U.S.NUCLEAR REGULATORY COMMISSION
REGION I

REPORT/DOCKET NOS. 50-317/94-02
50-318/94-02

LICENSE NOS. DPR-53
DPR-69

LICENSEE: Baltimore Gas and Electric Company
Post Office Box 1475
Baltimore, Maryland 21203

FACILITY: Calvert Cliffs Nuclear Power Plant, Units 1 and 2

LOCATION: Lusby, Maryland

INSPECTION DATES: February 7, 1994, through February 18, 1994

INSPECTOR: John A. Calvert 04/07/94
John A. Calvert, Reactor Engineer
Electrical Section, EB, DRS
Date

APPROVED BY: JM Trapp 4/7/94
James M. Trapp, Acting Chief
Electrical Section, EB, DRS
Date

Inspection Summary: Inspection on February 7, 1994 to February 18, 1994. (Inspection Report Nos. 50-317/94-02 and 50-318/94-02)

Area Inspected: This was an announced inspection to review the licensee's 10 CFR 50.59 modification process and documentation for the variable low temperature overpressure protection system (VLTOP) and the full range digital feedwater control system (FRDFCS.)

Results: No violations or deviations were identified.

- Consideration of digital upgrade issues, starting at the conceptual design stage, such as software documentation, verification and validation (V&V), configuration management, failure management, and electromagnetic interference (EMI) was very evident in the variable low temperature overpressure protection system (VLTOP) modification.

- The bases, requirement definition, analysis, correlation, and accuracy of the transfer to the software of the VLTOP setpoint curves was effective.

- The staff actions for the VLTOP project showed a determined effort to understand and address digital upgrade issues.

- The transfer of the VLTOP software requirements for the improvement in shutdown risk was not effective. However, corrective action was taken to insure that the necessary software requirements were implemented.

- The software self-assessment and corrective actions were effective, but not timely.

- The organization and completeness of the design requirements for the VLTOP was not sufficient to allow proper flow down of requirements to the software, which hindered traceability. This was captured in self-assessment and corrective action was taken.

- The program download method for the full range digital feedwater system (FRDFCS) does not provide for verification of the program after the downloading process. Although this is not a requirement, a verification method would reduce the risk of incorrect program loading. The software requirements traceability is not substantiated. Although this also is not a requirement, it could serve as a method to increase confidence in the code.

## DETAILS

## 1.0 PURPOSE AND SCOPE

The purpose of this 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 variable low temperature overpressure protection system (VLTOP), and the full range digital feedwater control system (FRDFCS). The inspection was conducted at the Calvert Cliffs Nuclear Power Plant Units 1 and 2, Lusby Maryland.

The inspector reviewed the systems based on NRC inspection manual guidance concerning design changes and modifications. The digital segments were assessed for the quality of the following areas: system bases and requirements; accuracy of analog-to-digital requirements translation; digital sampled data system analysis; licensee understanding of digital equipment hardware and software; hardware/software error management at the system and module level; human machine interface; software documentation traceability and accuracy; software configuration management; software verification and validation; system acceptance and operational testing; operator and maintenance training. After the quality of the unique digital segments was determined, the entire modification was audited to determine the degree of conformance to NRC and licensee's requirements.

## 2.0 VARIABLE LOW TEMPERATURE OVERPRESSURE PROTECTION SYSTEM (VLTOP)(FCR 90-137)

The licensee submitted a license amendment request (Letter, "License Amendment Request: Variable Low Temperature Overpressure Protection," September 3, 1993) which described changes to the LTOP system in conjunction with a lowered neutron fluence. This inspection concentrated only on the added digital equipment and not the 10 CFR Part 50 Appendix G, Technical Specification, or plant operation issues. The VLTOP system is scheduled to be installed in Unit 1 during the 1994 refueling outage.

### 2.1 System

The purpose of the variable low temperature overpressure protection system (VLTOP) is to increase the allowable operating pressure band in the low temperature overpressure protection (LTOP) range. The system will allow operators to cooldown to shutdown cooling (SDC) conditions while running one reactor coolant pump (RCP) in each coolant loop. The system, in conjunction with administrative controls, will avoid exceeding the Technical Specification pressure-temperature limits, which are established to prevent brittle fracture of the reactor vessel at low temperatures.

