NRC Research and/or Technical Assistance Rept

PDR

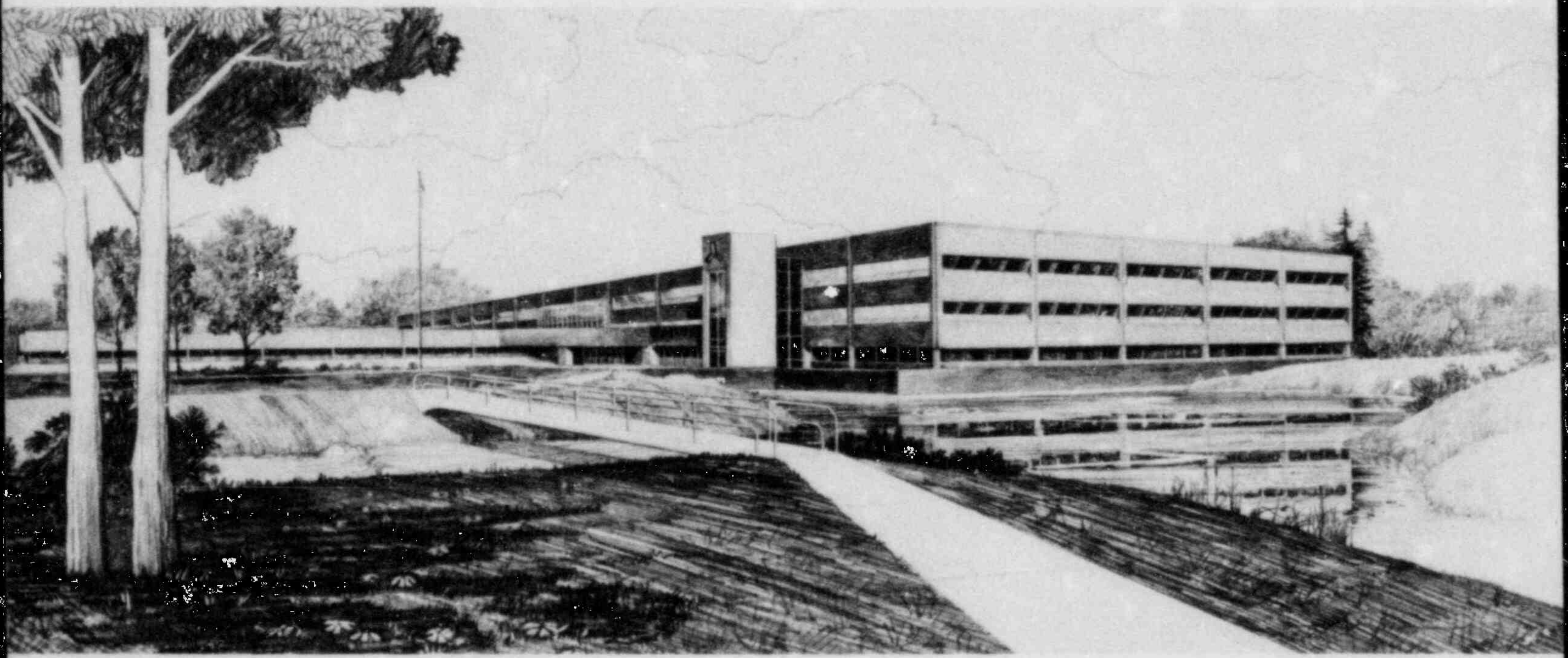
EGG-EE-6060

September, 1982

PRELIMINARY ASSESSMENT OF BACKFITTING CRITERIA FOR DIGITAL CONTROL AND PROTECTION SYSTEMS (TASK 6)

N. Wilde

Idaho National Engineering Laboratory
Operated by the U.S. Department of Energy



This is an informal report intended for use as a preliminary or working document

Prepared for the
U. S. NUCLEAR REGULATORY COMMISSION
Under DOE Contract No. DE-AC07-76ID01570
FIN No. A6370

EG&G Idaho

EG&G Idaho, Inc

FORM EG&G-398
(Rev 03-82)

INTERiM REPORT

Accession No. ______________

Report No. EGG-EE-6060

Contract Program or Project Title:

Research To Assess Microprocessor-Based System Design and Plant Control And Associated Isolation Devices

Subject of this Document:

Preliminary Assessment of Backfitting Criteria for Digital Control and Protection Systems (Task 6)

Type of Document:

Technical Report

Author(s):

N. Wilde

Date of Document:

September 30, 1982

Responsible NRC Individual and NRC Office or Division:

This document was prepared primarily for preliminary or internal use. It has not received full review and approval. Since there may be substantive changes, this document should not be considered final.

