condition, availability, or operability of any other equipment. It will not degrade the habitability of the Control Room to a degree to degrade the performance of the Operators or any equipment.

- 4.5.1 The other manual action associated with the operation of the new system is the restoration of the CREATS from isolation configuration back to normal configuration after environmental conditions have returned below alarm levels. The system does not automatically reset and return to normal. The Operator must take a deliberate action to push the Manual Control Room Isolation Reset Pushbutton. This pushbutton will clear the lock-out contact that has locked the initiating relay into the isolation configuration. If the reset pushbutton is pushed while any parameter is still above the high alarm level, the logic will not reset as the open contacts from the alarming device will prevent the isolation relay from re-energizing. This prevents the system from being restored to normal until all alarm conditions are cleared.
- 4.6 The setpoint limit calculated in design analysis DA-EE-2001-013 takes into consideration the spatial differences and geometric relationship of the location of radiation detection and the Control Room. The setpoints have been determined based on the most limiting locations for both the sensor in the air intake duct and the Operators in the Control Room. The Operator is assumed to be in the location in the Control Room that would maximize his exposure, which is the most conservative assumption for the calculated maximum possible exposure. Two sensors (one per train) have been determined adequate for in-duct measurement based on the geometry of the location. A straight piece of duct was selected to maximize uniformity of the air mix and flow through the duct. The sensors have been mounted in the center of the cylindrical duct to maximize exposure. No contaminated air can flow past the sensors without being detected. No baffles or dampers are in the area of the detectors to degrade the signal by shielding.
- 4.7 Equipment specification EE-171 lists the environmental and operating conditions that the equipment is required to operate during limiting conditions throughout which the safety system must perform. Environmental limits (radiation, temperature, humidity, pressure) are established based on UFSAR Table 3-11.1 for operating requirements of the equipment installed in the Control Room and Turbine Building for normal and accident conditions. Since environmental conditions for the detector location in the air intake duct are not listed in UFSAR Table 3-11.1, the limiting environmental conditions were taken from various sections in the UFSAR for limiting conditions of outside air environment. Table 1 lists the applicable conditions.
- 4.7.1 Each piece of electrical equipment has been evaluated to ensure that equipment electrical ratings meet the requirements of the system operating limits. This evaluation was performed in design analysis DA-EE-2001-009 Electrical Factors Evaluation. Specifically, the radiation monitoring equipment and control devices are supplied from safety related instrument buses. The Instrument Buses are required by Technical Specifications to have a regulated output voltage. DA-EE-2001-009 contains voltage drop calculations which demonstrate that the voltage at the equipment

remains within its design operating range. The power supply to this system is reliable. The instrument buses are fed from uninterruptible power supplies consisting of inverters supplied by station batteries. In the event that power is lost for any reason, the equipment fails to the safe position, which is Control Room isolation.

Table 1  
Design Conditions for PCR 99-004

The equipment will be installed in panels and conduits in the Turbine Building, in the Auxiliary Benchboard and RMS racks located in the Control Room, and in the CR air intake duct which experiences outside air conditions, and are subject to the following environmental conditions:

<u>Turbine Building – Operating Floor</u> (per UFSAR Table 3.11-1)	<u>Control Building (Control Room)</u> (per UFSAR Table 3.11-1)
Normal operation:	Normal operation:
Temperature: 50°F-104°F (77°F nom.)	Temperature: 50°F-104°F
Pressure: 0 psig	Pressure: 0 psig
Humidity: 60% (nominal)	Humidity: 60% (nominal)
Radiation: Negligible	Radiation: Negligible
 Accident conditions:	 Accident conditions:
Temperature: 220°F for 30 mins.	Temperature: Less than 104°F
Pressure: 0.7 psig for 30 mins.	Pressure: 0 psig
Humidity: 100%	Humidity: 60% (nominal)
Radiation: Negligible	Radiation: Negligible
Flooding: Not applicable	Flooding: Not applicable

Air Intake Duct – Outside Air Conditions (for detectors only)

Normal Operation:	
Temperature: -10°F - 104°F	(-10°F is per UFSAR 3.8.1.2.3.3 Maximum Thermal Load)
Pressure: 0 psig	
Humidity: 100%	
Radiation: Negligible	

- 4.8 The equipment has been specified, designed, and installed in a configuration and in locations that will not result in the degradation of safety system performance for any conditions described in the UFSAR for the applicable design basis events listed in section 4.1. All appropriate design provisions have been incorporated to retain the capability for performing the safety functions required for those events. Other events, (such as fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in a non-safety system, or missiles and pipe

breaks not listed in section 4.1), either do not degrade the system or do not result in a condition that will require the system to perform its safety function.

- 4.9 The appropriate reliability level requirements for this safety function have been determined by reviewing the operating requirements and comparing them to the criticality of operation of the safety function with respect to time and consequences. Factors considered in qualitatively evaluating reliability were redundancy of components, independence of the redundant trains, fail-safe operation of safety function actuating components, and cross-train connection of isolation signals to minimize the possibility of an actuating signal from being prevented. All of these factors have been incorporated into the design to maximize the reliability of the safety system, consistent with the criticality of the performance of this safety system.
- 4.9.1 A Probabilistic Safety Assessment (PSA) review of the modification design has been conducted to quantify the potential for a failure to impact the risk of release of fission product. The methodology for performing this PSA takes into account all design functions of the components, and the results are included in PSAER 2002-0009 Ref. 2.22. The resultant probability of failure to perform the intended safety function is  $1.93E-4$ . This probability is acceptable when consideration is given to the low frequency of expected need combined with the ability of the operators to mitigate the consequential conditions with a manual initiation if the failure were to occur.
- 4.9.2 Reliability of the digital components included in this system design have been considered in both the qualitative and quantitative approaches described above in this evaluation. The redundancies and fail-safe configuration of the overall system provides significant levels of defense in depth that maintains a very high level of reliability that make the uncertainties associated with the incorporation of digital devices in the design mathematically insignificant. Additional requirements on the qualification of digital devices are considered in determination of the likelihood of failure of a digital component that could result in reduced system reliability. Operating experience for this equipment has been considered in quantifying the impact on system operability in using these devices. Post modification testing verifies that each level of redundancy will function independent of the other system components to demonstrate the levels of redundancy and reliability. Factory testing of the units is extensive and documented in the Inovision Radiation Measurements Control Room Intake Radiation Monitors Operator's Instruction Manual provided via Inovision Shop Order number S157033. This testing was performed over a wide range of input conditions, specifically testing the digital components extensively. Test data for the units for this modification are included in the vendor manual.
- 4.9.3 This series of units has a history of reliable use in commercial and nuclear applications. Ginna Station has 25 radiation monitors of the same or similar model series installed, operating for up to 10 years. Our units have never experienced a failure due to software errors. The Inovision Appendix B program has been audited by NUPIC (see Audit ID no: 17889) to verify that documented measures are established and implemented to:
- Control software quality.
  - Assure that the life cycle activities are reviewed.
  - Acceptance testing for the software is performed to document the product baseline.

- Assure that changes to software are formally controlled commensurate with those applied to the original software developments.
- Assure that the software errors and failures from both internal and external sources are identified, documented, resolved, evaluated, assessed for impact on past and present applications, and resolved. Assures methods of notification are identified. (It was noted in this report that Inovision did not process any non-conformance pertaining to Firmware or EPROMs since the last NUPIC audit.)

