U. S. NUCLEAR REGULATORY COMMISSION
REGION I

DOCKET/REPORT NO: 50-244/94-11

LICENSEE: Rochester Gas and Electric Company (RG&E)

FACILITY: R. E. Ginna Nuclear Power Plant
Ontario, New York

DATES: July 18-22, 1994

INSPECTORS: J. A. Calvert, Reactor Engineer, DRS
L. M. Kay, Reactor Engineer, DRS
R. A. Skokowski, Reactor Engineer, DRS

SUBMITTED BY: John A. Calvert 9/16/94
John A. Calvert, Reactor Engineer Date
Electrical Section
Division of Reactor Safety

APPROVED BY: William H. Ruland 9/16/94
William H. Ruland, Chief Date
Electrical Section
Division of Reactor Safety

Areas Inspected: This was an announced safety inspection to review the modifications for the radiation monitoring system (RMS), the anticipated transient without scram (ATWS) mitigating systems actuation circuitry (AMSAC) system and the advanced digital feedwater control system (ADFCS). The emphasis was on the digital aspects of the systems. The inspection also evaluated management oversight involvement in the modification process, self-assessment, the continuous process improvement team, and the QA audit process improvement team.

Results:

- The present modification process with respect to digital modifications was found to be lacking the necessary elements to ensure the proper development and installation of digital upgrades. In addition, the members of the engineering staff interviewed were unfamiliar with industry information regarding digital upgrades.

- Two RMS modifications were found to be adequate, based on the specific plant application and industry guidance that was available at the time these modifications were developed. However, the lack of understanding regarding digital issues was considered a shortcoming.

9409260027 940916
PDR ADOCK 05000244
Q PDR

- The analysis and corrective action for the AMSAC, using operational experience feedback from NRC information notices, was done in a professional and timely manner.

- The AMSAC and ADFCS software changes were correctly implemented under site procedural control. The AMSAC system tests, after software changes were installed, tested all blocks of software and showed that the system function was not impaired.

- The ADFCS training subject coverage and depth were adequate for operation and repair of the equipment, but were not adequate for software changes beyond parameter editing. RG&E at the present time does not intend to change the functional software, so the course material is considered adequate.

- The need for technical training concerning EMI issues was self-identified. The education was applied successfully to understand, diagnose, and solve an ADFCS noise problem.

- In the management oversight area, key program elements have been established for improving the effectiveness of general engineering performance. Self-assessments performed to date demonstrated management support for identification of deficiencies.

DETAILS

1.0 PURPOSE

The purpose of the inspection was to assess the safety and engineering aspects of plant modifications, with special focus on the digital and software design areas. The inspection included review of documents, walkdowns, personnel interviews, and observations concerning the digital modifications.

The inspectors reviewed the systems based on NRC inspection manual guidance concerning design changes and modifications, IP37700.

The digital segments were selectively reviewed for the safety and quality of the following areas:

- system design bases and translation to digital requirements;
- accuracy of analog-to-digital requirements translation;
- digital sampled data system analysis;
- specification and design of digital equipment hardware and software;
- hardware/software error management at the system and module level (to include microprocessor bus and data link);
- human machine interface (HMI);
- software documentation traceability and accuracy;
- software configuration control;
- software verification and validation;
- system acceptance and operational testing;
- operator and maintenance training;
- electromagnetic interference (EMI) testing;
- qualification testing.

After the quality of the unique digital segments was determined, the entire modification was reviewed to determine the degree of conformance to NRC and licensee's requirements.

2.0 DIGITAL MODIFICATIONS

The inspectors reviewed several safety-significant modifications containing software-based equipment and one nonsafety-related modification. Additionally, the inspectors evaluated the RG&E modification process with respect to software-based modifications. According to RG&E, the safety-significant classification of equipment is defined as a subset of equipment not required to perform a nuclear safety function, but are subject to requirements established by the NRC or RG&E to institute greater quality assurance over the design, procurement, installation, testing, operations, and maintenance.

The modifications reviewed were:

- radiation monitors;
- anticipated transient without scram (ATWS) mitigating system actuation circuitry (AMSAC);
- advanced digital feedwater control system (ADFCS);
- main generator voltage regulator (nonsafety-related).

2.1 Radiation Monitors

The inspectors reviewed two radiation monitor modifications: EWR 4068C, radiation monitoring system (RMS) upgrade - replacement of channels R-15, R-16, R-17, R-18, R-19 and R-20 (process radiation monitors); and EWR 5161, steam line monitors R-31 and R-32. The design verification associated with EWR 4068C was approved October 2, 1991, and the design verification associated with EWR 5161 was approved February 17, 1994.

2.1.1 Background

- **Process Radiation Monitors**

The inspectors reviewed the modification associated with EWR 4068C, which replaced the process radiation monitors. The reason for this modification was to replace various monitors that failed to meet equipment accuracy requirements due to age. The affected process radiation monitors replaced were:

R15	air ejector & gland steam exhaust
R16	containment fan coolers heat exchanger service water discharge
R17	component cooling water (CCW)
R18	waste liquid disposal

R19	steam generator blowdown
R20A	spent fuel pool heat exchanger "A" service water
R20B	spent fuel pool heat exchanger "B" service water

The process radiation monitors are used mainly for indication; however, specific monitors do perform isolation valve control functions. Particularly, a R-17 alarm causes the vent valve (V017) on the CCW surge tank to close; R-18 alarm causes the liquid waste discharge valve (AOV18) to the discharge canal to close; R-19 alarm causes the steam generator blowdown valves (AOV5737 and AOV5738) and steam generator sampling line valves (AOV5735 and AOV5736) to close.

