

ATTACHMENT 4

**Verification and Validation Report for Square D Masterpact Circuit
Breaker (Coils Only), VVR-042181-1-COIL, dated October 2009**



**VERIFICATION AND VALIDATION REPORT
FOR
SQUARE D MASTERPACT CIRCUIT BREAKER
(COILS ONLY)**

NLI Report VVR-042181-1-COIL
Revision 0
October 2009

APPROVAL
VERIFICATION AND VALIDATION REPORT
FOR
SQUARE D MASTERPACT CIRCUIT BREAKER
(COIL ONLY)

This report has been prepared in accordance with the NLI Quality Assurance Program.

Prepared by: Charles Bee / and date 10/26/09

Verified by: V. Z date 10/27/09

Approved by: Jay Bell date 10/27/09

REVISION HISTORY

<u>Revision</u>	<u>Description</u>	<u>Date</u>
0	Original Issue	10/27/09

TABLE OF CONTENTS

- 1.0 SUMMARY OF RESULTS
 - 1.1 Scope
 - 1.2 Limitations
 - 1.3 Project Specific Activities
 - 1.4 Codes and Standards
 - 1.5 Conclusion

- 2.0 EQUIPMENT IDENTIFICATION
 - 2.1 Safety Function
 - 2.2 Equipment Configuration
 - 2.3 Human Machine Interface
 - 2.4 Cyber Security
 - 2.5 Traceability of the Test Specimen to the Production Units

- 3.0 SOFTWARE QUALITY ASSURANCE AND LIFECYCLE MANAGEMENT
 - 3.1 Software Quality Assurance Plan
 - 3.2 Software Lifecycle Management Plan

- 4.0 ABNORMAL CONDITIONS AND EVENTS
 - 4.1 Environmental Service Conditions
 - 4.2 Seismic Service Conditions
 - 4.3 Electromagnetic Interference/Radio Frequency Interference (EMI/RFI)
 - 4.4 Voltage Range
 - 4.5 Infant Mortality of Electronic Components
 - 4.6 Fault in Non Safety Plant System
 - 4.7 Hardware/Software Faults
 - 4.8 Loss of Power
 - 4.9 Overcurrent Condition

- 5.0 FAILURE MODES AND EQUIPMENT RELIABILITY
 - 5.1 Hardware Failure Modes and Effects Analysis
 - 5.2 Hardware Reliability
 - 5.3 Firmware Reliability
 - 5.4 System Failure Modes & Effects Analysis

- 6.0 REQUIRED SYSTEM CHARACTERISTICS
 - 6.1 Verification of Required System Characteristics
 - 6.2 Separation Criteria
 - 6.3 Common Mode Failure Evaluation

7.0 IMPLEMENTATION OF REQUIRED CHARACTERISTICS

- 7.1 Commercial Grade Audit of Schneider/Square D
- 7.2 NLI Testing
 - 7.2.1 Qualification Testing
 - 7.2.2 Dedication/Factory Acceptance Testing (FAT)
 - 7.2.3 Validation Testing
- 7.3 Operating History
- 7.4 Users Manuals

8.0 CONFIGURATION MANAGEMENT PLAN

- 8.1 Schneider Firmware Configuration Control and Error Reporting
- 8.2 NLI Configuration Control
- 8.3 Plant Lifetime Configuration Control

9.0 QUALITY ASSURANCE

10.0 MEASUREMENT & TEST EQUIPMENT

11.0 REFERENCES

ATTACHMENT A: LIST OF APPLICABLE SCHNEIDER PROCEDURES

1.0 SUMMARY OF RESULTS

1.1 Scope

This Verification & Validation (V&V) program was performed to demonstrate the acceptability of the coils used in the Square D Masterpact circuit breakers to meet the requirements for the use of digital components in safety related applications in nuclear power plants. This report specifically addresses the shunt trip device, UV (undervoltage) trip device, and close coil in the Masterpact NT and NW circuit breakers (referred to in the report as "coils"). These coils contain microcontrollers with firmware. There are no user configurable setpoints, configurable switches, or field modifications.

The typical application for the Masterpact breakers at nuclear plants in the United States is as part of low voltage switchgear or a replacement breaker to replace existing low voltage breakers. A summary of this application is as follows:

- The Masterpact breaker is manufactured by Schneider/Square D. Square D is the company that supplies the Masterpact breakers in the United States. Schneider is the parent company located in France. A summary of the Schneider/Square D activities and locations is presented in section 7.1 of this report.
- The Masterpact breaker is converted by Square D Services in West Chester, Ohio to the specific replacement breaker configuration. This involves the design and manufacture of the electrical and mechanical interfaces to the existing switchgear. Square D Services is a long term NLI partner. The Masterpact circuit breakers are also supplied in new Square D switchgear.
- Square D Services performs the ANSI design testing required in accordance with ANSI C37.59 and other applicable ANSI standards.
- NLI performs the required dedication activities:
 - Production controls and Quality Control oversight of Square D activities.
 - Dedication of materials.
 - Dedication/Factory Acceptance Testing (FAT) of the replacement breakers.
- NLI performs the required qualification activities, including the following:
 - Seismic qualification.
 - EMI/RFI qualification.
 - V&V as documented in this report.
 - Mild or harsh environment qualification.

Safety related breakers are supplied to nuclear plants in accordance with the NLI Nuclear Quality Assurance Program which meets the requirements of 10CFR50 Appendix B, 10CFR21, and ASME NQA-1.

The coils use microcontroller technology. This report documents the results of the V&V of the software/hardware used in the trip devices and coils.

Coil Configuration

The components addressed in the V&V report are the UV, shunt trip, and close coils for the Masterpact NT and NW circuit breakers:

- Shunt trip and close coil (nominal rating of 125vdc/120vac):
 - NW breaker: Square D p/n S33812.
 - NT breaker: Square D p/n S48493.
- Undervoltage trip (nominal rating of 125vdc/120vac):
 - NW breaker: Square D p/n S33821.
 - NT breaker: Square D p/n S48503.

This report is also applicable to coils with 240vac and 250vdc operating voltages. The same digital components and firmware are used in these devices.

Report Summary

This V&V report provides the following detailed information:

- Section 1.2: Limitations of this V&V program.
- Section 1.3: Activities that will be performed by NLI for each individual project where the components are supplied.
- Section 1.4: Summary of the codes and standards that are met by this V&V program. The detailed evaluation of the applicable standards is contained in the V&V Plan in Attachment D.
- Section 1.5: Report conclusion.
- Section 2.0: Detailed summary of the equipment configuration.
- Section 3.0: Summary of the Software Quality Assurance Plan. Summary of the Software Lifecycle Management Plan.
- Section 4.0: Identification and evaluation of the Abnormal Conditions and Events (ACE's).
- Section 5.1: Summary of the Failure Modes and Effects Analysis.
- Section 5.2 and 5.3: Equipment reliability information.
- Section 5.4: Systems level failure modes and effects analysis for the reactor trip breaker application.
- Table 6.1: Identification of the applicable critical characteristics, the acceptance criteria for each critical characteristic, the methods used to verify the critical characteristics, and the results.
- Section 6.2: Evaluation of separation criteria.
- Section 6.3: Evaluation of common mode failure.
- Section 7.1: Summary of the Schneider/Square D audits.
- Section 7.2: Summary of the NLI V&V activities.
- Section 7.3: Summary of the product operating history, including nuclear plant operating experience.
- Sections 8.1 and 8.2: Schneider/Square D and NLI configuration control activities.
- Section 8.3: Required plant configuration control activities.

The Schneider supporting documents are proprietary and are not included in the versions of this report that are released. These documents are available for review at the NLI facility.

1.2 Limitations

The following coil configurations are not addressed in this V&V program. The coils are not considered qualified in these configurations:

- The coils can be configured for external communications. This is not a qualified configuration.

1.3 Project Specific Activities

This V&V report documents the activities that were performed for the V&V of the coils for safety related applications. The following activities are performed for each specific project to verify the applicability of this report and dedicate and qualify the supplied equipment:

- Hardware and software configuration review to verify applicability of this report.
- NLI FAT/dedication testing on 100% of the supplied equipment. The FAT/dedication testing will include the following specific critical characteristics:
 - Test the circuit breaker across the plant specified range of control voltages. This includes operation of all of the coils.
 - Note: The dedication plan for each replacement breaker type will include additional critical characteristics that verify the proper operation of the entire breaker assembly.
- Verify that the plant specific ACE's and ACE levels are enveloped by this report and supporting documentation or testing is performed per the client specific requirements.
 - Seismic qualification: Seismic qualification is plant specific and specific to the configuration of the replacement breaker.
 - EMI/RFI.
 - Environmental service conditions.
 - Voltage range.
 - Additional ACE's as defined by the plant.

In addition to this report, the following documents will be prepared for each plant/breaker configuration, as applicable:

- Seismic qualification report.
- EMI/RFI qualification report.
- Design drawings.
- Instruction manual.
- ANSI design report.
- NLI Factory Acceptance Testing (FAT)/Dedication Test plan and report.