- 4.10 The critical points in time after the onset of a design basis event for the functioning of this equipment is variable, dependent on when radiation begins entering the CREATS system via the air intake duct. There is no initiating signal from any other system that is monitoring plant conditions or that would function due to a design basis event. Critical time for operation is based on the time for a volume of radioactive gas or particles being drawn through the air intake duct to cause the Control Room environment to reach levels that could result in exceeding GDC 19 thirty day limits if the radiation level in the Control Room was maintained. Section 4.4.1 above contains information from design analysis DA-EE-2001-013 that demonstrates that the safety system will be initiated before the Control Room environment can reach unacceptable dose rate levels. Specifically, protective actions are initiated upon the DBA cloud reaching the detector in the duct, where radioactive counts are detected and transmitted directly to the ratemeter. The ratemeter begins converting those counts to an equivalent dose rate. When dose rate alarm levels are reached, a Control Room isolation signal is initiated by an opening alarm contact, instantaneously de-energizing the isolation relays in the Auxiliary Benchboard. The dropout of these relays changes contact states to start the travel of dampers and starting of the charcoal filter fan, all to the isolation position. The protective action is completed when all of the dampers reach the isolation position. DA-EE-2001-013 calculation demonstrates that the time to initiate an isolation is within the critical time for protecting the Control Room environment and ensuring that dose rate levels are not reached.
- 4.11 There are no equipment protective provisions that will prevent the safety systems from accomplishing their safety function. All electrical protective devices (power supply breakers, isolating fuses) fail to the de-energized state which results in all equipment going to its fail-safe isolation position.
- 4.12 There are no other special design basis imposed on the system design, such as interlocks or additional diversity, that are associated with the safety functions or that could otherwise degrade the system.

**5.0 Safety System Criteria - IEEE 603 Sections 5.1 - 5.15 (with IEEE 7-4.3.2 enhancements)**

IEEE-603 Section 5 requires that the safety system shall maintain plant parameters within acceptable limits established for each design basis event. Each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. The design of the proposed safety system meets this high-level requirement. It has been designed to perform its function for all design basis events if radiation levels reach the setpoints of the new

radiation monitors, as previously described in section 4. There are two safety groups in this system, each of which can accomplish the safety function for any event. IEEE 7-4.3.2 has additional requirements on some of the criteria in section 5 which will be addressed.

## 5.1 Single Failure Criterion.

The proposed safety system will perform all required safety functions for a design basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions which cause or are caused by the design basis event requiring the safety functions. The guidance of Reg. Guide 1.53 and IEEE Std 379 was used to evaluate the system design for single-failure adherence. In lieu of a separate single failure design analysis, the following sections through 5.1.4 address the areas of review outlined in IEEE 379.

- 5.1.1 The safety function reviewed under the scope of this modification is the initiation of a Control Room isolation signal. The portion of the system enveloped by this review is from the radiation detectors in the air intake duct through the output contacts on the isolation relays in the Auxiliary Benchboard. It includes the power supplies and all inter-connected non-Safety related components. It will not include the isolation dampers and charcoal filter units controlled by the isolation relays - they are beyond the scope of the modification and their design has not been changed by this modification. Final post-modification functional testing does include testing of these devices to ensure that they perform their safety function and were not impacted by the changes.
  - 5.1.1.1 The protective action that is a result of the proper operation of this system is to provide initiating isolation signals to the isolation devices from the isolation relays upon detection of radiation levels above the setpoints.
  - 5.1.1.2 There are two redundant safety groups, A train and B train, that are capable independently of performing that function. Each functioning component in each group has a redundant component in the other train. There are two detectors, two ratemeters, two initiation relays, and two manual isolation pushbuttons, with power provided by two separate power supplies. The redundant relays result in two separate output contacts to each of the isolation devices, each contact capable of providing the signal to the isolation device to go to the isolation position.
  - 5.1.1.3 The design of the system demonstrates that independence between the two safety groups has been established. For initiation of the signals, there are no shared components. Each train is powered by a separate power supply, cables run in separate train-dedicated conduits, each relay will operate irrespective of the state of the other relay, manual isolation pushbuttons will provide isolation signals irrespective of the other button or of the status of the automatic isolation signals.
  - 5.1.1.4 The design of the logic includes cross-train signal connection so that an initiating event on A train (automatic or manual) will initiate an isolation signal to both relays, and likewise for B train. This was incorporated in the design to provide additional redundancy, so that failure of

one relay would not prevent a high alarm from the detector of the other train from initiating an isolation. The points of train cross-connection only add redundancy, and there is no resultant single-failure point caused. The points of cross-connections are limited to the wiring of normally open device output contacts into the actuation circuit of the other train. There is no manner in which the normally open contacts can fail that will disable the opposite train's actuation logic.

- 5.1.1.5 Mounting of all redundant components in the same structures (such as both detectors in the duct, both trains of logic in Auxiliary Benchboard, both trains of conduit sharing conduit supports) has been performed in a manner to preclude a single component failure (mounting bolt, etc.) from causing both trains to fail, including design basis seismic events.
- 5.1.1.6 The power supplies to the separate trains are independent, separated, and highly reliable, being fed from completely independent UPS systems. There is no common wiring point from the ratemeter location back to the ultimate supply source. Electrical protection in the form of breakers and current limiting transformers have been analyzed in design analysis DA-EE-2001-047 to be appropriately sized to protect all equipment, further reducing the potential for failure on one train of power propagating to devices on the other train. DA-EE-2001-047 also demonstrates the capability of both power supplies to independently supply power adequate for the operation of all equipment required to perform the safety functions. For further protection, all devices powered by the power supplies are configured so that on a loss of power, the output of the devices goes to the isolation initiation state.
- 5.1.2 System Portions Analysis (section 6.2 of IEEE 379)
  - 5.1.2.1 Both trains of equipment have outputs that supply a signal to the non-1E Plant Process Computer System (PPCS) and non-1E radiation recorders. These signals are analog outputs from each ratemeter to communicate radiation levels to the PPCS and the recorders, and this is a non-safety related function. A failure in either the PPCS or a recorder is prevented from causing a common failure in both ratemeters by insertion of independent qualified 1E optical isolators in the circuits that connect the ratemeters to PPCS and the recorders. The isolators themselves are isolated from the 1E power supply to them by putting 1E fuses in the supply circuit.
  - 5.1.2.2 Both trains of isolation actuation logic have signals from the non-1E toxic gas monitoring system (contacts from the toxic gas system processing modules). These signals and power to the toxic gas power supplies are all isolated from the safety related portion of the design by qualified fuses. Design analysis DA-EE-2001-009 reviews the design and provides assurance that adequate protection is there for isolation, and that coordination of protective devices will prevent a fault on the non-1E side of the fuses from causing loss of power to the safety related equipment.
  - 5.1.2.3 A review of the logic demonstrates that there is no single failure point in the circuitry. Refer to Attachment 1 for a block diagram of the system design. Design analysis DA-EE-2001-009 contains a section which describes in further detail the review for single failure. The conclusion is that there is no single failure in the system logic that will cause failure in the channels or actuation circuits that would cause loss of the safety functions.

- 5.1.2.4 Devices in the isolation logic circuits are configured to fail so that any de-energized equipment will fail to the position that provides an isolation actuation signal. Power cannot be maintained incorrectly on the actuator system terminals and cause a loss of safety function because multiple normally open contacts in series provide the actuation signal to the isolation relays, and the isolation relays output contacts likewise are normally open in the control circuits of the associated dampers.
- 5.1.2.5 Attachment 2 is the elementary wiring diagrams of this design, and the series of normally open contacts is apparent. This series of open contacts, coupled with the cross-train connection of the output contacts to each isolation device, provides assurance that even the mechanical failure of contacts to open upon a loss of power in one relay will not prevent the isolation function from occurring due to the opening of the contact in the other train of isolation initiation.
- 5.1.2.6 The connection of electrical power supplies is completely independent. The malfunction of a power supply in a manner that results in a high voltage would only impact a single train, again due to the cross connection only being via normally open contacts so that no voltage is being supplied from one train to the other.
- 5.1.3 All other systems or components that are coupled to these safety systems have been integrated so that they cannot fail in a manner to degrade the safety system. Maintenance bypass switches are designed and installed in the circuit so that a contact block failure will be detected by the indicating lamp associated with each switch. The bypass functions for each train have been connected with separation from the opposing train, and all components qualified and installed safety related. Section 5.1.2.2 addresses the toxic gas signals coupled to the actuation logic, and ensures that no failure can propagate back to the system in a way to preclude operation of the safety functions.
- 5.1.4 SRP Appendix 7.1-C Section 6 contains discussion of scope of review beyond IEEE 603 Single Failure Criterion as it pertains specifically to digital I&C equipment. The concerns with digital equipment in that section are centered around the sharing of data, functions, and process equipment inputs such that a design using shared databases and process equipment has the potential to propagate a common-mode failure of redundant equipment. This design feature is not applicable to the radiation monitors that are being installed as part of this modification. The redundant monitors do not share any data or process equipment inputs. The two monitors operate independently, with train-specific inputs from the detectors. The output alarm contacts that provide the protective functions will operate independently of the status or signals associated with the redundant train. Therefore, the digital nature of these monitors does not lead to the propagation of a common-mode failure of this type. The second concern of digital I&C systems is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. In the application of digital technology for this installation, the software functions are very limited in how they impact the system. The digital functions that are part of the safety functions are 1) the calculation of a dose rate based on input signal from the detector, and 2) the signal to the alarm relay to operate to change output contact states, based on user-set alarm setpoint. These two functions have no other inputs or variables other than the dedicated detector signal for that ratemeter. Both of these functions are completely tested before

