CONF-970607--37

TECHNICAL BASIS FOR ENVIRONMENTAL QUALIFICATION OF COMPUTER-BASED SAFETY SYSTEMS IN NUCLEAR POWER PLANTS*

Kofi Korsah
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6010 USA
(423) 576-6064
korsahk@ornl.gov

Christina E. Antonescu
U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, MD 20852 USA
(301) 415-6792
cea1@nrc.gov

Tina J. Tanaka
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0747 USA
(505) 844-2981
tjtanak@sandia.gov

Richard T. Wood
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6010 USA
(423) 574-5578
woodrt@ornl.gov

ABSTRACT

This paper summarizes the results of research sponsored by the U.S. Nuclear Regulatory Commission (NRC) to provide the technical basis for environmental qualification of computer-based safety equipment in nuclear power plants. This research was conducted by the Oak Ridge National Laboratory (ORNL) and Sandia National Laboratories (SNL). ORNL investigated potential failure modes and vulnerabilities of microprocessor-based technologies to environmental stressors, including electromagnetic/radio-frequency interference, temperature, humidity, and smoke exposure. An experimental digital safety channel (EDSC) was constructed for the tests. SNL performed smoke exposure tests on digital components and circuit boards to determine failure mechanisms and the effect of different packaging techniques on smoke susceptibility.

These studies are expected to provide recommendations for environmental qualification of digital safety systems by addressing the following: (1) adequacy of the present preferred test methods for qualification of digital I&C systems; (2) preferred standards; (3) recommended stressors to be included in the qualification process during type testing; (4) resolution of need for accelerated aging in qualification testing for equipment that is to be located in mild environments; and (5) determination of an appropriate approach to address smoke in a qualification program.

I. INTRODUCTION

Digital instrumentation and control (I&C) system upgrades are gradually replacing existing analog systems, since analog replacements are becoming increasingly difficult to obtain. Because of the potential benefits of digital systems, widespread use of the such technology in safety systems of nuclear power plants (NPPs) is inevitable. In fact, fully digital safety and control systems are envisioned for advanced light-water reactors (ALWRs)[1] such as the Westinghouse AP-600 or GE Advanced Boiling Water Reactor (ABWR).

While digital technology has several advantages and, in fact, has been in widespread use in the non-nuclear industry for several years, a concern with its use in safety-related systems in NPPs is the limited experience with the technology in these environments. For example, issues such as adequacy of present preferred test methods for qualification of digital I&C systems, preferred standards, recommended stressors to be included in the qualification process during type testing, and determination of an appropriate approach to include smoke as a stressor in a qualification program, all need to be addressed.

This paper presents the results of confirmatory research performed by two U.S. Department of Energy laboratories—Oak Ridge National Laboratory (ORNL) and Sandia National Laboratories (SNL)—to provide the technical basis for possible enhancement of regulatory guidance on environmental qualification of computer-based safety equipment in nuclear power plants.

*Research sponsored by the Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission. The opinions and viewpoints expressed herein are those of the authors and do not necessarily reflect the criteria, requirements, and guidelines of the U.S. NRC.

DISCLAIMER

II. ORNL STUDY: ENVIRONMENTAL EFFECTS TESTING OF AN EXPERIMENTAL DIGITAL SAFETY CHANNEL

This portion of the overall work investigated failure modes and vulnerabilities of microprocessor-based technologies when subjected to the environmental stressors of electromagnetic and radio-frequency interference (EMI/RFI), temperature, humidity, and smoke exposure. The effect of smoke exposure on digital equipment was of particular interest because this stressor had not previously been considered in safety system qualification testing. The smoke tests were performed jointly by ORNL and SNL.

Ranges of stress were selected at a sufficiently high level to induce errors so that failure modes characteristic of the technologies employed could be identified. Subsystems of the experimental digital safety channel (EDSC) assembled for the tests included computers, electrical and optical serial communication links, fiber-optic network links, analog-to-digital and digital-to-analog converters, and multiplexers. In addition, the EDSC was typical of ALWR trip system designs or some retrofits with respect to chip fabrication and packaging technology, board fabrication technology, component temperature ratings, reliability stress tests used during component quality assurance procedures, functions of individual subsystems, and communication protocols.[2]

Most failures of electronics components and systems fall into three categories:[3,4] hard failures, upsets,[5] and latent failures.[6] Of particular interest in the study were temporary or intermittent upsets caused by environmental stressors and how these upsets were likely to affect a digital trip system's performance. At the component level, some of the failure mechanisms associated with integrated circuits include cracked substrate, loss of hermetic seal, short circuits, changes in leakage current and offset voltage. At the board or system level, however, the effect of component upsets and failures include data errors due to bit changes in memory cells, communication failures, processor lock-up, and interface failures (e.g., timeouts on serial interfaces). Table 1 lists some specific examples of the generic stressor-induced upsets that were observed with the EDSC. Details of the EMI/RFI, temperature/humidity, and smoke exposure test procedures are given in references 2 and 3.