1.4 Codes and Standards

The firmware for the coils was developed under the controls of the Schneider/Square D ISO 9001-2000 quality assurance program. The hardware and firmware are being dedicated for safety related applications by NLI under the controls of the NLI Nuclear Quality Assurance Program [16]. The applicable codes and standards are identified in the sections of this report. These codes and standards form the basis for the V&V activities and this V&V report.

Note: Most of the codes and standards referenced in the V&V Plan are for controls of the entire software lifecycle. Many of the codes and standards are very prescriptive concerning the required activities and documentation. Since this project is the dedication of existing commercial software, only certain requirements of these standards are applicable.

1.5 Conclusion

This V&V program was performed in accordance with the guidelines of EPRI-TR-102348 [4] and EPRI TR-106439 [5]. The dedication program was performed in accordance with the NLI Nuclear Quality Assurance Program and it includes all of the provisions of EPRI-TR-106439. The dedication program was based on commercial grade audits of the Schneider facility and testing by NLI. The activities that were performed are summarized below.

- The coil requirements are documented in this report, based on the Schneider design documents.
- The coil design was performed by Schneider/Square D. The coil design is documented in the Schneider/Square D documents that were reviewed by NLI during the audits.
- Hardware Failure Modes and Effects Analyses (FMEA's) were performed by Schneider and supplemental FMEA analyses were performed by NLI.
- The ACE's were identified and addressed by testing or analysis (see section 4.0 of this report).
- The coil critical characteristics (electrical, mechanical, firmware, process, dependability) were identified by NLI based on the function of the equipment. The coil critical characteristics were verified based on audits of Schneider, testing at NLI, and evaluation of the operating history. The critical characteristics were found to meet the acceptance criteria. Table 6.1 identifies the critical characteristics of the coil, including the digital system.
- Lifetime configuration control of the components is as specified in section 8.0 of this report.
- Nuclear plant operating experience was reviewed and evaluated.

These activities ensure that the acceptance features in Figure 3-2 of EPRI TR-106439 were followed for the firmware dedication process. There was an acceptable blend of the NLI dedication efforts, product operating experience, and the vendor efforts to demonstrate that the components are acceptable for this safety related application. NLI has provided an acceptable level of control over the development, installation, testing, and maintenance of the firmware under the control of the NLI Nuclear Quality Assurance Program. The firmware are within the bounds of the dedication and all critical characteristics have been successfully verified by audits,

tests, and inspections. The operating history of the coils shows very good performance with no firmware problems in well over 100,000 installed coils. The coils were first issued in 2002 and there have been no revisions to the coil firmware since it was issued. The manufacturer, Schneider, has an excellent record for support and addressing past problems. Our review of the coils' overall architecture, hardware, and firmware design shows a high quality design without any weaknesses. This includes the failure analysis which was performed that shows that all failures are adequately addressed in the equipment design. All of these activities provide reasonable assurance that the coils will perform their safety-related functions. The quality of the coils, both hardware and firmware, is equivalent to equipment that is developed under the controls of a Nuclear Quality Assurance Program.

2.0 EQUIPMENT IDENTIFICATION

2.1 Safety Function

The safety functions of the coils are:

- UV: Allow the breaker to close during a normal voltage condition (coil energized). Trip the breaker in an undervoltage condition (coil de-energized, spring return). Not inadvertently trip the breaker.
- Shunt trip: Allow the breaker to close with no control voltage applied (coil de-energized). Trip the breaker with control voltage applied (coil energized). Not inadvertently trip the breaker.
- Close coil: Close the breaker with voltage applied (coil energized).

See the additional information in sections 2.2.2 and 2.2.3 on the operation of the coils.

2.2 Equipment Configuration

The configuration information is presented in this section.

2.2.1 Part Number and Revisions

The components addressed in the V&V report are the UV, close coils and shunt trips for the Masterpact NT and NW circuit breakers:

- Shunt trip and close coil (nominal rating of 125vdc/120vac):
 - NW breaker: Square D p/n S33812.
 - NT breaker: Square D p/n S48493.
- Undervoltage trip (nominal rating of 125vdc/120vac):
 - NW breaker: Square D p/n S33821.
 - NT breaker: Square D p/n S48503.

The identifier and current revisions are as follows:

- Programmed microcontroller part number: 51005451AA, revision B.
- Firmware revision: V15.

2.2.2 Coil Configuration

The configuration of the coils is as follows:

- The package, mounting, circuit board and configuration of the coils are all the same, except as evaluated below:
 - NW vs. NT part numbers: The wiring and connectors are different to mate with the electrical components in the breakers.
 - Operation of the shunt trip, close coil, and UV are the same, except as follows:
 - Shunt trip: The shunt trip is normally de-energized with the plunger retracted. The coil is energized for a short duration to extend the plunger. The plunger impacts the trip latch and trips the breaker. When the coil is de-energized, the spring returns the plunger to the retracted position.

- Close coil (same part number as the shunt trip): The close coil is normally de-energized with the plunger retracted. The coil is energized for a short duration to extend the plunger. The plunger impacts the close latch and closes the breaker. When the coil is de-energized, the spring returns the plunger to the retracted position.
- UV: With the coil de-energized, the plunger is extended and the breaker cannot be closed. The coil is energized to retract the plunger. This allows the breaker to be closed. When the voltage is lowered below the setpoint or removed, the coil is de-energized and the spring returns the plunger to the extended position. The extended plunger hits the trip latch and trips the breaker.

2.2.3 Circuit Breaker Configuration

The overall configuration of the circuit breaker is as follows:

- The low voltage power circuit breaker is installed in the low voltage switchgear. Each circuit breaker is in an isolated cubicle.
- The operation of the coils is as follows:
 - All of the coils are installed in the breaker.
 - The unextended UV and shunt trip coil plungers are in close proximity to the trip latch. Extension of the coil plunger hits the trip latch and trips the breaker.
 - The unextended close coil plunger is in close proximity of the close latch. Application of control voltage extends the plunger, hitting the latch and closing the breaker.
 - UV coil: The coil is energized with control voltage to retract the plunger. This allows the breaker to be closed. When the control voltage is removed or reduced below the dropout voltage of the coil, the spring return extends the plunger. The plunger hits the trip latch and trips the breaker.
 - Shunt trip coil: The coil plunger is normally retracted and the breaker can be closed. Application of control voltage extends the plunger, the plunger hits the trip latch and the breaker trips.

2.2.4 Coil Architecture

2.2.4.1 Summary of Operation.

MN: Undervoltage release (UVR). This release instantaneously opens the circuit breaker when its supply voltage drops to a value between 35 and 70% of its rated voltage. Any attempt to close the circuit breaker equipped with an MN (VR) release when its supply voltage is less than 85% of the rated voltage inhibits closing of the main contacts.

MX: Shunt trip release (SHT). This release instantaneously opens the circuit breaker whenever its supply voltage is 50% over its rated supply voltage. This release may have a continuous or transient supply.

XF: Shunt close (SHCL). This electromagnet closes the circuit breaker whenever its supply voltage is more than 50% of its rated supply voltage.

2.2.4.2 Architecture

The architecture of the coils is as follows:

- (1) The only difference between MX/XF actuators and MN actuator is mechanical. They have the same electrical characteristics (same microcontroller and coils).
- (2) Microcontroller : 8 bit MOTOROLA 68HC805P18
- (3) There have been no firmware revisions since the firmware was first issued in 2002.
- (4) There is no external communication in safety related configuration of the coils (connection of the communications feature is not a qualified configuration).
- (5) Programming language – assembler.
- (6) There are no unused software blocks or unused compiled code.
- (7) All measured parameters are stored in direct addressed RAM.
- (8) Program values are stored in an EEPROM and are read into the microcontroller RAM during initialization.
- (9) The microcontroller initialization sequence verifies hardware and firmware operation.
- (10) The total code consists of the following eight code modules
 - a. RESS.ASM
 - b. RAM.ASM
 - c. T_CARRE.ASM
 - d. T_U.ASM
 - e. T_IAPP.ASM
 - f. T_IMAI.ASM
 - g. T_BOB.ASM
 - h. CONST.ASM
- (11) There are no internal diagnostics other than a time-out watch dog during main loop program operation.
- (12) Power to the coils is from the plant control power. A 5 volt power supply is used to power the electronics. The FMEA did not identify the power supply as a critical part in the design life/mean time to failure (MTTF) of the coils.
- (13) There is no battery used.
- (14) The hardware/firmware system is testable. The NLI dedication/FAT testing tests the system on 100% of the supplied breakers.
- (15) The common mode failure evaluation is contained in section 6.3.

2.2.4.3 Firmware Operating Sequence

The firmware operating sequence is as summarized below:

Measurement phase

- Regulation of the maintain current:
 - Maintain current measurement
 - Activate the maintain transistor. Wait 34 μ s
 - Put CDE_I=1 during 10 μ s
 - Input the maintain current measurement
 - Comparison of the maintain current measurement with the previous measurement.
 - Management of transient failures
 - Actuate or inhibit of the maintain transistor.
- Network voltage
 - Read the network voltage
 - FIR filter, which gives an output value each 8 cycles
- Determination of the next condition
 - If the output data of the FIR filter is higher than the first threshold, go to the activation phase.