installation by the manufacturer, at the time of installation by post-modification calibration and functional testing, and at normal operating intervals via Technical Specification required channel checks, channel operability tests, and scheduled calibrations. All of this monitoring and testing throughout the operating range of the unit provides assurance that the software functions utilized to initiate the protective functions are properly programmed and operating for each unit, and that there is not a software programming error that will occur that will prevent the equipment from performing its safety function in a manner to cause both units to fail at the same time.

The vendor has provided a document citing the extensive use of these digital products throughout the industry and the high reliability of the equipment. Inovision has provided a summary of the product's operating history, stating that the digital firmware has been an extremely reliable product, with a large installed base and extensive control over any changes that have been incorporated. A search of the INPO OE data base resulted in no equipment or system failures due to the failure of the digital ratemeters produced by Inovision (or Victoreen). Combined, these two sources of industry experience indicate that the product has a high level of reliability for use in this application. The NUPIC audit results also state that there are no concerns or findings with the software qualification of this product.

## 5.2 Completion of Protective Action

The proposed safety system logic is designed to ensure that once the isolation signal is initiated, either automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Refer to Attachment 2, elementary wiring diagram. This diagram shows that any of the initiating signals, automatically from the ratemeters or manually from the pushbutton contacts, will immediately drop out the isolation relays R81A or R81B. Upon dropout, a normally open contact from the relay opens in the relays' circuits, locking the isolation signal out. This lock-out assures that the isolation will go to completion, that the output signals from the relays cannot change state back to normal and allow the isolation devices driven from the relay output contacts to go back to normal state. It requires deliberate operator action to push the reset pushbutton to clear the isolation lock-out contact and reset the isolation relays for restoration to normal state.

## 5.3 Quality

- 5.3.1 This modification installs a limited number of new components. All components required to maintain the safety functions and maintain independence for the installation were procured safety related from qualified vendors, or were commercial grade dedicated by the controls of the Ginna Quality Assurance Program. Both processes used in procurement of these components ensure that quality assurance provisions of 10CFR50 Appendix B were met. The handling and installation of all of these components is procedurally controlled to ensure they maintain their qualification after procurement.
- 5.3.2 Critical electrical components will be addressed specifically here. The isolation relays have been procured as safety related from a qualified supplier. Fuses and fuse blocks for isolation, independence, and protective functions have been procured commercial grade but have been

dedicated via a controlled, approved process as described in Ref. 2.18 electrical specification EE-100. All cable for power, controls, and signal has been procured safety related with appropriate quality requirements as dictated by the Ginna QA program. Isolators for interconnection to non-safety PPCS system have been procured safety related from a qualified vendor. The associated mounting hardware for these components is procured as part of the qualified package from the vendor with the electrical component, or if additional support hardware is required for field installation, only parts (screws, bolts, plating) that have been appropriately procured or dedicated to the requirements of the Ginna QA program are utilized, and all uses are analyzed for applicability to the specific point of use.

- 5.3.3 The radiation monitoring system, including detectors and digital ratemeters, have been procured safety related from Inovision, a vendor that is qualified to provide this equipment for use in safety related applications. RG&E implements a vendor oversight program to monitor vendor's quality control for safety-related products. This program falls under 10CFR50 appendix B Criterion VII which requires us to establish specific measures to assure that purchased material, equipment and services conform to procurement documents. Nuclear Assessment Procedure QA-PES-1 describes the methods used by Quality Assurance in evaluating a supplier's capability to be considered as a qualified Safety-Related, 10CFR50 Appendix B supplier, or as a qualified Commercial Grade Supplier, and the methods to be used for their periodic requalification. Included in this procedure are specific details relating to the review and use of third party audits (NUPIC). The use of outside organizations for auditing vendors is based on 10CFR50 Appendix B, and Reg Guide 1.144 which allows the use of outside organizations. The RG&E vendor oversight program was inspected by the NRC in January of 1996 (50-244/96-201) and it was determined to be effective. NUPIC audit number 17889 documents Inovision's qualifications as a supplier of safety related equipment in the industry. The NUPIC process is endorsed by the NRC. The Ginna QA Program requirements have been imposed on Inovision, and the equipment procured for this modification has been monitored under the full requirements of our program to assure quality standards are met.
- 5.3.4 IEEE 7-4.3.2 has additional requirements for this section of IEEE 603. These quality requirements relate to software development, qualification of existing commercial computers, software tools, verification and validation, and configuration management. Inovision has provided QA documentation which addresses these quality topics. The software was developed prior to existing requirements, therefore, no development tracking or formal verification and validation documentation has been developed. IEEE 7-4.3.2 Annex D provides guidance on addressing qualification of computers that were not developed per this standard. The objective of this qualification is to determine, with reasonable assurance, that the item being qualified satisfies the requirements necessary to accomplish the safety function. This involves identifying the safety functions that the computer must perform, identifying the characteristics the computer must possess in order to accomplish the safety functions, and demonstrating that the characteristics are acceptably implemented. The documentation that provides that assurance is provided on the Product Information Bulletin. In summary, the combination of actual operating experience in commercial and nuclear facilities, control of the firmware and changes, and functional testing that replicates the actual conditions and safety functions that must be performed, combine to provide adequate evidence that the unit will perform as designed.

## 5.4 Equipment Qualification

- 5.4.1 Table 1 contains a listing of the normal and accident environmental conditions for the areas in which the proposed new plant equipment will be installed. The equipment to be installed in each location has been reviewed to demonstrate applicability for installation in that environment, except for the condition in 5.4.1.1 below. For the most critical equipment, the radiation monitoring equipment, specification EE-171 was prepared and the vendor was required to provide documentation that the supplied equipment is qualified to operate through the full range of the environmental conditions specified in EE-171. Other components installed for the modification were reviewed by internal engineering review and design verification processes per procedure IP-DES-2 "Plant Change Process". All components have been demonstrated to be adequately rated by the supplier to operate in the environments that they will be mounted in for both normal and accident conditions.
- 5.4.1.1 The equipment in the Turbine Building is exposed to accident environment conditions listed in Table 1 for a Steam Line Break. The toxic gas equipment, as well as the cable connectors to the in-duct radiation detectors, were not procured to these accident conditions. This has been addressed in two ways. First, all non-safety related equipment, which includes all equipment in the CREP panels for the toxic gas system, has been electrically isolated by the installation of fuses inside the CR Auxiliary Benchboard before the cables go out to the Turbine Building. Therefore, no failure of the toxic gas equipment can propagate back to the radiation monitoring equipment or the isolation initiation logic, except to fail open in a manner to automatically initiate a CR isolation. Second, it could be postulated that the cable and connector to the radiation detector could fail at the connection to the detector as it goes into the duct. Therefore, the ratemeter has been configured to initiate an isolation via the FAIL alarm output contacts. The FAIL relay will operate for a loss of signal from the detector. If Accident Environmental Conditions in the Turbine Building cause of failure of the detector cable or connector, then the FAIL relay will actuate and initiate a CR isolation.
- 5.4.2 None of the equipment installed for this modification is dependent on any environmental control system in order to perform any safety function. Therefore, no single failure within an environmental control system can result in conditions that could result in damage to a safety system or prevent a safety system from accomplishing its safety function.
- 5.4.3 Specification EE-171 specifically requires that the instrumentation in the modification, provided by Inovision, be qualified to meet the requirements of EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants" to demonstrate that the equipment is qualified to operate in an environment with EMI and electrostatic discharge concerns. Inovision has provided documentation demonstrating compliance with the requirements of this EPRI document with respect to EMI/RFI qualification.
- 5.4.4 Qualification of the components used in this modification includes documentation to demonstrate that qualification to the seismic criteria applicable to the installed locations has been performed. The verification of the modification per procedure IP-DES-2, "Plant Change Process" reviews

component qualifications against design conditions and ensures that all equipment is qualified appropriately for the intended installation application. A certificate of conformance has been provided by the vendor documenting seismic qualification in accordance with IEEE 344.

