ENVIRONMENTAL TESTING OF A PROTOTYPIC DIGITAL SAFETY CHANNEL, PHASE I: SYSTEM DESIGN AND TEST METHODOLOGY

K. Korsah, G. W. Turner, J. A Mullens
Oak Ridge National Laboratory, Oak Ridge Tennessee 37831-6010

Submitted for presentation at the
22nd Water Reactor Safety Information Meeting
October 1994

Prepared for U.S. Nuclear Regulatory Commission
Washington, D. C. 20555
under Interagency Agreement DOE 1886-8179-8L

NRC JCN L1798

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Prepared by the
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6010
managed by
MARTIN MARIETTA ENERGY SYSTEMS, INC.
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-84OR21400

DISCLAIMER

ENVIRONMENTAL TESTING OF A PROTOTYPIC DIGITAL SAFETY CHANNEL, PHASE I: SYSTEM DESIGN AND TEST METHODOLOGY*

K. Korsah, G. W. Turner, and J. A. Mullens
Oak Ridge National Laboratory (ORNL), Oak Ridge, TN, 37831-6010

ABSTRACT

A microprocessor-based reactor trip channel has been assembled for environmental testing under an Instrumentation and Control (I&C) Qualification Program sponsored by the U.S. Nuclear Regulatory Commission. The goal of this program is to establish the technical basis for the qualification of advanced I&C systems. The trip channel implemented for this study employs technologies and digital subsystems representative of those proposed for use in some advanced light-water reactors (ALWRs) such as the Simplified Boiling Water Reactor (SBWR) and AP600. It is expected that these tests will reveal any potential system vulnerabilities for technologies representative of those proposed for use in ALWRs. The experimental channel will be purposely stressed considerably beyond what it is likely to experience in a normal nuclear power plant environment, so that the tests can uncover the worst-case failure modes (i.e., failures that are likely to prevent an entire trip system from performing its safety function when required to do so). Based on information obtained from this study, it may be possible to recommend tests that are likely to indicate the presence of such failure mechanisms. Such recommendations would be helpful in augmenting current qualification guidelines.

1. INTRODUCTION

Rising maintenance costs and a lack of spare parts are forcing an increasing number of nuclear utilities to consider upgrading analog safety systems with newer, more readily available technologies such as fiber optic transmission systems and microprocessors. In addition, advanced light-water reactor (ALWR) manufacturers intend to make even more extensive use of such technologies in the design of both control and safety (Class 1E) systems. However, many of the qualification standards used for nuclear plant instrumentation were developed for analog equipment and so they do not account for performance and functionality issues that are unique to digital equipment. In addition, the consequences of environmental stressor effects have not been clearly determined, in part due to the inability to completely map all possible relationships between inputs to a microprocessor and its outputs. As a result, investigative work is needed to characterize the failure modes and degradation mechanisms of technologies proposed for use in ALWR safety systems and/or future retrofits for existing LWRs. This information supports the determination of the likelihood of environmental stress for digital components and the expected effect. The result would be a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand and what symptoms should be indicative of an unacceptable response in type testing.

*Research sponsored by the Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission, under Interagency Agreement DOE 1886-8179-8L and performed at Oak Ridge National Laboratory, managed by Martin Marietta Energy Systems, Inc., for the U.S. Department of Energy under contract DE-AC05-84OR21400.

The vulnerabilities of "advanced" technologies such as fiber optic transmission systems, multiplexers, and microprocessor-based systems to environmental stressors is currently being investigated by ORNL as part of an NRC-sponsored I&C qualification research program[1-3]. The goal of this program is to establish the technical basis for augmenting the qualification process to accommodate advanced I&C systems. Initial studies in this regard have been documented in NUREG/CR-5904, *Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors*, where the likely impact of environmental stressors on safety systems and the failure mechanisms of fiber-optic transmission system components are examined. A methodology for identifying the need for accelerated aging in a qualification program for new I&C systems placed in benign environments was also suggested in the cited document. As a follow-on to that work, the safety channel and test methodology described in this present paper will be used to investigate *experimentally* the functional behavior and failure modes of a microprocessor-based trip system resulting from the application of environmental stressors such as electromagnetic interference (EMI), radio-frequency interference (RFI), temperature, humidity, and the presence of smoke.