Activation phase

- Regulation of activate current:
 - Initiation of the activate current measurement
 - Put G_activate =1
 - Input the activate current measurement
 - Comparison of the activate current measurement with the previous measurement.
 - Initiate or inhibit the activation transistor.
- Network voltage – is there a measured network voltage value or FIR value
- Determination of next condition
 - The firmware remains in the activation phase for 80ms
 - Go to the delay phase

Delay phase

- Regulation of maintain current :
 - Maintain the current measurement
 - Activate the maintain transistor. Wait 34 μ s
 - Put CDE_I=1 during 10 μ s
 - Input the maintain current measurement
 - Comparison of the maintain current measurement with the previous measurement.
 - Initiate or inhibit of the maintain transistor.
- Network voltage

- Read the network voltage
- FIR filter, which gives an output value each 8 cycles
- Determination of next condition
 - The firmware will stay in idle period phase for 30ms
 - Go to the maintain phase.

Maintain phase

- Regulation of maintain current :
 - Realization of the maintain current measurement
 - Activate the maintain transistor. Wait $34\mu\text{s}$
 - Put $\text{CDE_I}=1$ during $10\mu\text{s}$
 - Input the maintain current measurement
 - Comparison of the maintain current measurement with the previous measurement.
 - Activate or inhibit the maintain transistor.
 - When CDE_I is 0, all the current is through the coil to V_{in} , charging the C4 capacitor
 - When CDE_I is 1, the coil current crosses VT4 (shunt resistor) and the signal $I_MAINTAIN$ is measured on R24 resistor.
- Network voltage
 - Read of network voltage
 - FIR filter, which gives an output value each 8 cycles
- Determination of next condition
 - When the output data of the FIR filter is higher the setting of the second threshold, go to the activation phase (only once)
 - When the output data of the FIR filter is lower than the inhibit threshold, go to the inhibit phase.

The following definitions are used in the descriptions above:

- CDE_1 : signal that controls the initialization of the maintain current reading.
- FIR: *Finite impulse response filter* - This filter doesn't give a direct value of the RMS voltage but a value proportional to its square, averaged over 8 measurements. So, the settings read by the microcontroller for activation and inhibit thresholds will be also values proportional to the square of the RMS voltages.
- $G_activate$: output signal of the microcontroller which regulates the activate current.
- $I_MAINTAIN$: measurement signal of the maintain current (current converted in voltage through a shunt resistor) read by the microcontroller.
- Network voltage: network voltage filtered and rectified. It's used to :
 - Supply the coils (common point of the two coils)
 - Supply the V_{in} regulation circuit (for versions below 100V)
 - Generate the network voltage measurement.

2.3 Human Machine Interface

The coils do not have human-machine interfaces.

2.4 Cyber Security

The coils are hard coded microcontrollers that cannot be field modified. The microcontroller is mounted on a circuit board inside of the coil sealed plastic housing. Opening the plastic housing would destroy the coil. No cyber security requirements are applicable.

2.5 Traceability of the Test Specimens to the Production Units

Traceability of the test specimens to the supplied equipment is documented for each project. The following methodology is used to document the traceability:

- The hardware and firmware revision is not available by inspection of the equipment. NLI is in regular contact with Schneider/Square D to identify if there are any revisions. See section 8.2 of this report.
- There are no field configurable circuit board settings (DIP switches, jumpers, etc.) or user settings.
- The functional testing of the test specimen and the dedication testing of the production units will provide added assurance that the production units were manufactured to the same design standards and perform in an equivalent manner to the test specimen.

3.0 SOFTWARE QUALITY ASSURANCE AND LIFECYCLE MANAGEMENT

3.1 Software Quality Assurance Plan

Project activities were performed in accordance with the NLI Nuclear Quality Assurance Program [16], which meets the requirements of 10CFR50 Appendix B, 10CFR21, and ASME NQA-1. The NLI software quality assurance requirements are as specified in this report.

The firmware was developed under the controls of the Schneider ISO9001-2000 quality assurance program. A Software Quality Assurance Plan was developed and implemented for this firmware by Schneider. Additional details are presented in section 7.1 of this report.

3.2 Software Lifecycle Management Plan

IEEE 1012 provides a detailed prescriptive process for the development of software verification and validation plans. The process which is described includes verification and validation tasks throughout the lifecycle of the software, from the requirements specification to lifetime maintenance of the system. Technical, test, and documentation requirements are specified for each lifecycle step. This IEEE standard is not directly applicable since the software/firmware was previously developed by Schneider and verification and validation of many of the life cycle

phases were not documented in accordance with the standard. The specific format, content, and acceptance criteria in this standard were not used, since the software has previously been developed.

The lifecycle steps in IEEE 1012 Figure 1 were used as a basis to determine whether Schneider had the appropriate lifecycle controls and to document the NLI required lifecycle controls for the digital equipment. Utilizing IEEE 1012 as a guide, NLI determined that Schneider had sufficient life cycle controls in place to support dedication of the software.

The Software Lifecycle Management Plan addresses the following:

- NLI Lifecycle Activities: The lifecycle management of the computer system that was previously developed under the controls of the Schneider commercial quality assurance program.
- Plant Specific Activities: The plant specific activities that are performed.

Lifecycle Step	NLI Lifecycle Activities	Plant Lifecycle Activities
Concept	<p>None. This activity was performed by Schneider. It is not relevant to the V&V program being performed by NLI.</p>	Not applicable.
Requirements	<p>NLI audited Schneider. The audits verified that Schneider has the following documents:</p> <ul style="list-style-type: none"> • A detailed specification for the equipment. • Software specification. <p>Additional details are contained in section 7.1.7 of this report.</p>	<p>The plant specific requirements are documented in the plant equipment specification, including seismic, EMI/RFI, temperature, and voltage range.</p>
Design	<p>NLI audited Schneider. The audits verified that Schneider used a controlled process for the design of the equipment. The following Schneider documents are applicable:</p> <ul style="list-style-type: none"> • Coding specification. <p>See the specific critical characteristics in section 6.0 of this report. Additional details are provided in section 7.1 of this report.</p>	Not applicable.
Implementation	<p>NLI audited Schneider. The audits verified that Schneider used a controlled process for the implementation of the equipment design. The following Schneider documents are applicable:</p> <ul style="list-style-type: none"> • Coding specification. • Production control procedures identified in section 7.1.4 of this report. 	<p>The implementation is documented in the plant specific modification package.</p>

	See the specific critical characteristics in section 6.0 of this report.	
Component Testing	<p>NLI audited Schneider. The coils are simple devices and are tested at the component level. The following Schneider documents are applicable:</p> <ul style="list-style-type: none">• Acceptance test procedure and results. <p>See the specific critical characteristics in section 6.0 of this report and section 7.1.7.</p>	Not applicable.
Integration Testing	<p>NLI audited Schneider. The coils are simple devices that are tested at the component level. The following Schneider documents are applicable:</p> <ul style="list-style-type: none">• Acceptance test procedure and results. <p>See the specific critical characteristics in section 6.0 of this report and section 7.1.7.</p>	Not applicable.
System Testing	<p>NLI audited Schneider. The audits verified that Schneider used a controlled process for the testing of the equipment. The following Schneider documents are applicable:</p> <ul style="list-style-type: none">• Acceptance test procedure and results. <p>NLI performs dedication testing of all supplied equipment, including the coils in the circuit breakers.</p> <p>See the specific critical characteristics in section 6.0 of this report and section 7.1.7.</p>	Not applicable.

Acceptance Testing	Not applicable.	The plant performs acceptance testing prior to installation in accordance with plant procedures.
Installation and Checkout	Not applicable.	The plant performs installation and checkout in accordance with plant procedures.
Operation and Maintenance	NLI supplies plant specific Users Manuals.	The plant performs operation and maintenance in accordance with plant procedures.
Configuration Management	<p>NLI audited Schneider. The audit verified that Schneider has a controlled process for documentation and reporting problems.</p> <ul style="list-style-type: none">• The applicable Schneider documents are identified in section 8.1 of this procedure. <p>See section 8.2 of this report for details on the NLI configuration control activities.</p>	Not applicable. The firmware cannot be field modified. There are no user switch or software settings.

4.0 ABNORMAL CONDITIONS AND EVENTS (ACE's)

The guidance provided in Annex D of IEEE Standard 7-4.3.2-2003 [1] was used to identify the various ACEs that could impact the capability of the components to perform the intended safety functions. The Abnormal Conditions and Events (ACEs) that could impact the proper operation are identified in this section. The methods which are used to evaluate each of the ACE's are also presented.

Note: The ACE's and the ACE levels specified below are expected to envelope most of the Class 1E applications in nuclear power plants. Plant specific levels that are not enveloped will be evaluated and tested on a plant specific basis as specified in section 1.3 of this report. Plant specific qualification reports and dedication plans/reports will be prepared for each project.