The study found interfaces to be the most vulnerable elements of the EDSC. The majority of effects resulting from the application of the stressors were communication errors, particularly for *serial* communication links. Many of these errors were intermittent timeout errors or corrupted transmissions, indicating failure of a microprocessor to receive data from an associated multiplexer, optical serial link, or network node. Because of similarities in fabrication and packaging technologies, other digital safety systems are likely to be vulnerable to similar upsets. As was experienced with the EDSC, intermittent component upsets will typically impede communication, either at the board level (e.g., during bus transfers of data), or at the subsystem level (e.g., during serial or network data transfers).

Based on incidence of errors during testing, EMI/RFI, smoke exposure, and high temperature coupled with high relative humidity were found to be the most significant of the stressors investigated. The most prevalent stressor-induced upsets—as well as the most severe—were found to occur during the EMI/RFI tests. For example, these tests produced the only permanent failure of the EDSC (a multiplexer power supply failed at 72 V/m, 20 MHz). Also, the effect of the stressor was typically immediate, whereas the effects of high temperature/humidity and smoke exposure did not manifest themselves for some interval (i.e., tens of minutes) after the application of the stressor.

While the EDSC test demonstrated system-level effects for both *conducted* and *radiated* EMI/RFI, the commercial components used exhibited greater susceptibility to conducted EMI/RFI. This observation is consistent with general industrial experience by European EMI/RFI experts.[7] It should be noted that the relative susceptibility of particular systems can be mitigated by the use of proper grounding, shielding, isolation, and surge withstand practices.

With regard to temperature and humidity, the study found that the combination of high temperature and high relative humidity (RH) was the condition that caused the most significant effects on the EDSC functionality, rather than elevated temperature alone. High RH is not as likely in a controlled environment such as a control room, but still needs to be considered in qualification, especially for post-accident monitoring (PAM) equipment.

For smoke exposure, important failure mechanisms are not only long-term effects such as corrosion, but also short-term and perhaps intermittent effects such as increased current leakage. Smoke can cause circuit bridging and, thus, affect the operation of digital equipment. Because the card edge connectors and interfaces are typically uncoated, the most likely effect of the smoke is to impede communication and data transfer between subsystems.

During the exposure tests for various smoke densities, upsets for the EDSC typically were not encountered until about an hour into the exposure interval. Of particular note, the EDSC did not lose functionality when exposed to smoke equivalent to a large control room panel fire (smoke density of about 3 g/m^3). A large control room panel fire has been postulated by Nowlen[8] as the most severe fire likely to be experienced in the main control room. (In this scenario, a whole panel burns, all equipment within the panel is destroyed, and the smoke from this fire is dispersed throughout the control room. Because the smoke under this scenario was postulated to be uniformly distributed throughout the entire main control room, this represents the smallest smoke density of the three fire scenarios postulated

Table 1 Generic and observed environmental stressor-induced upsets

GENERIC STRESSOR-INDUCED ERRORS IN DIGITAL SYSTEMS	ERRORS OBSERVED WITH EDSC
Permanent component/board failures and upsets that lead to unintended (usually unsafe) digital actuation errors.	EMI-induced upset caused digital actuation signal to give erroneous result.
Component/module upsets that can usually prevent a channel from performing its intended function, but whose adverse effect in an actual plant safety system can typically be offset by careful engineering design.	Serial and network communication timeouts occurred due to parity and overrun errors.
Component/module upsets that have the *potential* to prevent a channel from performing its function. However, the affected component or module recovers in time for the required function to be performed.	The digital trip computer (DTC) had to retransmit data on the network on several occasions due to lack of acknowledgment of messages sent.
Component/module upsets that will typically not prevent a channel from performing its function in the presence of the stressor causing the upset. However, failure may occur at a future date, long after the stressor has been removed.	Changes in leakage currents, noise margins, pulse rise and fall times, and other component parameters that nevertheless remain within tolerance for the affected channel to perform normally. (NOTE: the tests were not designed to thoroughly investigate latent failures).
Component/module upsets that place the safety channel in a tripped state.	Digital nibble output stuck in a "tripped state." (NOTE: While this is a plausible example that could have occurred in the EDSC, the phenomenon was not actually observed).

in the Sandia study. Larger smoke densities were postulated for scenarios involving small panel fires with the smoke contained within the panel and for equivalent fires in small volume spaces.) Because of similarities between the EDSC and digital safety systems with regard to fabrication and packaging for circuit boards and chips, it is reasonable to postulate that commercial digital equipment will likely maintain functionality during its initial period of exposure to smoke equivalent to a large control room panel fire unless any of the equipment is contained in the burning panel or in close proximity to the fire source. Given early detection of a fire and subsequent application of fire suppression measures, digital systems can therefore be expected to maintain functionality (to allow safe shutdown) for up to an hour or more following exposure, provided the equipment is not directly exposed to the fire.