The system is implemented as a digital Power-Operated Relief Valve (PORV) actuation system that provides a variable PORV trip setpoint during low temperature operation, while retaining the single PORV trip setpoint during shutdown cooling (SDC) operations. The digital microprocessor is a Foxboro SPEC 200 MICRO that NRC has previously reviewed for safety-related applications at the Haddam Neck and D.C. Cook nuclear power plants.

## 2.2 **Review of 10 CFR 50.59 Evaluation**

The licensee performed a detailed failure modes and effects analysis (FMEA) for the components in the VLTOP loop, including the microprocessor. The common mode effects of electromagnetic interference (EMI) and software failures were considered in the 10 CFR 50.59 evaluation.

The inspector reviewed the part of the 10 CFR 50.59 evaluation that described common mode software failures. The evaluation stated that the failure of the microprocessors in both trains due to a common mode software failure was not considered credible. The inspector noted that no tests were performed that exercised the software program in all possible input combinations of the data and event domains, or showed that all program branches were exercised. Therefore, the inspector assessment was that a software common mode failure could be considered credible.

During the inspection, the licensee changed the evaluation (Issue Report IR0-0168-323) to state that common mode software failures were considered to be possible, but that no new failure modes at the system level were introduced, and therefore no new effects or consequences other than what had been considered. This would be valid for temperatures and pressures past the minimum pressure and temperature enable temperature (MPT), because events are analyzed for spurious opening of both PORVs and events that do not require the PORVs to actuate. The MPT enable temperature is the RCS temperature below which the VLTOP/LTOP controls are required to be in place to protect the 10 CFR Part 50, Appendix G limits.

The inspector noted that the evaluation was not clear for the case when the temperature would be below MPT. The issue in this region would be a common mode failure that prevented both PORVs from opening, if a pressure transient occurred. The licensee stated that: a) the operator would detect any transient of system pressure on the existing pressure indicators (P-100, P103, P105 indication loops), which are independent of the microprocessor system; b) if the operator were unable to get back within the administrative controls, he would open at least one PORV by pulling the HI PZR PRESS trip module out of its slot. The operator is trained on how to do this for feed and bleed cooling.
The inspector considered this explanation adequate, in that equipment and administrative actions are included in the "system." The inspector had no further questions regarding the 50.59 evaluation.

## 2.3 Requirements Review

### 2.3.1 Reliability

The licensee's reliability engineers concluded that the at power risk would not be affected by the VLTOP modification (letter RE-93-468, August 19, 1993). Their conclusion for the shutdown risk was that the modification would result in an overall improvement because the reduction in RCS loss of inventory frequency due to a PORV spurious opening, greatly offsets the increase in RCS loss of inventory frequency due to reactor vessel rupture following an overpressure transient.

The inspector questioned their conclusion for shutdown risk because of a statement in the VLTOP scope of work document that indicated the VLTOP modification would be 7% less reliable than the existing installation.

The inspector interviewed the reliability engineers that performed the reliability and probabilistic risk assessment (PRA) analyses to gain insight into the methodology used to support the statement. The reliability engineers said that the 7% reduction was based on parts count increase for the particular hardware block itself, not the overall probability. When the new VLTOP microprocessor functionality was factored into the probability of RCS loss of inventory due to vessel rupture because of both PORVs failing to open following an overpressure event, the increase was only 0.25%. This slight increase was considered insignificant, especially when the probability of experiencing an overpressure event during a typical outage is very due low due to the short period of time the RCS is not vented.

The probability of RCS loss of inventory, due to a PORV spurious opening, was significantly decreased because certain software features of the VLTOP microprocessor were incorporated into the analysis. During the design stage, at a meeting with the design engineers, the reliability engineers learned that the software could be configured to ignore large rapidly changing temperature and pressure signal inputs. When they incorporated the software feature into the analyses, the probability of a loss of RCS inventory in shutdown went from 9% increase to a decrease of 47%.

The inspector did not find the applicable software features listed in the software requirements specifications (SRS). The effect of this would be that the modification would not support the reliability analysis. The inspector brought this to the attention of the lead design engineer, who immediately wrote an issue report (IRO-0168-325), which started corrective action that will insure that the requirement will be properly documented in the SRS, and subsequently will be implemented and tested. The inspector had no further questions in this area.