2. PROTOTYPIC DIGITAL SAFETY CHANNEL DESIGN

2.1. Rationale for Design Choices

The reactor trip system designs for the *AP600* (Westinghouse), the *ABWR* and *SBWR* (General Electric), and the *System 80*$^+$ (Combustion Engineering) were reviewed to identify technologies that are different from present-day safety system implementations. Descriptions of these designs can be found in NUREG/CR-5904. ORNL's prototypic safety channel employs technologies that are representative of these advanced designs.

ALWR trip systems are typically implemented as four separate divisions. In ORNL's system, however, only one division is implemented; the trip information to/from the other three divisions is simulated by a *Host Processor*. This approach does not compromise the objectives of the task, since any vulnerabilities identified in the channel implemented in the ORNL system could be expected to be present in similar (redundant) channels.

2.2. System Level Design Description

Fig. 1.1 shows a block diagram of the prototypic reactor trip channel (PRTC). It consists of the reactor trip subsystem and an engineered safety feature (ESF) actuation subsystem (represented by a multiplexer unit). The inputs and outputs of these subsystems are established and monitored, respectively, by the Host Processor. The following is a description of the various subsystems and their functions:

Reactor Trip/Remote Multiplexing Unit

The function of the reactor trip/remote multiplexing unit (TRP/RMU) is to acquire analog process signals, convert them to digital form, and format them into frames suitable for transmission over a *Fiber Distributed Data Interchange* (FDDI) ring network. All process variables used for reactor trip (e.g., hot leg temperature, coolant flow rate, etc.) are simulated by a digital-to-analog multiplexer card contained in the Host Processor.

