No. 92-137 FOR IMMEDIATE RELEASE
Tel. 301/504-2240 (Monday, September 28, 1992)

NOTE TO EDITORS:

The Nuclear Regulatory Commission has received the attached letter-type report on reliability of digital instrumentation and control systems from its independent Advisory Committee on Reactor Safeguards.

In addition, the ACRS sent three letter reports to the NRC's Executive Director for Operations. They provide comments on:

1) a draft Commission paper, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs";

2) an NRC staff proposed resolution of issues identified in its evaluation of shutdown and low-power operations; and

3) General Electric Nuclear Energy's power uprate program and power increase request for the Fermi 2 nuclear power plant in Michigan.

#

Attachments:
As stated

September 16, 1992

The Honorable Ivan Selin
Chairman
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Chairman Selin:

SUBJECT: DIGITAL INSTRUMENTATION AND CONTROL SYSTEM RELIABILITY

During the 389th meeting of the Advisory Committee on Reactor Safeguards, September 10-12, 1992, we reviewed the staff's

proposed approach with respect to defense against common-mode failure of digital I&C systems, as discussed in policy issue "A" of the draft Commission paper entitled, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs," forwarded to the Commission on June 25, 1992. Specific comments on policy issue "A" are contained in a letter to Mr. Taylor dated September 16, 1992. The concerns we raise here are, however, more generally applicable, e.g., in connection with the staff's proposed generic letter on analog-to-digital replacements.

The trend in most industries over the last few decades has been toward the replacement of analog instrumentation and control systems with digital alternatives, and the nuclear industry has been no exception. This has been true for both functional replacements within existing nuclear facilities and for new designs, so it has been necessary for the staff to develop regulatory practices to deal with both the novel opportunities and the novel threats posed by these systems.

Experience, both military and industrial, has generally shown the digital systems to be more reliable and versatile than their analog counterparts. There are, however, some caveats and some regulatory conundrums. An advantage is that the digital systems are capable of more complex functions, so it is possible to build in self-testing capabilities that provide continuous assurance of operability with negligible system stress. In addition, the digital systems don't wear out; a billion activations of a CMOS gate are no more damaging than a thousand. While much has been made of the vulnerabilities of multiplexed data transmission systems, some of which are doubtless real, such systems generally provide greater fidelity and reliability of data transfer, along with greater fault tolerance through error-correcting coding. (If an analog signal is corrupted, it is often not possible to know it has happened.) Indeed, error detection and error correction can be carried to arbitrary lengths for digitized data. There are many other advantages, and the future clearly belongs to digital systems, where they can be used.

On the negative side, the available complexity of function afforded by digital systems invites the creation of complex software, which can be difficult to validate and can be subject to surprising error modes. Such systems are also hard to regulate, because only the simplest programs are amenable to formal validation and verification (V&V), in the sense of a complete analysis of the mapping of the input space to the output space. For more complex programs (relevant to nuclear control systems, but not necessarily to instrumentation or safety actuation systems), there are many analytical techniques in use, none perfect. That is also true of analog systems. Solid-state systems, whether digital or analog, are also peculiarly vulnerable to environmental damage, e.g., from overheating.

Finally, programmable digital systems have their own special vulnerabilities to human error.

The staff has concentrated its attention on one of these many issues, the vulnerability of digital systems to certain kinds of common-mode failures, principally through programming errors introduced into the software, and therefore common to all channels.

To deal with this supposedly special susceptibility to common-mode failure, the staff has proposed a set of regulatory requirements. The set includes some unarguable items, like the provision of adequate diversity to cope with common-mode failures that can affect safety systems, and analysis of the appropriate accident sequences. The set also includes some items whose desirability is less clear, and we now turn to these. Since each of these would require an extensive discussion to develop the point completely, and since our recommendation is that the staff revisit all these points, we will be brief. There is no special order.

