BNL-NUREG-62572

CONF-960521--9

ADVANCED DIGITAL I&C SYSTEMS IN NUCLEAR POWER PLANTS: RISK-SENSITIVITIES TO ENVIRONMENTAL STRESSORS

Mahbubul Hassan
Department of Advanced Technology
Brookhaven National Laboratory
Building 130
Upton, NY 11973
e-mail: hassan@bnl.gov

William E. Vesely
Science Applications International Corporation
655 Metro Place South
Suite 745
Dublin, OH 43017

ABSTRACT

Microprocessor-based advanced digital systems are being used for upgrading analog instrumentation and control (I&C) systems in nuclear power plants (NPPs) in the United States. A concern with using such advanced systems for safety-related applications in NPPs is the limited experience with this equipment in these environments. In this study, we investigate the risk effects of environmental stressors by quantifying the plant's risk-sensitivities to them. The risk-sensitivities are changes in plant risk caused by the stressors, and are quantified by estimating their effects on I&C failure occurrences and the consequent increase in risk in terms of core damage frequency (CDF). We used available data, including military and NPP operating experience, on the effects of environmental stressors on the reliability of digital I&C equipment. The methods developed are applied to determine and compare risk-sensitivities to temperature, humidity, vibration, EMI (electromagnetic interference) from lightning and smoke as stressors in an example plant using a PRA (Probabilistic Risk Assessment). Uncertainties in the estimates of the stressor effects on the equipment's reliability are expressed in terms of ranges for risk-sensitivities. The results show that environmental stressors potentially can cause a significant increase in I&C contributions to the CDF. Further, considerable variations can be expected in some stressor effects, depending on where the equipment is located.

I. INTRODUCTION

Advanced digital systems based on microprocessors are proliferating in the area of process instrumentation and control because of their increased capabilities and superior performance compared to those based on analog devices. This technology also is being implemented in nuclear power plants in the United States to replace existing analog I&C systems which are reaching either the end of their useful life or becoming obsolete because spare parts are no longer available.

A concern with using advanced digital I&C systems in NPP applications, particularly for safety-critical equipment, is their potential sensitivities to NPP environments including common-cause vulnerabilities. Digital technology was introduced relatively recently in the nuclear power industry, mostly in the last fifteen years and mostly in non-critical control applications. Therefore, relevant experience is rather limited, and relatively little information is available on their performance. Specifically, there is no database on the effects of NPP environments on the reliability of this equipment.

A large variety of microprocessor-based digital I&C equipment is available with major differences in semiconductor or packaging technology, the complexity of the devices, their ruggedness, and quality. Significant variations can be expected in reliability performance, depending on the equipment chosen and the particular application. Because of possible variations in the characteristics of stressors, such as their intensity, duration and uncertainties in our knowledge of their effects, the risk effects can be determined only in the form of ranges of, or bounds on, potential effects.

This lack of data on digital equipment in NPP environments required that we utilize experience with the equipment in other applications for our risk-sensitivity evaluations. We reviewed the literature, including military documents, records of operational events in nuclear power plants, and journal publications to assemble the information available to estimate the effects of environmental stressors.

In this paper, we present the results of a risk-sensitivity analysis of potential stressors in a NPP (a pressurized-water reactor) assuming digital I&C systems are used. For stressors that can affect safety systems whose function is to prevent core damage, the risk sensitivity is related to the possible increase in plant CDF, calculated using a PRA.

II. SCOPE OF THE STUDY

Instrumentation and control systems in nuclear power plants associated with reactor protection and safety-system actuations consist of different components, such as process sensors, transmitters, sensing lines, and cabling as well as various logic units and switching devices. The upgrades are implemented primarily by using various digital microcircuits, including microprocessors, to replace analog logic and switching functions in the I&C systems. The existing sensors, transmitters, and cabling in the I&C systems are expected to remain the same, at least in the near future, although fiber-optic cables and components eventually may replace much of this equipment. Consequently, in evaluating risk-sensitivities associated with environmental stressors, the impact of NPP operating environments on various digital microcircuit devices is most relevant.

I&C equipment in NPPs generally can be found in all major plant locations, such as the control building, the auxiliary building, and the containment. However, logic and switching equipment associated with safety-critical I&C are primarily located in the control building. Depending on the specific plant, the control building areas where I&C cabinets may be located can include the control room, relay room, cable-spreading room, and switchgear room. Consequently, in our analysis, we assumed that the digital I&C equipment is located in these areas. Presently, nuclear utilities have no plans to locate microprocessor-based equipment in the harsh environments of the containment.