The solder mask on commercial electronic boards appears to be effective in preventing catastrophic and/or permanent failure of the board even when the boards are exposed to a reasonably high level of smoke. The lower limit that necessitates cleaning of circuit boards, due to chloride deposits from smoke, is often specified[9] to be 10 μg chloride/cm^2. For comparison, analysis of the largest smoke load used in the ORNL/SNL tests (160 g/m^3) showed the chloride deposition to be 742 μg chloride/cm^2. (Tests by SNL with uncoated boards using comparable smoke loads showed a marked decrease in resistance.[10])

III. SNL STUDY: IMPACT OF SMOKE ON DIGITAL COMPONENTS

This portion of the study consisted of smoke exposure tests on digital components and circuit boards, with a focus on short-term effects such as circuit bridging in typical components and the factors that can influence how much effect the smoke will have. These factors include the component technology and packaging, physical board protection, and environmental conditions such as the amount of smoke, temperature of burn, and humidity level. The likelihood of circuit bridging was tested by measuring leakage currents and converting those currents to resistance in ohms. The lower the resistance, the higher the

likelihood of shorts. Details of the study are given in reference 10.

The study found that many different factors may influence whether a digital I&C system will function reliably during or after a smoke exposure. One of the failure mechanisms for digital equipment is circuit bridging, so the SNL tests studied factors that could possibly affect circuit bridging in typical digital electronic components. The factors that were studied can be divided into three categories: component technology and packaging, circuit board protection with coatings or enclosures, and smoke generation factors. The factors in the first two categories can be controlled through design, fabrication, and installation practices, whereas the last category can be controlled by reduction of fuel available, control of the environment during a fire, and other traditional fire protection measures.

With regard to technology and packaging, the tests using 16K memory chips showed ceramic packages to be more robust than their plastic package counterparts in a smoke environment.

The voltages at which the digital electronics operate vary according to the digital chip technology. Resistance measurements on comb patterns indicated that higher voltage (tens of volts) patterns are affected by smoke more than lower voltage (several volts) patterns. The higher voltage lowers the equivalent resistance before the smoke is applied because the comb pattern is not a linear resistor, however, when smoke is applied the equivalent resistance increases more on the high voltage patterns than the low voltage patterns. Visually, it was observed that soot tends to accumulate more around the high voltage patterns.

Two hex inverter chips were included in the tests to determine the difference between a small out-line integrated circuit (SOIC) package and a dual-in-line package (DIP). The test results showed no appreciable difference between these two packages except with respect to the *rate* of degradation at high fuel loads. When the fuel available for smoke production was high, both packages shorted; however, components with small contact spacing shorted earlier. Thus, the DIP package resisted shorting longer than the SOIC package. When the available fuel was low, the resistance dropped for both packages slightly, and then recovered with little difference observed between the chip packages. A reason for the inability to detect differences in this case may be that the low fuel loads were too low to cause much change in resistance.

Bare boards were highly affected by smoke, while coated boards seemed to be less affected. Housing the boards in a PC chassis containing a fan protected the boards only minimally. Visually, some of the boards that were placed within the chassis looked worse than those that were unprotected because clumps of soot were deposited on the board. For the high fuel tests, however, virtually all components were shorted in these situations and little difference could be observed in the resistance measurements.

Several observations can be made from the component tests: the most significant smoke generation factors are humidity, fuel level, and burn temperature. High humidity has been shown to affect the surface insulation resistance of printed circuit boards in environmental testing.[11] Other fire corrosivity tests which used comb patterns also showed that the resistance of exposed comb patterns is strongly affected by humidity.[12] As more fuel is burned, resistance drops. (Smoke from the combustion of plastic leaves a film, which is black and powdery if the plastic is burned in the flaming mode with adequate oxygen. The film is white and oily if produced without a flame and black and oily if produced with a flame lacking in oxygen.) For low fuel loads, the resistance generally dropped during the smoke exposure but recovered after the smoke was vented. This recovery was not often the case with the high fuel loads; once the circuit was shorted, it never recovered.