In addition to the replacement of the monitors, several enhancements were made. These enhancements included the relocation of the monitors and the addition of drain and root valves. The relocation was necessary to place the monitors in a lower background radiation environment. The details of these enhancements were not reviewed as part of this inspection.

- Steamline Radiation Monitors R-31, R-32

The inspectors reviewed the modification associated with EWR 5161 that replaced the main steamline radiation monitor chart recorders with software-based continuous indication display units. This modification was initiated to address an apparent weakness in the control room operators' ability to discern main steamline radiation monitor readings from installed chart recorders. This weakness was identified during an NRC audit of Ginna's emergency operating procedures (EOPs) as documented in Inspection Report 50-244/89-80.

2.1.2 Scope of Review

To perform the review of these modifications, the inspectors had discussions with members of the RG&E staff, performed a walkdown of the associated equipment, and reviewed the following documents: design criteria; design verification; procurement documentation; safety analysis/safety evaluation; and various test procedures.

The inspectors focused their review on several aspects associated with these two radiation monitor modifications, including:

- requirement specifications;
- hardware;
- software and software verification and validation (V&V);
- safety analysis/evaluation;
- industry information;
- testing;
- maintenance history;
- configuration control; and
- technician training.

2.1.3 Technical Review

- Requirement Specification

The performance and control functions for both modifications were provided in the respective design criteria. The inspectors found no detailed functional specification nor software specifications associated with either modifications. Discussions with the RG&E staff indicated that the functional specifications for the replacement monitors were verified to meet or exceed those of the previously installed monitors. However, no upfront hardware specifications, software specifications, or software V&V requirements were described by the licensee.

Industry experience indicates that specifying the hardware, software, and software V&V initially minimizes the number of system errors. Additionally, an understanding of the hardware and software is essential to the ensure that the system testing is adequate.

The inspector noticed several improvements in the more recent design criteria for EWR5161, when compared to the design criteria for EWR 4068C. These improvements included the detailed documented description of the following:

- environmental conditions for normal and accident plant conditions;
- interface requirements;
- operational requirements for plant startup, normal plant operation, plant shutdown, plant emergency operation, and special or infrequent plant operation.

The design criteria identified the required normal and accident environmental conditions for temperature, pressure, humidity, and nuclear radiation. However, the service conditions for electromagnetic interference (EMI) and total harmonic distortion (THD) were not considered.

The inspectors also noticed that the procurement specifications associated with EWR 5161 requested the vendor to supply a software flowchart and the source code. RG&E had not been able to obtain this information by the completion of this inspection, but stated that they do intend to continue pursuing the matter.

- **Hardware**

The microprocessors for both modifications are 6802/6808, each with a monolithic 8-bit microprocessor with 16-bit memory addressing. The system operates at 1 MHz. The operating program for the systems is contained in ultra-violet (UV) erasable programmable read only memory (EPROM), and the setpoints are contained in electrically-erasable memory (EEPROM).

The system is provided with a master processing unit (MPU) failure function, which checks the main processor function. If the fail timer circuit is allowed to timeout due to a hardware failure, a failure condition will be indicated. Therefore, the MPU failure function prevents the failure of the microprocessor from going undetected.

At the time of this inspection, the licensee was not sure whether the systems associated with both modifications included the MPU failure function. The licensee discussed this with the vendor and verified that the systems associated with both modifications contained this function. RG&E stated that the fail timer was a hardware function that receives a signal generated through the software. The inspectors were concerned with the capability of the MPU failure function, since no review of the software had been performed by the licensee. Discussions with RG&E indicated that the operators monitor the radiation monitors every four hours. In addition, the monitors face the main control panel and rarely remain at a constant reading; therefore, a failure of the processor is unlikely to go unnoticed by the operators.

The inspectors walked down the control room location where the monitors were installed and found it adequate.

- **Software and Software Verification and Validation (V&V)**

Prior to this inspection, RG&E had not reviewed the software associated with these modifications, nor did they perform a review of the software V&V. Through discussions with RG&E staff, the inspectors learned that the bases for this were twofold. First, RG&E believed that it was unnecessary to review the software structure, function, or error management because the software was

stored in PROMS, which could not be changed. Second, RG&E considered the "black-box" testing of the equipment to be adequate. Due to this inspection, RG&E did obtain more detailed information regarding the software from the vendor. This software information included:

- Assembly programming language;
- approximately 20,500 lines of code;
- approximately 210 subroutines;
- no operating system used; and
- the software is the same software used by the vendor, Victoreen, in their safety-related equipment.

No information was supplied by Victoreen concerning how the software was developed or verified and validated.

Due to the nature of software-based equipment, "black-box" testing is normally not considered adequate for the design of safety-related equipment according to current industry guidance. Also, based on the complexity and program language used by the radiation monitors, a review of the software and the vendor's software development process, including V&V, would have been prudent regardless of the whether the software was changeable or not.

The purchase order for EWR 5161 stated, as a minimum, a copy of the software flowchart and a copy of the source code, as applicable, should be supplied. Although the procurement specifications requested the software code and flowchart be provided, Victoreen had not provided this information.

- Safety Analysis/Evaluation

The process radiation monitors and the steamline radiation monitors provided the operators with indication of radiation levels. Indications of abnormal radiation levels may require operator action. Operator action is of particular concern in the event of a steam generator tube rupture. To determine the extent to which the operators rely on radiation monitoring, the inspectors reviewed various EOPs and held discussions with the manager of operations. The inspectors determined that the operators do not rely solely on the information provided by the radiation monitors to determine required actions. Technical Specifications only require periodic grab samples to be performed when a radiation monitor is out of service.