Risk-sensitivities are investigated for an example plant for temperature, humidity, vibration, EMI (electromagnetic interference), and smoke. These five stressors, in addition to radiation, were identified from a literature review as having a potential to degrade the digital microcircuits' reliability, and consequently, the reliability of the system. Radiation was not included since in NPP locations where there is digital I&C equipment, significant sources of this stressor are not expected. In the case of EMI, data were available only on interference events caused by lightning. The risk-effects of other sources of EMI were not evaluated because of lack of data. A probabilistic risk analysis specific to the example plant was used to quantify the risk-sensitivies using the existing I&C models in the PRA.

III. APPROACH

The risk-sensitivity of a stressor is the change in plant risk which occurs given its presence, and is quantified by estimating its effect on the occurrences of I&C failures, and then by determining the effect of these failures on plant risk. A PRA may be used to identify risk-sensitive I&C component sets whose failure cause large change in risk for the plant.

If we let

I = expected value of CDF

L = likelihood of the stressor

C = CDF contribution from the I&C equipment

F = factor increase in the I&C failure rate caused by the stressor

N= number of I&C components simultaneously affected by the stressor

then

$$I = LF^{N}C \qquad (1)$$

The increase in CDF due to a stressor then can be obtained by quantifying or estimating ranges for L and F.

When the stressor is assumed to occur, i.e. L=1, equation 1 reduces to

$$I = F^{N}C \qquad (2)$$

We assumed that the stressor has the same effect on failure rates of all components. However, if these effects differ, then the term F^N in Equations 1 and 2 is substituted by ΠF_i where

ΠF_i = product of factor increases, F_i, in failure rates of individual components, i, affected by the stressor

In general, equations 1 and 2 apply to the case where there is one dominant combination of equipment failures (i.e. one dominant minimal cutset) which contributes to the CDF. If there are several dominant combinations, then I is determined for each combination, i.e. each minimal cutset, using the above formula and then summed over the contributions.

The risk-sensitivity of the stressor is defined as the conditional increase in the CDF (from some reference value), which occurs given the stressor.

The effects of environmental stressors on equipment failures can be estimated from historical data, plant operational characteristics, and by applying engineering judgment. The likelihood of a stressor is given by the likelihood of the given environment and of the stressors in it. If the stressor can occur in different environments, then the likelihood of the stressor in the environment is the sum over all different environments. The stressor's effect on components is reflected through an increase in their failure rates. The magnitude of such increases generally will depend on the intensity and duration of the stressor.

If the effects of the stressor on I&C failure rates can be determined or bounded, then the different possible I&C failure rate factors can be input to a PRA, to determine the resulting risk sensitivity. As an upper-bound evaluation, the I&C equipment which can be affected by the stressor can be assumed to fail, and the resulting increase in CDF determined.

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.

IV. DATA

Digital systems have a wide application and operational experience with them has accumulated, such as that by the U.S. military in various field applications. The information reported in Refs. 1, 2 and 3, was used to estimate the effects of temperature, humidity, and vibration, on digital microcircuits in NPP environments in terms of factor increases in their failure rates over a given reference value (failure rates in a benign environment, such as the controlled environment of the NPP control room). Licensee Event Reports (LERs), which are records of NPP operational events in the United States (Licensee Event Reporting System, USNRC), were used to estimate the frequency of lightning-related EMI events. Estimates of frequencies for potential fires in the example plant at relevant locations (reported in Ref.4) were used to approximate the frequencies of smoke events.

Temperature

Digital equipment failure mechanisms associated with temperature are electrical shorts and open circuits. Temperature-dependent conversion factors for mean-time-between-failures (MTBF) are reported in Ref.2 for a collection of discrete semiconductor devices and integrated circuits. Using these values for the change in MTBF for all devices in the collection including digital microcircuits, and assuming that the mean-time-to-repair is negligible, failures rate factors (multipliers to reference failure rate) are developed; these are shown for some selected temperatures in Table 1, normalized to 75°F (the assumed control room temperature).

Table 1
Temperature-Dependent Failure Rate Factors

Temperature °F	Factor Increase
75	1.0
86	1.06
104	1.06
122	1.35

Humidity

For humidity, the time-to-failure of microcircuit devices is reduced through corrosion, thereby increasing the effective failure rate. While corrosion is an important concern for all microcircuits, it is more so for today's high-density microprocessors and other digital circuits because of their closer interconnect spacings and thinner metallic sections used to achieve the needed compactness. However, the humidity effect also depends upon ambient temperature. Table 2 shows the failure rate factors at selected temperatures and humidity levels, normalized to 75°F and 60% relative humidity (assumed control room environment) obtained using the acceleration factors for temperature-humidity environment reported in Ref. 1.