The lack of explicit and quantifiable safety standards for instrumentation and control systems is particularly troublesome here. The staff speaks of reliability for digital systems in the same terms (failures per demand) that it uses for items which do wear out, like relays and switches. The entirely different failure mechanisms make this an inappropriate transfer of terminology. Indeed, a simple software-based system, in which the hardware is kept within its environmental constraints, and whose software is simple enough to have been subjected to a full validation and verification (in the sense used above) can be expected to never fail. (Never is only a slight exaggeration.) The failure anecdotes we all know are typically in systems that are too complex for formal V&V, leaving the door open to software errors, or have been mistreated, opening the door to hardware failures. The latter problem is not unique to digital systems.

In view of the lack of explicit standards for the reliability of the digital systems, the staff seems to have drifted to what has been called the "bring me a rock" posture, in which the industry is asked to analyze its own vulnerabilities, after which the staff will make its ruling about the adequacy of the design. The spirit of the safety-goal initiative was presumably to help make regulation more predictable, and this approach is clearly in the other direction.

The focus on common-mode failures is troublesome. Software errors in single systems can lead to accidents just as serious as those due to common-mode failures in redundant systems, and the entire question of software reliability greatly transcends the issues raised here. We have been conducting a coordinated series of meetings on the safety issues involved in the inevitable computerization of the industry, already in progress. When we

report on these, we will doubtless raise the question of whether sufficient talent, both in quantity and in experience, is being directed at these issues by NRC. That question is also an underlying issue here.

For the specific issue of protection against common-mode failures, whether for digital systems or such devices as diesel generators, there is a set of standard prophylaxes like diversity and defense in depth, which are useful when applied sensibly. (Slogans can be overplayed. It makes no sense to insist that multi-engine aircraft have a suitable mix of turbine and piston engines.)

The most controversial specific position taken by the staff is that there must be a safety-grade set of displays and controls located in the control room, independent of the computer systems, and "conventionally hardwired" to the lowest level practicable. Though the intent of the words in quotations is unclear, we were assured that it was to require analog backup systems. We do not concur in this proposed requirement. We think that the staff is unnecessarily mixing up the issues of digital/analog, hard wire/multiplex, and software/hardware.

Each instrumentation and control system that is important to the safety of a plant ought to meet some identifiable standard of reliability and fault tolerance, regardless of the hard-ware/software basis used in designing and fabricating the system. It is not necessary that any given element of the system be perfect, but that the system as a whole meet some recognized standard, presumably in the form of a relevant surrogate for the Commission's safety goals. Both the identification of that standard and the evaluation of conformance for the system in question pose problems, but each should somehow be completed before, not after, a regulatory position is established. For example, the staff proposes to require that a backup system provide protection equivalent to that of the primary system, whereas the need is for sufficient protection to assure the adequate safety of the plant. It is not at all uncommon for backup systems to be designed to lower standards than the primaries, taking into account the fact that they will be called upon less often. (Consider spare tires.)

It is entirely possible that a digital system may turn out to be a better backup than an analog system. (The proposed position does accommodate this idea, but the staff briefings did not.) For some situations a light beam is a more reliable means of communication than a hard wire. A general-purpose microprocessor that is in widespread commercial use may be more reliable (and more thoroughly tested) than a special-purpose analog switch. And so forth.

In each case it is necessary to make a specific reliability analysis, measured against a reasonable standard, and the staff

gave no evidence of having done so for any case. Instead, it has adopted a general requirement for an analog backup for all cases, and we were not convinced by the justification provided.

We recommend that the staff revisit these issues, augment its own capabilities, and broaden its interaction with those elements of the outside world who have previously dealt with such problems. It would be unwise, however, to read too literally into the nuclear arena the considerations that are relevant to far more complex systems. We are dealing here with the relatively simple safety-centered parts of the computerized instrumentation and control system, and an architecture that exploits this fact may be more robust.