### 2.3.2 **Calculations**

The inspector reviewed the calculations for the minimum pressure and temperature (MPT), the variable low temperature overpressure protection system (VLTOP) individual instrument uncertainties, the VLTOP PORV set pressure and maximum operating pressure curves, and the VLTOP response time. Any parameters that were required for the software were tracked to verify that they were installed correctly in the microprocessor.

- **MPT Enable Temperature**

The MPT enable temperature is the RCS temperature below which the VLTOP/LTOP controls are required to be in place to protect the 10 CFR Part 50, Appendix G limits. The MPT calculation (B-MECH-CALC-046, revision 00) established the analytical limits of a cooldown MPT of 331.4°F and a heatup MPT at 60°F/hr of 359.05°F; the heatup value was the most limiting, so the licensee chose it to represent the MPT value.

The instrument loop uncertainty for RCS cold leg temperature calculation (I-91-070, revision 1) set the loop uncertainty at ±4.3°F, but the VLTOP system calculation (B-MECH-CALC-047, revision 01) used ±6°F for more conservatism. The conservatism was warranted because the licensee calculation for the temperature loop uncertainty was ±5.5°F (I-93-27 revision 0). The MPT was set at 365.05°F per the VLTOP system calculation, which was 6°F above the limiting heatup temperature of 359.05°F.

The actual MPT set in the microprocessor software data base was 365.1°F per the approved setpoint change transmittal sheet (SCTSs 1-PY-103E, 1-PY-103E-1, revision 1A FCR 90-137), which accounted for the resolution of the microprocessor. The value of MPT in the licensee Technical Specification amendment submittal of September 3, 1993 was 365°F. When loop uncertainties of ±6°F are taken into account, the difference between the installed MPT the analytical limit of 331.4°F for cooldown is 27.7°F; for the heatup analytical limit of 359.05°F, the difference is 0.05°F. The inspector concluded that the calculations for MPT included loop uncertainties and were acceptable.

- **VLTOP PORV Trip**

The inspector reviewed the calculations and uncertainties concerned with the VLTOP RCS pressure versus temperature curve, which is composed of seven straight line segments, and is used for the PORV trip.

The calculation for uncertainties of the individual instruments in the VLTOP system (I-93-27, revision 01) showed that the correct Rosemount temperature effect values were used in accordance with the 10 CFR Part 21 notification for Model 1154 series H pressure transmitters. Foxboro assumptions for the microprocessor were that conversion uncertainties were calculable for the following: current-to-voltage (I/V) converters; voltage-to-current converters (V/I); analog-to-digital converters (A/D); and digital-to-analog converters (D/A).

There were no uncertainties associated with software control blocks. The assumption that digital processing errors were limited to analog conversion devices was used in all calculations.

The uncertainty equations for the PORV setpoint pressure line segment curves were developed as a function of the slope of the straight line segments (I-93-58, revision 1). The inspector verified the actual uncertainties calculated (B-MECH-CALC-047, revision 01, table 5) were in accordance with the uncertainty equations. The inspector verified that the break points on the maximum PORV opening pressure versus temperature graph in the licensee amendment submittal (Figure 3.4.9-3) were at or above the actual installed values in the microprocessor plus the uncertainties.

The inspector noted that the conservatism margin between the analytical limit of PORV opening pressure and the Technical Specification graph (Figure 3.4.9-3) varied between 23.2 PSIA at 90°F and approximately 45 PSIA at the MPT, 365.1°F (B-MECH-CALC-047, revision 01, table 4). The conservatism margin between the Technical Specification graph and the seven straight line segments of the programmed PORV opening pressure setpoint varied between 19 PSIA at 90°F and 72.4 PSIA at the MPT, 365.1°F; these differences accounted for the loop uncertainty.

- **VLTOP PORV Pre-Trip**

A PORV pre-trip alarm for the operator is implemented, which has more margin from the Technical Specification graph (3.4.9-3) than the programmed PORV trip opening setpoint. The alarm is implemented in seven straight line segments that are 10 PSIA below the maximum operating curve, which in turn is below the PORV VLTOP setpoint curve.

The difference between the PORV VLTOP trip setpoint curve and the operator pre-trip alarm curve varies from 24 PSIA at 90°F to 106 PSIA at MPT of 365.1°F. The alarm will alert the operator when the pressure is approaching the maximum operating pressure and allow time for operator action prior to lifting a PORV. The licensee calculated that at a pressurization rate of 15 psi/minute, the operator would have 30 seconds to take action.