EG&G Idaho, Inc.
Idaho Falls, Idaho **83415**

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C.
Under DOE Contract No. **DE-AC07-76ID01570**
NRC FIN No. A6370

INTERIM REPORT

CONTENTS

ABSTRACT

This EG&G Idaho, Inc. interim report identifies the issues and scopes the problems associated with using programmable digital computers for backfitting nuclear power plants.

FIN No. A6370

1. TASK DESCRIPTION

The NRC Office of Nuclear Regulatory Research has authorized EG&G Idaho to conduct a research project entitled Research to Assess Microprocessor-Based System Design and Plant Control and Associated Isolation Devices. The NRC Form 189 description of the objective of proposed work is:

> This research project is concerned with the potential safety issues associated with programmable, digital, computer-based nuclear plant control and protection systems and with the adequacy of isolation methods in nuclear power plants.
>
> The use of programmable, digital, computer-based systems in plant control and protection systems represents a major departure from the systems which have been used in the past. The regulatory requirements currently in use were developed prior to the use of stored program systems for reactor control and protection functions. For these reasons, the Nuclear Regulatory Commission (NRC) needs to determine the safety issues and develop criteria which are applicable to these new systems.
>
> Isolation devices are used to prevent failures from propagating between systems. No Regulatory Guide (RG) currently exists to provide standards for these devices. The NRC needs to determine the adequacy of current isolation devices and to provide an adequate criterion which assures an acceptable level of isolation.

Task 6 of this project is entitled Backfitting Criteria. The object of this task is to ". . . develop a proposed criterion for the evaluation of retrofitting or backfitting from analog to digital systems for reactor control and protection systems." The FY-1982 effort was limited to identifying issues and scoping the Task. This report is the result of the FY-1982 effort. In FY-1933. the need and nature of criteria will be studied. Assuming that special criteria are necessary, the FY-1984 task will be the drafting of backfitting criteria. The draft will be written in an interactive process with NRC and industry representatives acting as contributors and reviewers.

2. REVIEW OF REGULATORY LITERATURE

A review of regulations, guides and standards was conducted to locate items related to backfitting in gene:al and digital devices specifically. In addition, detailed discussions were held with several engineers who are knowledgeable and currently active in applying regulatory criteria. These engineers are well versed in both analog and digital systems. The results of this review are now presented.

The Code of Federal Regulations (10 CFR 50.109)[1] gives the NRC authority to require backfitting of a facility. The regulation reads as follows:

BACKFITTING

50.109 Backfitting.

a. The Commission may, in accordance with the procedures specified in this chapter, require the backfitting of a facility if it finds that such action will provide substantial, additional protection which is required for the public health and safety or the common defense and security. As used in this section, "backfitting" of a production or utilization facility means the addition, elimination or modification of structures, systems or components of the facility after the construction permit has been issued.

b. Nothing in this section shall be deemed to relieve a holder of a construction permit or a license from compliance with the rules, regulations, or orders of the Commission.

c. The Commission may at any time require a holder of a construction permit or license to submit such information concerning the addition or proposed addition, the elimination or proposed elimination, or the modification or proposed modification of structures, systems or components of a facility as it deems appropriate.

[35 FR 5318, March 31, 1970]

As a result of the TMI accident, a number of backfitting changes are being required by the NRC. To avoid undue expense to the utilities, these requirements are subjected to two conditions on an individual plant bases. The first is a cost-vs-risk consideration. NUREG-0737[2] is the document describing the required changes and includes the following condition:

> It is expected that the requirements contained herein will be met. However, it is recognized that licensees have proceeded with implementation of some of these items prior to issuance of these clarifying criteria. The staff will consider requests for relief from various aspects of these criteria. Such requests should explain the need for relief, include a clear description of design features of the proposed installation, and provide a safety rationale supporting the adequacy of the proposed installation. A licensee or applicant seeking relief from any element of our criteria should submit a request for relief, along with supporting justification, in response to this letter.

This allows due consideration to be given not only to the direct cost of backfitting but also to the indirect factors of (1) cost and inconvenience of downtime, (2) cost of operations and maintenance, (3) training for a new system, and (4) safety aspects of installation (for example, human risk due to radiation exposure).