5.4.5 IEEE 7-4.3.2 has additional requirements for this section of IEEE 603. Equipment qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish the safety function shall be exercised during testing. These requirements are met during the factory testing of this unit, and the documentation has been provided to RG&E in the vendor manual issued with the units. This testing demonstrates that design basis performance requirements have been met.

## 5.5 System Integrity

5.5.1 Section 5.4 discusses the equipment qualification of all of the components utilized in the design of this safety system, and demonstrates that the components individually are qualified to operate within the range of conditions under which they will be subjected in their installed location. The installation of the components in the manner designed to fulfill their safety function requirements has been designed as prescribed by the PCR process utilized by Ginna Station, as dictated and controlled by engineering procedure IP-DES-2 "Plant Change Process". This procedure applies design requirements and subsequent review and verification processes to ensure that the design is technically adequate and appropriate conservatism is incorporated into all design aspects to assure operation of the system to perform its safety functions over the complete range of operating conditions. Cross-discipline reviews are incorporated into this process to ensure appropriate application of components into various systems and locations. Appropriate design reviews and analyses are performed to either qualitatively or quantitatively assure integrity of the overall system to perform its functions. Examples of such reviews are structural review of equipment mounting in cabinets to assure conditions are appropriate for components and that cabinet integrity for seismic qualification is not degraded by the addition of more components. The Appendix R program is reviewed to demonstrate that all requirements of that program are met. A Change Impact Evaluation (CIE) form is completed per procedure EP-3-S-0306 to act as a checklist to ensure a review of all applicable programs or system interactions is considered in the design process.

5.5.2 Special concerns for digital-based systems as discussed in IEEE Std 7-4.3.2 section 5.5 have also been considered in the system design. When testing or calibration is performed with the unit bypass modes, the redundant train, including the computer, is not effected by the bypass condition. The system will still have full protective functions to isolate the control room. Post-modification testing has been structured to demonstrate that system response will be adequate in the configuration installed in the plant, in both active and bypass modes.

5.5.3 Engineered safety feature actuation system functions should fail to a predefined safe state, as stated in SRP 7.1-C section 10. This aspect has been incorporated into the system design as discussed in a number of previous sections. At many points in the logic, the system has been

designed to fail in a manner that the isolating devices (dampers) will travel to the isolating position, completing the safety function of the system. It is also designed with adequate redundancy and cross-train logic so that failure of one device will not prevent the system from performing its safety function if the other system sustains a subsequent failure. The digital components (ratemeters) are configured so that upon detection of inoperable input instruments (i.e. detector failure), automatic actuation of the protective functions associated with the failed instrument are initiated. Attachment 2 shows the Fail relay output contact in series with the Alarm relay output contact for each train. Failure of digital hardware or software of the system in the ratemeters will not inhibit manual initiation of protective functions. This is evident in attachment 2 wiring diagram that shows the manual isolation pushbutton contacts in series with ratemeter outputs so that if ratemeter outputs failed to the closed contact position, a manual initiation would still drop out the isolation relays and the system would perform its function.

## 5.6 Independence

- 5.6.1 A review of the design of the electrical systems associated with the proposed design has been performed to demonstrate that compliance with the requirements of IEEE Std 384, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits", (Ref. 2.15). A and B train components have been separated into separate compartments in the Auxiliary Benchboard and the RMS racks, so there is physical separation between A and B train redundant components.

Redundant trains of wiring are routed in separate train-specific conduits for the interconnection of all equipment where the cables have to route outside of cabinets. When cables enter enclosures, such as the Auxiliary Benchboard or Radiation Monitoring System (RMS) racks, wiring is run to maintain physical separation between redundant trains of wiring. Where cables are routed through the cabinets to the compartments containing components of the opposite train, the minimum 6" separation is maintained. The "defense-in-depth" design concept that results in the cross-connection of the redundant trains has resulted in a number of cables that are associated with both trains. Separation is maintained up to the points of interconnection between the two logic circuits (relays and terminal blocks). In the RMS racks, the cables have been designated as being associated with the train in which they are logically connected to the isolation initiation relay (if in the R81A circuit, then A train cable). These cables are designated associated to that train and separation from the other train is maintained except at the point of termination at terminal blocks.

In the Auxiliary Benchboard, the cross train logic is encountered where contacts are connected in series from R81A to R81B for signals to the individual isolation devices (dampers, fan, MCB annunciator). The connecting cables go directly from an A train device to a B train device, and since they are not train specific at those points, separation cannot be maintained, so the cables are routed together, separate from all other train specific cables. Since the points of connection between the two trains is the relay contacts, isolation can be credited since relay contacts are considered qualified isolators per IEEE 384 section 6.2.2.2).

There is no physical way to separate the wires to these non-train specific points at the contact terminals from the train specific wires to the relay coils. This has been determined to be

acceptable per a review of the logic and the Auxiliary Benchboard layout as follows: The wiring in the Auxiliary Benchboard cabinet is for the logic to the isolation relays. A review of that logic wiring demonstrates that any fault in the cabinet that causes failure of a wire will result in an opening of the associated circuit. Any open circuit will result in the isolation relay to drop out, automatically causing the initiation of the safety function to perform and put the CREATS in isolation. This is true for either a single train failure or a failure that propagates between both trains due to less than optimal separation. There is not a credible failure mode that would result in a condition in which faulted or failed wires in the Auxiliary Benchboard would prevent the safety system from performing its execute function if an actuation signal was present. The only way to prevent the system from performing this function would be for 120 VAC being applied to the logic circuits of both trains within this cabinet, energizing the relays even after the output contacts of the initiating devices (ratemeter or manual pushbutton) have opened. There are only a few wires that are still energized after an initiation signal in a manner that could cause this type of unlikely "hot short" in either logic train, where a wire could be disconnected and contact the relay with 120 VAC. Since the two R81 relays are in separate compartments in the Auxiliary Benchboard, there are no points where such a condition could also cause a second wire of the other train to fail and energize the opposite train's R81 relay. In addition, failure of any wires in the Auxiliary Benchboard due to inadequate separation between the trains can not propagate back to the ratemeters and cause them to fail in a manner that would prevent the system from performing its safety function.

Wiring for the radiation monitoring cabling, for power to the detectors, and for signal wiring between detector and ratemeter, maintains the minimum separation criteria of IEEE 384 between wiring of redundant trains. Outside of enclosures, the cable is inside of conduits that provide the physical separation between trains. There are only A Train or B Train cables in any conduit, and any non-IE circuits routed with either train in the conduits carrying safety related circuits are train specific associated circuits that are physically separated from or electrically isolated from the opposite train. In the RMS racks, the minimum 6 inches of physical separation is maintained between redundant trains for power and signal wiring. The power cables that were effected by this modification are from terminal blocks in the RMS racks supplied by existing power cables from the instrument buses. Separation has been maintained for all of the new power wiring.