4.1 Environmental Service Conditions

The following service conditions are defined:

- Operating time: continuous
- Temperature range: 40-104°F (note 1)
- Relative Humidity: 98% (non-condensing) maximum
- Radiation: 5E3 rad gamma

Notes:

1. The maximum temperature of 104°F is the maximum ambient temperature. The components are demonstrated to be acceptable for a total temperature of 121°F (104°F ambient + 17°F in-switchgear temperature rise).

The mild environment qualification is in accordance with IEEE 323-1974/1983 [2], IEEE C37.81-1989 [12], and IEEE C37.82-1987 [13].

Environmental qualification is performed on a plant specific basis, as required to meet the plant specifications.

4.2 Seismic Service Conditions

Seismic qualification of the components on the breaker is performed for each specific breaker configuration per the plant requirements. The seismic qualification includes the following:

- Seismic qualification is by testing in accordance with IEEE 344-1975/1987 [3], IEEE 323-1974/1983 [2], IEEE C37.81-1989 [9], and IEEE C37.82-1987 [10]. The test plan provides detailed acceptance criteria for the seismic testing.
- The test specimen includes the replacement breaker with the components installed.
- The TRS envelopes the plant specific RRS. The breaker is qualified to the amplified in-switchgear RRS.

The seismic service conditions are met by testing of the components on the breaker for each breaker configuration.

4.3 Electromagnetic Interference/Radio Frequency Interference (EMI/RFI)

EMI/RFI qualification testing was performed on the coils in accordance with EPRI TR-102323, revision 3, as documented in reference [23].

4.4 Voltage Range

Dedication/FAT testing is performed on 100% of the supplied breakers. The testing includes operation of the coils at the plant specific worst case degraded voltage conditions. This demonstrates proper operation for the plant specific requirements.

4.5 Infant Mortality of Electronic Components

NLI does not have information that the coils are burned-in at Schneider. A burn-in is not considered required as follows:

- The electrical circuit in the coils is a simple circuit.
- The coils are exercised during the dedication testing of the breakers.
- There have been no failures of the coils during the dedication testing.

There have been no coil failures reported to NLI from installed breakers.

4.6 Fault in Non Safety Plant System

The coils receive safety related control power, so it is electrically isolated from non-safety plant systems.

The EMI/RFI qualification [23] verifies that EMI/RFI emissions from non-safety plant equipment do not impact the operation of the coils.

Since the trip devices and coils are physically and electrically separated from non-safety related plant systems, faults in these systems will not impact these components.

4.7 Hardware/Software Faults

Hardware and software faults/failures are identified and evaluated as documented in this report. There are no unacceptable software/hardware faults identified.

4.8 Loss of Power

By design and construction, the coils are designed to be unpowered for an indefinite amount of time.

NLI testing verified that the coils operate properly following loss of power with no loss of programming. The following testing is performed:

- The supplied coils will have been unpowered from the time they were tested in the factory until tested by NLI. It is estimated that this is 1 month to 1 year. This will verify proper operation following an extended time unpowered.

4.9 Overcurrent Condition

The coils operate on the control voltage, which is protected from overcurrent conditions by fusing or circuit breakers, in accordance with plant design requirements.

5.0 FAILURE MODES AND EQUIPMENT RELIABILITY

5.1 Hardware Failure Modes and Effects Analysis (FMEA)

5.1.1 FMEA Methodology

Schneider performed detailed hardware FMEA's which were reviewed by NLI (Schneider document 51311620). A summary of the FMEA methodology is as follows:

- An external functional analysis was performed. This methodology shows the ties between the studied item and its environment in order to determine a failure relationship. The methodology used is M.I.S.M.E (method of systematic inventory of the surrounding environment). Note: This technique was used as part of the functional and safety requirements analysis performed by the European Organization for Nuclear Research for the CERN Safety Alarm Monitoring System.
- An internal functional analysis by functional block diagram was performed in accordance with MIL-HDBK-217F.
- A dysfunctional analysis was performed showing the consequences of a failure on the operability of the device.
- Reliability calculations were performed in accordance with MIL-HDBK-217F. The results are summarized in section 5.2 of this report.
- An A.M.D.E.C. quantified for a temperature of 40°C in a stationary environment. Note: AMDEC is a technique used for the development of products and processes in order to reduce the risk of failures and to document the actions undertaken. It is part of the QS 9000 'whole quality system' methodology.

5.1.2 Coil FMEA

The results of the Schneider FMEA for the coils is summarized as follows:

- Function of coil to actuate: The critical parts are the integrated circuit, regulator, comparator, transistors and varistors. The calculated reliability is presented in section 5.2.
- Function of energized coil to not inadvertently release (UV release and trip breaker): The critical parts are the transistors and regulator. The calculated reliability is presented in section 5.2.
- The microcontroller and the power supply are not identified as parts that limit the reliability of the coils.
- The reliability of the hardware is identified in section 5.2. The reliability of the hardware is based on the individual components. No especially sensitive components were identified.

NLI performed supplemental testing. Radiation exposure was used to disable the microcontroller. Note that this is a microcontroller hardware failure, not a firmware failure. The results were as follows:

- With the microcontroller disabled, the coils will not respond to the applied voltage and will spring return to the de-energized position:
 - UV coil:
 - If the coil is de-energized, it cannot be energized and the breaker cannot be closed.
 - If the coil is energized, it will spring return the plunger to the extended position and trip the breaker.
 - Shunt trip coil will not pick up.
 - Close coil will not close the breaker.
- This failure mechanism is equivalent to an electrical failure of the same components in the original breakers (spring return to the de-energized position). The microcontroller failure does not introduce an additional breaker failure mechanism.

As identified above, the Schneider FMEA identified that the microcontroller was not one of the components that limits the reliability of the circuit.

5.1.3 Conclusions

The Schneider/Square D FMEA's were performed in a rigorous manner and addresses the relevant potential failure modes.

The NLI testing did not identify any additional unacceptable failure modes.

No potential failure modes have been identified that have unacceptable consequences.

5.2 Hardware Reliability

A hardware reliability simulation was performed by Schneider in accordance with MIL-HDBK-217F. The calculated hardware failure rates are as follows:

- Failure rate at 105°C:
 - Coil does not energize: 4.61 E-6 h^{-1}
 - Coil inadvertently releases: 1.28 E-6 h^{-1}
- Failure rate at 40°C:
 - Coil does not energize: 1.27 E-6 h^{-1}
 - Coil inadvertently releases: 3.7 E-6 h^{-1}

The coils have a small number of components, a simple architectural design, and a small amount of microcode. The hardware failure rates of the coils are low.

5.3 Firmware Reliability

A software failure modes and effects analysis was not performed. NLI concludes that the firmware is highly reliable. No software flaws or software coding flaws have been identified. The following information is provided:

- A highly controlled process was used to develop and test the software and the software/hardware system (see the details in section 7.1 of this report).
- A highly controlled process is used during production of the coils. (see the details in section 7.1 of this report).
- Schneider emulation and black-box testing sufficiently verify compliance with design requirements.
- The operating history identifies a highly reliable design (see details in section 7.3 of this report).
- No firmware failures have been identified during NLI testing. No coils have been returned to NLI with failures due to the firmware.

5.4 System Failure Modes and Effects Analysis

A system level failure modes and effects analysis was performed for the application of the coils in reactor trip circuit breakers. In this configuration, the Masterpact circuit breaker contains a UV device, shunt trip device, and close coil.

5.4.1 Methodology

The following methodology is used:

- The effects of the coil failures are evaluated for the following two conditions:
 - The circuit breaker and plant are evaluated in the normal operating mode:
 - Plant is operating.
 - Breaker is closed with the UV energized and the shunt trip de-energized.
 - The circuit breaker is responding to a valid reactor trip signal.
- The output of the microcontroller performs the function of energizing/removing power from the transistors that power the activation and maintain coils. There are no other outputs of the microcontroller for this application. Therefore, non-mechanistic failures of the software will be postulated only based on their impact on the powering/removing power from the two transistors.
 - Since the transistors are on/off devices, no intermediate conditions will be evaluated.

5.4.2 Acceptance Criteria

The acceptance criteria is that the breaker opens and allows the reactor to trip. Inadvertent opening of the breaker and tripping of the reactor is not desirable, however, it is acceptable.

The following effect is not acceptable:

- The postulate failure mode prevents both the UV and shunt trip from opening the breaker.

A failure mode that prevents either the UV or shunt trip from opening the breaker (one or the other, but not both) is acceptable because the breaker will still open.

5.4.3 Failure Analysis-Normal Operation Conditions

The condition of the breaker and UV and shunt devices in this evaluation are as follows:

- The breaker is closed.
- UV configuration:
 - External relay contact is closed and supplying power to the UV.
 - Activation coil is de-energized.
 - Maintain coil is energized and the plunger is not extended.
- Shunt trip configuration: The contact external to the breaker is open and there is no power to the shunt trip.

The impacts of the failures are dispositioned as follows:

- “No impact”: This postulated failure causes the normal operation of the device.
- “Acceptable”: This postulated failure mode causes one of the following to occur:
 - An inadvertent trip of the breaker. This is acceptable per the plant design basis.
 - A failure of the specific device (UV or shunt trip) to operate. The other device (UV or shunt) performs the safety function of tripping the breaker.
- “Not acceptable”: This postulated failure mode prevents both the UV and shunt trip from opening the breaker.