The inspectors reviewed the safety analysis/safety evaluation for the two modifications and found them adequate for the application of the radiation monitors. This acceptance is based on the industry guidance that was available at the time these modifications were developed, and the application. Recently established industry guidance regarding digital upgrades ought to be considered for future safety-related modifications.

- **Industry Information**

RG&E performed an operational assessment review for both RMS modifications as required by the respective design criteria. As a minimum, applicable NRC bulletins and information notices and Institute of Nuclear Power Operations (INPO) communications were reviewed. The results of these reviews were included in the respective design verifications. The inspectors considered this review to be beneficial, but noted that it was limited to "radiation monitors," "radiation monitoring," and the manufacturer's name, but did not consider the broader topic of "digital/software-based equipment."

- **Testing**

The inspectors reviewed a sample of the various testing performed on the radiation monitors. These tests were considered appropriate for testing the functionality of the equipment. RG&E stated that, according to the vendor, test routines test all active subroutines and branches of the software. However, without a detailed knowledge of the software, it is not possible to adequately assess the thoroughness of the tests performed.

- **Maintenance History**

The inspectors asked the licensee if there were any major problems associated with the Victoreen radiation monitors. A review by the licensee found no concerns associated with the logic or software of the equipment. However, nonconformance report (NCR) 92-291 was developed to address a licensee identified concern with the anti-jam device. The anti-jam circuitry shuts down the high voltage to the detectors and actuates an alarm relay when it senses the detector is in a high radiation field and is about to saturate. If the radiation field is high enough, a fuse in the anti-jam circuitry blows to protect the detector.

The process radiation monitors were designed with the option allowing the fuse to be bypassed without affecting the operation of the anti-jam device. Operation department staff observed that stopping and starting the sample pumps for these monitors occasionally actuated the anti-jam circuitry. These actuations caused the fuse to blow, requiring down time for the equipment until maintenance technician replaced the fuse. The corrective actions associated with this NCR was to bypass the fuse. Also, guidance was provided to the operating staff to determine whether anti-jam shut down was caused by a momentary spike, noise/interference, loss of power, or some other cause. The inspectors considered the licensee's corrective actions adequate; but considered the lack of a documented root cause analysis to be an indication of less than the expected rigor for safety-significant equipment.

Additionally, RG&E discussed with Victoreen the maintenance history of the radiation monitors. According to Victoreen, there are well over 1,000 units installed and in operation in the nuclear industry. Furthermore, Victoreen representatives could not recall any software related failures. Beside the use of 10 CFR Part 21 reportability process, no information was available, at

the time of this inspection, regarding the methods used by Victoreen to evaluate field generated maintenance information. The inspectors considered the industry information as undefined, because there was no information on the rigor applied to the collection, depth, and classification of the data.

- **Configuration Control**

The inspectors discussed with RG&E the methods employed to ensure the control of software/firmware associated with the Victoreen radiation monitors. RG&E verified with the vendor that all PROMS carry revision numbers to ensure proper software version. PROMS are ordered by that revision number. Additionally, the licensee stated that the vendor verifies in-house records for PROM-related discrepancies prior to filling all orders.

- **Technician Training**

The inspectors evaluated the training provided to the I&C technicians regarding the Victoreen radiation monitoring systems. The inspectors reviewed the training lesson plan and discussed the contents with the writer/ instructor. The inspectors found the lesson plan to be thorough and cover the information provided in the vendor manual. This course is on RG&E's five-year training plan. The last time it was given was in late 1992, and six technicians attended.

2.1.4 Conclusion

The review of the radiation monitor modifications identified several shortcomings as described in the preceding sections of this report. These shortcomings included:

- the tendency to not specify the hardware, software, and software V&V requirements during the design or procurement phase;
- the tendency to not perform a review of the software;
- incomplete understanding regarding the MPU failure function;
- incomplete understanding of the development of the maintenance history information provided by the vendor;
- the failure to determine the root cause associated with NCR 92-291 regarding the anti-jam circuitry fuses.

However, the inspectors considered the two RMS modifications adequate, based on the application, and the industry guidance that was available at the time these modifications were developed.

The inspectors noticed several improvements in the more recent design criteria for EWR5161, when compared to the design criteria for EWR 4068C.

2.2 AMSAC Modification (EWR 4230, Engineering Change Notice [ECN] 4230-10)

The AMSAC is the system that automatically initiates actions to mitigate the consequences of an ATWS event. The RG&E classifies this system as safety-significant.

2.2.1 Background

The AMSAC signal processing hardware uses the Foxboro SPEC 200 MICRO digital processing equipment and was installed and tested in 1989, under EWR 4230. In July 1992, the NRC issued Information Notice (IN) 92-06, Supplement 1, that pointed out design, quality control, and test problems that licensees had experienced. The RG&E design engineer was assigned to review the IN and found that the AMSAC equipment had two discrepancies. The response to this operational experience feedback via the NRC IN is discussed in Section 2.2.3.

The ADFCS modification eliminated the feedwater flow channels from the protection cabinets. Since the channels also served the AMSAC, the feedwater flow inputs (two per loop) were routed to the ADFCS input analog-to-digital conversion cards. The flow transmitter currents are routed to the ADFCS input analog-to-digital conversion cards, to the processors, through the digital-to-analog current output cards, and finally to the AMSAC current-to-voltage converter input cards. This set of connections delivered the same functional variable (feedwater flow) to the AMSAC, but did not change the form, fit, or function of the AMSAC hardware.