- 5.6.1.1 The design of the safety system precludes the use of components that are common to redundant portions of the safety system, such as common switches or sensing lines, which could compromise the independence of redundant portions of the safety system, with one exception. The manual reset pushbutton is the one switch that is common to both trains, and has been evaluated to demonstrate that it does not compromise the independence of the system to perform safety functions. That pushbutton is used to reset the system and allow return to normal configuration after all initiating signals have cleared. Attachment 2 wiring diagram shows the switch (identifier PB/CRIR). The single reset button is acceptable because it cannot fail in a manner to prevent the automatic safety function from being performed for any mode of failure. Even if the pushbutton sticks closed, blocking the lock-out of both trains, an automatic isolation signal from either train will drop out the isolation relays in both trains and initiate the safety function. As long as the automatic initiation signal is in, the system will maintain its isolation position.

5.6.2 All of the safety system equipment that is required to mitigate the consequences of the design basis events listed in section 4.1 are independent of, and physically separated from, the effects of the design basis event. There are no conditions created by the design basis events that impact the physical independence or electrical independence of any equipment, or result in any equipment not maintaining the capability to perform its safety functions due to a reduction in independence.

5.6.3.1 Isolation between safety related system parts and non-safety components has been achieved using approved isolation devices. This includes the following places where safety and non-safety are connected:

- Fuses are used to isolate the toxic gas system power and input contact circuits from the safety related circuits. These fuses are located in the Control Room in the Auxiliary Benchboard so the isolation occurs before entry into the Turbine Building.
- Optical isolators are used to isolate the analog output of the ratemeter from the station non-1E PPCS and recorders. Power to the isolators is connected on the non-1E side of unit, so power to the isolators is also fused to provide electrical separation on the power circuits. On the non-1E signal side of the isolators, the two trains of non-1E signal cable are run together in a single conduit to the PPCS multiplexer. This is acceptable since they are non-1E circuits, and fuses are installed before they are routed together, providing adequate isolation has been provided so that no failure can prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function.

All fuses used in the system to provide isolation between non-safety components and safety components are classified as part of the safety system, the components are qualified safety related and installed per safety related procedures. The isolators are also classified safety related. Due to the electrical isolation devices and the physical separation of components, there is no credible failure on the non-safety side of the isolation devices that could prevent any portion of a safety system from meeting its performance requirements.

5.6.3.2 Equipment in other systems that is in proximity to the new Control Room Radiation Monitoring System in the following locations:

- in the Radiation Monitoring System (RMS) racks, the only equipment within those racks that are closer than the six inch physical separation requirements are the recorders for the radiation monitoring points. All electrical components within the recorders are contained in an enclosure that provides a physical barrier between the electrical components of the safety and non-safety equipment, so this is acceptable. The recorders are not physically located above the ratemeters, so a physical failure will not result in the recorder falling on the 1E components.
- in the Auxiliary Benchboard right section, there are switches and relays for the balance of the Control Room HVAC isolation system, all of which is classified as safety related.
- in the Control Room Environmental Panel (CREP) panels in the Turbine Building, the components in the toxic gas system are physically separated by the six inch criteria, except where they are terminated to the isolation devices (fuse blocks), which is

acceptable per IEEE 384 section 6.2.2.1.

All of other equipment in the turbine building maintains the six inch physical separation or is physically separated by the train-specific conduits and is electrically isolated by fuses located in the Control Room.

5.6.4 IEEE Std 7-4.3.2 has additional requirements associated with the independence of data communications and software. The data communications for this system is not susceptible to degradation based on a failure of data equipment of the nonsafety classified equipment. Data is sent out of the safety ratemeters through an optical isolator to the nonsafety PPCS, with no communication or data requirements from the PPCS to the ratemeters. There is no dependence on the PPCS for information to support the ratemeter's ability to perform its safety functions. In addition, there is no data communication between the redundant trains of safety related equipment. The ratemeters operate independently of each other, and neither share common data sources nor send or receive data between the two units. There is no logical or software malfunction in one portion that could affect the safety functions of the redundant portions.

## 5.7 Capability for Test and Calibration

5.7.1 Periodic testing and calibration of this equipment will be consistent with safety system testing standards as required by the proposed Technical Specification amendment and plant operating guidelines per periodic surveillance testing standard IEEE 338. Testing of this system can be performed in any operating mode. Test requirements will include periodic channel checks , periodic functional testing of the complete system to ensure that any system initiation signal, automatic or manual, for either train, will result in the execute features performing to completion and the safety functions being performed, and calibration to ensure the equipment maintains the tolerances calculated in the setpoint total instrument uncertainty analysis.

5.7.2 The test provisions have been reviewed for adequacy with consideration to the digital system used for automatic initiation. A channel operability test is performed on a frequent interval through the use of a check source that will ensure that the radiation monitors will respond appropriately to a high radiation source. This test provides adequate assurance that the digitally controlled portion of the system has not had a system failure due to data errors or computer deadlock. Periodic testing as prescribed in the amendment submittal will provide adequate full system checks for all other digital functions.

5.7.3 Post modification testing will be completed to ensure that all safety functions of each component will perform independently. This includes isolating redundant components or jumpering redundant contacts to ensure that the specific component being tested can perform its functions without the redundant component being functional. Failure of components was simulated to ensure that the system performs as expected and no safety functions are lost on any single failure.

## 5.8 Information Displays

5.8.1 IEEE Std 497 requirements are specifically for instrumentation that is required for monitoring to

determine if operator actions are required for which no automatic control is required. The instrumentation displays of this safety system have no functions that require manual control. For a design basis event that results in radiation detected above the alarm setpoint, the system will perform its safety function without operator actions. Operator manual initiation features have been added as additional redundancy and defense-in-depth, and do not require an Operator to read, interpret, and take action based on any of the information displays installed per this modification. Therefore, though the guidance of IEEE 497 was followed in design of this system's displays, the requirements of IEEE 497 are not mandatory for this design so it will not be further addressed in this document.

- 5.8.2 The digital displays of the ratemeters are mounted in a very prominent place in the Control Room, within site of all Operators at the board. Size and location are adequate for viewing and distinguishing the value displayed. Resolution of the value is appropriate for the values that can be displayed and may be evaluated.
- 5.8.3 Bypass switch indication is provided redundantly. Switch position is clearly marked as to the intended position of the switch, indicating channel status. Directly above the switches are Red/Green indicating lights appropriate for this location that indicate channel status. The Bypass switches are positioned directly above the associated ratemeter and are all clearly labeled so that there is no mistaking which piece of equipment it is associated with.
- 5.8.4 Lighting on the Auxiliary Benchboard for system status and indicating completion of the safety functions upon an isolation initiation are all appropriate for the intended application. All locations of indication are consistent with the requirements for easy identification and interpretation by the operator.

## 5.9 Control of Access

Access to all equipment associated with this system that could impact the performance of the safety functions is administratively controlled by plant procedures, including adherence to Technical Specification requirements. The bypass switches are in view of Operators at all times, so operation of those switches cannot be performed without an appropriate procedure. The RMS rack cabinets that house the ratemeters and power supplies are locked, and key distribution is controlled by the Control Room Foreman and/or Shift Supervisor so that permission must be obtained to open that cabinet. The Auxiliary Benchboard is screwed closed and is in the operating area of the Control Room so that it cannot be accessed without explicit Operator permission. No work can be performed on any equipment associated with the system without an approved work package, which is reviewed by Operations for applicability of use based on present plant operating conditions. Equipment in the Turbine Building is not accessible for any access to test points or means for changing setpoints.

## 5.10 Repair

Design of the system installation has been performed to facilitate access for repairs, calibration, and testing. As described in Failure Modes section above, most failures will result in the system

automatically performing its safety function and going to the isolation position. This action will immediately be recognized by operations due to the MCB annunciator alarm that will annunciate coincident with the safety system initiation. Appropriate troubleshooting per approved maintenance procedures will commence.