Sincerely,

David A. Ward, Chairman
Advisory Committee on Reactor Safeguards

References:

1. Memorandum dated June 25, 1992, from James M. Taylor, Executive Director for Operations, NRC, for The Commissioners, Subject: Review of the Draft Commission Paper, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs"
2. 57 Federal Register, 36680, August 14, 1992, Proposed Generic Communication; Analog-to-Digital Replacements Under the 10 CFR 50.59 Rule

---

September 16, 1992

Mr. James M. Taylor
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Taylor:

SUBJECT: DRAFT COMMISSION PAPER, "DESIGN CERTIFICATION AND LICENSING POLICY ISSUES PERTAINING TO PASSIVE AND EVOLUTIONARY ADVANCED LIGHT WATER REACTOR DESIGNS"

During the 389th meeting of the Advisory Committee on Reactor Safeguards, September 10-12, 1992, we reviewed the NRC staff's positions and recommendations concerning the certification issues for evolutionary and passive light water reactor designs contained in the draft Commission paper, which was forwarded to the Commission on June 25, 1992. Our Subcommittee on Improved Light Water Reactors met on September 9, 1992, to review this subject.

During these meetings we had the benefit of discussions with representatives of the NRC staff and EPRI. We also had the benefit of the document referenced. We previously provided comments to you on other policy issues related to design certification in our letters of May 13, 1992 and August 17, 1992.

Our comments and recommendations on the proposed policy issues contained in the draft Commission paper are given below. Issues A, B, C, D, E, and G apply to evolutionary and passive plant designs and Issues F and H apply only to passive plant designs. The issue titles and letter designations correspond to those of the draft Commission paper.

A. Defense Against Common-Mode Failures in Digital Instrumentation and Control (I&C) Systems

It is our view that the thrust of the staff recommendations concerning defense against common-mode failures in digital I&C systems as underlined in Issue A of the draft Commission paper is appropriate. We agree with the staff that the applicant should be required to assess the defense in depth and diversity of the proposed designs for the events postulated in the Safety Analysis Report, and demonstrate an acceptable plant response for each. The staff proposes that the instruments, controls, and equipment required to demonstrate an acceptable response be independent of any common-mode failure mechanisms associated with the event. We view this requirement to be essential, but remain open as to the best approach. The staff proposes an independent set of safety-grade displays and controls in the main control room. We believe that other arrangements might be shown to be acceptable.

In a separate letter to Chairman Selin dated September 16, 1992, we have provided additional comments and advice regarding the general approach being taken by the staff in its review of digital instrumentation and control systems.

B. Analyses of External Events Beyond the Design Basis

To assist in the closure of severe accident issues, the staff recommends that (1) analyses submitted in accordance with the requirements of 10 CFR 52.47 (concerning the contents of applications for standard design certification) include an assessment of internal and external events and (2) during the design certification review, the staff should evaluate those external events that are not site dependent (e.g., fires, internal floods) and certain bounding analyses. We agree with this staff recommendation.

C. Elimination of the Operating Basis Earthquake from Seismic Design

The staff is still reviewing this issue and has expressed only an interim position. We believe the staff is taking an appropriate approach in its interim position.

D. Multiple Steam Generator Tube Ruptures (MSGTRs)

The staff is recommending that the applicant for design certification perform additional analyses to determine the AP600 response to multiple breaks of up to 5 steam generator tubes. We agree with the staff's recommendation, but believe the staff should have a better technical basis for estimating the frequency of occurrence of such multi-tube breaks.

The staff is also recommending that the applicant for design certification of a passive or evolutionary PWR assess design features necessary to mitigate the amount of containment bypass leakage that could result from MSGTRs. We agree with the staff's recommendation.

E. Probabilistic Risk Assessment (PRA) Beyond Design Certification

The staff is recommending that, throughout the duration of the combined or operating license, the PRA be revised to address significant plant modifications, operating experience, and other developments that may affect previous PRA insights.