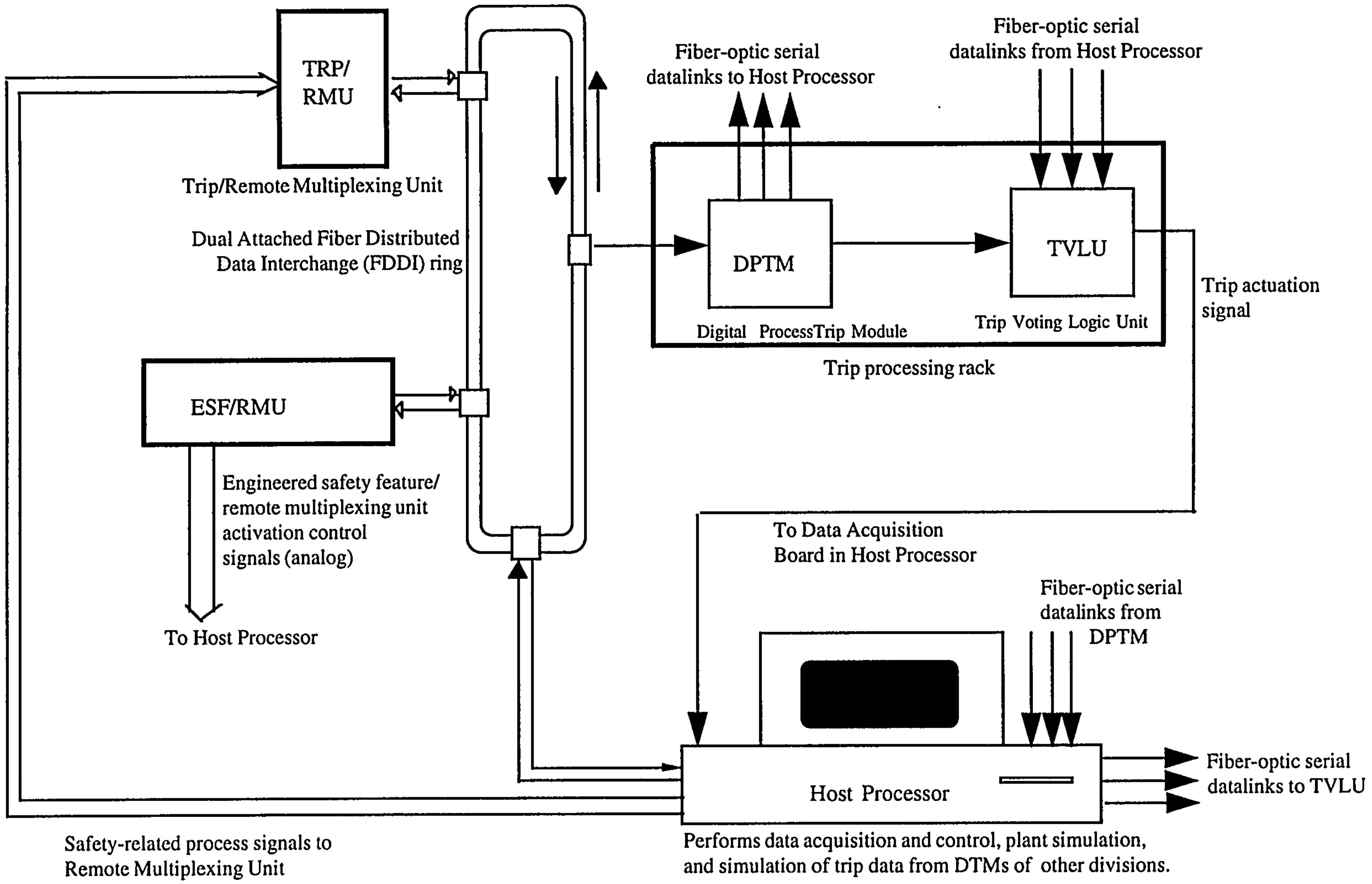

Fig. 1. Diagram of the prototypic reactor trip channel.

Digital Process Trip Module and Trip Voting Logic Unit

The digital process trip module (DPTM) acquires the digital values of the process signals off the FDDI network. The DPTM compares individual process values with trip setpoint values and *for each variable* sends a separate trip/no trip indication to the trip voting logic unit (TVLU). At the same time, it sends identical information to the Host Processor via optical fiber serial datalinks. Note that in a typical ALWR trip system, the trip/no trip information from the DPTM would be sent to the three other divisions' TVLUs via optical fiber datalinks, whereas in this implementation, the Host Processor will simulate the functions of the DPTMs and TVLUs of the three other divisions.

The Host Processor

The Host Processor (HOSTP) monitors all information going to and from the reactor trip subsystems, performs diagnostic checks when requested, and stores general information on system performance. In particular, the HOSTP performs the following activities:

- Simulates process signal variables typical of either normal or accident conditions, and sends the variables to the TRP/RMU;

- Acquires the data sent over the network by the TRP/RMU. (Note that the data from the TRP/RMU is also acquired by the division's DPTM processor.) In this way the HOSTP verifies that the process signals it sent to the TRP/RMU have not been corrupted as a result of passing through the network;

- Simulates *process trip* conditions assumed to come from the DPTM of the three other divisions. This "Process Trip" information is sent over three separate optical serial datalinks to the TVLU of the division under test;

- At the same time, the HOSTP receives process trip information from the DPTM of the division under test. It then performs a 2-out-of-4 (software) voting based on the process trip information from this division, as well as the process trip information assumed to have come from the "other three divisions" (but actually simulated by the HOSTP);

- Monitors the voting result from the TVLU of the division under test. Prior to this time, the TVLU of the division under consideration would have received both the process trip information from the "DPTM of the other three divisions" (actually simulated by the HOSTP and sent via three independent fiber optic datalinks as shown in the figure), *and* the process trip information generated by the DPTM in its own division. The TVLU would have performed its own 2-out-of-4 voting, and sent *divisional trip* information to the HOSTP;

- Provides specified pump, valve, and other ESF actuation signals to the ESF/RMU under simulated accident conditions (e.g., a loss of coolant accident (LOCA) or steam line break).