#### 5.11 Identification

Labeling of all components on the Auxiliary Benchboard and in the RMS racks is clear and consistent with the requirements of the Ginna Human Factors Manual, which was developed following the guidance of NUREG - 0700, Guideline for Control Room Design, and is controlled by Ginna procedure EP-3-P-0133, Human Factors Review. No color coding is used for component identification, however, labels clearly indicate train designation for redundant components consistent with Ginna construction Specification GC-76.10 "Installation, Testing and Inspection of Wire and Cable", which ensures all cable labeling matches the associated circuit schedule and/or CCD drawing. Description on labels is clear and complete to preclude the need for reference materials to distinguish components or trains.

#### 5.12 Auxiliary Features

There are no auxiliary features associated with this safety system function.

#### 5.13 Multi-Unit Stations

There are no shared displays and controls in this safety system design. Each radiation monitor has a dedicated, independent digital display. All controls on the Auxiliary Benchboard for manual operations are dedicated to the designated equipment.

#### 5.14 Human Factors Considerations

A Human Factors Review of the proposed layout of equipment in the Control Room and the location of the ratemeters in the RMS racks and the manual controls on the Auxiliary Benchboard has been performed consistent with procedure EP-3-P-0133. This is reviewed by Operations management and representatives from Operations were involved in the design as part of the modification follow team. All requirements, both administratively required and input from operators based on design document reviews, have been incorporated into the modification configuration.

#### 5.15 Reliability

- 5.15.1 A reliability analysis was conducted using a fault tree model, and component failure rates from the Ginna Station Probabilistic Safety Assessment (PSA), to determine the probability that the control room radiation monitor circuitry fails to perform its intended function (i.e. to send a signal to isolate the control room HVAC system), given that a high radiation condition exists. PSAER 2002-0009 contains the supporting documentation. The resultant probability of failure to perform the intended safety function, given a demand for that function, is 1.93E-04. A review of the cutsets produced from the quantification of the fault tree model indicates that no single failure modes exist. The failure probability is dominated by the common cause failure of the radiation elements, RE-45 and RE-46, as well as independent failure of both elements. These

two failure modes contribute 96% to the overall failure probability. The remaining failure probability is from failures of one radiation element combined with a failure of another component within the system (4%) and two independent failures of other components (<1%). These results are consistent with the design of the circuitry in that the failure of some components (e.g. the radiation elements, the processor in the ratemeter, or the relay in the ratemeter) will affect both trains, but not completely fail both trains (i.e., at least one more failure must occur in each train to fail that train), while the failure of other components (e.g. R81A, R81B, or a short circuit across the R-45 and R-46 relay contacts) can completely fail a single train. However, there are no components whose failure will completely fail both trains.

5.15.2 IEEE Std 7-4.3.2 has additional requirements pertaining to the reliability of the computer portion of the modification. It states that the method for determining reliability may include combinations of analysis, field experience, testing, and software error recording. Inovision has provided evidence that this product has adequate operating history and error tracking to demonstrate design reliability, and that Inovision QA engineering control and testing provides assurance that the specific units shipped to Ginna for this application will meet the operating requirements with the same levels of reliability.

## **6.0 Sense and Command Features - Functional and Design Requirements - IEEE 603 Sections 6.1 - 6.8**

### **6.1 Automatic Control**

This system has been designed, and verified to provide automatic initiation of the execute features to perform the safety functions. No operator action is required to achieve the safety system function. Optional operator control of the system functions is provided and a manual initiation of the safety functions can be performed by the operator. Automatic operation for the design basis event conditions that require operation have been evaluated to demonstrate that the setpoints, margins, errors, and response times have been analyzed and are appropriate. DA-EE-2001-013 and DA-EE-2000-009 setpoint analyses demonstrate these factors have been evaluated. The digitally-based portion of the automatic actuation circuitry has also been evaluated for real-time performance with respect to the systems requirements in these design analyses and found appropriate for the system to perform its functions.

### **6.2 Manual Control**

Manual control is provided in the Control Room to allow operators to initiate the safety systems features with a single manipulation - depressing either manual pushbutton. The pushbuttons are easily identifiable and operable. All indications that the isolation equipment performs the intended functions are located on the same board as the manual pushbutton, so the operator has immediate and clear indication that the appropriate system functions have been performed. No additional action is required of the operator to maintain the system in its safe configuration. After restoration of plant parameters to normal, and high alarms have been cleared, the system can be returned to normal by the Operator through the single manipulation of the reset pushbutton.

### 6.3 Interaction Between Sense and Command Features

Attachment 2 is a wiring diagram that illustrates the automatic lock-out feature of the logic design. This ensures that protective actions will go to completion for any initiating event signal - manual or automatic. A return to normal signal from the ratemeter will not restore the system to its normal alignment until deliberate operator action is taken to restore the system.

### 6.4 Derivation of System Inputs

The command feature inputs for the automatic execute features is a measurement of radioactive activity in the air coming into the Control Room HVAC system. The radioactive activity is directly measured in the duct, and a signal corresponding to the activity in "counts" is transmitted to the ratemeter. The ratemeter interprets the counts and calculates an equivalent "dose rate" that exposure to that activity would equate to. The setpoint for performing the protective functions is based on that value. Ref. 2.6 design analysis describes the relationship between the condition and the setpoint, and demonstrates the direct correlation between the measured variable and the requirement to perform the execute features.

### 6.5 Capability for Testing and Calibration

6.5.1 Testing and Calibration of the instrumentation that senses and determines the values of the monitored values is performed by exposing the sensor to known, calibrated exposures of the variable to be monitored. For radiation monitoring equipment, radioactive sources of known values are installed in a calibrated device that maintains a fixed geometry. This ensures that when the sensor is placed into this custom calibrator, that the sensor will be exposed to an exact known amount of radioactive activity, which has previously been calculated to convert to a dose rate value. This dose rate value will be compared to the digital output value on the ratemeter. This testing is very accurate, and documentation qualifying the validity and accuracy of the calibrator was provided from the qualified supplier as part of its Appendix B program. Calibration and other testing is performed on an interval to assure that adequate accuracy is maintained between calibrations. This is controlled by PM program activities based on vendor recommendations and also by the procedures that control the review of data collected during calibration and testing. Any anomalies are immediately evaluated to explicit criteria for operability. The equipment being installed will be included in the station Maintenance Rule program so that all failures and anomalies will be evaluated to determine if calibration, testing, and other monitoring is on the appropriate interval to maintain system reliability to specific reliability criteria.

6.5.2 Check source channel check capability will be available in the post-accident period to test operational availability of the sensors. Additionally, the sensors have been specified to operate and retain their calibration throughout an event so that they will remain functional during the post-accident time period even after maximum radiation exposure.

### 6.6 Operating Bypass

The only bypass incorporated into the design is the individual channel maintenance bypasses installed at each ratemeter to allow testing and calibration of an individual channel without causing an actuation of the safety system to perform its full functions. There is no Operational

Bypass feature on this equipment.

#### 6.7 Maintenance Bypass

Each channel has a maintenance bypass switch, which allows testing or calibration of an individual ratemeter without safety system actuation. Capability of the safety system to accomplish its safety function is retained while one channel is in maintenance bypass.

Procedurally, only one bypass switch will be permissible at a time, and that will require entering an LCO which will put a time constraint until the system must be restored or put in manual isolation. When a single channel is in bypass, the system is still functional and automatic isolation will be performed if the redundant train detects radiation above the alarm levels.

#### 6.8 Multiple Set Points

6.8.1 DA-EE-2000-009 provides the methodology and calculation to demonstrate the allowance for uncertainties between the process analytical limit and the device setpoint, as documented in section 4.4.

6.8.2 Each channel has a single setpoint for automatic actuation of the safety system functions. A warning alarm is set in the ratemeter to provide early indication of the signal trending toward the actuating setpoint, but no automatic or manual actions are required in response to the warning signal. The setpoint analyses in DA-EE-2001-013 and DA-EE-2000-009, as described in section 4, illustrate that adequate margin exists between operating limits, safety limits, and setpoints. The analyses demonstrate that there is adequate margin such that the system initiates protective actions before safety limits are exceeded. There is a low probability of inadvertent actuation of the system due to the margin between normal levels and setpoint level.