We are convinced that it is worthwhile for a plant operator to have an up-to-date PRA and are, therefore, reluctant to recommend against this position. However, if this is to be required, the staff should more clearly specify how it intends to use the updated PRA and what is meant by keeping it current. We think such guidance is part of the overall issue of appropriate use of PRAs in regulation and would be helpful to licensees and to the staff.

F. Role of the Operator in a Passive Plant Control Room

We agree with the first part of the staff's position "that sufficient man-in-the-loop testing and evaluation be performed ... to demonstrate that functions and tasks are integrated properly into the man/machine interface design" of passive ALWR control rooms.

The second part of the staff's underlined position states "that a fully functional integrated control room prototype is necessary for passive plant control room designs to demonstrate that functions and tasks are integrated properly into the man/machine interface design." We pointed out to the staff that the non-underlined last sentence of this paragraph is inconsistent with this language in that it would permit an applicant to "demonstrate that a control room prototype of reduced scope is sufficient." We also pointed out that the non-underlined paragraph preceding the underlined paragraph states that such a prototype "would likely" be required (not would be required) to demonstrate that functions and tasks are integrated properly into the man/machine interface design. We believe that the staff

should clarify its intent by reconciling these various statements.

The staff believes that operators of passive plants will be confronted with a new operating philosophy. The staff argues that "the operators of passive plants must understand the operation of 'investment protection' systems and their interfaces with the safety-related passive systems" and that they will be confronted with "new functions and tasks unlike those required for evolutionary plants" (or current plants) "due to the new approach in operational philosophy" and "the increase in automation, and the greater use of advanced technology in the passive plant designs." As a result of our discussions with the staff and EPRI, we believe that the staff may be overreacting to the "newness" of these issues. It appears to us that additional discussion of this issue among the staff and EPRI and the vendors is needed.

G. Control Room Annunciator (Alarm) Reliability

We agree with the staff's position that the alarm system for ALWRs should meet the requirements of the EPRI Utility Requirements Document.

H. Regulatory Treatment of Nonsafety Systems

We were told that the staff is still engaged in significant on-going discussions and review of this issue and that the associated position and recommendations are subject to modification. We believe the issue is substantial and has broad implications with respect to such items as use of PRAs in regulation, safety goal implementation, and reduction of regulatory burdens, and we expect to have additional future interactions with the staff and the industry. Consequently, we are not prepared to express a position on this issue at this time.

Sincerely,

David A. Ward, Chairman
Advisory Committee on Reactor Safeguards

Reference:

1. Draft Commission Paper dated June 25, 1992, from James M. Taylor, Executive Director for Operations, NRC, for the Commissioners, Subject: Review of the Draft Commission Paper, "Design Certification and Licensing Policy Issues Pertaining to Passive and Evolutionary Advanced Light Water Reactor Designs"

September 15, 1992

Mr. James M. Taylor
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Taylor:

SUBJECT: NRC STAFF'S PROPOSED RESOLUTION OF ISSUES IDENTIFIED IN ITS EVALUATION OF SHUTDOWN AND LOW-POWER OPERATIONS

During the 389th meeting of the Advisory Committee on Reactor Safeguards, September 10-12, 1992, we reviewed the staff's proposed Generic Letter (GL) 92-XX concerning resolution of the issues identified in its evaluation of shutdown and low-power operational risk (Draft NUREG-1449). The staff plans to issue this GL for public comment. Our Plant Operations Subcommittee considered this matter during its September 9, 1992 meeting. During these meetings, we had the benefit of discussions with representatives of the NRC staff and NUMARC. We also had the benefit of the documents referenced. We previously provided comments to you on the staff's program to resolve these issues in our letters of August 13, 1991 and April 9, 1992.

The proposed GL describes those actions that the staff believes are needed by holders of OLs and CPs to resolve shutdown and low-power operational risk issues. It also includes a regulatory analysis in support of the need for these actions. We note that NUMARC had not seen the proposed GL prior to our meetings and was therefore limited in its ability to comment at this time.