The inspector reviewed the calculations for the operator pre-trip alarm curve and concluded that instrument loop uncertainties were included in the calculations. The inspector also verified that the programmed software points were 10 PSIA below the maximum operating curve calculated points (B-MECH-CALC-047, revision 01).

- **Response Time**

The inspector observed that the assumption was made in the VLTOP system calculation (B-MECH-CALC-047, revision 01, paragraph 5.5) that the system response time for PORV actuation was 1.5 second maximum. The inspector reviewed the VLTOP response time calculations (I-93-028, revision 1) to determine conformance with the 1.5 second assumption.

The PORV and associated actuation relay response time were determined by test. The response times of the pressure trai.smitter and microprocessor were determined by published specifications.

The microprocessor controller has a scan rate of 5 times per second and executes the following functions in the following order every 0.2 seconds: a) process input conversions; b) process control blocks in sequence; and c) process output conversions. The calculation correctly assumed that the actuation pressure transient had occurred just after the completion of the process input conversion such that the trip condition would not be realized by the controller until after the completion of the succeeding scan period of 0.2 seconds. Therefore, the response time for the microprocessor was assumed to be 2 scan times, or 0.4 seconds. The inspector concluded that the calculated responsc time of 0.9 second was appropriate and was within the 1.5 second assumption used in the system calculation.

## 2.4 Software Documents, Verification & Validation

- **Software Requirements Specification (SRS), Software Design Description (SDD)**

The inspector examined the VLTOP software requirements specification (SRS, revision 1, January 31,1994) for requirement accuracy, traceability and consistency. The SRS was reviewed by 7 cognizant engineering organizations, but was not yet issued for project implementation. The requirements that involved processing that used the inputs were incorrect because of incorrect table references. The traceability was primarily to a document entitled "Design Evaluation of VLTOP System Components," (December 2, 1993); this document was not referenced in the design input record. The processing requirements in response to various input/output failures were ambiguous in that hardware and software responses were mixed. There was no reference to the software functional diagram of the microprocessor (15337-06, revision OB) in the hardware interfaces or the references sections.

The inspector reviewed the Software Design Description (SDD) and noted that the functions and detailed parameters of each of the 6 control blocks were accurate and clearly described. However, the traceability matrix did not contain enough detail to audit requirement flow-down from the software requirements specification (SRS).

- **Software Document Review Process**

During the inspection, an independent engineering reviewer from the licensee's Information Systems Department audited the VLTOP software process and documents. The reviewer identified that the requirements traceability from the design requirements to the SRS, the software design description (SDD), and the software acceptance test plan (ATP) was not well defined.

Based on these concerns, the lead design engineer issued software problem reports (SPR) and developed a plan to revise the design bases so that proper flow-down of requirements and traceability could be done. The project manager issued a plan to coordinate review/walkthrough activities and defined responsibilities for reviewers in their areas of expertise. The inspector's assessment was that the appropriate corrective actions were taken, but not in a timely manner.

- **Vendor V&V Program**

The licensee developed a Class 1E purchase specification (SP-630) that underwent two revisions in negotiations with the vendor, The Foxboro Company, using the SPEC 200 MICRO product. The major revisions were caused by the vendor's exception to the IEEE standards for software verification and validation (V&V) plans, and software test documentation.

The vendor substituted a software V&V plan using the guidance of ANSI/IEEE-ANS-7-4.3.2 1982, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generation Stations," as a basis. The vendor considers the product line to be configurable, but not programmable, in the strict sense that the algorithms are in EPROM and not programmable. Since there no standards for configurable products, the vendor maps its V&V program to the guidelines of the ANSI standard. The vendor also performs similar mapping to the guidelines of International Electrotechnical Commission (IEC) Standard Publication 880 "Software for Computers in the Safety Systems of Nuclear Power Stations." The licensee accepted this approach after a review of vendor documents and concluded that a rigorous controlled approach for V&V was used.

The inspector questioned how this approach could be justified for a Class 1E purchase order of this type. During the inspection, the lead design engineer said that the microcontroller hardware was purchased Class 1E because certain cards are connected to Class 1E circuits; however, the system equipment and the software are classified Augmented Quality (AQ-PORV). This means that the vendor can substitute a V&V program not in strict accordance with ANSI-7.4.3.2. Under the AQ-PORV quality classification for this application, the inspector audited the same vendor documents and determined that the licensee's conclusion that a controlled approach for V&V was based on adequate information.