#### 7.0 **Executive Features - Functional and Design Requirements - IEEE 603 Sections 7.1 - 7.5**

The requirements listed subsections of IEEE 603 Section 7 are addressed in Section 6 above.

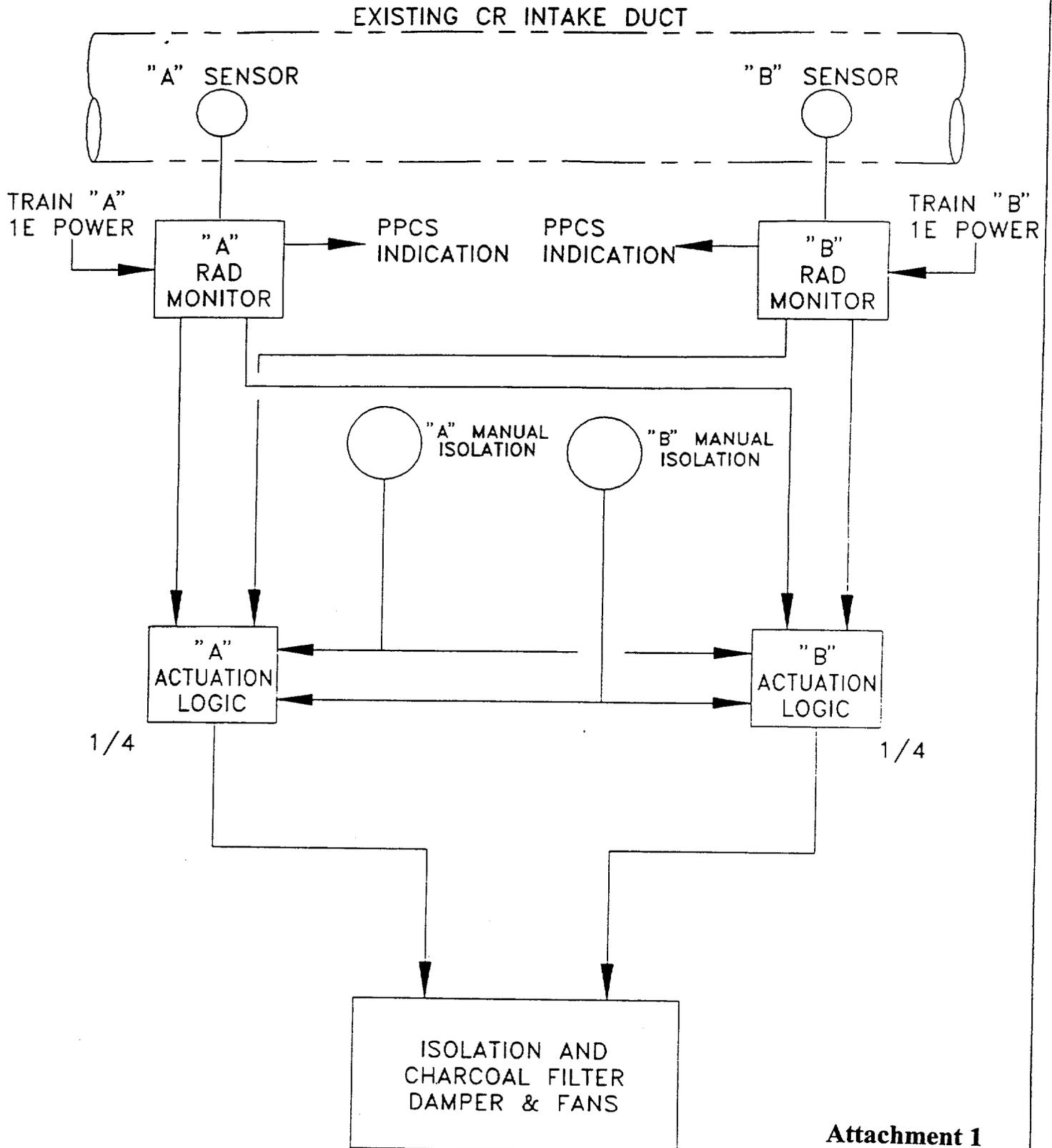
#### 8.0 **Power Source Requirements - IEEE 603 Sections 8.1 - 8.3**

8.1 The electrical power sources that supply power to the safety equipment in this modification are safety related sources. Each train has a separate and independent power source. Reliability of the sources is of the highest level, being fed from constant voltage transformers (CVTs) that provide a high degree of voltage regulation. These CVTs are supplied by inverters, whose ultimate power supply is the large 1E station batteries. This system provides a very reliable uninterruptible power system with excellent voltage regulation. Additionally, the system is designed so that a loss of power to either train will result in actuation of the safety system to perform its function.

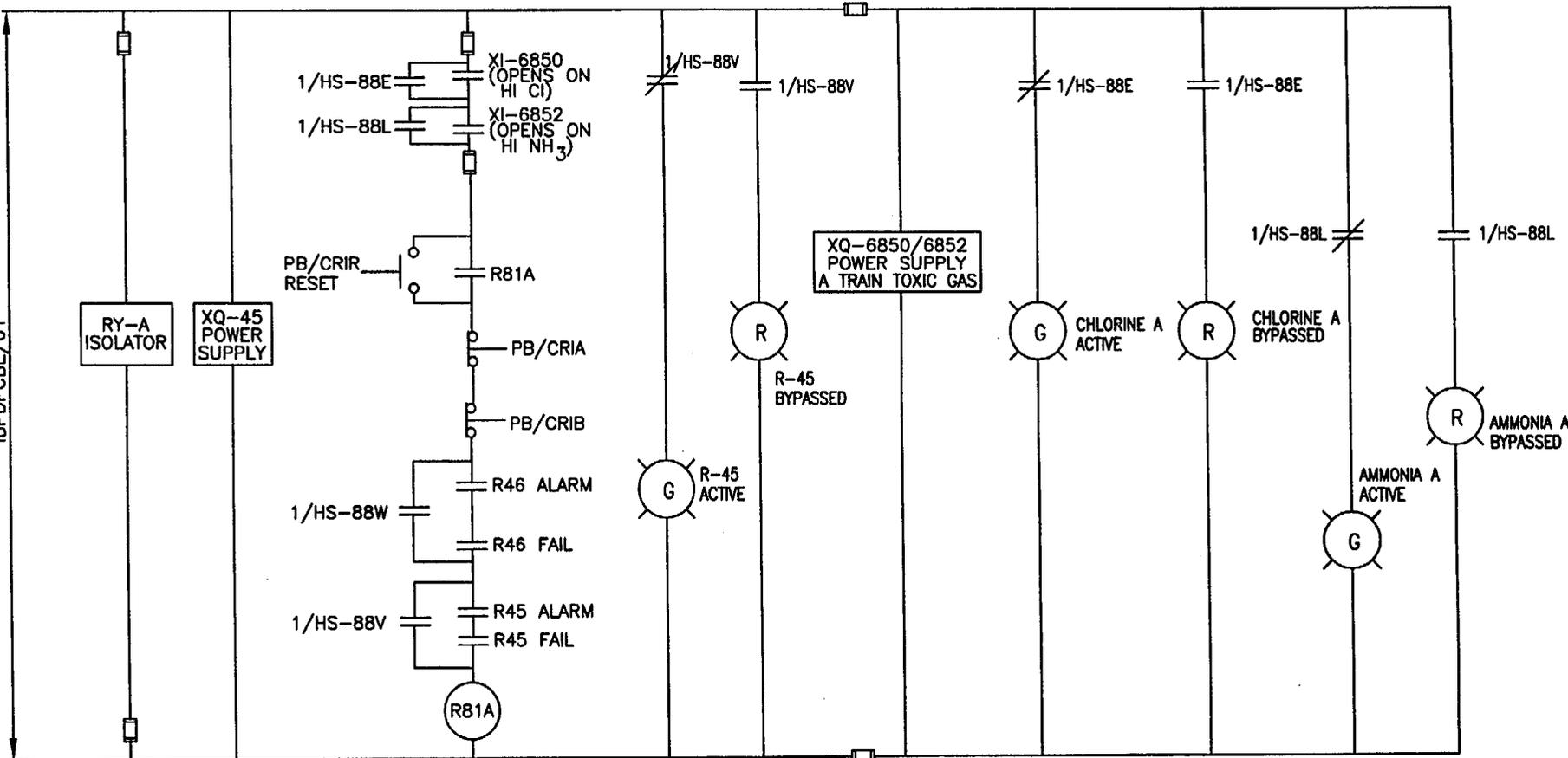
8.2 There are no non-electrical power sources in the new radiation monitoring equipment or isolation initiation logic.