The proposed GL represents a generally appropriate means of dealing with these issues. We have several comments, noted below, that we believe the staff should consider before releasing this GL for public comment.

- The staff proposes a technical specification (TS) for PWRs that would require that containment integrity (at least a single barrier in all penetrations) be maintained for the first seven days after shutdown. We agree that containment integrity should be maintained during any reduced inventory operation that takes place when decay heat is at a high level. We found many problems with the staff's proposed implementation of this requirement during this review. The staff has told us that it will make appropriate revisions to this TS requirement and expects to interface with industry groups on this issue during the public comment period.

- The staff proposes that a fire hazards analysis be performed for decay heat removal (DHR) equipment used during cold shutdown and refueling. Licensees would be required to document the results and develop a DHR restoration

contingency plan. On the basis of our discussion with the staff and NUMARC, we believe that the guidance provided in the proposed GL could lead to fire-analysis requirements far beyond those that have been justified by the staff. We believe that more dialogue between the staff and industry is needed on this issue.

- The staff has prepared a regulatory analysis in support of the proposed GL. If taken at face value, the quantitative aspects of this analysis support the conclusions reached by the staff. However, the needed PRA input is not yet available and many questionable assumptions were made. The staff is in the process of completing two shutdown risk PRAs (Surry Power Station and Grand Gulf Nuclear Station). These will not be finished until the spring of 1993. While we agree that the staff's regulatory analysis provided some insights and should be issued for information, it does not justify the imposition of the GL requirements. The staff told us that it believes that the GL could be issued on the basis of a qualitative substantial additional protection argument. (The word "substantial" remains undefined.) A qualitative argument is already the basis for the fire-protection requirement of the GL.

In the past we have raised five related issues. The staff indicated that it would provide a response to these issues in the near future. In addition, we would like to be kept informed on the status of the follow-up study that the staff intends to perform on the issue of the control of switchyard and grid activities with the plant operating at power.

We expect to comment on the proposed final version of this GL after public comments have been reconciled.

Sincerely,

David A. Ward, Chairman
Advisory Committee on Reactor Safeguards

1. Memorandum (Undated) to Holders of Operating Licenses or Construction Permits for Light-Water Power Reactors, Subject: Resolution of Issues Identified in the NRC Staff's Evaluation of Shutdown and Low-Power Operations Pursuant to 10 CFR 50.54(f) (Generic Letter 92-XX), transmitted by memorandum dated August 6, 1992 from Gary M. Holahan, Office of Nuclear Reactor Regulation, NRC, for Raymond F. Fraley, ACRS
2. U. S. Nuclear Regulatory Commission, NUREG-1449, "Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States," Draft Report, February 1992

3. Letter dated April 9, 1992, from David A. Ward, Chairman, ACRS, to James M. Taylor, Executive Director for Operations, NRC, Subject: Evaluation of the Risks During Shutdown and Low-Power Operations for U.S. Nuclear Power Plants
4. Letter dated August 13, 1991, from David A. Ward, Chairman, ACRS, to James. M. Taylor, Executive Director for Operations, NRC, Subject: Evaluation of Risks During Low Power and Shutdown Operations of Nuclear Power Plants

---

September 17, 1992

Mr. James M. Taylor
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Mr. Taylor:

SUBJECT: GENERAL ELECTRIC NUCLEAR ENERGY POWER UPRATE PROGRAM/FERMI, UNIT 2 POWER INCREASE REQUEST

During the 389th meeting of the Advisory Committee on Reactor Safeguards, September 10-12, 1992, we reviewed the General Electric Nuclear Energy (GE) generic program supporting power uprates for operating boiling water reactors (BWRs), and the associated application of the Detroit Edison Company (DECo) for a power level increase for the Fermi, Unit 2 nuclear power plant. The Committee was initially briefed on this matter during its 384th meeting (April 2-4, 1992). Our Subcommittee on Thermal Hydraulic Phenomena held meetings on March 26 and August 18, 1992, to review this matter. During this review, we had the benefit of discussions with representatives of the NRC staff, GE, and DECo. We also had the benefit of the documents referenced.

