

OAK RIDGE NATIONAL LABORATORY LIBRARIES



3 4456 0604237 8



CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

OAK RIDGE NATIONAL LABORATORY

operated by
UNION CARBIDE CORPORATION

for the
U.S. ATOMIC ENERGY COMMISSION

1

ORNL-NSIC-51

UC-80 — Reactor Technology

DESIGN PRINCIPLES OF REACTOR PROTECTION INSTRUMENT SYSTEMS

S. H. Hanauer

C. S. Walker

OAK RIDGE NATIONAL LABORATORY
CENTRAL RESEARCH LIBRARY
DOCUMENT COLLECTION

LIBRARY LOAN COPY

DO NOT TRANSFER TO ANOTHER PERSON

If you wish someone else to see this
document, send in name with document
and the library will arrange a loan.

UCN-7969
13 3-67

NUCLEAR SAFETY INFORMATION CENTER

NSIC

Printed in the United States of America. Available from Clearinghouse for Federal
Scientific and Technical Information, National Bureau of Standards,
U.S. Department of Commerce, Springfield, Virginia 22151
Price: Printed Copy \$3.00; Microfiche \$0.65

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

- A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or
- B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

Contract No. W-7405-eng-26

Nuclear Safety Information Center

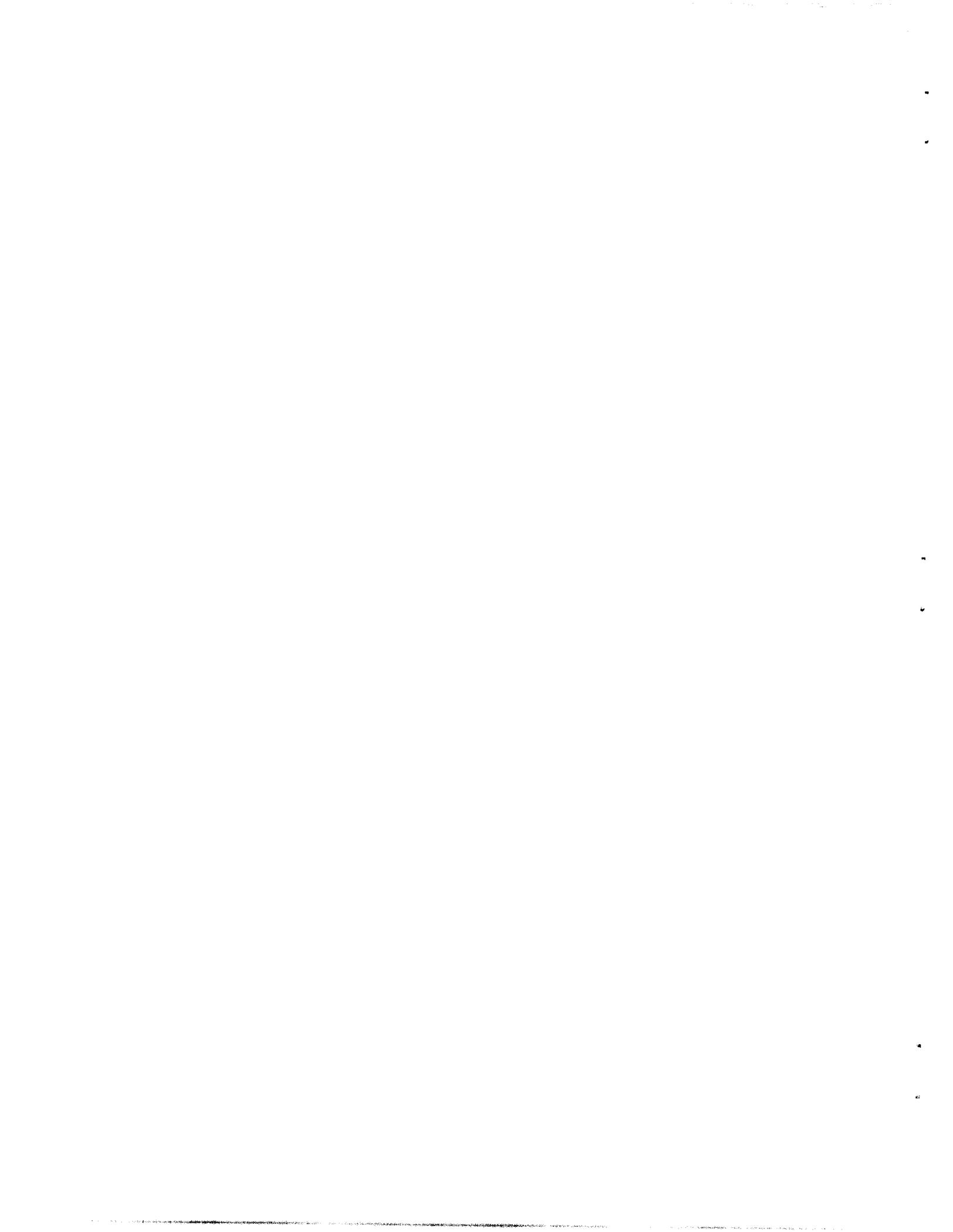
DESIGN PRINCIPLES OF REACTOR PROTECTION INSTRUMENT SYSTEMS

S. H. Hanauer
Department of Nuclear Engineering
University of Tennessee

C. S. Walker
Instrumentation and Controls Division
Oak Ridge National Laboratory

SEPTEMBER 1968

OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee
operated by
UNION CARBIDE CORPORATION
for the
U.S. ATOMIC ENERGY COMMISSION



FOREWORD

Despite the great concern for nuclear reactor safety, the safety research now under way, and the efforts at nuclear facility standardization, there is a surprising dearth of information and lack of agreement on the requirements of reactor protection instrument systems. This document establishes and justifies a consistent set of principles for the design of such systems. These principles are based on the combined knowledge and experience of two of the foremost experts in this country on the subject, S. H. Hanauer of the University of Tennessee's Department of Nuclear Engineering and C. S. Walker of ORNL's Instrumentation and Controls Division. It is too much to expect that all persons concerned with the design and/or operation of reactor protection instrument systems will accept all the principles outlined herein. On the other hand, if one accepts the initial objectives it is virtually impossible to escape the logic developed in the remainder of the report. It is our hope that the problem and the principles so convincingly discussed in this report will provide a needed impetus in the development of criteria which will then lead to the development of definitive standards which are now so sorely needed by reactor designers.