The second condition is a grandfather clause. Older plants will be evaluated by older standards. This condition is covered in NUREG-0588.[3]

> Certain modifications and clarifications to the positions as a result of the TMI-2 event are anticipated, as, for example, in radiation source term requirements described in the staff responses to some of the public comments. In the interim, however, and until the final rule is established, the staff requires that all plants licensed after May 23, 1980 conform to NUREG-0588. In accordance with Regulatory Guide 1.89, all Operating Licenses for facilities whose Construction Permit SER is dated July 1, 1974, or later will be reviewed against IEEE Standard 323-1974. Thus for these licensees, the Operating License applicant is required to qualify equipment to the Category I requirements in NUREG-0588. For Operating Licenses issued after May 23, 1980, whose Construction Permit SER is dated before July 1, 1974, the Operating License applicant is required to qualify equipment to at least Category II requirements in NUREG-0588--unless the licensee made commitments in the Construction Permit application to use the 1974 standard, or unless the Operating License application indicates that the 1974 standard is to be used. In such cases, Category I requirements of NUREG-0588 are to be used. In addition, all parts used to replace installed equipment shall also be qualified to the Category I requirements unless adequate bases are established to justify exceptions.

Category I applies to equipment qualified in compliance with IEEE Standard 323-1974 and is the more stringent requirement. Typical of these requirements are stand-by power sources, redundant channels and similar high reliability features. Category II equipment requirements are less stringent and must comply with IEEE Standard 323-1971.

These three documents establish that the NRC can require backfitting subject to a cost-vs-risk consideration and a grandfather clause. This means that mandated backfitting may well be customized on an individual plant bases. Utility originated backfits would be reviewed with respect to public health and safety on an individual case. It is intended that the NUREGs treat generic problems only, not specific cases.

The literature review included a search for technical items specific to programmable devices and computers. The only item found was in Regulatory Guide 1.97[4] which describes the regulatory position on accident-monitoring instrumentation.

1.3.1 Design and Qualification Criteria--Category I

a. The instrumentation should be qualified in accordance with Regulatory Guide 1.89, "Qualification of Class 1E Equipment for Nuclear Power Plants,: and the methodology described in NUREG-0588, "Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment." Qualification applies to the complete instrumentation channel from sensor to display where the display is a direct-indicating meter or recording device. Where the instrumentation channel signal is to be used in a computer-based display, recording, and/or diagnostic program, qualification applies from the sensor to and includes the channel isolation device. The location of the isolation device should be such that it would be accessible for maintenance during accident conditions.

Part b continues with a discussion of single failures and the use of redundant and diversed instrument channels and concludes with:

> "At least one channel should be displayed on a direct-indicating or recording device."

These criteria require an analog channel to be qualified from sensor to analog read-out device. If one or more channels feed a computer-based system, there will be an isolator at the input of the computer-based system and only the analog portion from sensor to isolator need be qualified. However, there must still be at least one completely qualified analog channel in parallel.

Regulatory Guide 1.97 is presently being revised. It is not known if the preceeding criteria will be effected.

Adams and Rohrdanz[5] have summarized the current NRC review methods and status. The review of two computer-based systems were reported in detail. The first is the combustion Engineering Core Protection Calculator System. The NRC review is reported in NUREG-0308.[6] The second system is the Westinghouse RESAR-414 Integrated Protection System and the NRC review is reported in NUREG-0493.[7] The criteria for evaluating these systems were (1) "engineering judgment" and (2) the "audit principle". The experience gained from these earlier evaluations can contribute greatly to the development of criteria.

3. CLASSES OF BACKFITTING

In this report, backfitting is defined as the process of up-grading or up-dating plant instrumentation and control systems by replacing analog equipment with digital equipment. This type of backfitting can be subdivided into three classes:

1. Single Function Backfitting

2. Multiple Function Backfitting

3 New Function Backfitting.

These classifications are not intended to be final and certainly are not all inclusive. Conceivably, there are backfitting activities which will not clearly fit into one of the three classes.

Single Function Backfitting

This is the process of replacing one piece of equipment with another. The function being performed remains unchanged. The number of inputs and the electrical properties of inputs and outputs remain unchanged. The power requirements are compatible with existing power sources and the new equipment can operate in the existing environment. In other words, it is a one-to-one replacement which meets the specification of the function to be performed under the conditions imposed.

In the area of reliability, it must be determined that the following statistics for the new unit are acceptable.

1. Reliability--The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

2. Availability--The characteristic of an item expressed by the probability that it will be operational at a randomly selected future instant in time.

3. Others of importance (i.e., maintenance impact, common-mode failures, etc.).

Analysis such as the single failure analysis, failure mode and effect analysis, fault tree analysis and others will probably not be effected in a one-to-one replacement. However, it would be prudent to check these analysis.