2.2.2 Scope of Review

The review of the modification involved interviews with members of the RG&E technical site and corporate engineering staff, review of design and test documentation, and a walkdown of the equipment at the site. The inspectors reviewed documents associated with the modification as follows:

- Westinghouse design basis;
- design criteria;
- design analysis;
- design verification;
- system functional test report (vendor);
- software revision control and configuration management;
- installation test reports; and
- safety analysis and evaluation report.

The inspectors focused their review on the IN engineering response, verification of the timer lock-in change and dynamic tests, software configuration control, and the safety analysis report.

2.2.3 Technical Review

- Operational Experience Feedback (OEF) Response

The RG&E design engineer, assigned to analyze and respond to the IN, uncovered two discrepancies. First, the dynamic testing of the turbine lag software blocks was not implemented in plant calibration procedures, although they were tested during the vendor acceptance test and the site installation test, and known to be working correctly at that time. Second, the variable turbine power timer function was not locked in at the time point corresponding to an actuation of the low feedwater flow logic. The lock-in requirement was not known to the design engineer during the design of the AMSAC.

The cause of the lock-in discrepancy was traced by the licensee to the fact that the complete requirements for the feature were distributed between two documents. The first part of the requirements were in a Westinghouse Owners' Group report to the NRC. The second part of the requirements were found in the cover letter that transmitted the report to the NRC. The RG&E design engineer uncovered this by contacting engineers from the utilities mentioned in the IN. The design engineer then contacted Westinghouse to validate the requirements. Westinghouse confirmed that the report cover letter was the only reference to the lock-in and that associated analyses were performed with the assumption that the variable timer lock-in was installed. The RG&E design engineer then contacted Foxboro to begin the software modification process.

The software modification was then designed that added the variable timer lock-in of turbine first stage pressure at the moment the three out of four low feedwater logic is satisfied. The modification involved eight changes to the database with no hardware or wiring changes.

The inspectors concluded that the analysis of the OEF was done in a professional and timely manner. The industry contact method that the design engineer used to determine and validate the timer lock-in requirement was performed in a logical and efficient manner.

- Software Configuration Control

The AMSAC software is classified by the licensee as safety-significant. Master current disk copies and historical copies are stored in the Technical Support Center. Duplicate current disk copies are stored in the I&C area for AMSAC calibration and maintenance/repair purposes.

Software changes are tracked by the software change request (SCR) and the software change notice (SCN), both of which are controlled by site procedures. The SCR requests a change or reports a problem with the software. The SCN

provides the method for approving, controlling, and documenting the installation of a change to software. Software changes go through the same plant procedures that are used to control equipment modifications.

The design engineer worked with the vendor to develop the software changes. A bench test on a spare processing module with the new code was tested to confirm that the timer seal-in feature functioned correctly. Then engineering change notice 4230-10 was written, which delineated the changes to the AMSAC software and test procedures. All the software was tested for functionality, including the changed code.

The inspectors examined the listing of the software before and after the change to verify that the specified design solution was entered. The inspectors also verified that the plant calibration procedure (CPI-AMSAC-INSTR-3, April 20, 1994) was updated to test the turbine lag blocks and the timer lock-in additions. The test report for the ECN and the referenced test procedure were verified for proper test of the timer lock-in addition.

The inspectors concluded that software changes, regarding the database were correctly implemented under procedural control. The system testing, after the changes were installed, tested all blocks of software and the system function was not impaired.

- Safety Analysis/Evaluation

The inspectors reviewed the safety evaluation summary form attached to the test procedure used for the timer lock-in change. The written justification concluded that, since the lock-in was assumed operable in the Westinghouse ATWS evaluation, adding it would not increase the consequences of the event.

The change involving the feedwater inputs derived from the ADFCS was evaluated as part of the ADFCS safety analysis. The justification was that the new feedwater inputs are derived from safety-significant equipment and the configuration of the AMSAC rack equipment did not change.

The inspectors concluded that the safety evaluations were not in conflict with NRC requirements.

2.2.4 Walkdown

The inspectors walked down the AMSAC cabinet in the relay room. An I&C technician was interviewed on the use of the software configuration program using a personal computer (PC). The use of the PC for AMSAC maintenance and/or repair is controlled by procedure (M-3, April 20, 1994). The procedure covers the connection/removal of the PC, verification of the downloaded data, and memory battery replacement in the AMSAC equipment.

The technician pointed out that the Foxboro configuration program on the PC will overwrite the original data displayed on the screen with the uploaded control card program memory data, when in the memory verification (checkpoint)

mode. This can cause the database diskette to have the wrong version program. The technician found this out in a Foxboro instruction for a previous retrofit and had a precautionary note added in the PC procedure.

The inspectors concluded that the I&C technicians assigned to the AMSAC were very knowledgeable about the equipment and the software change process using the PC.

2.2.5 Conclusions

The analysis and corrective action using the OEF was done in a professional and timely manner.

The software changes were correctly implemented under procedural control. The system testing, after the changes were installed, tested all blocks of software, and the system function was not impaired.

The I&C technicians assigned to the AMSAC were very knowledgeable about the equipment and the software change process using the PC.

The safety evaluations were not in conflict with NRC requirements.

2.3 Advanced Digital Feedwater Control System (ADFCS) Modification (EWR 4773)

The ADFCS modification replaced an analog control system for steam generator water level control with an advanced digital feedwater control system (ADFCS) by Westinghouse. The main purpose of the modification was to minimize plant unavailability due to reactor trips caused by the analog system component failures and low power instability. The licensee classified the ADFCS as safety-significant, but not safety-related. The ADFCS was installed during the 1991 refueling outage.