Wm. B. Cottrell, Director
Nuclear Safety Program



PREFACE

The Nuclear Safety Information Center was established in March 1963 at the Oak Ridge National Laboratory under the sponsorship of the U.S. Atomic Energy Commission to serve as a focal point for the collection, storage, evaluation, and dissemination of nuclear safety information. A system of keywords is used to index the information cataloged by the Center. The title, author, installation, abstract, and keywords for each document reviewed is recorded on magnetic tape at the central computer facility in Oak Ridge. The references are cataloged according to the following categories:

1. General Safety Criteria
2. Siting of Nuclear Facilities
3. Transportation and Handling of Radioactive Materials
4. Aerospace Safety
5. Accident Analysis
6. Reactor Transients, Kinetics, and Stability
7. Fission Product Release, Transport, and Removal
8. Sources of Energy Release Under Accident Conditions
9. Nuclear Instrumentation, Control, and Safety Systems
10. Electrical Power Systems
11. Containment of Nuclear Facilities
12. Plant Safety Features
13. Radiochemical Plant Safety
14. Radionuclide Release and Movement in the Environment
15. Environmental Surveys, Monitoring and Radiation Exposure of Man
16. Meteorological Considerations
17. Operational Safety and Experience
18. Safety Analysis and Design Reports
19. Bibliographies

Computer programs have been developed that enable NSIC to (1) produce a quarterly indexed bibliography of its accessions (issued with ORNL-NSIC report numbers); (2) operate a routine program of Selective Dissemination of Information (SDI) to individuals according to their particular profile of interest; and (3) make retrospective searches of the references on the tapes.

Other services of the Center include principally (1) preparation of state-of-the-art reports (issued with ORNL-NSIC report numbers); (2) cooperation in the preparation of the bimonthly technical progress review, Nuclear Safety; (3) answering technical inquiries as time is available, and (4) providing counsel and guidance on nuclear safety problems.