Postulated Failure	Potential Impact on the UV	Potential Impact on the Shunt Trip
Power to the maintain coil transistor	Normal condition. No impact.	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
Temporary power to the activation coil transistor.	The UV device is already picked up and the maintain coil is energized. No impact.	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
Power maintained to the activation coil transistor for an extended duration.	The activation coil is not designed to be energized for an extended duration. The activation coil could burn out. One of two scenarios will occur: <ol style="list-style-type: none"> 1. The maintain coil will maintain the UV energized. No impact. 2. The activation coil will damage the maintain coil and the maintain coil will drop out. The spring return will trip the breaker. Acceptable. 	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
The activation coil transistor cycles on and off.	The activation coil is not designed to be energized for an extended duration. The activation coil could burn out. One of the following scenarios will occur: <ol style="list-style-type: none"> 1. The maintain coil will maintain the UV energized. No impact. 2. The activation coil will damage the maintain coil and the coil will drop out. The spring return will trip the breaker. Acceptable. 	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
The maintain coil transistor cycles on and off.	The coil will drop out and the spring return will trip the breaker. Acceptable.	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
Activation coil transistor is off.	The maintain coil is maintaining the UV in the picked up condition. No impact.	Contact external to the breaker is open. There is no power to the shunt trip. No impact.
Maintain coil transistor is off.	The coil will drop out and the spring return will trip the breaker. Acceptable.	Contact external to the breaker is open. There is no power to the shunt trip.

		No impact.
Activation and maintain coil are on simultaneously.	Activation coil could burn out as identified above.	Contact external to the breaker is open. There is no power to the shunt trip. No impact.

There are no postulated failure modes identified as “Not Acceptable”.

5.4.4 Failure Analysis-Reactor Trip Signal Initiated

The condition of the breaker and UV and shunt devices in this evaluation are as follows:

- The breaker is closed.
- UV configuration:
 - External relay contact is open. The power to the UV coil is removed.
- Shunt trip configuration: The contact external to the breaker is closed and there is power to the shunt trip. Note that the shunt trip function only requires the activation coil to be energized for a short duration to trip the breaker. Energization of the maintain coil is not required to perform the breaker trip function.

The impacts of the failures are dispositioned as follows:

- “No impact”: This postulated failure causes the normal operation of the device.
- “Acceptable”: This postulated failure mode causes one of the following to occur:
 - An inadvertent trip of the breaker. This is acceptable per the plant design basis.
 - A failure of the specific device (UV or shunt trip) to operate. The other device (UV or shunt) performs the safety function of tripping the breaker.
- “Not acceptable”: This postulated failure mode prevents both the UV and shunt trip from opening the breaker.

Postulated Failure	Potential Impact on the UV	Potential Impact on the Shunt Trip
Power to the maintain coil transistor	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The breaker has already tripped due to energization of the activation coil. No impact.
Temporary power to the activation coil transistor.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	Power to the activation coil performs the safety function of tripping the breaker. No impact.
Power maintained to the activation coil transistor for an	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the	The initial power to the activation coil performs the safety function of tripping the breaker. Power to the

extended duration.	breaker. No impact.	activation coil for extended duration may damage the coil, however, the safety function will already be completed. No impact.
The activation coil transistor cycles on and off.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The initial power to the activation coil performs the safety function of tripping the breaker. Cycling the activation coil for extended duration may damage the coil, however, the safety function will already be completed. No impact.
The maintain coil transistor cycles on and off.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The initial power to the activation coil performs the safety function of tripping the breaker. Power to the maintain coil is not required for tripping the breaker. No impact.
Activation coil transistor is off.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The shunt trip will not energize and will not trip the breaker. The UV will trip the breaker. Acceptable.
Maintain coil transistor is off.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The initial power to the activation coil performs the safety function of tripping the breaker. Power to the maintain coil is not required for tripping the breaker. No impact.
Activation and maintain coil are on simultaneously.	Contact external to the breaker is open. There is no power to the UV. The spring return will trip the breaker. No impact.	The initial power to the activation coil performs the safety function of tripping the breaker. If the activation coil is on for an extended duration, it may be damaged, however, the safety function will already be completed. No impact.

There are no postulated failure modes identified as "Not Acceptable".

6.0 REQUIRED SYSTEM CHARACTERISTICS

6.1 Verification of Required System Characteristics

The required system characteristics that the hardware/software systems must possess are identified in Table 6.1. The following information is presented for each critical characteristic:

- Acceptance criteria.
- Results of the V&V activities.
- Reference documents.

Section 7 of this report provides the details on the activities that were performed to verify that the coils possess the required attributes.

COIL SOFTWARE V&V CRITICAL CHARACTERISTICS
TABLE 6.1

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
<u>Quality Assurance Program</u> Quality Assurance Program that controlled the development of the software/hardware.	The software and hardware were developed under the controls of the Schneider ISO 9001-2000 quality program.	Verified during the audit of Schneider/Square D. See the summary in section 7.0 of this report. Acceptable.	This report.
Industry standards used to control the development and testing of the software.	The software is developed and tested in accordance with industry recognized codes and standards.	Verified during the audit of Schneider/Square D. See the summary in section 7.0 of this report. Acceptable.	This report.
<u>Software Lifecycle</u> Software specification/software requirements.	Software specification documents the detailed software requirements.	Verified during the audit of Schneider/Square D. See the summary in section 7.0 of this report. Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Procedural controls used during software development.	Software development controlled by Schneider procedures. Document the procedures used and evaluate process.	Verified during the audit of Schneider/Square D. See the summary in section 7.0 of this report. See section 7.0 for the data on the coils. Acceptable.	This report.
Failure Modes & Effects Analysis	Failure Modes & Effects Analysis performed and used during software development.	Verified during the audit of Schneider and review of the hardware FMEA by NLI. NLI performed supplemental FMEA analysis. See details in section 5.0 of this report. Acceptable.	This report.
Development and testing approach.	Schneider developed and tested the software in small function based blocks of code. Development and testing documented.	See the summary in sections 2.2 of this report. Acceptable.	This report.
Independence of software development and testing.	Independent personnel used.	See the summary in section 7.0 of this report. Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Integrated hardware/software testing.	Integrated testing of the hardware/software system was performed.	See the summary of Schneider activities in sections 7.0 of this report. NLI performs dedication testing on 100% of the supplied equipment (see section 7.2 of this report). Acceptable.	This report. (project specific dedication plan)
Product operating history.	Installed units operating properly. Specify number of operating units, time in service, and number and types of identified problems.	See the summary in section 7.3 of this report. Acceptable.	This report.
Error handling.	<ol style="list-style-type: none">1. Code errors are identified, documented, evaluated, and reported in a controlled manner by Schneider.2. Mechanism for reporting and evaluating user reported problems.	The audit of Schneider verified a controlled program to identify, evaluate, and report errors and changes. NLI configuration control activities meet the requirements for safety related equipment. See the details in Section 8.0 of this report. Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Problem reporting to plant.	Identified problems are evaluated and reported to the client.	<p>The audit of Schneider verified a controlled program to identify, evaluate, and report errors and changes.</p> <p>NLI configuration control activities meet the requirements for safety related equipment.</p> <p>See the details in Section 8.0 of this report.</p> <p>Acceptable.</p>	This report.
Software updates and service bulletins.	Schneider has a formal process to alert customers concerning software updates and provides service bulletins.	<p>The audit of Schneider verified a controlled program to identify, evaluate, and report errors and changes.</p> <p>Section 8.0 of this plan identifies the Schneider and NLI actions.</p> <p>Acceptable.</p>	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
<u>Configuration Control</u>			
Revision control.	Revision control used on code, chips, and boards.	The audit of Schneider verified a controlled program for revision control. NLI configuration control activities meet the requirements for safety related equipment. See the details in Section 8.0 of this report. Acceptable.	This report.
Hardware configuration.	Hardware per Schneider and NLI design documentation and drawings.	The audit of Schneider verified the required production controls. NLI dedication testing verifies proper operation and configuration. Acceptable.	This report. (Project specific dedication plan)

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Electrical interfaces including wire, terminations, and grounding.	Per Schneider/Square D and NLI design drawings.	The audit of Schneider verified the required production controls.	This report.
		NLI dedication testing verifies proper operation and configuration.	(Project specific dedication plan)
		Acceptable.	
Manufacturing controls of code.	Controls to assure correct code installed on each unit. Traceability between development and production code is documented.	The audit of Schneider verified proper revision control. See sections 7.0 of this report for a summary of the production controls.	This report.
		NLI configuration control activities are per section 8.0 of this report.	
		Acceptable.	
Regression testing or evaluations.	Regression testing or evaluations performed when code is revised.	The audit of Schneider documented that regression testing has not been required since there have been no changes to the code.	This report.
		NLI dedication testing of replacement parts will document compatibility with the original configuration.	Dedication plan for each project.
		Acceptable.	