- **Vendor Software Control**

The licensee performed two quality surveillance audits on the vendor. The focus of the first audit was on the qualification program, the software quality assurance program, and the adherence to the equipment specification (P-630) requirements. The second audit determined the conformance of the equipment by review of factory test and system checkout data plus other documentation.

The inspector reviewed the licensee quality surveillance reports (QAO93-579, QAO 94-027) and noted that a limited system level thread surveillance of the requirements and design documents for configurable software blocks used in the VLTOP application was performed. The inspector determined that the limited thread surveillance was well organized.

## 2.5 Configuration Management

- **Program Downloading**

The inspector observed the configuration process of the stand-alone control microprocessor in the I&C lab. A vendor display station provided the interface between the microprocessor controller and a vendor configurator program resident in a personal computer. The configurator program allows the display of the status and allows on-line changes to be made to a controller.

Access for configuration of the controller was by the administrative means of checking out the personal computer and display station. There are no passwords used in the configurator program. There are two specific menu selections that have to be made in order to change the configuration, so that one random key-stroke at the first menu would not change controller configuration. At the second menu, one of five specific key-strokes must be made to allow any changes to be made to the configuration. At the end of any of the five change sequences, it is necessary to press a specific function key in order to download any change. The inspector concluded that the administrative means of access to the equipment to change configuration, coupled with the very specific menu key-strokes was adequate to aid in the prevention of inadvertent or unauthorized changes to the controller configuration.

The inspector noted that the actual installed image of the downloaded configuration was not verified for accuracy of the downloading and installation data communication process. The lead design engineer said that a download verification method would be part of the ATP, surveillance, and configuration management procedures.

- **Change Control**

The licensee's software engineer reviewed the vendor configuration data base and wrote eight software problem reports (SPR); one SPR changed startup manual recovery and I/O flunk parameters. One SPR reported an intermittent discrepancy in the printout of configuration reports. The other six SPRs accepted vendor differences between the original and factory acceptance test data bases. The inspector concluded that there was cross-checking of the data base configuration and monitoring of vendor software by the software engineering staff.

## 2.6 Electromagnetic Interference (EMI)

The purchase specification (SP-630) did not specify the EMI requirements for the VLTOP controller, power supply and card chassis (nest). However, the vendor conducted the following tests: a) conducted susceptibility, power leads, per MIL-STD-461C, test CS01; b) electrostatic discharge per International Electrotechnical Commission (IEC) 801-2; c) radiated susceptibility, high frequency per IEC 801-3; d) high frequency transient per IEC 801-4; and e) electrical surges per IEC 801-5.

The licensee's engineering reviewed the vendor's EMI test reports and justified the results with respect to the proposed "EPRI Guide to EMI Susceptibility Testing for Digital Safety Equipment in a Nuclear Power Plant (Revision 0)."

The inspector reviewed the licensee's report "Radio Frequency Interference Monitoring at Calvert Cliffs Nuclear Power Plant" (Report No. 17729, September 2, 1992). EMI data was collected at a location near the VLTOP installation over a 30 day period that included shutdown, startup, power ascension, and other plant conditions during the 1992 refueling outage. The maximum field strength was 0.018 Volts/meter.

The VLTOP equipment was justified to be used in a radio exclusion area for field strengths of less than 5 Volts/meter (letter G:SES-081093102, "VLTOP: Review of Foxboro Spec 200 EMC Testing," August 12, 1993.) The inspector concluded, with respect to the Augmented Quality classification, that: a) an adequate battery of EMI qualification tests were performed on the vendor equipment; b) that there is sufficient margin between the EMI qualification levels and the actual EMI levels at the point of installation.

## 2.7 Walkdown

The inspector walked down the Unit 1 control room location where the VLTOP microprocessor will be mounted. A hinged sheet metal door was mounted on the cubicle in the panel where the microprocessor will be mounted. The door had a number of fuses mounted on it that could potentially cause a personnel safety or equipment safety problem during the modification, or when future maintenance is performed. The lead design engineer wrote an issue report (IR0-0168-324) that identified the problem. The inspector considered this an appropriate action to initiate corrective action.