Services of the NSIC are available without charge to government agencies, research and educational institutions, and the nuclear industry. Under no circumstances do these services include furnishing copies of any documents (except NSIC reports), although all documents may be examined at the Center by qualified personnel. Inquiries concerning the capabilities and operation of the Center may be addressed to

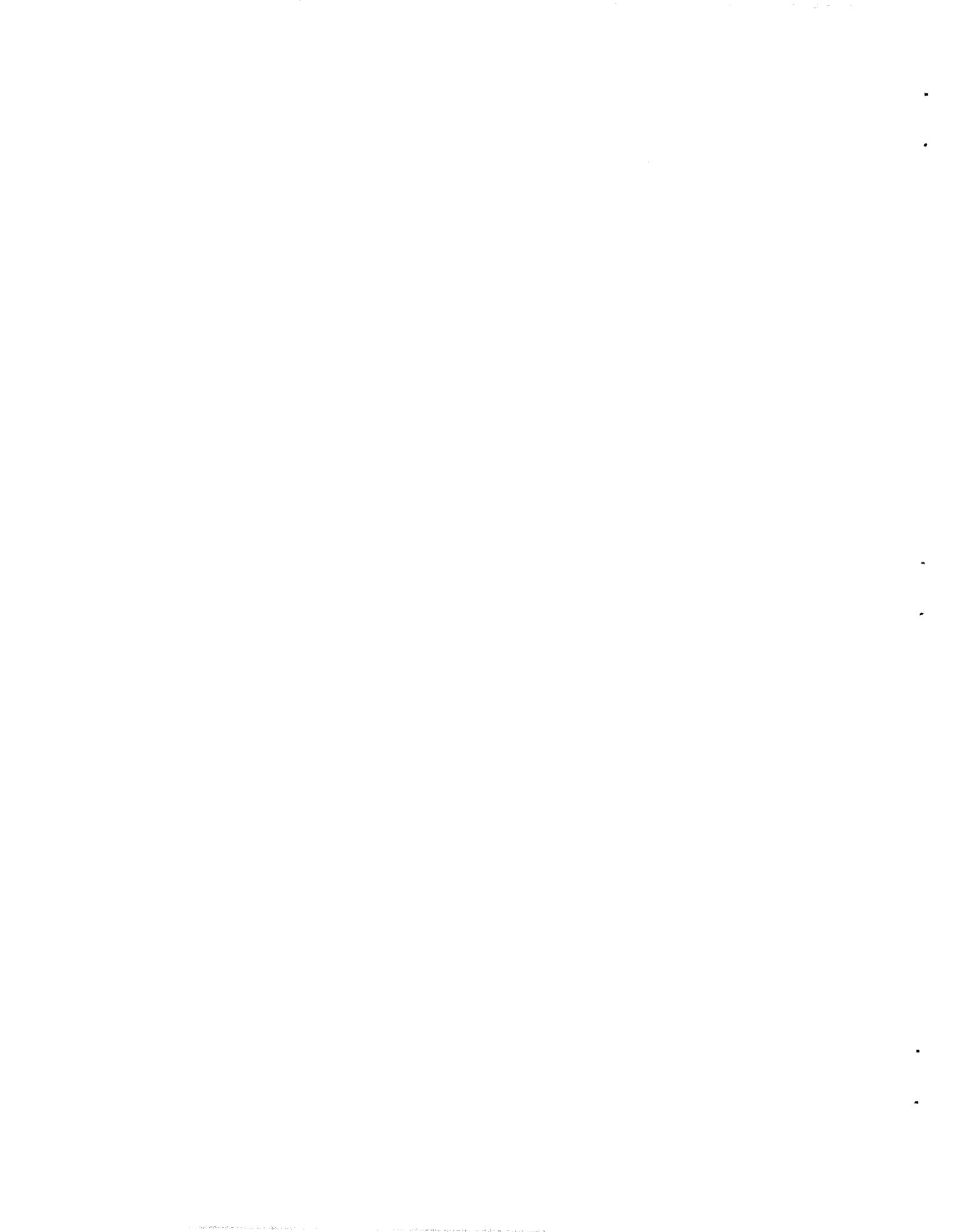
J. R. Buchanan, Assistant Director
Nuclear Safety Information Center
Oak Ridge National Laboratory
Post Office Box Y
Oak Ridge, Tennessee 37830
Phone 615-483-8611, Ext. 3-7253
FTS 615-483-7253