Table 2
Factor Increase in Device Failure Rate Due to Corrosion

Temp °F	% Relative Humidity		
	60	80	100
75	1.0	2.37	4.63
86	2.01	4.76	9.29
104	6.03	14.31	27.94
122	16.96	40.19	78.50

Vibration

Military experience[1,2] shows that vibration-induced excitation frequencies encountered in various field applications are much lower than those needed to damage microcircuit devices. Environments for digital I&C equipment in NPPs are not expected to include vibration sources which are either higher in frequencies or amplitude than those encountered in various military applications (details of these applications and environmental effects are given in Ref. 5). Therefore, we conservatively estimated that for relevant NPP locations, changes in failure rates of up to a factor of 4 over the reference failure rate should adequately account for the effects of vibration.

EMI

EMI events in digital I&C systems in NPPs, identified as the root cause of a significant number of system malfunctions or failure[6], have been documented in LERs. Of the EMI/RFI sources which can affect digital I&C systems in NPPs, a significant amount of information is available only for lightning-induced events. Lightning also is the more frequent source of EMI events in NPPs.

Based on a study on surge-protecting devices in U.S. NPPs[7] from 1980 to 1994, 29 events could be attributed to perturbations or failures of I&C systems resulting from lightning-induced electrical spike or noise generated through electromagnetic couplings, and involved both digital and analog systems (details are given in Ref. 5). The number of reactor years of operation during 1980-1994 for all operating U.S. nuclear plants was estimated at 1409.4 years[7]. Since digital systems operate at lower voltages than analog equipment, they are more vulnerable to electrical disturbances and overstress. Assuming that electrical perturbations which affect analog equipment also would affect digital equipment under similar circumstances, the frequency of lightning-related EMI events (f) averaged over all U.S. plants is estimated as follows.

$$f = 29/1409.4 = 2.06E\text{-}02 \text{ /plant-yr} \qquad (3)$$

Assuming a resulting probability of equipment failure of 1.0 in such events, and using surveillance test intervals of 31 days to detect the failure, equipment unavailability, q, due to lightning-induced EMI events can be estimated as:

$$q = f \times T_i/2 = 8.75E\text{-}04 \qquad (4)$$

This unavailability value is an average over all U.S. plants and represents the probability that the affected equipment will be unavailable and unable to function in an accident. The unavailability, q, depends on thunderstorms in the region where the plant is located. In the United States, this varies from a low of 10 events per year in the northwest to as high as 100 per year in parts of the south[8], or a factor of 10 difference in frequency between the high and the low. Assuming a factor of 10 difference also between high and low values of q, and using Equation 4 as the mid-value, the following range is obtained for q:

$$q_{high} = 2.77E\text{-}3 \;,\quad q_{low} = 2.77E\text{-}04 \qquad (5)$$

Smoke

Extensive facility-wide damage to telecommunications equipment from smoke following fires has been reported[9]. The damage to equipment from smoke is caused by the transport and deposition of products of combustion, such as carbon soot and other chemicals, including many corrosive compounds. Smoke particles, deposited on microcircuit devices, can cause contact failures, contact bridging, and corrosion. Some of these processes can further be enhanced by other environmental factors, such as high relative humidity.

We did not identify any published data either on frequencies of smoke events in NPPs or on smoke-related failure of digital equipment which could be used in risk-sensitivity evaluations. Consequently, a bounding approach was used to evaluate plant risk-sensitivity to smoke by assuming that the digital equipment failed with a probability of 1.0 when the smoke event occurred. The frequencies of smoke events were assumed to be the same as fire frequencies in relevant areas of the plant.

Table 3 shows mean fire frequencies developed for the example plant[4] based on the number of fire events which have occurred in specific compartments of light water reactors during commercial operation and the number of operational years that the industry has accumulated. The generic fire occurrence data was updated in Ref.4 to determine plant-specific fire event frequnecies.

Table 3
Fire Initiating Event Frequencies

Fire Area	Mean Frequency (/yr)
Control Room	1.8E-3
Cable/Vault Tunnel	7.5E-3
Electrical Switchgear Room	8.0E-3

Following the same approach as shown in Equation 4 and using the event frequencies given in Table 3, equipment unavailability, q, due to smoke events was estimated (Table 4).