If the reliability statistics of the replacement unit are known and the unit meets the functional and operational specifications, the exact technical nature or even the technology used at the sub-unit level is immaterial. In fact this lack of detailed technical knowledge is a rather common situation with such hardware devices as integrated circuits, micro-electronics and encapsulated circuits. Many times this knowledge is unavailable because it is proprietary information. In the same sense, programmable digital devices having known functional and operating specifications and known reliability statistics do not require hardware/software evaluation. If it is known by previous evaluation and/or past experience that the software reliably performs the intended function, then there is no need for a software evaluation. However, if these characteristics are not known, then they must be determined by one or more of the following:

1. By examination and analysis of the details of the device

2. By applying tests which measure the characteristics of the device, i.e., verification of performance and application of stress to enable prediction of reliability.

3. By an analysis of field data on this device or similar devices.

Multiple Function Backfitting

The second class of backfitting consists of replacing equipment such that functions are combined. A given piece of equipment now performs several functions. The functions are combined in the sense that they are being operated upon by some common device such as a microprocessor. All of the considerations for a single function backfitting apply. However, the act of combining functions can result in two new problem areas. The first problem concerns the need for sufficient isolation between functions to avoid interference or propagation of failures. Functional isolation eventually translates to hardware and/or software isolation. As an example, data isolation can be achieved by using two data buses or by the software-controlled time-multiplexing of a single data bus.

The second problem is the increased probability of common mode failure. This is a failure which can disable more than one function at a time. A hardware failure of the multiplexed data bus can effect all functions using the bus.

The techniques of evaluating these problem areas already exist but may have to be reapplied to new systems. This includes determination of characteristics as described in the previous section as well as application of present probability risk assessment techniques.

New Function Backfitting

The third and last class of backfitting covers replacement of old functions and equipment with new functions and equipment. The magnitude of this change may be that the old performance characteristics and reliability analysis are no longer applicable to the new functions and equipment. Hence, the system must be treated as a new system with an entirely new reliability evaluation. The use of a computer in this type of backfitting may well require the development of new analysis techniques. This class of backfitting will probably be more common then the first two classes.

4. EVALUATING BACKFITTING

When evaluating hardware for a given application, it is recognized that there is no such thing as failure-free hardware. Methods have been developed to reduce the probability of a failure to an acceptable level. These methods include redundancy, diversity, fault-tolerant designs, quality assurance in manufacturing and probablistic risk assessment in analysis.

The consideration of computers introduces a new component into the system software. Unfortunately, there is no practical way of guaranteeing "bug-free" software any more than there is a practical way of guaranteeing failure-free hardware. For software, it would appear that the approach should parallel the approach for hardware. Methods are needed to reduce the probability of a failure to an acceptable level. The methods presently being used and under development are conceptually similar to the hardware methods. One of the major advantages of software (programmable) devices is that they can be programmed to check themselves. Both software and hardware can be checked.

When first approaching the application of computers, it is a natural tendency to want to separate the application into software and hardware in order to make the work more manageable. However, after some consideration it becomes apparent that software and hardware are so highly interactive that total separation is impractical. The application must be approached from a systems or functional point of view.

There is a second point to consider. Any evaluation method based on present software characteristics or techniques, may well become outdated before it is perfected. Software technology and development are expected to experience dramatic changes in the near future. The reasons for the changes are the high cost of the labor, intensive programming activity and the anticipated shortage of programmers. New methods are being developed to minimize these problems.

A suggested approach to evaluating computer related backfitting is based on systematic engineering design. Typically, there are five phases:

1. Statement of Objectives

2. Specification Development

3. Implementation

4. System Test

5. Installation and Final Test.

The evaluation method consists of asking various questions related to each phase.

The first phase, Statement of Objectives, is evaluated by examining the documentation to see if the objectives are valid, safe and applicable. Have emergency situations been covered? Has the problem been adequately defined? Have the right functions been selected?

The second phase, Specification Development, is evaluated to determine if the specified system will perform the functions previously described. Do the hardware/software trade-offs represent good engineering practices? Has the "right software" been specified? Have systems been isolated? Does the system meet its intended objectives?

The third phase, Implementation, includes the hardware design and construction phases as well as the software design and coding phase. Both preliminary hardware and software debugging take place here.

The fourth phase is System Testing. The results of the final testing are evaluated to assure that the intended functions are being performed. It is the proof-of-performance test derived from the original phase two specifications. It should answer the question, "How do we know that the system will do the right thing especially in an emergency?"

