NUCLEAR LOGISTICS INC

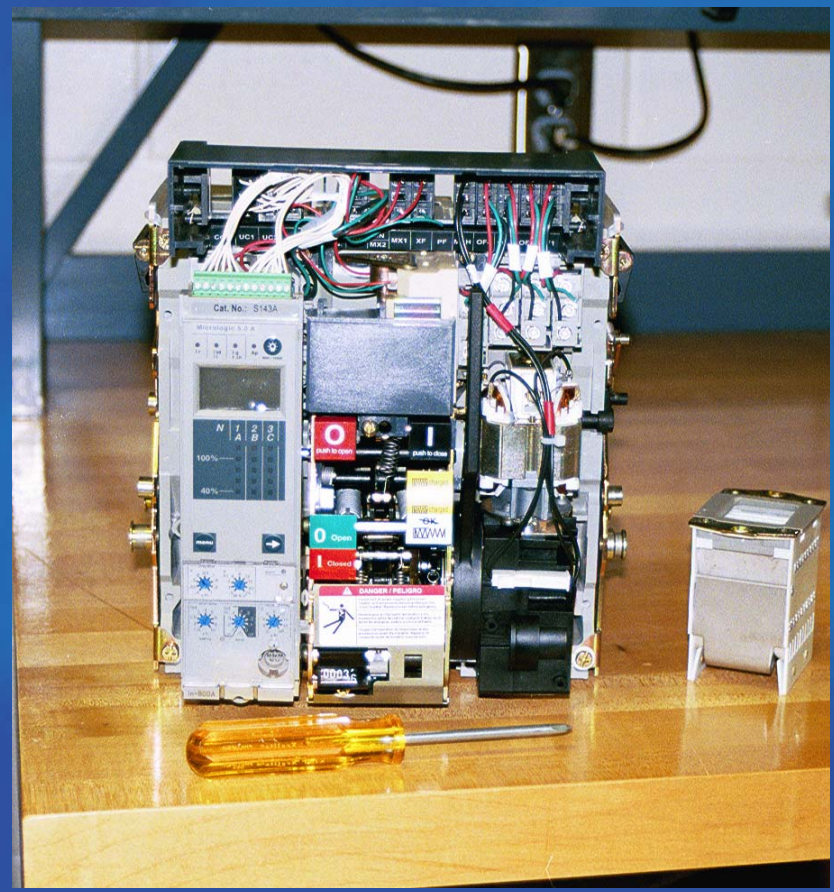
Qualification of Digital Trip Unit

PRESENTED BY:
Craig S. Irish
VP, Sales & Marketing

Digital Trip Unit

NLI
NUCLEAR LOGISTICS INC

Equipment Identification: Digital trip unit on the Square-D Masterpact low voltage (LV) switchgear circuit breaker. The breaker, with trip unit, is a direct replacement for existing LV switchgear breakers.



Safety Function of Digital Trip Unit

NUCLEAR LOGISTICS INC

- The safety function of the trip units are:
  - Maintain low voltage power circuits during normal conditions, including no spurious tripping.
  - Interrupt low voltage circuits in overcurrent conditions.
  - The non-safety related features (display, communications, etc.) cannot interfere with the proper operation of the trip unit.

Verification and Validation

NUCLEAR LOGISTICS INC

- **Verification & Validation** [IEEE 7-4.3.2 and EPRI TR-102348 revision 1] : The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specific requirements.
- All activities associated with upgrading digital equipment including seismic testing, environmental analysis, EMI/RFI testing, software assurance, FMEA, dedication, etc. are considered Verification and Validation for digital equipment.

Required Standards

NUCLEAR LOGISTICS INC

- **The primary documents for the upgrade of commercial grade digital equipment are:**
  - IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
  - EPRI TR-102348 (NEI 01-01), "Guidelines for Licensing of Digital Upgrades", revision 1.
  - EPRI TR-106439, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications".
  - ASME NQA-2a-1990, Part 2.7
  - NRC Regulatory Issue Summary 2002-22

Additional Standards

NUCLEAR LOGISTICS INC

- **The following documents are typically applicable or partially applicable to commercial grade digital equipment upgrade projects:**
  - IEEE 323-1974/1983, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”
  - IEEE 344-1975/1987, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations."
  - IEEE 730-1989, “Software Quality Assurance Plans.”
  - IEEE 1012-1986, “Standard for Software Verification and Validation Plans.”
  - IEEE 1028-1988, “IEEE Standard for Software Review and Audits.”
  - IEEE 828-1990, “IEEE Standard for Software Configuration Management”.
  - IEEE 829-1990, “IEEE Standard for Software Test Documentation”.
  - IEEE 830-1984, “IEEE Standard Guide for Software Requirements Specification”.
  - IEEE 1008-1987, “IEEE Standard for Software Unit Testing”.