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
<u>Software/Hardware Critical Characteristics</u>			
Data storage.	Per Schneider design specifications.	See the data in section 2.2.4 Acceptable.	This report.
Signal conditioning and logic functions	Per Schneider design specifications.	See the data in section 2.2.4. Acceptable.	This report.
System response time.	Per Schneider design specifications.	See the data in section 2.2.4. Acceptable.	This report.
Remote alarms and indications.	None used in the safety related configuration.	None. The communications features are not connected in the safety related configuration. Acceptable.	This report.
Watchdog timer.	Per Schneider design.	Timeout watchdog during the main loop program operation. See section 2.2.4 of this report. Acceptable.	This report.
Timing and clock control.	Per Schneider design.	See the data in section 2.2.4. Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Output alarms.	None used in the safety related configuration.	None. The communications features are not connected in the safety related configuration. Acceptable.	This report.
Features which could impact operation.	No features which could interrupt operation (interruptions, diagnostics, manual inputs, non-essential application programs, unauthorized programs or data modifications).	The audit of Schneider, review of Schneider documents and NLI testing did not identify any features that could interrupt operation. Acceptable.	This report.
Cyber Security.	The firmware is coded on the microcontroller and cannot be field modified.	The firmware is coded on the microcontroller and cannot be field modified (see section 2.4). Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Processor restart and initialization.	Following removal of power, the microcontroller maintains the code.	<p>By design and Schneider testing, hard coding is used. The initialization sequence verifies hardware and firmware operation (see section 2.2.4 of this report).</p> <p>NLI dedication testing verifies proper operation following extended duration with no power.</p> <p>Acceptable.</p>	This report.
Data validity checks.	Per Schneider design documents.	<ul style="list-style-type: none">• There are no input range checking provisions or data validity checks during operation. They are not required due to the deterministic operation.• The microcontroller initialization sequence verifies that there no hardware or firmware problems.• There are no intermediate results. <p>Acceptable.</p>	This report.
User configurable input values.	There are no user configurable input values.	<p>There are no user configurable input values (see section 2.2.4 of this report).</p> <p>Acceptable.</p>	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Loss of input instruments.	There are no input instruments.	There are no input instruments (see section 2.2.4 of this report). Acceptable.	This report.
Diagnostics.	Not applicable. The programming is deterministic and diagnostics are not required.	Not applicable (see section 2.2.4 of this report).	This report.
Coils operation on Masterpact NT and NW breakers across voltage range.	Coils mount and interfaces properly with the Masterpact NT and NW breakers, including physical mounting, wiring, and latch interface.	Dedication testing by NLI on 100% of the supplied breakers verifies proper operation. Testing is performed across the plant specific control voltage range (see section 7.2.2 of this report). Acceptable.	This report. (Project specific dedication plan).
Coil settings.	There are no coil settings.	Not applicable (see sections 1.1 and 2.5 of this report). Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
No spurious tripping.	There is no spurious operation of the coils (energization or de-energization as applicable).	No spurious operation has been documented by Schneider or during NLI testing. EMI/RFI testing identified no spurious operation. The Schneider FMEA addressed the hardware failure rate for spurious operation. Highly reliable device (see section 5.0). Acceptable.	This report.
Non safety functions do not interfere with safety related trip function.	Connection of the communication features is not a safety related configuration.	Not applicable (see section 1.2 of this report). Acceptable.	This report.
Position upon loss of control power.	Per Schneider design documents.	Spring return of the plunger retracted (shunt trip and close coils) or plunger extended (UV) verified during NLI dedication testing. See section 7.2.2 of this report. Acceptable.	This report.

<u>Critical Characteristic</u>	<u>Acceptance Criteria</u>	<u>Results</u>	<u>Reference</u>
Battery function.	No batteries are used.	There is no battery installed (see section 2.2.4 of this report). Acceptable.	This report.
Coil performance upon loss of microcontroller.	Per Schneider design documents.	The coil returns to the spring return position. Per the Schneider FMEA, microcontroller failure is not a significant reliability issue (see section 5.0). Acceptable.	This report.
<u>Human Interface Critical Characteristics</u>	There are no human-machine interfaces for the coils.	Not applicable (see section 2.2.4 of this report).	This report.

Critical Characteristic

Acceptance Criteria

Results

Reference

ACE's Critical Characteristics

The following ACE's are identified:

- Environmental service conditions.
- Seismic service conditions.
- EMI/RFI.
- Voltage range (undervoltage to overvoltage).
- Infant mortality of electronics.
- Fault in non-safety plant system.
- Hardware/software faults.
- Loss of power.

Components operate properly when exposed to the identified ACE's.

NLI testing and analysis.

The evaluation of each ACE is documented in section 4.0 of this report.

Acceptable.

Section 4.0 of this report.

6.2 Separation Criteria

The following information on the Masterpact shunt trip, close coil, and UV trip that is related to separation criteria is presented:

- The coils are self-contained on each circuit breaker. They are located within the switchgear cubicle for each breaker, as are the currently installed devices. Installation of the replacement breaker with the coils installed does not change the physical location or separation of the breakers or the coils.
- The electrical interfaces to and from the coils are fully contained on each breaker.
 - Each coil in a breaker is electrically and physically independent.
 - The coils are powered from external control power.
 - The coils receive their signals from the plant logic outside the switchgear.
 - The output of the coils is a mechanical function (plunger actuation). There is no electrical or digital output.
 - In the qualified configuration, the coils do not communicate with any other devices in the plant.
 - The electrical interfaces of the coils are the same as the currently installed coils.

Installation of the Masterpact coils maintain the same level of physical and electrical separation as the existing coils on the low voltage switchgear breakers.

6.3 Common Mode Failure Evaluation

The following activities were performed by Schneider/Square D and NLI to verify that the components operate as intended:

- The equipment architecture is robust by design and manufacture.
- The components use simple microcontroller architecture. It is deterministic with all commands executed sequentially in every cycle without interrupts.
- By design, the number of components was minimized. This resulted in a highly reliable system with a very low failure rate.
- With an installed base of over 100,000 coils, there have been no reported firmware related failures. The firmware has not been revised since 2002.
- The component's design and development was performed in a rigorous manner and is well documented.
- Rigorous production controls are used by Schneider/Square D to assure that 100% of the supplied coils meet the design requirements.
- Extensive production testing is performed, including the following:
 - Schneider tests the supplied coils.
 - NLI performs dedication testing on 100% of the supplied breakers, with the coils installed, as applicable.
- Detailed quality assurance/quality control processes and procedures are implemented throughout the lifecycle of the coils, by both Schneider/Square D and NLI.
 - Activities performed by Schneider/Square D are controlled by their ISO 9001 quality assurance program. Based on the NLI audit, Schneider/Square D has a

- comprehensive program for the control of the coil design, development, testing, and manufacture.
- Activities performed by NLI are performed under the controls of the NLI Nuclear Quality Assurance Program.
 - The applicable ACE's have been identified and addressed by testing or analysis. Based on these activities, no ACE's have been identified that would prevent operation of the devices.
 - Each coil is electrically and physically isolated from the other coils on the breaker and in the plant. The different coils in the breaker (UV, shunt, close) are electrically isolated from each other.
 - Known ACE's have been identified and addressed by testing or analysis.
 - There are no identified single events that could cause failure of multiple coils.

Based on the extensive design, development and testing performed by Schneider/Square D and NLI and the equipment configuration in the nuclear plant, common mode failure of the coils is highly unlikely.

7.0 IMPLEMENTATION OF REQUIRED CHARACTERISTICS

The activities identified in this section are performed to verify that the components possess the required characteristics identified in section Table 6.1.

7.1 Commercial Grade Audit of Square D/Schneider

In December 2008, an audit was performed of the Schneider facility in France involved in the design, manufacture and testing of the coils. Additional data was collected electronically from Schneider in January and February 2009. Previous audits were performed on the Micrologic trip device, which is not addressed in this report.

The audit verified implementation of the critical characteristics specified in Table 6.1. The audit demonstrated that the Schneider technical, management, and quality assurance program controlled the applicable critical characteristics as identified in Table 6.1.

7.1.1 Summary of Audited Facilities

The firmware was developed by Square D/Schneider under the controls of their commercial ISO 9001-2000 quality assurance program. NLI performed commercial grade audits of the Schneider design and manufacturing facility. The following Schneider/Square D facilities are involved in the design and manufacture of the components and breakers:

- Schneider facilities in France that were audited by NLI:
 - Grenoble, France: Equipment design and engineering.
 - Moirans, France: Manufacture, assembly and testing of the Masterpact breaker modules. The Masterpact breaker is a modular breaker with bolts and screws used to assemble the modules. The various modules include the 3 contact modules, mechanism module, etc. All of the modules are manufactured and tested in fixtures at the Schneider facility in Moirans, France.
- The Square D Services in West Chester, Ohio was audited. This facility receives the assembled and tested Masterpact breakers and assembles them into the replacement breakers with carriages.
- The Square D assembly facility in Columbia, SC was not audited. Some of the Masterpact modules are assembled and tested in this facility. An audit of this facility is not required for the V&V based on the following:
 - No design or manufacturing of the components occurs in this facility. The coils are modules that are attached to the breaker.
 - NLI dedication/FAT testing is performed on 100% of the supplied breakers and confirms that the coils operate per design.