2.3.1 Background

The ADFCS provides automatic control of steam generator water level without operator intervention at all power levels above 2%. Inventory in the steam generators is maintained by automatically positioning the main feedwater and bypass valves to control feedwater flow to each steam generator. Part of the ADFCS also automatically controls the modulation of the atmospheric relief valves (ARV). There are automatic/manual control stations for all the feedwater valves and the ARVs.

The ADFCS control algorithms were based on a design originally developed in Belgium, then further refined by Westinghouse. The evaluation of the basic control algorithm, signal validation and man-machine interface techniques was done with a prototype at the Sequoyah plant simulator. ADFCS designs similar to Ginna are installed and operating at Prairie Island and Diablo Canyon nuclear power plants.

The protective system low feedwater flow trip, which involved steam flow/feed flow mismatch, was eliminated. Three narrow range steam generator level inputs per loop were added to the ADFCS to compensate for the elimination of the low feedwater flow trip. The narrow range steam generator level inputs are continuously validated in the ADFCS by a median signal selection (MSS) software comparison technique. The purpose of the MSS is to prevent a failed instrument channel from causing a disturbance in the ADFCS, which could then initiate a plant transient that could require protective action. The elimination of the RPS low feedwater trip and the use of the MSS software technique was previously reviewed and approved by NRR in Amendment 41.

The control of the atmospheric relief valves (ARV) was added to the ADFCS. Additional cooldown transients, that accounted for failure conditions of both the feedwater control valves (FCV) and the ARVs, were analyzed. The results showed that safety criteria were met. The steam pressure inputs required for the ARV control are validated in the ADFCS using the MSS technique.

The ADFCS modification eliminated the feedwater flow channels from the protection cabinets for the AMSAC. The inputs (two per loop) are now routed through the ADFCS cabinets. This is discussed in Section 2.2.1 above.

The ADFCS is implemented using the Westinghouse Eagle Distributed Processing Family (WDPF) and is powered from the redundant instrument buses, which are backed by battery inverter units. The system has redundant distributed processor units (DPU) connected as a failover pair. The DPU uses an Intel 8086 microprocessor. Only one DPU controls the system; the backup DPU receives current data over the data highway, monitors the status of the control DPU, and performs diagnostics. Automatic switchover to the backup DPU occurs on power interruption, failure of the control processor itself, or its shared memory, or math co-processor, or data highway interface. When automatic switchover occurs, the backup DPU processes active data from the input/output (I/O) bus, and the algorithms incorporate measures to insure bumpless transfer. The I/O points are distributed on the cards so that a single card failure will not cause a loss of the ADFCS function.

Two types of input signal validation using software techniques are employed. The first technique is the MSS, where the median of three inputs is used for the control algorithms. This prevents high or low failures of a single input from affecting the control system. The steam generator levels, steam flow, steam pressure, and feedwater flow are validated using the MSS technique. The second technique is arbitration, where two inputs are compared; and, if they agree to a preset criterion, their average is used for the control algorithms. If the two channels differ from the criterion, they are compared to an estimate of the variable that is calculated using other process measurements. The input that is closer to the estimate is then used for the control algorithms. Feedwater temperature, feedwater header pressure and turbine first stage pressure are validated using the arbitration technique.

Diagnostics are incorporated that are automatically executed during the normal operation of the system and do not disrupt the real-time performance of the process. Should a malfunction occur, the active DPU will failover to the backup DPU, and a trouble alarm will be generated.

An engineer/operator workstation connects to the system over the data highway and provides the software engineering tools required to configure and maintain the ADFCS. The engineer mode allows construction of graphics for the operator mode, configuration of software, and downloading of application software for use in the DPUs. The operator mode allows graphics to be presented that allow defined actions, such as changing selected alarm and process variables along with viewing process values. The workstation access is controlled by keylock and, at Ginna, is intended to be used by system engineers and I&C technicians. In normal operation, after the programs and constants have been downloaded to the DPUs, the workstations do not perform any control system functions.

2.3.2 Scope of Review

The review of the modification involved interviews with members of the RG&E technical site and corporate engineering staff, review of design and test documentation, and a walkdown of the equipment at the site. The inspectors reviewed documents associated with the modification as follows:

- Westinghouse design basis;
- design criteria;
- design analysis;
- design verification;
- integrated assessment;
- instrument calibration and uncertainty design basis document;
- software QA reports;
- software revision control and configuration management;
- factory acceptance test (FAT) reports;
- installation test reports;
- training;
- electromagnetic interference (EMI) trouble shooting reports;
- maintenance history logs; and
- safety analysis and evaluation report.

The inspectors focused their review on the design basis, setpoint and loop uncertainty calculations, software configuration control, training, EMI troubleshooting, and the safety analysis report.

2.3.3 Technical Review

- Design Basis

The Westinghouse design basis document covered criteria for the process sampling rates, anti-aliasing filters, and processing delays based on engineering judgement, but there were no references to any specific analyses for sampling rate or filters for Ginna. The inspectors were advised that Westinghouse did address the issues, but were not able to respond during the inspection. The inspectors concluded that engineering judgement based on operational experience at other ADFCS plants and with simulations most likely formed the bases for the Ginna values of the sampling rates, anti-aliasing filters, and processing delays.

- Setpoints and Loop Uncertainties

Westinghouse developed the design bases for the setpoints and software constants prior to startup tests using data from similar plants and review of past Ginna startup data. The Westinghouse design bases were updated after startup to show the final values. RG&E developed the calibration and scaling parameters for the instrumentation and the associated uncertainties for incorporation into the installation test. The inspectors noted that the design inputs, assumptions, and reference documents were comprehensive. The analyses of the uncertainties included system block diagrams that showed the relationship between components, signal levels, and calibration ranges. The inspectors concluded that the control of setpoints and the calculation of loop uncertainties were adequate.