DECo has requested an amendment to its technical specifications to increase the licensed thermal power limit from 3293 MWt to 3430 MWt, a 4.2 percent increase. This request is based on the generic BWR power uprate program developed by GE. For this program, the staff has limited the core power increase to no more than 5 percent. Licensees for twenty BWR units have expressed interest in similar power uprates pursuant to this generic program. The DECo uprate request represents the lead plant effort.

Nine U.S. BWR units are licensed to operate at the uprated power and, as a result, there are 229 reactor-years of operational experience. Many BWRs have the capability to increase core power well beyond the 5 percent limit assigned to the GE generic uprate program at this time. Power increases of 15-20 percent have already been accomplished at BWR nuclear power plants located overseas, albeit at some additional hardware expense. The Fermi

plant will still have at least an additional 5-10 percent margin in its safety systems (using their design basis) following adoption of this uprate.

We concur with the staff's conclusion that there is reasonable assurance that the health and safety of the public will not be endangered by the proposed power uprates, and that DECo should be issued its requested amendment. We commend the staff, DECo, and GE for a job well done. The detail in the staff's analysis represents a thorough safety evaluation and clearly supports its conclusions. We do, however, offer the following comments for consideration.

During this review, it came to our attention that the design basis for plant equipment is used in analyses supporting determination of safety margins. This is done in spite of demonstrated substantial equipment performance margins. This is an example of unnecessarily compounded conservatism. Safety margins should be determined using actual data, when available.

During the August 18, 1992 subcommittee meeting, GE presented the results of calculations with a computer code (SHEX) that was not known to us. Had these calculations not been peripheral to the main topic of the meeting, we would have been required to delay the review process. We recommend that whenever the industry or staff plans to discuss the results of calculations performed by a computer code that we have not reviewed, advance notice be given to us and if necessary the computer code documentation be made available to us before the presentation.

We see no need for further Committee review of the present GE power uprate program and associated plant-specific applications for power level increases of no more than 5 percent. The Committee does request, however, that it be afforded the opportunity to review any requests for core power increases in BWRs that go beyond the 5 percent power increase addressed in this letter.

Sincerely,

David A. Ward, Chairman
Advisory Committee on Reactor Safeguards

References:
1. GE Licensing Topical Report, NEDC-31897P-1, "Generic Guidelines for General Electric Boiling Water Reactor Power Uprate," June 1991 (Proprietary Information)
2. GE Licensing Topical Report, NEDC 31984P, "Generic Evaluations of General Electric Boiling Water Reactor Power Uprate," Volumes 1 and 2, July 1991 and Supplement 1 dated October 1991 (Proprietary Information)

3. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to Amendment No. 87 to Facility Operating License No. NPF-43, Detroit Edison Company Fermi-2, Docket No. 50-341," received September 11, 1992
4. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of Nuclear Reactor Regulation Concerning General Electric Licensing Topical Report NEDC-31984P, Generic Evaluations of General Electric Boiling Water Reactor Power Uprate," Volumes I and II (undated), received August 11, 1992
5. General Electric Company Response to Issues Raised by the ACRS Regarding Generic BWR Power Uprate Program (undated), received August 11, 1992 (Proprietary Information)
6. Memorandum dated July 6, 1992, from Detroit Edison Company for U.S. Nuclear Regulatory Commission, "Detroit Edison Response to Issues Raised by the Advisory Committee on Reactor Safeguards (ACRS) Regarding Fermi 2 Power Uprate Program Submittal (TAC No. M82102)" (Proprietary Information)
7. SECY-91-401, dated December 12, 1991, from James M. Taylor, Executive Director for Operations, NRC, for the Commissioners, Subject: Generic Boiling Water Reactor Power Uprate Program