The test results from phase five, Installation and Final Test, are reviewed as a final check to see that everything is as intended. Does it meet its performance requirements?

Three on-going activities which parallel these five phases are (1) the management function of planning and control, (2) the reliability function of quality assurance and probability risk assessment and (3) the documentation function. The reliability document is of major interest and must be reviewed for compliance.

5. QUESTIONS TO BE ANSWERED

The previous discussions raise a number of questions. It is the intent of this section to phrase the questions and present a short discussion of each for the purpose of clarification. It is not the intent of this section to answer these questions. Seeking answers to the questions may represent areas of future work. Following is a list of the questions.

1. Are backfitting criteria needed?

It is not clear why backfitting criteria are needed. What is unique about backfitting that requires special criteria? With respect to the use of computers, how should these criteria differ from digital system design criteria?

2. What is the intended application and who is the intended user of the criteria?

The criteria could be intended for guidance by utilities and their suppliers when backfitting. In this case, the criteria would specify requirements to be met. On the other hand, the criteria could be intended for those individuals who evaluate backfitting designs. Now the criteria should present methods of evaluating computer-based systems to determine if compliance has been met. The nature of these two criteria are different.

3. In backfitting from analog to digital systems, should the analog system be used as the reference baseline?

The performance of the digital system can be compared to the analog system it is replacing and an evaluation made as to its performance. It may not be as good or it may be better. It may also be different such as performing logical functions that were not done by the analog system. Maybe the baseline reference should be the function required rather than the analog system.

4. Hcw does the criteria for backfitting differ from the criteria for new plant design?

In a new plant, a component cannot be compared to its predecessor since it doesn't exist. The comparison must be made to the function to be performed. If backfitting were also compared to the function to be performed, there would appear to be no difference, at least in concept.

5. Should criteria be generic or specific when addressing programmable devices and their software?

Any specific hardware/software specifications which ties criteria to the state-of-the-art and must be changed when technology advances. However, generic specifications with respect to softwarc are not well defined at this time.

6. Are there more items in the NRC literature which would influence the use of computers?

The preliminary literature search conducted for this report was not intended to be final. More literature search may be needed.

6. CONCLUSIONS AND RECOMMENDATIONS

The preliminary review of regulatory literature did not reveal any backfitting criteria directed specifically at analog systems. Since analog systems do not require extra backfitting criteria, why should digital? What is unique about digital systems that would require special backfitting criteria. When the technical state-of-the-art of instrumentation and control systems is changing as rapidly as it is today, there would appear to be a hazard in relating criteria to technical characteristics. The hazard is having constantly obsolete criteria. It is preferable to have these criteria describe the function to be performed and the reliability level to be achieved. Criteria should address "what" is to be accomplished rather than "how" to accomplish it. Also, criteria should be viewed as establishing minimum acceptable levels thus permitting and even encouraging higher levels of performance.

The real problem with implementation of new technology is developing evaluation methodology to determine compliance of systems with the functional criteria. How do we know that a system employing some new technology is indeed meeting the intent of the criteria? It is the evaluation methodology that should be changing to match the changes in new technology.

A recommended program would be as follows:

1. Determine if a digital backfitting guidance criteria is needed. If the answer is yes, then determine how it may differ from <u>or</u> be integrated with the other task in this project and then proceed with the criteria development.

2. If a backfitting guidance criteria is <u>not</u> needed, then the efforts of this task should be redirected towards developing a compliance methodology. A method for showing compliance of

hardware/software microprocessor system with functional and reliability criteria is definitely needed. This method must be based on current and near-future technology. The first step would be defining this effort.

7. REFERENCES

1. 10 CFR 50.109, Code of Federal Regulations, Title 10-Energy, Chapter 1-Nuclear Regulatory Commission (NRC).

2. NUREG-0737, Clarification of TMI Action Plan Requirements, USNRC, November 1980.

3. NUREG-0588, Interim Staff Position on Environmental Qualification of Safety-Related Electric Equipment, USNRC, July 1981.

4. USNRC Regulatory Guide 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, NRC, December 1980.

5. Adams, D. M., Rohrdanz, R. R., Preliminary Assessment of Design Issues Related to the Use of Programmable Digital Devices for Safety and Control Systems, (Draft), EG&G Idaho, Inc., July 1982.

6. NUREG-0308, Safety Evaluation Report Related to Operation of Arkansas Nuclear One, Unit 2, USNRC, November 1977.

7. NUREG-0493, A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System, USNRC, March 1979.