7.1.2 Summary of Audit Activities

The following activities were performed during the audit:

1. Review of the procedures that control the design, testing, and manufacture of the coils.
2. Reviews of the equipment design documents with the Schneider's design team and quality assurance representatives, inspection of test facilities, verification of measurement and test equipment calibration, reviews of equipment design methodology, development documentation, control and testing requirements, and analysis of test results and documentation at Schneider Electric's design and testing facilities in Grenoble, France. Additional information was collected during teleconference calls.
3. Interviews with production and quality control personnel, inspection of circuit breaker production, testing, and packaging operations, analysis of receipt, in-process and post-production inspection and test methods, test equipment certification, and documentation of test results at Schneider Electric's production facilities in Moirans, France.
4. Review of the 8 coil code modules and coders notes with the design specification.
5. Additional information was transmitted electronically to NLI, to support the V&V activities.

7.1.3 Design and Development Controls

A summary of the design and development controls used by Schneider for the Micrologic equipment is presented:

- The equipment design team management and quality assurance activities comply with the intent, where applicable, of the following IEC documents: 1131-1-1992; 1131-2-1992; 1131-3-1992; and 1131-4-1995 for microcontrollers, which correlate, where applicable, to the requirements of IEEE Standards 830-93, 603-91, 828-90, 1042-87, 1008-87, and 1042-87. The titles and content follow European format and in some cases requirements are combined in a single document.
- During prototype coding, the designer performed simulations. All integrated testing was performed by second party or peer reviewers. This approach is consistent with the intent of IEEE Standards 1008-1987 and 829-1983.

The following Schneider/Square D controlling procedures were used to control the design process:

- *Software Quality Assurance.*
- *Requirements Definition.*
- *Subcontracting Design Requirements.*
- *Validation of Technical or Design Requirements.*
- *Project Startup and Progress Tracking (Form).*
- *Software Quality Assurance.*
- *Qualification of Products and Systems.*
- *Storage and Distribution of Quality Document.*
- *Software Quality Reviews.*

These procedures were reviewed by NLI. They provide a high level of control over the software design, testing, and quality assurance functions.

7.1.4 Production Controls and Testing

The following summary of the production controls used during the manufacture and testing of the equipment is presented:

- After production release, engineering oversight was transferred to the sustaining/product improvement organization.
 - This transfer of responsibility was accomplished in accordance with procedure *Transfer of Technical Management after Product Release*.
 - Activities after product release are performed in accordance with procedure *Project Activities after Product Release*.
- The following Schneider/Square D procedures control the production processes:
 - The requirements for procurement are identified in procedure *Purchasing of Inventory Items*. Items are purchased from two levels of approved suppliers. Certified supplier's products are accepted without additional testing based upon a defined grading system. Products from uncertified suppliers are subject to acceptance testing, which are performed in accordance with documented plans. Incoming certified products are differentiated from non-certified products by a two-alpha prefix on the item's part number.
 - Production planning and control is accomplished in accordance with the following procedures:
 - *Design Review and Production Startup (Form)*.
 - *Production Planning*.
 - *Modification of Production Plans*.
 - *Distribution and Modification of the Production Plan*.

A high level of control and quality is maintained by Schneider/Square D throughout the production process.

These procedures were reviewed by NLI. The production testing performed by Schneider provides a very high level of confidence that the supplied coils are in accordance with the design documents.

7.1.5 Product Support

The long term product support that will be provided by NLI and Schneider is summarized in section 8.0 of this report.

7.1.6 Audit Documents

Extracts of the design, testing, and production documents have been obtained and are in NLI's possession. Complete versions of the design documents are available for review at the Square D facility in Cedar Rapids, IA. Test plans and reports, quality manuals and procedures, and implementation methods and techniques, and production and testing documentation are available at NLI's facility in Fort Worth, TX.

The Schneider documents which were made available to NLI are maintained in accordance with the NLI Quality Assurance Program. Some Schneider documents are proprietary to Schneider and were reviewed during the audit but will not be released to NLI.

7.1.7 Coil Specific Documentation

The following specifications and procedures are applicable to the coils. These documents were reviewed and the applicable information was extracted and included in this report.

- **Technical Design Requirements:** multi-part specification document # 5100512854, Revision B, *PROXIMA Auxiliary Design File Parts 1/7 – 7/7 Technical Specifications; Control Electronics; Activation Conditions; Inhibition Conditions; Input Circuit; Regulator and Reset Generator; 10V Vin Power Supply; and Choice of Electronic Board Components.*
- **PROXIMA Auxiliaries Relay Software Specification:** Schneider Electric document 5100512993, Revision B, Description of PROXIMA Auxiliary Software (English Translation), dated 12/12/2005.
- **Coding Specification:** Schneider Electric document 5100511735, Revision 4, Manual for the Development of Program Code, dated 9/14/2001.
- **Acceptance Test Requirements:** Schneider Electric documents GHD1219700, Revision C, *Auxiliaries MN (includes Navy)*; GHD12220000, Revision C, *Auxiliaries MX/XF*; GHD1219800, Revision C, *Auxiliaries MX/XF (Navy)*, and 5100561500, Revision A1, *Functional Test Specification for MN-MX-XF PROXIMA Auxiliaries.*
 - a. The Schneider methodology for documenting the satisfactory completion of an acceptance test is the release of the product version with Form PRC 703-1c. The form for the release of the firmware design documented in SE specification 5100512993, Revision B. The form was reviewed by NLI during the NLI Software V&V of Schneider Electric. This document was not released to NLI.
- **FEMA Documents:** Schneider Electric document 51311620, Revision B, Study of Reliable Function of PROXIMA Auxiliaries, dated 1/20/2003 (references MIL-HDBK-217) – firmware not considered.

These documents control the design, coding, acceptance testing and FMEA for the coils. The NLI review identified that they provide a high level of control for the required activities.

7.1.8 Product Error Reporting

The Schneider error reporting controls are identified in section 8.1 of this report.

7.2 NLI Testing

Testing and analysis is performed by NLI to fully document the V&V of the components. The testing and analysis address the critical characteristics identified in Table 6.1, as applicable.

7.2.1 Qualification Testing

Qualification testing and analysis will be performed in accordance with the requirements for each utility. The testing will be performed on a single test specimen which is the same configuration as the production units which are being delivered. This testing will include the following:

- EMI/RFI testing.
- Seismic testing.
- Mild environment analysis.

Sections 4.1-4.3 provide details on the qualification testing.

The qualification reports are separate documents.

7.2.2 Dedication Testing/Factory Acceptance Testing (FAT)

The dedication testing includes testing across the plant specific control voltage range, including undervoltage and overvoltage conditions. This testing is performed on 100% of the supplied circuit breakers.

7.2.3 Validation Testing

Based on the information supplied by Schneider, it was determined that no additional validation testing was required for the coils.

7.3 Operating History

The following information was provided by Square D/Schneider. This information is applicable to the current revision of the coil firmware.

- There have been no revisions to either the code or the hardware since the production release in 2002.
- Schneider has been shipping the same version since 2002. To date, none have been recalled. No firmware failures have been identified.
- Approximately 100,000 units have been sold in the past 2 years.
- No outstanding, uncorrected firmware errors exist at this time.

- Presently, no microcode revisions are planned.
- Schneider intends to support this product for the foreseeable future.

NLI dedication tests 100% of the coils across the plant specified control voltage. Approximately 240 circuit breakers with coils have been supplied by NLI (combination of safety and non-safety related). There have been no coil failures during dedication. NLI has no coils returned due to field failures.

The large installed base with no reported software problems and no software revisions indicates a high level of equipment reliability.

No hardware modifications have been made to the coils since they were released in 2002. No hardware issues have been identified by NLI or Square D. No coils have failed NLI dedication testing (100% sample size) and no coils have been returned from the client due to failures in the field. No nuclear plant operating experience issues (OE's) have been identified for the coils.

7.4 Users Manuals

The Schneider/Square Users Manuals have been reviewed by NLI. The manuals are accurate and provided the required level of detail.

NLI prepares Users Manuals for the supplied equipment. The NLI Users Manuals address the plant specific requirements and nuclear industry specific issues. The NLI Users Manuals include copies of the applicable Schneider/Square D manuals.

8.0 CONFIGURATION MANAGEMENT PLAN

8.1 Schneider Firmware Configuration Control and Error Reporting

The activities summarized below are performed by Schneider for the long term support of the Micrologic coils.