IV. CONCLUSIONS AND FOLLOW-ON WORK

The research described in this paper is addressing environmental compatibility issues for microprocessor-based I&C systems to provide the technical basis for environmental qualification of computer-based safety equipment in nuclear power plants. Conclusions resulting from the research at the two national laboratories include the following:

1. Interfaces were found to be the most vulnerable elements of the EDSC. The majority of effects resulting from the application of the stressors were communication errors, particularly for serial communication links. Many of these errors were intermittent timeout errors or corrupted transmissions, indicating failure of a microprocessor to receive data from an associated multiplexer, optical serial link, or network node. Because of similarities in fabrication and packaging technologies, other digital safety systems are likely to be vulnerable to similar upsets. As was experienced with the EDSC, intermittent component upsets will typically impede communication, either on the board level (e.g., during bus transfers of data) or on the subsystem level (e.g., during serial or network data transfers). Thus, qualification testing should confirm the response of any digital interfaces to environmental stress.

2. Smoke is an important stressor on safety equipment because of the possibility of multiple equipment failures. Nevertheless, some coatings on commercial electronic boards appear to be effective in preventing catastrophic (permanent) failure of digital electronics boards, even when they are exposed to smoke from the most severe fire that is likely to be experienced in the control room.

3. The investigation of stressor effects using the EDSC indicates that EMI/RFI can produce undesirable effects for microprocessor-based I&C systems.

The results and insights obtained from the studies described in this paper have been used to develop a methodology for environmental qualification of microprocessor-based I&C equipment for nuclear power plants. This methodology will be reported in a forthcoming NUREG/CR report.

ACKNOWLEDGEMENTS

The research presented in this paper was sponsored by the Office of Nuclear Regulatory Research, U. S. Nuclear Regulatory Commission. The environmental effects study was performed at Oak Ridge National Laboratory under Job Control Number L1798 and the smoke impact study was performed at Sandia National Laboratories under Job Control Number W6051. Oak Ridge National Laboratory is managed by Lockheed Martin Energy Research Corp. for the U. S. Department of Energy under contract DE-AC05-96OR22464. Sandia National Laboratories are managed by Sandia Corporation, a Lockheed Martin Company, for the U. S. Department of Energy under contract DE-AC04-94AL85000.

REFERENCES

1. Electric Power Research Institute, *Advanced Light Water Reactor Utility Requirements Document*, EPRI NP-6780, Revision 6, December 1993.

2. K. Korsah, T. L. Wilson, and R. T. Wood, "Environmental Effects Testing of an Experimental Digital Safety Channel," *Proc. of the 1996 ANS Int'l Topical Meeting on Nuclear Plant Instr., Control, and Human-Machine Interface Technologies*, Vol. 2, pp. 1203-1211, University Park, PA, May 1996.

3. K. Korsah, T. J. Tanaka, T. L. Wilson, and R. T. Wood, *Environmental Testing of an Experimental Digital Safety Channel*, NUREG/CR-6406, Oak Ridge National Laboratory, September 1996.

4. O. M. Clark and R.E. Gavender, "Lightning Protection for Microprocessor Based Electronic Systems", *IEEE Conf. Record of 36th Annual Petroleum & Chemical Industry Technical Conf.*, pp. 197-203, New York, NY, 1989.

5. R. J. Hanson, "Conducted Electromagnetic Transient-Induced Upset Mechanisms: Microprocessor and Subsystem Level Effects," *Proc. of EOS/ESD Symposium (EOS-9)*, p. 104, Griffiss AFB, NY, 1987.

6. P. E. Gammil and J. M. Soden, "Latent Failures Due to Electrostatic Discharge in CMOS Integrated Circuits," *Proc. of EOS/ESD Symposium (EOS-8)*, pp. 78-79, Griffiss AFB, NY, 1986.

7. D. J. Bardsley, S. R. Dillingham, and K. McMinn, "European Standards and Approaches to EMC in Nuclear Power Plants," *Proc. Of the USNRC 22nd Water Reactor Safety Information Meeting*, NUREG/CP-0140, Vol. 1, pp. 99-105, Bethesda, MD, October 1994.

8. S. P. Nowlen, "Defining Credible Smoke Exposure Scenarios," Letter Report to USNRC, Sandia National Laboratories, Albuquerque, NM, September 1994.

9. L. Cider, "Cleaning and Reliability of Smoke-Contaminated Electronics," *Fire Technology*, National Fire Protection Assoc., Boston, MA, Third Quarter 1993.

10. T. J. Tanaka, S. P. Nowlen and D. J. Anderson, *Circuit Bridging of Components by Smoke*, NUREG/CR-6476, Sandia National Laboratories, October 1996.

11. R. L. Iman, R. V. Burress, D. J. Anderson, and others, *Evaluation of Low-Residue Soldering for Military and Commercial Applications: A Report from the Low Residue Soldering Task Force*, Sandia National Laboratories, Albuquerque, NM, 1995.

12. L. M. Caudill, J. T. Chapin, R. B. Comizzoli, *et al.*, "Current State of Fire Corrosivity Testing: Preliminary Electrical Leakage Current Measurements," *International Wire & Cable Symposium*, pp. 432-437, Atlantic City, NJ, 1995.