Additional Standards

NUCLEAR LOGISTICS INC

- IEEE 1016-1987, “IEEE Recommended Practice for Software Design Descriptions”.
- IEEE 1063-1987, “IEEE Standard for Software User Documentation”.
- IEEE 1074-1995, “IEEE Standard for Developing Software Life Cycle Processes”.
- EPRI TR-102323, “Guidelines for Electromagnetic Interference Testing in Power Plants”, revision 1.
- ASME NQA-1a-1995, Appendix 7A-2, “Nonmandatory Guidance for Commercial Grade Items”, 1995.
- EPRI 5652,”Guidelines for the Utilization of Commercial Grade Items in Nuclear Safety-Related Applications.”
- IEEE 384-1977/1981/1992, “Criteria for Separation of Class 1E Equipment and Circuits”.
- NRC R.G. 1.75, “Physical Independence of Electrical Systems”.
- NRC R.G. 1.89, “Qualification of Class 1E Equipment for Nuclear Power Plants”.
- NRC R.G. 1.100, “Seismic Qualification of Class 1E Equipment for Nuclear Power Plants”.

Certification Process

NUCLEAR LOGISTICS INC

- Full V&V included:
  - Mild environment analysis in accordance with IEEE Std. 323-1983
  - Seismic qualification by testing in accordance with IEEE Std. 344-1987
  - EMI/RFI in accordance with EPRI TR-102323
  - Software/hardware review in accordance with:
    - IEEE 7-4.3.2
    - EPRI TR-102348
    - EPRI TR-106439

Digital Trip Unit V&V

NUCLEAR LOGISTICS INC

- The Program consisted of the following activities:
  - Preparation of design drawings.
  - Preparation of the Instruction Manual.
  - ANSI C37 design testing.
  - Seismic qualification by testing per IEEE 344-1975.
  - Mild environment qualification by analysis and testing per IEEE 323-1974.
  - EMI/RFI qualification by testing per EPRI TR-102323, revision 1 and 2.

Digital Trip Unit V&V

NUCLEAR LOGISTICS INC

- Hardware/Software System Review activities consisted of the following:
  - Audit/critical design review at the Square D facilities:
    - Grenoble, France: Trip unit design and engineering.
    - Montmelian, France: Trip unit manufacture.
    - Moirans, France: Manufacture, assembly and testing of the Masterpact breaker modules.
    - Cedar Rapids, Iowa: Trip unit design and development.
  - Software written under ISO 9001-2000 QA program.

Access to Software & Controls

NUCLEAR LOGISTICS INC

- The key to successful V&V is having access to the software and controls which were in place during the software development.
- If you can not get access to the software or the software is not in a language which can be understood V&V can not adequately be done.
- This requires cooperation by the vendor and usually requires confidentiality agreements, and other legalities to be accomplished prior to the software being made available.

Audit Activities

NUCLEAR LOGISTICS INC

- Face-to-face interviews with engineering personnel, reviews of testing documents, and analysis of the Micrologic trip unit design documents at Square D's engineering and test facilities in Cedar Rapids, IA.
- Reviews of the Micrologic trip unit design documents with the Schneider's Micrologic design team and quality assurance representatives
- Interviews with production and quality control personnel, inspection of trip unit production, testing, and packaging operations, and analysis of assemble methods, test equipment certification, and test reports at Schneider Electric's Micrologic production facilities in Montmelian, France.
- 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 Masterpact production facilities in Moirans, France.

Abnormal Conditions & Events

NUCLEAR LOGISTICS INC

- Abnormal Conditions and Events (ACE's)
  - Trip unit ACE's:
    - Environment
    - Seismic.
    - EMI/RFI.
    - Voltage range.
    - Infant failures of electronics.
    - Loss of power.
    - Fault in non safety related plant system.
    - Hardware/software faults.
    - Overcurrent Condition

Trip Unit FMEA

NUCLEAR LOGISTICS INC

- 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.
- 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 trip unit.
- 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.

FMEA Results

NUCLEAR LOGISTICS INC

- There are two credible failure modes that could impact ASIC operation. These failure modes are identified and evaluated below:
  - Loss of clock (gate pulse).
  - Loss of 24 volt DC power.
- Both of these failures are acceptable as follows:
  - These are hardware failures in the system and are not a function of the software. The hardware is manufactured with a minimum number of components and is highly reliable.
  - Hardware failure of a proven product like the Micrologic trip device, is a random event. Common cause failure of this type of hardware is not credible.