- Configuration management requirements are documented in Schneider Electric controlled procedures. The configuration management activities comply, as applicable, with the intent of IEC 1131-1-1992, IEC 1131-4-1995, and IEEE Std. 1042-1987.
- Management, resolution, and communication of customer reported defects are controlled in accordance with the following Schneider/Square D procedures:
 - *Managing Customer Complaints.*
 - *Managing Customer Returns.*
 - *Communication of Product Defects.*
- Upon receipt, a customer complaint is documented in a worldwide product quality database (*Product quality database (LV InSchneider area)*). Locally developed decisions are reviewed and validated at Schneider Electric corporate design and quality assurance. Solutions outside of local capabilities are submitted to Schneider Electric corporate for resolution. Once a solution is implemented and verified, the defect and its resolution are made available to all Schneider Electric service centers for distribution.
- Schneider's corrective action complies with the requirements of ISO 9002-1994 and 9001-2000.
- The mechanism used to implement the customer feedback process is for customer reported errors to be processed and resolved in the USA through the Square D customer service program, which receives updates from the world wide Schneider Electronics network.
- Code revisions: No changes to the code are planned. If revisions are made, the configuration control activities would be as specified above.
- The metrics that are used for product trends are field failure ranked for the following:
 - Hardware.
 - Software.
 - Electrical.
 - Display.

NLI reviewed the Schneider procedures and implementation. They provide a high level of control over the identified activities.

8.2 NLI Configuration Control

The following process is used by NLI to identify, document, evaluate, and report firmware modifications and errors:

- NLI contacts Schneider every year and any modifications or reported errors will be identified.
- Errors will be documented and evaluated in accordance with the NLI Nonconformance Report (NCR) process [20]. Notification in accordance with 10CFR21 will be made in accordance with NLI procedures [20], if required.
- Design changes which are not the result of errors will be evaluated by NLI for impact on the existing system and future replacement.
- NLI will submit all NCR's and 10CFR21 reports associated with the hardware and software to the client. Evaluation of design changes will also be submitted.

This approach is based on the following:

- The Schneider audits and the NLI testing will verify the as-supplied configuration.
- Schneider will not make the source codes available to NLI. Schneider will not freeze the hardware or software configuration.
- Schneider has a controlled program for the following activities :
 - Document revisions to hardware and software.
 - Perform regression testing and/or analysis to fully evaluate the impact of the hardware and software changes on the system. The test method and results are documented in an auditable form.

8.3 Plant Lifetime Configuration Control

There are no plant lifetime configuration control requirements for the coils. The coils are factory programmed and are not field configurable. There are no electronic or switch setting on the devices.

9.0 QUALITY ASSURANCE

Project activities were performed in accordance with the NLI Quality Assurance Program which meets the requirements of 10CFR50 Appendix B, 10CFR21 and ASME NQA-1 [16].

10.0 MEASUREMENT & TEST EQUIPMENT

Measurement & Test Equipment used by NLI during testing is controlled by the NLI M&TE program (procedure NLI-QUAL-05, latest revision). The NLI test data sheets document the M&TE that is used during the testing. The calibration of M&TE is traceable to NIST or equivalent standards.

11.0 REFERENCES

Note: (project specific) indicates NLI documents that are developed for each specific breaker supply project.

Industry/Regulatory Documents

1. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
2. IEEE 323-1974/1983, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
3. IEEE 344-1975/1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
4. EPRI TR-102348, "Guidelines for Licensing of Digital Upgrades", 12/1993.
5. EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", Final report, October 1996.
6. EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," revision 3.
7. IEEE 1012-1986, "Standard for Software Verification and Validation Plans."
8. EPRI 5652, "Guidelines for the Utilization of Commercial Grade Items in Nuclear Safety-Related Applications."
9. IEEE C37.81-1989, "IEEE Guide for Seismic Qualification of Class 1E Metal-Enclosed Power Switchgear Assemblies".
10. IEEE C37.82-1987, "IEEE Standard for the Qualification of Switchgear Assemblies for Class 1E Applications in Nuclear Power Generating Stations".
11. IEEE 384-1977/1981/1992, "Criteria for Separation of Class 1E Equipment and Circuits".
12. NRC R.G. 1.75, "Physical Independence of Electrical Systems".
13. NRC R.G. 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants".
14. NRC R.G. 1.100, "Seismic Qualification of Class 1E Equipment for Nuclear Power Plants".
15. IEEE C37.59-2002, "IEEE Standard for Conversion of Power Switchgear Equipment".

NLI and Schneider/Square D Documents

16. NLI Quality Assurance Manual, Rev. 8, 12/14/07.
17. NLI design drawings (project specific).
18. NLI dedication plan with dedication test data (project specific).
19. NLI Instruction Manual (project specific).
20. NLI Procedure NLI-QUAL-08, "Nonconformances and 10CFR21 Reporting," (latest revision).
21. NLI EMI/RFI plan and report (project specific).
22. Seismic plan and report (project specific).
23. NLI report QR-042181-5, "EMI/RFI Qualification Report for Masterpact Circuit Breaker Shunt Trip and Undervoltage Trip", (latest revision).

ATTACHMENT A

LIST OF APPLICABLE SCHNEIDER DOCUMENTS

The Schneider documents are proprietary. Some of these documents are available at the NLI facility for review. The remainder were reviewed by the NLI auditor at the Schneider/Square D facility.

<u>Document #</u>	<u>Title</u>
MQ MDE-E Rev. A	Group Schneider QA Manual
No Document #	Grenoble ISO 9001-2000 ISO Certification for Design and Testing
PAQ 00 H 01 1	AFI Moirans QA Manual
No Document #	Moirans ISO 9001-2001 and ISO 14001-1996 Certificates
PAQ 02 H06 0 00 B	AFI Moirans Receipt Inspection Procedure
No Document #	Montmelian QA Manual, Revision B
No Document #	Montmelian ISO 9001-2001 and ISO14001 -1996 Certificates
Procedure 07, Rev. D	Group Schneider Requirements Definition
Procedure 09, Rev. C	Group Schneider Subcontracting Design Requirements
Procedure 13, Rev. D	Group Schneider Validation of Technical or Design Requirements
Procedure 15, Rev. E	Group Schneider Managing Customer Complaints
Procedure 16, Rev. C	Group Schneider Managing Equipment Returns
Procedure 17, Rev. D	Group Schneider Communication of Product Defects
Procedure 18, Rev. A	Group Schneider Corrective and Preventative Actions
Form PRC 703-1c	Group Schneider Design Review and Production Startup Form
Procedure PAEL-G01	Group Schneider Software Quality Assurance
Procedure PCO-01, Rev. F	Group Schneider Technical and Manufacturing Development Processes
Procedure PCO-03, Rev. B	Group Schneider Purchasing of Inventory Items
Procedure PCO-09, Rev. G	Group Schneider Qualification of Products and Systems
Procedure PCO-10, Rev. D	Group Schneider Project Activities after Product Release
Procedure PCO-11, Rev. E	Group Schneider Transfer of Technical Management after Product Release
Procedure PCO-13, Rev. F	Group Schneider Management of M&TE
Procedure PCO-15, Rev. D	Group Schneider Product Protection Checklist
Procedure PCO-16, Rev. C	Group Schneider Production Planning
Procedure PCO-17, Rev. C	Group Schneider Distribution and Modification of the Production Plan
Procedure PCO-18, Rev. C	Group Schneider Modification of Production Plans
Procedure PCO-19, Rev. D	Record of Proving Test Storage and Distribution of Quality Documents
Procedure PAEL-G01	Group Schneider Software Quality Assurance (Extract)
Spec. 5100512854, rev B	PROXIMA Auxiliary Design File (technical design requirements)
Spec. 5100512993, rev B	PROXIMA Auxiliaries Relay Software Specification
Spec. 5100511735, rev 4	Manual for Development of Program Code (coding specification).

Spec. 5100561500, rev A1 Functional Test Specification for PROXIMA Auxiliaries (acceptance test requirements).

Spec. 51311620, rev B Study of Reliability Function of PROXIMA Auxiliaries (FMEA)

No Document # Group Schneider Index of Activity and Process Instructions and Procedures

UL and ANSI Certification Test Report for Masterpact NW NW08H1

UL and ANSI Certification Test Report for Masterpact NW NW08H2

UL and ANSI Certification Test Report for Masterpact NW NW08L1

UL and ANSI Certification Test Report for Masterpact NW NW08N1

UL and ANSI Certification Test Report for Masterpact NW NW16H1

UL and ANSI Certification Test Report for Masterpact NW NW16H2

UL and ANSI Certification Test Report for Masterpact NW NW16L1

UL and ANSI Certification Test Report for Masterpact NW NW16N1

UL and ANSI Certification Test Report for Masterpact NW NW20H1

UL and ANSI Certification Test Report for Masterpact NW NW20H2

UL and ANSI Certification Test Report for Masterpact NW NW20L1

UL and ANSI Certification Test Report for Masterpact NW NW32H1

UL and ANSI Certification Test Report for Masterpact NW NW32H2

UL and ANSI Certification Test Report for Masterpact NW NW32L1

UL and ANSI Certification Test Report for Masterpact NW NW40H2

UL and ANSI Certification Test Report for Masterpact NW NW40L1

UL and ANSI Certification Test Report for Masterpact NW NW50H2

UL and ANSI Certification Test Report for Masterpact NW NW50L1

ANSI C37_90_Test Report Electromagnetic Compatibility

Schneider Electric Response to NLI Questions (MS PowerPoint)