- Software Configuration Control

One set of the ADFCS master disks is stored in the technical support center at the site. RG&E has requested a backup set from Westinghouse. The software database is maintained by the I&C department using the workstation. The planned maintenance of the database is to adjust tuning constants and other parameters, not to create new functional software for process loops or configurations. The workstation is used primarily for on-line monitoring of control loops, and process inputs, outputs, alarm status, hardware status, and high/low limits.

The ADFCS software is classified under RG&E categories as safety-significant. The software configuration control procedures are discussed in Section 2.2.3.

The inspector examined two SCNs (ADFCS 94.1, 94.2), both of which were classified as minor changes. The changes involved parameter conversion coefficients. The authorizing change document numbers were recorded for traceability. The functional descriptions of the changes were clear and reference work orders under which subsequent testing was performed were recorded. The results of tests were recorded as being satisfactory. The inspectors concluded that there were documented procedures for software configuration control and that for the minor parameter changes examined, the procedures were followed.

- **Technical Training**

Selected technical staff completed Westinghouse formal ADFCS training. Four I&C technicians completed the five-week maintenance course. The two-day system overview course was completed by 36 of the staff.

Technical staff are trained on site with the ADFCS training system, which allows realistic training and facilitates troubleshooting. Technicians have been trained in a three-week course that covers the details of the hardware and software, with troubleshooting exercises. A two-day system overview course is provided for engineers. Informal training was given to selected members of the technical staff. Some of the staff observed operating ADFCS simulators and systems at two nuclear plants. The engineering staff contacted the ADFCS design engineer at a nuclear plant. Seven technical staff participated in the factory acceptance test.

Selected members of the site engineering staff were trained in grounding, shielding, and diagnostic techniques for EMI noise problems associated with electronic instrumentation in May 1989. The corporate engineering and site engineering staff were trained in electromagnetic compatibility principles and applications in June 1992. The training was prompted by suspected electrical noise problems on the DC system, control room annunciators, digital meters, and the ADFCS.

The inspectors concluded that the ADFCS training subject coverage and depth were adequate for use and repair of the equipment, but not adequate for software changes beyond parameter editing. RG&E, at the present time, does not intend to change the software, so the course material is adequate. The EMI training is noteworthy because the licensee identified the need and used the training to understand, diagnose, and solve plant noise problems.

- **EMI Testing**

The ADFCS system was tested by Westinghouse for EMI-radiated susceptibility with the cabinet doors open and closed. The susceptibility field strength from 20 MHz to 1 GHz was 3 volts/meter; from 20 MHz to 500 MHz the field strength was 20 volts/meter. The I/O cards have surge-withstand capabilities, according to Westinghouse.

In November 1991, at the Ginna plant, an electromagnetic noise spike on both shielded feedwater header pressure inputs caused the feedwater control valves to open and rapidly increase flow. The problem was identified as being coincident with the start of the diesel fire pump, which is unrelated to, and independent of, the ADFCS. The spiking occurred two times before, but the ADFCS handled the situation. All grounding and shielding was checked and found to be correct. The electrical engineering staff evaluated the cable tray database and identified possible diesel fire pump cables and ADFCS input cables. A test was devised that used inductive and capacitive probes, storage scope and high speed recorders, that correlated the spike with the feedwater header pressure inputs to the ADFCS. The problem was traced to a spike from a relay deenergizing on a 125 Vdc power cable to the fire relay panel that

shared some cable trays with the ADFCS feedwater header pressure input cables. The spike affected the two feedwater header pressure signals at the same time. The signals were apparently arbitrated correctly by the software, and accepted as valid input signals. The problem was solved by rerouting the feedwater header pressure cable in conduit. The identification, diagnosis, and solution of the transient electromagnetic noise pulse that caused the misoperation of the ADFCS showed excellent application of the EMI training courses that were taken by members of the site engineering staff.

- Safety Analysis/Evaluation

The RG&E safety analysis/evaluation for the ADFCS covered the combined set of modifications that:

- removed the reactor trip channels involving the steam generator low level in coincidence with steam flow/feed flow from the protection system;
- added triple redundant narrow range steam generator level and MSS signal validation as ADFCS input;
- incorporated the ARV control function into ADFCS;
- replaced the single output isolators in the protection racks with multiple output isolators;
- removed/relocated or added instruments on the main control board.

The description of the scope, along with the reference documents, made the analysis very clear. The evaluation covered each part of the modification and answered each 10 CFR 50.59 question with supporting reasons that were traceable to the analysis and design documents. The inspectors review determined that the conclusions were adequately supported.

2.3.4 Walkdown

The inspectors walked down the ADFCS installation at the site. The processing and I/O cabinets are in the relay room, and the workstation is in the plant computer room. Access to the relay room and plant computer room is controlled by card key. The inspectors observed a qualified I&C technical assistant walk through the monitoring of the ADFCS system using the workstation. The ADFCS cabinets had louvered doors installed after an infra-red thermography scan showed hot spots within the cabinet. The RG&E staff was cognizant of the location, system self-test, and replacement cycle of the lithium batteries used in the DPUs. The inspectors concluded that front and rear access to the cabinets was adequate and that the interior temperature rise of the cabinets was not excessive.

2.3.5 Conclusions

The bases for the Ginna values of the sampling rates, anti-aliasing filters, and processing delays were most likely based on engineering judgement formed from the vendor's simulations and operational experience at other ADFCS plants.

The technical content, calculations, and control of setpoints and loop uncertainties were adequate.

The site procedures for software configuration control were followed.