## 3.0 FEEDWATER DIGITAL UPGRADE (FCR-87-0090)

The full range digital feedwater control system (FRDFCS) was designed to replace the analog feedwater system, which had many control system related transients that resulted in plant trips. The FRDFCS for Unit 2 was installed in 1993; Unit 1 FRDFCS is to be installed in the 1994 outage period.

The FRDFCS controls the water level for each of the two steam generators from 2% to 100% power, and has 4 modes of operation. Each system regulates the respective main and bypass feedwater control valves and the speed of one feedwater pump. Each system consists of a dual redundant computer configuration connected to three non-redundant digital controllers.

### 3.1 Analog-to-Digital Requirements Translation

The procurement specification was brief and was system performance and design feature oriented. The vendor had previous design experience with the Calvert Cliffs analog feedwater system and digital feedwater systems at other nuclear plants. The main source of the available technical material was in the vendor manual (VTM #12104-159, April 4, 1991), and a summary of specifications entitled "Full Range Digital Feedwater Control System Position Paper, November 1992." The position paper provided the FRDFCS design requirements and equipment specifications. The inspector did not note any sampled data system analysis for the digital system. Detailed performance acceptance criteria were documented in the acceptance test plan (ATP), but the inspector was unable to find all of the corresponding system performance specifications in the position paper. Therefore, the inspector was not able to trace detailed requirement flow down or to assess the accuracy of the analog-to-digital translation accuracy. However, the inspector was able to reconstruct the design bases, characteristics of the analog system, and additional design requirements from the design input record (DIR) for the FRDFCS. The inspector concluded that the licensee concentrated more on documenting the design rather than specifying the detailed system and software requirements.

### 3.2 Dual Redundant Computer Implementation

Each computer in a dual redundant system for each steam generator receives identical inputs, processes the inputs using identical programs, and delivers a set of separate isolated outputs to each of the three digital controllers per steam generator. The field analog inputs are redundant. The digital controllers and final controlled actuators are not redundant.

Power is supplied by two AC busses and redundant power supplies such that a loss of either bus will not cause failure of level controls for both steam generators. One bus and 5 Vdc power supply are used for the primary computers for both steam generators; the redundant bus and power supply is used for the backup computers. Redundant 24 Vdc power supplies are used for the six digital controllers (3 per steam generator) used for both steam generators.

One computer is designated as the primary and one computer is designated as the backup. Each set of computer outputs includes functional control signals and failure indication contacts. The failures covered are power failure and processing halt (watchdog timer). The digital controllers use the failure contacts to determine the correct set of computer functional control signals, primary or backup, to use. The digital controllers also send the computers status and tracking information. The digital controllers can perform automatic or manual control.

The field transmitter inputs are isolated in the computer. If deviation and out-of-range checks indicate failure, the software takes corrective action to notify the operator and is programmed to minimize failure effects on plant operations. The inspector audited the deviation check software flow charts for steam generator water level, steam flow, feedwater flow, neutron flux, feedwater temperature, and determined that the programmed actions were in consonance with the fault tolerant objectives of the design.

### 3.2.1 **Hardware**

The computers are Analogic microMAC 6000, which are industrial grade Intel 80188 (16 bit) based, operate at 8 Mhz and have a watchdog timer. The computer can be programmed either in the BASIC language or the C language. The computer has isolated analog, digital input/output (I/O) interfaces to support stand-alone systems. The bandwidth of the analog input interfaces is 4 Hz. The I/O types used in the each FRDFCS are: 16 analog inputs; 3 analog outputs; 7 digital inputs; 8 digital outputs.

For each computer, a touch sensitive plasma display unit (PDU) provides for operational control, information, and set point entry.

There are 3 digital controllers on the control board for each steam generator. The digital controllers have a cycle time of 0.1 second.

Radiated electromagnetic interference (EMI) was considered. The inspector reviewed the specifications of the computer and digital controller vendors versus the actual levels measured near the control room panel in the licensee's report "Radio frequency Interference Monitoring at Calvert Cliffs Nuclear Power Plant" (Report No. 17729, September 2, 1992). The inspector determined that there is sufficient margin between the equipment specifications and the actual measured values in the report.

Memory back-up battery replacement for the computers, digital controllers was considered. Battery periodic maintenance, replacement schedules were covered in the training course.

The inspector walked down both installation areas of the FRDFCS equipment in the combined control room. The location was adequate from the maintenance, operator access and heat load aspects.