Table 4
Estimated Unavailabilities from Smoke Events

Plant Area	Average Unavailability
Control Room	7.64E-05
Cable/Vault Tunnel	3.18E-04
Electrical Switchgear Room	3.40E-04

V. EXAMPLE CASE

The SURRY Unit 1 IRRAS (Integrated Risk and Reliability Analysis System) PRA Data Base[10] was used in the following way in the evaluations:

- The PRA was used to generate a list of minimal cutsets.

- The minimal cutsets containing I&C basic events then were identified.

- Where information on the effects of environmental stressors on I&C failure rates was available, the basic event probabilities were modified accordingly and used to recalculate changes in CDF .

- Where there was information on stressor effects on I&C in the form of stressor-related equipment unavailabilities, the unavailability values were used to calculate the expected changes in CDF.

- The CDF contributions from each of the minimal cutsets containing I&C basic events were summed to obtain the total change in CDF from the affected equipment.

- The sum of the I&C contributions was divided by the plant baseline CDF (i.e. CDF without the stressors) to obtain the relative contribution of I&C to CDF in each case.

- Stressor risk-sensitivities were expressed in terms of these relative contributions to CDF.

In the SURRY PRA model, the detail available for the I&C equipment is at the actuation train level. Relevant I&C components are combined together and modeled as a single *basic event (actuation train). The probability of failure assigned* to the I&C basic events then is the combined unavailability of the entire train.

The total baseline CDF was calculated to be 3.647E-05 /yr, while I&C contributions to CDF were 5.55E-08 /yr. The base case CDF values are obtained using the components' failure probabilities as given in the PRA. Credit was not taken for any recovery actions in either case.

The following additional assumptions were made in calculating stressor risk-sensitivities:

i. the requirements for qualifying I&C equipment were treated as the same in all plant locations, which translates to the same susceptibility to environmental stressors at all locations;

ii the effects of stressors were treated as the same on all I&C equipment, partly because of the lack of detail in I&C models in the PRA, and partly because of lack of information on the effects of different stressors on different technologies;

iii a likelihood of 1.0 was assumed for the occurrences of temperature, humidity, and vibration as stressors since these are plausible from present information;

iv a failure probability of 1.0 was assumed for all I&C equipment for common-cause events, such as for EMI and smoke.

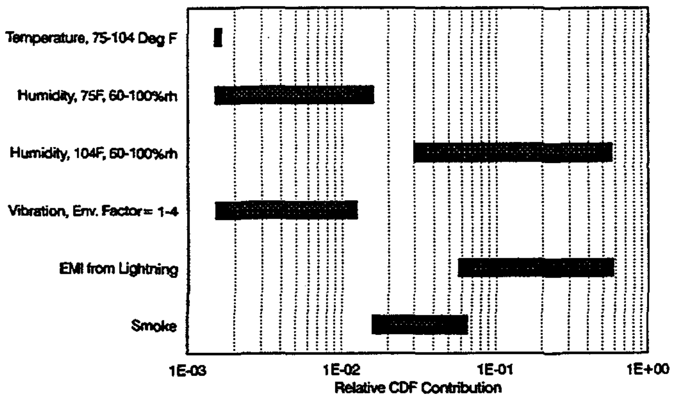
VI. RESULTS

Figure 1 compares the plant's risk-sensitivities to different environmental stressors; relative sensitivities to CDF are represented and not absolute contributions. The risk-sensitivities to temperature are shown for temperatures under normal control-room operation to those in the switchgear room under accident conditions. Risk-sensitivities to humidity are given for these two different temperatures; risk-sensitivities are significantly higher at the higher temperature. The relative CDF contribution also is high (~0.6) for lightning-related EMI events.

The results show that there are significant differences among the environmental stressors in terms of their potential impact on plant core damage frequency (CDF). The risk effects range over two orders of magnitude, from a relatively small CDF contribution of a 0.0015 to close to 0.6. Furthermore, the largest risk-sensitivities are caused by lightning-related EMI events, and by humidity at higher ambient temperatures. Risks from other EMI sources could not be evaluated because there are no data. Smoke also is an important stressor because of the possibility of multiple equipment failures. For the stressors and stressor levels which were analyzed, risk contributions from *digital I&C equipment showed the least sensitivity to* temperature, and to potential vibration effects.