The ADFCS training subject coverage and depth were adequate for use and repair of the equipment, but not adequate for software changes beyond parameter editing. RG&E, at the present time, does not intend to change the functional software, so the course material is considered adequate. The EMI training was noteworthy because the licensee identified the need and used the training to understand, diagnose, and solve plant noise problems.

The conclusions of the safety analysis and evaluation were adequately supported by the review of selected design, analysis, and test documentation.

2.4 Main Generator Voltage Regulator (EWR 5262)

The inspectors reviewed selected portions of EWR 5262, Revision 0, "Main Generator Voltage Regulator Replacement," to determine the solid state interfaces of the modification and to assess the impact of the regulator change on safety-related equipment. This modification was selected to evaluate digital aspects of a nonsafety-related modification installed during the previously completed 1994 outage.

The replacement of the voltage regulator was an RG&E commitment to the NRC as described in Licensee Event Report LER-92-002, dated March 4, 1992. The voltage regulator controls the voltage delivered to the generator field. This regulates the voltage and power that is output from the generator. By varying the generator field, the amount of power generated to the grid can be controlled in a precise manner.

The inspectors determined that the solid state components installed under this EWR were associated only with the control room annunciator and did not interface with any safety-related equipment. The digital aspects of the annunciator included a common-services module that receives information in the form of voltages switched on or off in the field. Continuous monitoring and detection of changes in the status of input to the module would activate an alarm status annunciation in the control room.

The inspectors concluded that no new failure modes had been introduced as a result of this modification and no impact was made to safety-related equipment or components.

2.5 Modification Process For Digital Upgrades

The inspectors assessed the RG&E modification process to determine the effectiveness of the process for digital modifications. To complete this assessment, the inspectors reviewed the following aspects of the modification process:

- engineering design specifications and drawings;
- technical evaluation; and
- 10 CFR 50.59 safety evaluation.

2.5.1 Modifications

Modifications at the Ginna Station are initiated through the engineering work request (EWR) process. EWRs dispositioned as modifications require several steps to ensure adequate completion. The inspectors' discussions with the RG&E staff indicated the following: (1) that RG&E had no digital modifications planned for the near future; (2) that the RG&E staff members interviewed were unfamiliar with industry information regarding digital upgrades; (3) that no means were established to ensure that the preparer recognizes the special circumstances associated with digital modifications. Some of the circumstances that industry guidance considers for digital modifications are:

- ensuring that the appropriate personnel are involved with the modification;
- ensuring that the appropriate system requirements are specified up front;
- ensuring that the appropriate software and hardware requirements are specified up front;
- ensuring that the appropriate software V&V is specified up front; and
- ensuring that the service condition is appropriately specified, particularly with respect to EMI emission and susceptibility.

As a result of this assessment, the licensee stated that the modification process regarding digital upgrades would be reviewed for enhancements.

2.5.2 Technical Evaluations

The inspectors reviewed the technical evaluation (TE) process as described in Procedure A-305, Revision 7, "Technical Evaluations." TEs may be used for certain changes to the plant systems, structures, and components (SSC) not requiring the extensive design process utilized for minor and major

modifications. The TE is an analysis that demonstrates that the proposed change meets or conservatively exceeds the requirements of the original configuration and does not alter the design, function, or method of performing the function of any SSC.

Since the differences in the method for performing the function are subtle between analog and digital equipment, and even more subtle between one digital device to another, the inspectors were concerned that the TE process may be used for digital upgrades. This is a concern because, even though the differences in the method of performing their function are subtle, their failure modes and effects can vary greatly.

RG&E staff indicated the TE process was not intended to be used for digital upgrades. However, they also stated that there was the potential for digital upgrades to be made through the TE process. As a result of this assessment, the licensee stated that the modification process regarding digital upgrades would be reviewed for enhancements.

2.5.3 10 CFR 50.59 Safety Evaluation

The inspectors reviewed Procedure EP-3-P-135, "Preparation, Review, and Approval of the 10 CFR 50.59 Safety Evaluation," Revision 0, identified no specific guidance for safety evaluations of digital upgrades. The inspectors were concerned because the failure modes and effects of digital equipment are more subtle and may vary greatly from those of analog equipment. Therefore, digital upgrades need to be treated accordingly in the 10 CFR 50.59 safety evaluation. Guidance regarding the treatment of digital upgrades in the 10 CFR 50.59 safety evaluation is provided in the Electrical Power Research Institute (EPRI) Document EPRI TR-102348, "Guideline on Licensing Digital Upgrades."

The inspectors reviewed the guidance provided Procedure EP-3-P-135, Attachment C, "List of Documents Comprising the Safety Analysis Report." The guidance provided in the attachment identified that the safety analysis report, as referred to in the context of 10 CFR 50.59, is considered to be a body of information, rather than a specific document. This guidance was considered appropriate.

2.5.4 Conclusion

The inspectors' assessment of the RG&E modification process with respect to digital modifications was that the process lacks the necessary elements to ensure the proper development and installation of digital upgrades. In addition, the members of the RG&E staff interviewed were unfamiliar with industry information regarding digital upgrades. This was considered a weakness by the inspectors.

As a result of this assessment, the licensee stated that enhancement would be made to the modification process regarding digital upgrades. Additionally, RG&E stated that there are no plans for safety-related digital upgrades in the near future.

The guidance provided in the 10 CFR 50.59 procedure regarding the documents that comprised the safety analysis report was considered to be appropriate.

3.0 MANAGEMENT OVERSIGHT

The inspectors reviewed selected engineering activities to evaluate the quality of program elements and to assess the effectiveness of the Nuclear Engineering Services (NES) Department to influence engineering performance by use of these findings. The activities reviewed included a self-assessment performed by Ginna site engineering and an audit on process improvements for performing audits. Key program elements included feedback on performance, assessment of results, and implementation of corrective action.