### 3.2.2 Software Design, Verification & Validation (V&V), Configuration Management, and Test

- **Software Design**

The software was developed by ABB Combustion Engineering, using interpreted BASIC. The program had approximately 1900 source lines. The inspector audited the program flow charts in the technical manual and noted that they were adequate to convey the top level functions and structure.

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

The licensee did not review the software verification and validation (V&V) of the vendor because the application was not safety-related. The inspector reviewed the vendor system software test descriptions and noted that a vendor simulation model was used to test the installed code in a quasi-plant environment for steady state, transient and single failure scenarios. The inspector concluded that the functional capabilities of the code for major plant occurrences were covered, but there was no clear mapping as to what part of the code was actually exercised.

The inspector reviewed the code source listing and noted that it contained approximately 240 GO TO statements. The inspector asked the licensee if the GO TO statements were all tested. The licensee said that the vendor performed an independent code review, but that probably most of the GO TO statements were tested in the vendor demonstration test or at the software acceptance test. The inspector noted that no software tools were used to find out if all branches of the program were tested, and that no analytical or test data was found to show how many GO TO statements were actually checked. The inspector concluded: a) that at least some of the GO TO statements are not tested or checked; b) that the risk to incorrect functional performance while not quantifiable, may actually be bounded by the tests that were performed.

- **Software Configuration Management Plan**

The software configuration control plan for the FRDFCS covered the responsibilities, activities, change V&V, vendor control and record collection/retention, software downloading and media storage. A new operational baseline is established when a change is made to the algorithms; the disk and listing would be identified by a change in the first digit version number of the software, from 3.1 to 4.0, for example. When a change is made to the tuneable parameter values, the disk and listing would be identified by a change in the second digit release number, from 3.2 to 3.3, for example. The Unit 2 and Unit 1 software configurations are kept separate. The inspector audited the configuration management plan and found it sufficient. The inspector noted that the project manager requested the software engineer to review vendor code for correct incorporation of changes (letter, "V&V of the FRDFCS Rev. 5.0 Software Unit 2," August 4, 1993), which caught errors that could have affected plant operations. The inspector viewed this as an example of proper attention to software details and indicated effective implementation of the software configuration plan.

- **Program Downloading**

The inspector reviewed the portable PC method of downloading the program to the computers. Character parity, block checks, or check sums methods of data integrity checking on the communication link were not used. There was no verification of the downloaded installed data versus the program disk data. The downloaded program is installed into battery-backed non-volatile RAM (NVRAM). The processor then moves the setpoints to volatile RAM for faster execution. An enhancement will add the capability to display the program version number on the PDU. The inspector noted that because minimum data integrity checks are employed for the download, the installed program could be subject to errors; and since the actual installed program in NVRAM is not verified after downloading, any data corruption would not be detected. Furthermore, any data corruption during the time between program downloads would not be detected. The inspector assessment was that: a) with the enhancement described above, the version control would be adequate; b) there is the possibility of reduced program integrity because bit error detection methods were not employed.

- **Set Point Changes**

The inspector observed that set point changes require the respective computer to be put into the test mode using the auto/test key switch, or the three digital controllers to be put into the manual mode. A security code must be entered before set points can be changed via the plasma display units (PDU). Changes to set points are controlled by procedure and made from the PDUs and loaded into volatile RAM. A tag is placed on the panel after a set point change. If a power outage occurs, the operator will know by the tag that a computer reset will result in using the old setpoints and therefore he will call the cognizant software engineer. The configuration management plan requires that the program be updated and downloaded to reflect changed set points within five days after any change. The inspector assessment was that the administrative procedure for the control of set point changes was adequate to assure that inadvertent changes would not be introduced into the software.

- **Software Change Control During Test Phases**

The inspector examined data concerning the software changes for the Unit 2 full range digital feedwater control system (FRDFCS). The data was classified as critical, minor, enhancement, or setpoint software changes. The inspector calculated the percentage of total software changes (85 total, excluding setpoint changes) in the major project stages as: 13% independent code review; 62% integration/demonstration test; 13% pre-operational site testing; 12% operational phase. The percentage of the total critical software changes (20) in each project phase was calculated as: 65% integration/demonstration test; 20% pre-operational site testing; 15% operational acceptance phase. The critical software changes involved such errors as: CPU lock-up when bypassing an input; CPU failure on turbine trip if bypass valve reset was too soon after the trip; instabilities in the 60% to 75% power range. The software changes caused the microprocessor cycle time to increase to 0.79 sec from 0.6 sec. The fact that 35% of the critical software errors were identified by the licensee's system, I&C design, and software engineers after vendor testing showed alert, effective interdisciplinary problem solving.