8.3 The maintenance bypass does not interact in any way with the sources of power to the equipment.

# CR RADIATION INTAKE MONITORING INSTRUMENTATION (PROPOSED)



"A" TRAIN  
120 VAC FROM  
IBPDP/01

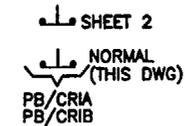
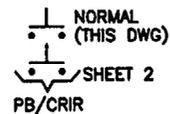


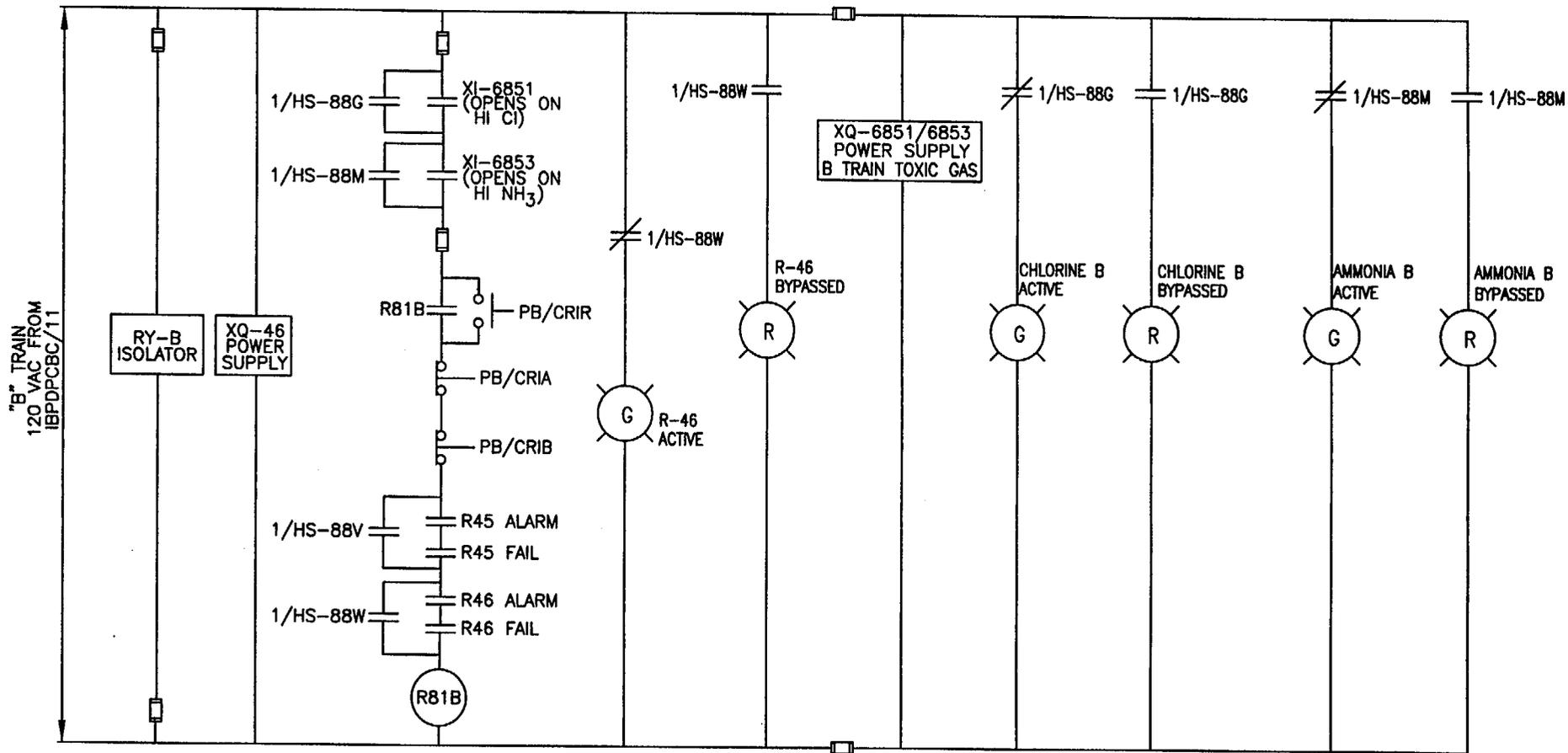
- R81A - CR ISOLATION RELAY A
- R80B - CR HI RADIATION RELAY FROM R36/R37/R38
- PB/CRIA - PB CR MANUAL ISOLATION A TRAIN
- PB/CRIB - PB CR MANUAL ISOLATION B TRAIN
- PB/CRIR - PB CR ISOLATION RESET
- 1/HS-88B - R80B ISOLATION OVERRIDE
- 1/HS-88E - HANDSWITCH A TRAIN CHLORINE BYPASS
- 1/HS-88L - HANDSWITCH A TRAIN AMMONIA BYPASS
- 1/HS-88V - HANDSWITCH A TRAIN RADIATION BYPASS
- 1/HS-88W - HANDSWITCH B TRAIN RADIATION BYPASS
- (CONTACTS FOR 1/HS-88B, 1/HS-88E, 1/HS-88L, 1/HS-88V, 1/HS-88W ARE SHOWN IN ACTIVE OR NORMAL POSITION)

CONTACT BLOCK	CIRCUIT POSITION	
	L	R
	NO	NC
NORMAL TRIP SIDE 	2 POSITION MAINTAINED KEY LOCK SWITCH	

CONTROL ROOM AHU SUPPLY  
DAMPERS CONTROL  
(EP-82) (DWG:10905-196)  
14532S

- SPARE 1 2\*
- SPARE 3\*
- VENT DAMPER SV-81A (DWG:10905-295.SH.1) 4\*
- THIS DRAWING 5\*
- CONT. RM. VENT SYSTEM FIRE MODE (DWG:10905-542) 6\*
- RELIEF DAMPER SV-81B (DWG:10905-295.SH.1) 7\*
- TOILET EXHAUST DAMPER SV-81C 8\*
- CHARCOAL FILTER FAN (DWG:10905-224) 9\*
- SPARE 10\*
- SPARE 11\*
- ANNUNCIATOR E-111 (DWG:10905-0384) 12\*
- R81A
- R81B





R81B - CR ISOLATION RELAY B  
 PB/CRIA - PB CR MANUAL ISOLATION A TRAIN  
 PB/CRIB - PB CR MANUAL ISOLATION B TRAIN  
 PB/CRIR - PB CR ISOLATION RESET  
 1/HS-88G - HANDSWITCH B TRAIN CHLORINE BYPASS  
 1/HS-88M - HANDSWITCH B TRAIN AMMONIA BYPASS  
 1/HS-88V - HANDSWITCH A TRAIN RADIATION BYPASS  
 1/HS-88W - HANDSWITCH B TRAIN RADIATION BYPASS  
 (CONTACTS FOR 1/HS-88G, 1/HS-88M, 1/HS-88V, 1/HS-88W  
 ARE SHOWN IN ACTIVE POSITION)

ATTACHMENT 2

PAGE 2 OF 2