3.1 Modification Process Self-Assessment

The inspectors reviewed RG&E 1994 business plan strategies for the NES department. These strategies included the establishment of a performance goal to improve the effectiveness of the NES by evaluating major processes. A self-assessment was conducted by Ginna site engineering to evaluate the modification process based on those modifications implemented during the 1994 outage.

At the time of this inspection, the self-assessment report was in draft form. However, the inspectors reviewed the findings to assess the quality of the findings and recommendations for any corrective actions. The findings included identification of the need for enhanced communications between the modification project team members for improvement in planning and scheduling and improved procedures. The need for improved procedures was a result of recent organizational changes within the site engineering department. These changes included combining the duties of the construction engineer and liaison engineer within the duties of the modification implementation engineer. The self-assessment identified that a redefinition of individual's responsibilities was necessary to eliminate duplicated efforts by differing departments.

The inspectors concluded that, based on the findings presented in this self-assessment, the licensee had established a means for monitoring plant performance associated with the modification process. The inspectors noted that this assessment demonstrated management support for identifying deficiencies from which corrective action could be taken.

3.2 Continuous Process Improvement

RG&E began a focus in late 1993 to establish a continuous process improvement (CPI) project to improve continuously the effectiveness of engineering processes. This project team was structured using corporate and site personnel. The team developed a CPI model to define the required steps and substeps necessary to define and document a process needed for improvements or changes, measuring performance, and evaluating the results. This model also included guidance for development of key activities and tools to be used in identifying problem areas, needs, and process boundaries from which improvements or changes could be based.

RG&E has also recognized changes in the scope of upcoming engineering work for the Ginna facility. These changes included a decreasing trend for implementation of major modifications and an increasing trend for daily plant support. Based on this recognition, RG&E management has addressed assessing the future needs of the NES Department to maintain and improve its effectiveness based on these identified changes.

The licensee has begun evaluating training and skills of the NES department to ensure an adequate balance between skills and process controls for the recognized work scope changes. This evaluation included eliminating training courses of minimal value and optimizing process controls by streamlining processes, increasing the accountability of individuals, and improving procedures.

The inspectors concluded that RG&E management was notably involved in examining and evaluating NES Department skills and processes. During this inspection, digital aspects of the modification process were assessed and described in Section 2.5. As a result of this assessment, the licensee stated that enhancement would be made to the modification process regarding digital upgrades.

3.3 Quality Assurance Audit on Audit Process Improvements

The inspectors reviewed a recently performed quality assurance (QA) audit of the audit process. This review was initiated by the licensee under the corporate CPI Project. This review was conducted because of a noted dissatisfaction with audit reports and misunderstanding of individuals' responsibilities during audit activities. The goal of this review was to establish and implement the proper corrective actions to produce audit reports that convey clear and accurate indication of auditee performance and root cause analyses.

At the time of this inspection, the audit results were in final draft form requiring only approval signatures. All affected departments were found to have been briefed on the audit findings.

The inspectors found the audit results to be thorough for evaluating key elements of the audit process and considered it as self-initiated with appropriate management involvement.

3.4 Conclusion

The inspectors concluded that key program elements had been established for improving the effectiveness of engineering performance. Assessments performed by the licensee were found by the inspectors to demonstrate management support for the identification and correction of deficiencies. The inspectors also noted RG&E's efforts for evaluating and improving the effectiveness of the engineering departments, based on recognized changes in the scope of upcoming engineering work.

4.0 EXIT MEETING

The inspectors met with the licensee's personnel denoted in Attachment 1 of this report at the conclusion of the inspection on July 22, 1994. At that time, the scope of the inspection and inspection results were summarized.

The licensee management agreed with the inspection findings. The technical contacts for this report are Mr. Charles Forkell, and Mr. George Wrobel.

The inspectors received proprietary material during the inspection and used the material only for technical reference. No part of the material was knowingly disclosed in this inspection report.

Attachment: Persons Contacted

ATTACHMENT 1

Persons Contacted

Rochester Gas and Electric Company

*	C. Anderson	Manager, Quality Assurance
	R. Appleton	Electrical Engineer
*	D. Baker	Electrical Engineer
	R. Bozarth	Engineering Assistant
	R. Bryan	System Engineer
	K. Cona	Engineering Assistant
*	C. Edgar	Manager, Electrical/Instrumentation and Controls Maintenance
*	C. Forkell	Manager, Electrical Engineering
*	G. Hermes	Lead Engineer, Nuclear Safety and Licensing
	J. Gashlin	Construction Engineer
	R. Jaquin	Engineer, Nuclear Safety and Licensing
	T. Joachimczyk	Technical Instructor
*	T. Kaza	Supervisor, Computer Systems
*	N. Oliva	Electrical Engineer
	R. Popp	Station Engineer, Electrical/Instrumentation and Controls Maintenance
	M. Preik	Quality Assurance Engineer, Procurement
	J. Smith	Electrical Engineer
*	B. Stanfield	Quality Assurance Engineer, Operations
	S. Stinson	Technical Assistant, I&C
	T. Werner	Director, Technical Processes
	T. White	Manager, Operations
*	P. Wilkens	Manager, Nuclear Engineering Department
*	G. Wrobel	Manager, Nuclear Safety and Licensing
	J. Zapetis	Electronic Technician, I&C

U. S. Nuclear Regulatory Commission

*	W. Ruland	Section Chief, Electrical Section, Region I
	T. Moslak	Senior Resident Inspector

* Indicates those in attendance at the exit meeting held on July 22, 1994.