CONTENTS

| | <u>Page</u> |
|---|-------------|
| ABSTRACT | xi |
| 1. SUMMARY | 1 |
| 2. INTRODUCTION | 5 |
| 2.1 Definition of Protection System | 6 |
| 2.2 Scope of Protection System | 7 |
| 2.3 Identification of Components | 10 |
| 2.4 Definition of Operation System | 10 |
| 3. PERFORMANCE AND SYSTEMATIC FAILURES | 12 |
| 3.1 Need for Correct Functioning | 12 |
| 3.2 Reasons for Performance Failures | 13 |
| 3.2.1 Equipment Functioning Impossible | 13 |
| 3.2.2 Equipment Paralyzed by Accident | 13 |
| 3.2.3 Operation Without Protection | 14 |
| 3.2.4 Consequential Failures | 14 |
| 3.2.5 Interaction Between Protection System and Operation System | 14 |
| 3.3 Validity of Instrument Outputs | 14 |
| 3.4 Accuracy of Measurements | 15 |
| 3.5 Speed of Accident and Response Time of Instruments | 16 |
| 3.6 Functioning Under Accident Conditions | 17 |
| 3.6.1 Effect of Accident on Plant Configuration | 17 |
| 3.6.2 Effect of Accident on Instrument Signals | 18 |
| 3.6.3 Instrument Module Behavior in Accident Environment | 19 |
| 3.7 Functioning Under Special Nonaccident Conditions | 21 |
| 3.8 Confirmation of Performance | 22 |
| 4. RELIABILITY AND RANDOM FAILURES | 24 |
| 4.1 Safety and Serviceability | 24 |
| 4.2 Quality of Apparatus | 27 |
| 4.3 Monitoring and Testing | 29 |

| | | |
|-------|--|----|
| 4.4 | Redundancy | 31 |
| 4.5 | Probabilistic Calculation of Reliability | 33 |
| 4.5.1 | Simple Redundancy | 34 |
| 4.5.2 | Coincidence | 38 |
| 4.5.3 | Safety or Danger in Numbers | 41 |
| 4.5.4 | The Meaning of Operating Experience | 43 |
| 4.6 | Channel Independence | 44 |
| 4.6.1 | Interdependence Arising from Common Elements | 45 |
| 4.6.2 | Interdependence Arising from Common Environment | 47 |
| 5. | RELATIONSHIP BETWEEN PROTECTION AND OPERATION SYSTEMS | 48 |
| 5.1 | Interaction Between Need for Protection and Failure Probability | 48 |
| 5.2 | Role of Operation System in Need of Protection | 49 |
| 5.3 | The Consequences of Interdependence | 50 |
| 5.4 | Modes of Interdependence | 51 |
| 5.4.1 | Common Elements | 51 |
| 5.4.2 | Interdependence Arising from Operational Use of Protection Instruments | 53 |
| 5.4.3 | Use of Protection System Signals for Quasi- Protection Functions in the Operation System | 54 |
| 5.4.4 | Identical Devices for Protection and Operation | 56 |
| 5.5 | The Case for Independence | 57 |
| 5.5.1 | Independence of Function in Spite of Interdependence of Equipment | 58 |
| 5.5.2 | Extra Redundancy | 59 |
| 5.5.3 | The Benefits of Interdependence | 59 |
| 5.5.4 | The Benefits of Independence | 61 |
| 6. | THE ROLE OF THE HUMAN OPERATOR IN PLANT PROTECTION | 62 |
| 6.1 | Human Surveillance | 62 |
| 6.2 | Manual Initiation or Inhibition of Protection Action | 64 |
| 6.3 | Other Manual Operations Affecting Safety | 67 |
| 6.4 | Administrative Control of Protection Systems | 68 |

| | |
|---|----|
| 7. CONCLUSIONS | 71 |
| 7.1 Lack of Information | 71 |
| 7.2 Design Criteria | 71 |
| 7.3 Reliability | 73 |
| 8. RECOMMENDATIONS | 74 |
| 8.1 Protection Instruments | 74 |
| 8.2 Criteria | 74 |
| 8.3 Determination of Safe Conditions | 74 |
| 8.4 Performance Testing | 74 |
| 8.5 Reliability | 75 |
| 8.6 Publication | 75 |
| REFERENCES | 76 |
| APPENDIX A. NOMENCLATURE | 81 |
| APPENDIX B. PROPOSED IEEE CRITERIA FOR STANDARD NUCLEAR POWER PLANT PROTECTION SYSTEMS | 87 |



ABSTRACT

The protection instrument system of a reactor includes those assemblies of instruments, and only those, whose failure to function when needed would be intolerable. Instruments and control devices not part of the protection system constitute the operation system. The protection and operation systems should be as nearly independent as possible. Reliability (probability of the system's functioning when called upon) and performance (protection provided when the system functions as designed) are both required of the protection system. Reliability depends on quality, redundancy and independence of redundant devices, testing, and freedom from failures caused by an accident. Performance can be affected by validity of signals, the manner in which an accident develops, effects on instruments of the accident environment, and other design problems. Protection system design criteria are urgently needed. Research, development, and testing related to instruments, system performance, and the prediction and measurement of component and system reliability would enhance the reliability and performance of protection systems and thus augment reactor safety.