NLI FMEA Testing

NUCLEAR LOGISTICS INC

- NLI performed supplemental FMEA testing. The FMEA testing is included with the Validation testing The following potential failure modes were tested by NLI:
  - Remote communications, alarms, and interlocks do not impact operation of the trip unit. Note that these functions are not electrically connected.
  - Trip unit operates properly with battery removed or a dead battery.
- The trip unit responded as specified in the Schneider design documents during the FMEA testing.

Validation Testing

NLI
NUCLEAR LOGISTICS INC

- Verification of all trip settings
- Programmer operates on Square D Masterpact NT or NW breaker.
- Programmer operates per design with ratings plugs.
- Output alarms are per design.
- Remote communications, alarms, and interlocks do not impact trip unit operation.
- No spurious tripping.
- Operation of the reset button.
- Programmer restarts after loss of power.
- Programmer operates properly with battery removed or dead battery.
- Memory does not impact trip unit operation.
- Secondary test set does not impact trip unit settings.
- Function defeat switches operate per design
- Operation across voltage range

Equipment Reliability

NUCLEAR LOGISTICS INC

- A reliability simulation was performed by Schneider Electronic in accordance with MIL-HDBK-217F. The calculated failure rates were as follows for ground fixed applications:
  - 3.11 E-6 h-1@40°C.
  - 5.64 E-6 h-1@100°C.
- The design of the trip unit ASIC is based on the previous generation of the Masterpact ASIC design, whose core protection functions were accomplished through the use of 350 components. The present Micrologic ASIC design performs the same core protection functions using 53 components. The smaller number of components significantly increases the reliability of the system.
- All of the microcode for the present ASIC digital protection is new, though the function of the trip unit is conceptually very similar to the previous design.
- Due to the reduced number of components, architectural design, and small amount of microcode, the trip unit is more reliable than any previous analog or digital overload protection model designs.

Operating History

NUCLEAR LOGISTICS INC

- There have been no revisions to either the THROM/MCROM microcode or the ASIC hardware since its production release in 1998.
- Over 50,000 Micrologic trip devices using the current ASIC MCROM microcode are in use, with approximately 17,000 deployed in the United States.
- Schneider has been shipping the same version since product rollout during 1998. To date, none have been recalled.
- No outstanding, uncorrected software errors exist at this time.
- Presently, no microcode revisions are planned.
- The large installed base with no reported software problems and no software revisions indicates a high level of equipment reliability.

Separation Criteria

NUCLEAR LOGISTICS INC

- The Micrologic trip units are self-contained on each circuit breaker.
- The electrical interfaces to and from the trip units are fully contained on each breaker.
  - The trip units are powered from the CT's on the breakers, which are powered from the primary bus.
  - The trip units receive their input signal from the CT's.
  - The trip units send their output signal to the actuator on the breaker.
  - In the qualified configuration, the trip units do not communicate with any other devices in the plant.
  - The electrical interfaces of the Micrologic trip units are the same as the currently installed solid state trip units.
- If the Micrologic trip units are replacing electromechanical trip units, there are no CT's and wiring. The separation of the Micrologic trip units is still maintained from this configuration.
- Installation of the Micrologic trip units maintains the same level of physical and electrical separation as the existing trip units on the low voltage switchgear breakers.

Common Mode Failure Evaluation

NUCLEAR LOGISTICS INC

- The equipment architecture is robust by design and manufacture.
- The trip unit design and development was performed in a rigorous manner and is well documented.
- Rigorous production controls are used by Square D to assure that 100% of the supplied trip units meet the design requirements.
- Extensive production testing is performed.
- Detailed quality assurance/quality control processes and procedures are implemented throughout the lifecycle of the trip units, by both Schneider/Square D and NLI.

Common Mode Failure Evaluation (Continued)

NUCLEAR LOGISTICS INC

- The applicable ACE's have been identified and addressed by testing or analysis. Based on these activities, ACE's are not credible failure mechanisms for the trip units.
- With an installed base of over 50,000 trip units, there have been no reported software related failures. The software has not been revised since it was released in 1998.
- The detailed FMEA by Schneider/Square D and FMEA testing by NLI did not identify any unacceptable failure modes. The two credible failure modes that were identified are hardware failures. The robust Schneider design and NLI burn-in of 100% the supplied trip units eliminate these hardware failures as potential common mode failure mechanisms.
- Each trip unit is electrically and physically isolated from the other trip units in the plant.
- **Based on the extensive design, development and testing performed by Square D and NLI and the equipment configuration in the nuclear plant, common mode failure of the Micrologic trip units is not considered credible.**