- Monitors the ESF/RMU outputs to verify that:

  a. A condition requiring a trip actuation was successfully analyzed by the subsystems in the division;

b. Any ESF actuation signals generated by the HOSTP were successfully sent across the FDDI ring network, as well as correctly interpreted by the ESF/RMU.

3. TEST METHODOLOGY

As indicated earlier, a major objective of this study is to investigate the failure modes, under various environmental stresses, of representative digital technologies that are likely to be employed in future nuclear power plants or in retrofits. The study is expected to result in a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand and what symptoms should be indicative of an unacceptable response in type testing.

A previous study of proposed ALWR protection systems conducted by ORNL staff determined that multiplexing equipment used in the safety system will most likely be located outside reactor containment in "divisional clean areas."[1] In addition, this equipment will be placed at locations that are geographically separate from the protection system cabinets installed in "mild" (i.e., control room) environments. Thus, it appears reasonable to divide the equipment to be tested into two major subsystems, so that tests can be conducted on each major subsystem separately. The major subsystems are defined as:

- The multiplexing equipment used for acquiring process information (TRP/RMU in Fig. 1). This is designated *subsystem 1.*

- The trip modules and ESF actuation multiplexing equipment. This is designated *subsystem 2.*

Subsystem 1 will first be subjected to all the tests; the tests will then be repeated on subsystem 2. All tests will be performed under software control from the Host Processor. A brief outline of the general test procedure is as follows:

- *Configure the PRTC;*
- *Place the subsystem to be tested in the test chamber;*
- *Apply a chosen stressor for a specified period of time;*
  - *generate test signals typical of both normal and various accident conditions;*
  - *for each set of test signals, verify system response and log any errors;*
  - *increase the severity of the stressor;*
  - *repeat the tests.*

The stressors to be applied are temperature, humidity, EMI/RFI, and smoke. Since the objective is not to qualify the system hardware, the subsystems will be stressed considerably beyond what they are likely to experience in a normal nuclear power plant environment. The procedure followed in applying the stressors is briefly described as follows:

Steady State Humidity Tests:

- Initial conditioning [122°F (50°C) at 30% RH] for 24 hours.
- Continued testing until system is brought down to ambient.
- Steady state tests [106°F (41°C) at 93% RH] for 24 hours.

Accelerated Humidity Tests:

- Initial conditioning [122°F (50°C) at 93% RH] for 24 hours.
- Continued testing while system is brought down to ambient.
- 10 cycles of the following: temperature ramping from 75°F to 150°F in 2-1/2 hrs at 94% RH.

Smoke Tests:

- Initial conditioning at 73°F and 50% RH for 24 hours.
- Increment of RH to 60%
- Burning of cable specimens while equipment under test (EUT) is in test chamber.
- Placement of EUT in test chamber and continued testing for additional 8 hours.
- Physical examination and analysis of EUT for damages.
- Repetition of tests at increments of 10% RH up to and including 90% RH, or until permanent failure, whichever comes first.

EMI/RFI Tests:

These tests will be performed to MIL-STD 462D specifications:

- CS01 - Conducted susceptibility; low frequency;
- CS02 - Conducted susceptibility, high frequency;
- CS06 - Conducted susceptibility, spikes;
- RS01 - Radiated susceptibility, magnetic fields;
- RS02 - Radiated susceptibility, spikes;
- RS03 - Radiated susceptibility, electric fields.

The following industry standards were used as guidelines to develop the temperature/humidity/smoke test procedures:

- ANSI/EIA/TIA-526-1992, "Standard Test Procedures for Fiber Optic Systems."
- ANSI/EIA/TIA-455-5A-1990, "Humidity Test Procedure for Fiber Optic Connecting Devices."
- ANSI/EIA/TIA-455-3A-1989, "Procedure to Measure Temperature Cycling Effects on Optical Fibers, Optical Cable, and Other Passive Fiber Optic Components."
- CNS C6046, "Environmental Testing Methods and Endurance Test Methods for Discrete Semiconductor Devices (Cycle Test for Temperature and Humidity)."
- ASTM/D 5485-94, "Standard Test Method for Determining the Corrosive Effect of Combustion Products Using the Cone Corrosimeter."