1. SUMMARY

A fundamental requirement in any discussion of reactor protection instrument systems is a suitable definition of the subject. Opinions as to what is and what is not part of a protection instrument system have ranged from inclusion of only those devices associated with dropping the safety rods to inclusion of everything that has any bearing, however remote, on safety. Based on some recently established definitions, we state that a system whose failure when needed would be unacceptable should be designated as a protection system. We further state that the protection system should include only the assemblage of instruments whose failure to provide protection when needed is not tolerable.

A companion phrase is needed to refer to all the instrumentation and control devices that are not part of the protection system. We have chosen the term operation system for this purpose.

In this report, we are concerned with the designs of systems rather than with the designs of instruments. Principles for the design of protection systems are necessary, since the field of protection system design is not an established "old art." We do not expect complete agreement with all the principles we have set forth in this report, and we recognize, for example, that the principle of independence of the protection and operation systems discussed in Chapter 5 is not universally accepted.

Both reliability and performance are key elements in protection system design. Reliability is associated with the probability of the system's functioning when called upon; performance is associated with the ability of the system to provide protection when it functions as designed. Performance, then, is not related to the random failure of instruments; rather, it is related to the capability of the system to cope with the accident. We are not aware of any reactor accident in which reliability has been a factor; all known accidents wherein the protection system did not function correctly were the result of inadequate or erroneous performance.

Factors important to performance include the validity and accuracy of sensed variables as indicators of plant condition, the rate and manner in which the accident develops, effects on the instruments of gross variations in the sensed variables or in the physical environment caused by

the accident, and interaction between the protection and operation systems. Demonstration of adequate performance is a difficult task, and the ultimate experimental method would require an accident situation.

System reliability, as distinguished from component reliability, can be enhanced through redundancy. Exploitation of this concept requires independence of the redundant portions of the system. A result of the application of redundancy has been the single-failure criterion. The objective is to prevent any single failure from causing a system failure; however, defining a single failure and determining the limits of the various systems to which the single-failure criterion should be applied is a problem whose solution is still being worked out.

Coincidence can reduce system reliability, but it opens the way to on-line testing and on-line maintenance. Adequate testing and maintenance can increase system reliability far more than any original loss. Both local and general coincidence are found in present designs. Of the two, general coincidence is simpler and is easier to test, but it may not have the desired logical structure.

We wish to emphasize that adequate tests are those that find the first failure that reduces redundancy. The equipment tested should include the entire channel from sensors and input devices to the final actuators. In those cases where the final actuator can be operated without seriously disturbing the plant, the final actuator should be included in the on-line tests.

One of our major concerns is that of the relationship between protection and operation systems. We believe that isolation of these two systems from each other should be maximized. It is essential that no event initiate a situation requiring protection and at the same time cause failure of the protection system.

It has been argued that an extra redundant instrument channel can be used for both operation and safety. For example, four channels would be installed, with one of them furnishing signals to both systems. Failure of the common channel could then be tolerated, since three channels would remain to give protection. We suggest that complete independence of channels is really impossible, and the common channel provides additional potential for reducing the desired independence. In addition,

the remaining channels must have sufficient reliability after failure of the fourth and common channel. We believe the extra channel used in common with the operation system tends to reduce the overall safety.

Another example of an interconnection is that of averaging signals from protection system channels for use in the operation system. Even when isolation amplifiers are used, we remain concerned over the possibility of interaction of the two systems.

The use of a single bus to which all the safety devices are connected provides a possible means for a single failure to inhibit protection system operation. Buses usually have multiple sources of power, and coincidence is sometimes obtained by the requirement to shut off all the sources. A single event, such as the inadvertent connection of a source to such a bus, could prevent protection action.

