



UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

ACRSR-1555

PDR

February 17, 1994

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

Dear Chairman Selin:

SUBJECT: DIVERSITY

On occasion the NRC staff has proposed, and in some cases either formally or informally mandated, the use of some form of diversity as a protection against conjectured common-cause failures in redundant components or systems. In some cases this requirement has been deemed met by the use of different manufacturers of identical systems, in others functional diversity has been required, and in still others differences in design, personnel or physical principles have been required. In some of our memories the issue dates back to the subject of Anticipated Transients Without Scram, while others' memories are longer. Our most recent encounters have been in the contexts of digital controls and of water-level indicators for boiling-water reactors. The staff argument has been that hypothetical and otherwise unidentified common-cause failures are more likely to afflict identical than dissimilar systems, so that diversity per se is almost axiomatically a safety benefit. Though the argument has an incontestably solid core, we don't recall any case in which it has been quantified beyond that point.

The Commission has long been challenged by the problem of determining the proper level of safety to be reasonably required of the nuclear power industry, and the 1986 Safety Goal Policy Statement made explicit what had long been recognized—that a policy that demands any improvement in safety simply because it is an improvement is both unwise and unsupportable. The Safety Goals made explicit statements about the Commission's intent, and the subsequent crystallization of the Commission's Backfit Rule dealt with the guidelines for safety improvements beyond the "adequate safety" criterion. Continuing the same trend, the Commission is now engaged in a long-term metamorphosis into a risk-based regulatory agency, meaning that regulatory decisions will be, in the end, justified in terms of their expected impact on the health and safety of the public and the workers. Implementation of this grand strategy requires both the will and the capability to analyze regulatory proposals for their consistency with the policy, which

9403040346 940217
PDR ACRS
R-1555 PDR

RS01
1/0

in turn requires increased reliance on analytical methods of risk assessment. It is precisely at that point that the diversity arguments always seem to fall short.

Of course we do not argue that diversity is always bad—only that a diversity requirement imposed by the NRC demands more justification than a flat assertion that diversity is desirable in the abstract. In any specific case the detailed arguments may force the conclusion either way, but the outcome cannot be known in advance, without analysis. The argument that analysis is not needed because there may be unspecified common-cause accidents for which diversity might be beneficial is inconsistent with the Commission's policies mentioned above.

Now we turn to a more-or-less random list of circumstances in which diversity has a negative safety impact, also in the abstract, just to provide a counterpoint to the assertion that it is always good. As we have said, the essence of rational regulation in the interest of public safety requires that, in each case, the advantages and disadvantages of a diversity requirement be weighed against each other, and the winner judged against the higher standards of either "adequacy" or the cost-benefit criteria of the Backfit Rule, as appropriate.

It is almost never true that a requirement for diversity will result in diverse instruments, components, or systems that are equally reliable. Since it would make little sense to choose the inferior of two options for the primary system, diversity will necessarily require a known and intended sacrifice in component reliability, in return for protection against hypothesized common-cause failures. Should an elevator be held up by a steel cable and a backup Manila rope? Should an airplane have a piston engine to back up its jet engines? Those are farcical cases, but the question of whether a steam-driven pump should back up an electrically driven pump addresses a known potential common-cause failure, and may yield a different answer.

Diversity increases risk by increasing complexity—simplicity is usually a safety advantage. This effect shows up through the availability, stocking, and interchangeability of parts, proliferation of operational and maintenance manuals, training of operational and maintenance personnel, interpretation of symptoms in an upset condition, a larger variety of failure modes and effects, unfamiliarity with the characteristics of the backup system if it is normally held in reserve, and so forth. There have been many industrial accidents in which complexity has introduced confounding factors that either caused or exacerbated the accident.

Diversity introduces new accident paths, and introduces components whose reliabilities are likely to be less well known than that of the primary component. Accident analysis, and therefore plant

February 17, 1994

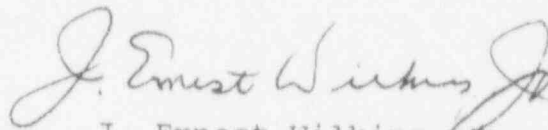
design, becomes more difficult as one has to deal with a greater variety of potential upset paths.

When dealing with diverse or redundant sensing systems, one has always to resolve the issues of voting logic. There can be few more perilous conditions than to have comparably credible instruments that disagree. The questions of voting logic for diverse combinations of instruments are far more subtle and deep than the simple considerations that go into the traditional nuclear voting logic. Many accidents in other industries have been compounded by inappropriate voting logic.

We offer this list simply to counter the staff's apparent mindset (evident in many places) that diversity is always a desirable system attribute. As we move in fits and starts, but inevitably, toward some form of risk-based regulation, it is incumbent on the staff to make a balanced case for any diversity requirement it seeks to mandate, on the merits. We wish only to supply some of the cons that must be balanced against the pros, so the outcome is not decided by slogan.

We seek no action through this letter, only increased sensitivity of both the Commission and the staff to the fact that it is all too easy to oversimplify the case for diversity.

Sincerely,



J. Ernest Wilkins, Jr.
Chairman