From these results, we can categorize the environmental stressors in terms of order of magnitude differences in risk-sensitivities, such as stressors which result in less than 0.01 in relative contributions to CDF from I&C failure events, those causing between 0.01 and less than 0.1, and those which cause greater than 0.1. The latter are most important from risk perspective and digital I&C systems need to be designed and qualified with careful attention to them. Further research also can reduce the uncertainties about their degrading effects on equipment. In implementing digital I&C systems in NPPs, it will also be important from a risk perspective, to control the effects of stressors in the second category (relative CDFcontributions 0.01-<0.1) which are still significant. The risk sensitivities from stressors with relative CDF contributions of less than 0.01 are minimal and well within PRA uncertainties; these stressors do not warrant additional attention except, perhaps, in special cases.

Figure 1 Risk-Sensitivties to Environmental Stressors



Relative CDF Contribution= CDF Contribution from I&C / Baseline Plant CDF

VII. SUMMARY AND CONCLUSIONS

This paper describes an approach for evaluating plant risk-sensitivities to environmental stressors when digital I&C

equipment are used in safety and mitigating systems. Stressor risk-sensitivities are compared, based on their effect on relative CDF contributions, using ranges or bounding evaluations where data are sparse. This approach ranks the stressors in terms of their relative risk impacts without requiring absolute evaluations. The study included reviewing data on the effects of stressors on digital I&C failures; methods developed were applied to prioritize environmental stressors in an example plant using its specific PRA.

We reviewed the literature, including military documents, NPP operational events records, and journal publications to identify information on the effects of environmental stressors on digital equipment. The available information is sparse, particularly in terms of the reliability of digital equipment. Further, there are uncertainties in estimates of the effects on reliability due to possible variations in parameters associated with the application of stressors, such as their intensities, duration, and also the diversity of the equipment. Therefore, these data were used for broad comparison of risk-sensitivities from different stressors based on estimated ranges of, or bounds on, potential effects.

Our evaluations of stressor risk-sensitivities are based on existing I&C models in the PRA. Also, only one plant was used as an example. Nevertheless, the application shows the usefulness of the approach in quantifying stressors' impacts on plant risk. The results for the example plant show that environmental stressors potentially can significantly increase I&C contributions to core-damage frequency.

Risk from stressors depends not only on the physical effects of the stressors on the digital I&C equipment and their likelihoods, but also on the specific equipment that is affected, its failure modes, and risk-importance. Consequently, to more accurately represent the effects of stressors on plant risk, the following steps are needed:

1. extending current I&C models in the PRA to reflect the digital system's characteristics.
2. obtaining reliability data on digital I&C components to support these models.
3. gathering information to resolve uncertainties in current assumptions in stressor risk quantifications.
4. using plant-specific information to resolve plant-specific issues.

ACKNOWLEDGEMENTS

This work was sponsored by the U.S. Nuclear Regulatory Commission. The views expressed in this paper are those of the authors and do not reflect any position or policy of the U.S. Nuclear Regulatory Commission.

REFERENCES

1. "Reliability Analysis/Assessment of Advanced Technologies", RADC-TR-90-72, Rome Air Development Center, Griffiss Air Force Base, NY, May 1990.
2. "The Rome Laboratory Reliability Engineer's Toolkit", Systems Reliability Division, Rome Laboratory, Griffiss Air Force Base, NY, April 1993.
3. "Reliability Prediction of Electronic Equipment", MIL-HDBK-217F, December 1991.
4. NUREG/CR-4550,"Analysis of Core Damage Frequency, SURRY Unit 1, External Events", Vol.3, Rev.1, Part 3.
5. M. Hassan and W.E. Vesely, "Risk-Based Prioritization of Environmental Stressors Which Can Affect Advanced Digital I&C Equipment In Nuclear Power Plants", Draft letter report to NRC, December 1995.
6. "Computer-Based Digital System Failures", Technical Review Report, AEOD/T94-03, Reactor Analysis Branch, Safety Programs Division, Office of Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, July 1994.
7. NUREG/CR-6340 (Draft), "Aging Assessment of Surge Protective Devices in Nuclear Power Plants", July 1995.
8. Clark, O.M. and Gavender, R.E., "Lightning Protection for Microprocessor Based Electronic Systems", Proc. of 36th Annual Petroleum & Chemical Industry, pp 197-203, Industrial Applications Society, IEEE, New York, NY, 1989.
9. Mowrer, F.W. and Pecht, M.G., "Exploratory Research on Nonthermal Damage to Electronics from Fires and Fire-Suppression Agents", Proc. Ann. Reliability & Maintainability Symp., 1995, pp 1-5, IEEE Reliability Society.
10. Fowler R.D., Judd, D.L. and Wolfram, L.M., SURRY Unit 1 IRRAS Version 5.0 PRA Data Base, Idaho National Engineering Laboratory, April 28, 1993.