Loss of the source of energy to instruments is a failure that must be considered. The concept of redundancy and coincidence requires multiple sources of power for the protection instrument system. Probability of a loss of enough of the energy sources to prevent normal protection signals is finite; therefore, we believe that the design should provide that a gross loss of power produces a safety trip of the affected instrumentation.

Techniques and approaches to the design of protection systems are in transition. Protection system design criteria are undergoing both development and change. Although the work on standards by the professional societies and the regulatory criteria of the AEC are inducing better designs, we believe that, in addition, there are at least three other areas that need attention. These are reliability studies, performance testing, and failure studies.

Better test programs are needed to determine the reliability of protection system instruments. Much of the equipment being designed into the newer systems has no past history. Data on failure rates, so vital to the selection of a testing rate, are not available. Standardization of modules, such as amplifiers, trip units, and logic units, could do much to alleviate the magnitude of the testing program. A careful appraisal of the assumptions used in the calculations of reliability is needed, also. The basic assumptions do not all conform to the real world.

A few words of caution regarding operating experience and statistical data seem in order. Operation of a plant for several years with no particular difficulty involving the protection system is not proof that the system is adequate or that good criteria were used in its design. Unfortunately, only the arrival of a sufficient number of events requiring protection can determine the adequacy of the protection system by statistical methods. We hasten to point out that statistics alone are insufficient and that careful analyses of the data so gained, together with judicious interpretations, would be needed in determining whether the system was designed according to sound principles.

Realistic tests to gauge the performance capabilities of protection systems should be carried out. These tests should simulate all the accident conditions associated with the system or subsystems involved. The objective of these tests would be to determine whether an accident could prevent successful operation of the system through some consequential effect.

The first steps in preventing the effects of failures are to recognize and examine possible sources of failures. Sources of failures that are not identified in a review of the design are likely to be found only in a review of an accident. Therefore, we recommend that protection systems be studied in a perverse manner with the intent of finding all possible sources of failures. The more failure possibilities that are found and designed out of the system, the greater is the chance of the system working if needed.

2. INTRODUCTION

Reactor protection instrument systems are notorious for causing trouble, both in plant operation and in regulatory review. This trouble can be taken to indicate that the state of the art of protection system design is not very far advanced. The problem is being intensified by the large increase in the number of reactors built or proposed each year. A trend toward more densely populated sites may also be relevant. On the other hand, some recent standardization activities on the part of the nuclear power industry give some hope that a new attitude toward protection system design may alleviate some of the problems in building, operating, and licensing reactors.

This report is an attempt to review the principles of protection system design. We have chosen to be tutorial, because we believe that the subject needs a systematic exposition. Although we have drawn heavily on experience throughout the industry in formulating the precepts we present, they are ours and do not necessarily represent an industry consensus. In some respects they are controversial; we have tried to indicate opposing views where we believe they should be represented. In some areas, our strictures may seem to be mere platitudes, but we assure you that their repeated violation in the past justifies their present inclusion.

It is often pointed out that the available experience with protection systems has been obtained from production, research, testing, and power reactors mostly of relatively low power and rather ancient design. This is true; it is a matter of some concern to what extent such experience can help in the design and evaluation of present plants. The answer will not be known with any certainty until comparable experience has been gained with the current generation of power reactors. In the meantime, the lessons learned from past experience should be applied to current designs as appropriate. In our opinion, the most important lesson to be learned is that competent and experienced designers and operators do make mistakes. It is our hope that this report may help in minimizing the frequency and consequences of inevitable future errors. It seems to us to be worth stating at the outset that correctness of design principles is not enough; like any other system, correct functioning of

a protection system throughout its lifetime comes not only from application of correct principles but also requires competent attention to detail in design, operation, and maintenance of the system.

It is unfortunate but true that safety and economy are goals which often diverge and sometimes directly oppose each other in protection system design. The economy problem is a large and important one that relates not to the relatively minor cost of the protection system components but to the necessary and inevitable compromises in plant design necessary to achieve an acceptable level of safety. What this level must be, and how it shall be attained, are matters of judgment. The discussions in this report are thus expressions of our judgment in these matters. We have formed these judgments as a result of our experiences, particularly at the Oak Ridge National Laboratory, although this report is not an expression of the Laboratory's opinion. It is a pleasure for us to acknowledge our indebtedness to our colleagues there, especially to Mr. E. P. Epler. One of us (S. H. Hanauer) has also benefited greatly from his many discussions with applicants for reactor licenses, members of the AEC Regulatory Staff, and his colleagues on the AEC Advisory Committee on Reactor Safeguards, but this report is in no way related to the ACRS, and no regulatory implications should be inferred.