Electromagnetic Interference/Radio-Frequency Interference (EMI/RFI) tests will be performed on the PRTC according to applicable test criteria and methods stipulated in MIL-STD-461 and MIL-STD-462, respectively. MIL-STD-461 establishes the military's emission and susceptibility requirements for electronic, electrical, and electromechanical equipment and subsystems. It also provides a basis for evaluating the electromagnetic characteristics of equipment and subsystems by setting operational acceptance criteria. The test methods corresponding to the MIL-STD-461C requirements are described in MIL-STD-462.

The objective of the EMI/RFI tests under this task is to identify how EMI/RFI-induced upsets in the EUT can affect the reactor trip systems's ability to fail safe. The tests are *not* intended to ascertain whether the subsystems meet emissions and susceptibility criteria called out by MIL-STD-461. Thus, only applicable *susceptibility* criteria and test methods will be used in conducting the tests.

The smoke tests will be performed in collaboration with Sandia National Laboratories (SNL). There is currently no standard for smoke tests of electronic equipment; existing "smoke standards" or draft standards have a focus that is different from the objectives of this task. For example, Underwriters' Laboratory (UL) Std 1685, "Vertical Tray Fire Propagation and Smoke Release Test for Electrical and Optical Fiber Cables," is designed to determine values of cable damage height and smoke release from electrical and optical-fiber cables when the cables are subjected to a flaming ignition source. The standard does not investigate the toxicity of the products of combustion or decomposition, nor does it address how an equipment's susceptibility to smoke should be measured.

IEEE draft Std 1202.1, "Standard for Measuring the Release Rates of Smoke and Heat of Wire & Cable for Use in Industrial and Commercial Occupancies," is expected to be similar in content and focus to UL Std 1685.

In the design of a test chamber for ORNL's smoke tests, SNL is following an ASTM draft standard,"Standard Test Method for Measuring the Corrosivity of Smoke from the Burning or Thermal Decomposition of Materials and Products." However, this standard focuses on a test method for determining the corrosive effects of smoke on metals under specified conditions, rather than on the potential for degradation or failure of electronic equipment. ORNL and SNL have used this draft standard, UL 1685, and ASTM/D 5485-94 as guidelines in developing the smoke test chamber and test procedures that will be used in this work.

4. CONCLUDING REMARKS

This paper has discussed the design of a digital safety channel employing technologies similar to those likely to be used in the next generation of nuclear power plants. We have also summarized the test methodology to be used to investigate the vulnerabilities of these technologies to various environmental stressors. Based on information obtained from this study, it will be possible to determine the expected effect of a stressor on digital subsystems likely to be used in nuclear power plants. This information, combined with a knowledge of the likelihood of the stressor in the environment, can provide a more clear definition of what stressors (and to what level) digital equipment should be qualified to withstand, and will provide the technical basis that will be helpful in augmenting current qualification guidelines.

At the time of this writing, the hardware design is complete, the assembly of the hardware is nearly finished, and the software test algorithms are nearing completion. Actual system tests in stressing environments are expected to commence in December 1994.

REFERENCES

1. Korsah, Kofi, Robert L. Clark, and Richard T. Wood, *Functional Issues and Environmental Qualification of Digital Protection Systems of Advanced Light-Water Nuclear Reactors*, NUREG/CR-5904, April 1994, U.S. Nuclear Regulatory Commission.

2. Ewing, P. D., and K. Korsah, *Technical Basis for Regulatory Guidance on the Susceptibility of Digital Systems to Electromagnetic and Radio-Frequency Interference*, NUREG/CR-5941, ORNL/TM-12221, May 1993, Oak Ridge National Laboratory.

3. Korsah, K., R. L. Clark, and D. E. Holcomb, "A Methodology for Evaluating 'New' Technologies in Nuclear Power Plants," *Instrumentation, Controls, and Automation in the Power Industry, Vol. 37, p. 131-148*, Proceedings of the 4th Annual ISA/EPRI Joint Controls and Automation Conference, Orlando, FL, June 1994.