Trip Unit Dedication Testing

NUCLEAR LOGISTICS INC

- Dedication testing/FAT of 100% of the supplied circuit breakers:
  - Record the trip unit configuration data (part number, serial number, code and revision).
  - Burn-in for 48 hours.
  - Secondary injection testing of the trip unit to verify a sample of the trip curve points for each active function (L, S, I, G).
  - Primary injection testing on the supplied circuit breaker.
    - » Verify a sample of the trip curve points for each active function (L, S, I, G).
    - » Verify proper operation of the trip unit with the CT's, ratings plug, and actuator.
  - Primary injection testing at degraded and over voltage conditions to verify proper operation of the trip unit across the primary voltage range (the trip unit is powered from the CT's on the primary bus).
  - Note: The dedication plan for each replacement breaker type includes additional critical characteristics that verify the proper operation of the entire breaker assembly.

Trip Unit Traceability

NUCLEAR LOGISTICS INC

- Traceability of the test specimen to the production units was performed. The following methodology was used to document the traceability:
  - The test specimens and the production units were shown to have the same hardware and configuration.
  - Programmer physical configuration.
  - Circuit board and chip part and revision.
  - The test specimens and the production units were shown to have the same firmware configuration (firmware revision).
  - There are no field configurable circuit board settings (DIP switches, jumpers, etc.).
  - The functional testing of the test specimen and the dedication testing of the production units provided the added assurance that the production units were manufactured to the same design standards and perform in an equivalent manner to the test specimen.

Trip Unit Software Configuration Control

NUCLEAR LOGISTICS INC

- The following process is used to identify, document, evaluate, and report firmware modifications and errors:
  - The as-built firmware configuration of the supplied units is documented and controlled as specified in previous slide.
  - NLI contacts Schneider every 6 months and any modifications or reported errors are identified.
  - Errors are documented and evaluated in accordance with the NLI Nonconformance Report (NCR) process . Notification in accordance with 10CFR21 will be made in accordance with NLI procedures, if required.
  - Design changes which are not the result of errors are evaluated by NLI for impact on the existing system and future replacement trip units.
  - NLI will submit all NCR's and 10CFR21 reports associated with the trip unit hardware and software to end users. Evaluation of design changes will also be submitted.

Trip Unit V&V - Conclusions

NUCLEAR LOGISTICS INC

- Micrologic is a very simple ASIC (Application Specific Integrated Circuit) architecture.
- Digital protective function has built in analog backup. If the digital portion of the trip unit fails the breaker will still trip using the analog feature. This is built in diversity.
- OEM didn't verify all set points. NLI tested all set points to verify the shape of the timing curve.
- The non-safety related display and communication features are isolated from the safety related trip function.
- Limitations: No communication lines connected.

Key Issues/Lessons Learned

NUCLEAR LOGISTICS INC

- Is the project upgrading commercial grade digital equipment or development of digital equipment under a 10CFR50 Appendix B quality assurance program?
  - Dedication of commercial grade digital equipment.
  - Development of digital equipment under a 10CFR50 Appendix B program.
  - Combination of both.
    - Firmware developed by manufacturer and dedicated.
    - User software developed by 10CFR50 Appendix B manufacturer.

Key Issues/Lessons Learned

NUCLEAR LOGISTICS INC

- Electromagnetic Interference / Radio Frequency Interference (EMI/RFI) qualification by testing per EPRI TR-102323 is often an iterative process:
  - Often requires modification of equipment to pass the susceptibility testing.
  - Interface conditions are key and must be a conservative representation of the plant configuration.
    - Wire type.
    - Conduit.
    - Grounding.

Key Issues/Lessons Learned

NUCLEAR LOGISTICS INC

- Additional testing is always required during the V&V of commercial grade digital equipment.
  - Failure Modes & Effects Analysis (FMEA) testing is always required, even if it was previously performed by the manufacturer. Nuclear power plants have postulated failure modes that are different from commercial application.
  - Validation testing of the hardware/software system is always required. The manufacturer's validation testing is not adequate to meet safety related requirements.
  - Dedication testing/Factory Acceptance Testing (FAT) is required on 100% of the supplied equipment. The manufacturer's FAT testing is not adequate to meet safety related requirements.

Key Issues/Lessons Learned

NUCLEAR LOGISTICS INC

- The utility must evaluate the installation of the digital equipment in accordance with 10CFR50.59. NRC Regulatory Issue Summary 2002-22 provides additional details.
- An integrated program of auditing and testing is required for a successful program.
  - Audit/critical design review of the manufacturer.
    - Experience of the audit personnel.
    - Commercial manufacturers have a wide range of programs and documentation.
  - Supplemental testing required.
    - Meet nuclear plant specific requirements.
    - Address weaknesses in the manufacturers program.