2.1 Definition of Protection System*

This report deals only with protection instrument systems for nuclear power plants. An instrument system is considered to cover sensors and transducers, the devices that control actuators (control rods, valves, pumps, etc.), and everything in between. All protection instrument subsystems are part of the protection instrument system, including those required to initiate containment isolation or emergency core cooling, as well as those for emergency insertion of the control rods. The actuators themselves are not discussed; that important subject must some day be the subject of another report. Similarly, subjects such as core physics, heat transfer, and fluid dynamics are not treated herein.

*An extended discussion of nomenclature for protection instrument systems is given in Appendix A.

Our study has been directed principally at system design rather than at design of individual components or instruments. Besides restricting usefully the length of this report, this emphasis is, in our opinion, directed toward the aspect of protection systems that is presently least well understood, most controversial, and thus in greatest need of discussion.

The definition and delineation of the protection instrument system of a nuclear power station, hereinafter called, simply, protection system, are not simple matters. Criteria of the Institute of Electrical and Electronics Engineers (IEEE) give the following definition (see App. B):

"For purposes of these Criteria, the nuclear power plant protection system encompasses all electrical and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protective function. These signals include those that actuate reactor trip and that, in the event of a serious reactor accident, actuate engineered safeguards such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning."

A similar definition is given by an IEC Recommendation:¹

"Protection System. The system which acts to prevent the reactor conditions from exceeding safe limits* or to reduce the consequences of their being exceeded. The protection system includes the safety shutdown system and where provided, the containment isolation system, the system which initiates emergency cooling, etc."

2.2 Scope of Protection System

The two definitions given above are essentially equivalent and do not appear to offer any difficulty in application. Unfortunately, the apparent simplicity is illusory. The question of what is and what is not included in the protection system of a given plant has no generally accepted answer at the present time. Extreme viewpoints might be represented by the following statements:

*Although this definition might literally include parts of the operation system, that is not intended; see also Section 2.4.

1. (Wide) Since almost anything can ultimately affect safety, it is useless to define a protection system; everything in a reactor plant is important to plant protection.

2. (Narrow) The devices which drop the safety rods constitute the entirety of the protection system.

Neither of these approaches has found wide acceptance and neither is adequate for the purposes of this report. We have adopted here a viewpoint intermediate between the two extremes. We did this because of the demonstrated usefulness of differentiating between the protection system and all other equipment. This point is discussed at length in Chapter 5.

The criterion adopted here for inclusion or not of a class of devices within the protection system can be inferred from the consequences of hypothesized failures of the safety functions enumerated in the definitions given above (scram, containment isolation, core spray, etc.). Failures of these protection functions when needed would clearly have intolerable consequences. Extending these examples leads to the following criterion:

The protection system includes those groups of devices, and only those, whose failure to provide protection when needed would have unacceptable consequences.

In other words, these things have to work. As will be shown later, protection systems are designed so that their safety functions will be performed even if one component (or module - see App. B) should fail. This is the reason the criterion deals with groups of devices; it is the group function that must be performed when needed. A component or module is part of the protection system when it is a member of such a group, even though the redundant design may be such that the failure of any given single component is tolerable because its companion can do the job.

Judgments regarding acceptability of consequences will vary according to the design of the plant and also according to the people whose acceptance is under discussion. Obviously failures of engineered safety features, as cited in the protection system definition in the IEEE Criteria, are unacceptable. Failures of such features to operate when needed in an accident situation would (not inevitably, but with nonnegligible probability) lead to overexposure of the public to radiation, and the consequences would thus be intolerable on any rational basis. It is more

difficult to decide in other cases. For example, the successful operation of most large reactors requires adherence to a required pattern for control rod positions and maneuvers. The degree of automation of rod motion and the degree of protection needed against incorrect rod motion vary widely among plants. In plants where moving an incorrectly selected rod could cause melting of a small portion of the core, the consequences might be unacceptable to the stockholders of the utility corporation but not to the public. The consequences to operating personnel must also be considered. In addition, the "small portion" melted in the core would have to be evaluated, as well as the accuracy with which the predicted amount would be ascertainable. Judgments regarding tolerability of consequences of failure are, in general, outside the scope of this report, since factors such as heat transfer, core physics, and meteorology must be considered.