The Unit 1 FRDFCS was at the initial stages of the pre-operational site testing and had 5 software changes, of which 1 was critical and 4 were enhancements. The critical change involved a race condition in the detection of feedwater flow input failure that caused unpredictable processor failover modes.

- **Test**

The inspector audited the Unit 1 FRDFCS acceptance test in the I&C lab. The test will be conducted using 23 test cases and 12 plant transients using the PC simulator. The inspector observed the tests for the step load changes and the failed feedwater flow transmitter. The output steam generator level transient response curves on the PC screen had similar characteristics to the transient response curves from the vendor demonstration test. The active computer response to the failed feedwater flow was correct.

### 3.2.3 **Training**

Following the 1993 refueling outage installation of the FRDFCS, a reactor trip occurred as a result of low steam generator level. The licensee conducted a root cause investigation (CCER 93-03) that determined one of the causes was inadequate operator training on the digital controllers. The details concerned the new membrane push-button control for manual control of the bypass valve. The new push-button controlled the position of the bypass valve in a different manner than the previous knob control. The operating staff had received formal and simulator training on the FRDFCS, but the automatic features were covered in more detail than the manual control features. One of the corrective actions was to provide better hands-on training for manual valve control using the new push-button on the digital controller. FRDFCS project technical support was not a factor, because there was coverage for all shifts before the incident.

The inspector reviewed the on site training manual (February 1993) for the system. The manual covered the system configuration, the simulation model, steam generator theory, software algorithms, simulated transients, maintenance, computer procedures and troubleshooting guidelines. The inspector assessment was that the training manual adequately covered topics necessary to understand the theory, operation and maintenance of the equipment.

## 4.0 UNRESOLVED ITEMS

Unresolved items are matters about which additional information is necessary to determine whether they are acceptable, a deviation, or a violation. There are no unresolved items.

## 5.0 EXIT MEETING

The inspector met with the licensee's personnel denoted in Attachment 1 of this report at the conclusion of the inspection on February 18, 1994. At that time, the inspection results were summarized, and the licensee acknowledged the results. The technical contacts are R. Szoch and B. Geddes.

## ATTACHMENT 1
## PERSONS CONTACTED

### Baltimore Gas & Electric Company

| | |
|---|---|
| *A. Anuje | Supervisor, Nuclear Quality Assurance |
| L. Arnesen | Systems Analyst, Information Systems |
| M. Bowman | Lead Engineer |
| L. Brown | Engineer, Procurement Engineering |
| P. Bukowski | Engineer, Design Engineering, Feedwater Project |
| K. B. Cellars | General Supervisor,Design |
| G. Cordell | Analyst, Reliability |
| *B.Geddes | Senior Engineer, I&C Design Engineering, VLTOP Project |
| *P. Katz | Manager, Nuclear Engineering Department |
| *R.F. Lackwitz | Senior Project Administrator, Information Systems Department |
| R. Mervine | Information Technology Consultant, Power Systems & Services Section |
| *B. Morris | Supervisor, Nuclear Systems Unit, Information Systems |
| G. Pavis | General Supervisor, Plant Engineering |
| K. Peterson | Design Engineer, ABB-CE Site Office |
| W. Ramstedt | Engineer, Quality Audits |
| B. Rudell | Project Management |
| L. Shanley | Senior Engineer, Reliability |
| *C. D. Sly | Engineer, Licensing & Compliance |
| G. Stallings | Engineer, Information Systems Department |
| R. Stattel | Engineer, System Engineering |
| *R. Szoch | Principal Engineer, I&C Design |
| W. Williams | Project Manager, Feedwater Project |
| J. Wood | Engineer, Quality Audits |
| *J. Wright | Project Manager, VLTOP Project |
| C. J. Yoder | Senior Engineer, Life Cycle Management Unit |

### U.S. Nuclear Regulatory Commission

| | |
|---|---|
| P. Wilson | Senior Resident Inspector |
| *K. Lathrop | Resident Inspector |

* denotes attendance at exit meeting 2/18/94