In general, there are three barriers between fission products and the public: the fuel cladding, the primary system pressure envelope (pressure vessel, pipes, pump casings, etc.), and the containment or confinement system. Although these barriers are not completely independent, the multiple-barrier concept is comforting and useful. For the more probable (but still unlikely) malfunctions, the protection system prevents damage to the cladding. For less probable, more severe malfunctions, cladding damage cannot be prevented, and the protection system prevents damage to the primary envelope. For highly improbable accidents in which the primary system is hypothesized to fail, the protection system initiates a variety of protective functions, including emergency core cooling and closing and maintaining closure of the containment system.

The current trend seems to be toward an increase in the number and types of devices included in the protection system. This trend may be good (in the direction of increased safety) if it has arisen as a result of improved awareness of failure consequences and potential hazards. The trend may also result from greater need for protection in larger and more complex plants. On the other hand, it is possible to carry things too far, since such might lead, for example, to inclusion in the protection system of the primary safety device, then the control device whose failure might provoke safety action, then the power source for the control

action, then the information used by the operator to initiate control action, etc., etc. By such extension, the protection system would be enlarged to the extreme position quoted above as the "wide" viewpoint. We believe that this is unwise and that the protection system should include only the safety devices whose failure might result in unacceptable consequences. Failure of control devices, for example, could call for safety action, but the consequences would presumably be tolerable (but see Sect. 2.4).

2.3 Identification of Components

It is important to identify all components of the protection system for the benefit of designers, operators, and maintenance personnel. Experience has shown that identification of electric wiring in the protection system is particularly necessary; log books are full of electricians' mistakes that were made when they had no idea they were anywhere near the protection circuits.

2.4 Definition of Operation System

It would be convenient to have a term to designate "all instrumentation and control devices not included in the protection system." Since no generally accepted term exists for this concept, we have adopted operation system to use in this report. Generally, the operation system includes equipment for regulation of process variables; equipment for measurements for information, operator surveillance (readout devices and annunciators), and financial control; equipment for optimization of process parameters; and "aids to navigation" for the operator to promote ease and efficiency of operation.

Failures in the operation system could lead to consequences that might not be negligible. The resulting off-normal operation might be inefficient, expensive, or illegal (outside technical specification limits or other limits set by various regulatory bodies). Plant production might be reduced or interrupted, with resultant loss of revenue and maybe annoyance or even danger to the public in an electric power blackout. Often,

action by the protection system might be initiated that would lead to plant shutdown, loss of production, and transients to the system that might shorten its life or even cause damage, such as thermal shock to heat-exchanger tubing. By definition of the operation system, however, these consequences are tolerable; otherwise, the equipment would be a part of the protection system.

It can thus be seen that one objective of the operation system is to avoid excursions of process variables outside rather narrowly determined limits and similarly, that one objective of the protection system is to suppress such excursions if they should occur or to deal with the consequences of excursions. Avoidance of protection action is an operation function, not a protection one, because failure of the operation function can produce only a tolerable protection action.

In some large or experimental plants, it is desirable to take unusual precautions to avoid excursions, either because of a high economic penalty or because of the technical value of the operating data that might be lost in an excursion. In such cases, protection system design techniques are often applied to portions of the operation system in the hope of increasing reliability. These are legitimate objectives and procedures, but the resulting resemblance between such an operation system and most protection systems is not an indication that the protection system includes the operation equipment. The distinction remains in terms of the consequences of failure.

3. PERFORMANCE AND SYSTEMATIC FAILURES

The basic function of protection instruments is to initiate or to inhibit action. Thus the output of the instruments is binary; that is, it has two states: go and not-go. This action, or more precisely this decision as to which of the two possible output states will occur, is made on the basis of the present (or, possibly, present and past) value of one or more input signals. The input signals can be binary also (for example, whether or not a valve limit switch is actuated) but are often continuously measured values of system variables.

The oldest example of a reactor protection system consisted of one or more neutron-sensitive ionization chambers, amplifiers, and relays which opened a circuit when the neutron flux exceeded a preset value and thus deenergized magnets and dropped safety rods into the reactor core. More sophisticated examples abound in present technology. The decision may be based on the values of more than one variable, and the trip level may be a function of another variable. A coincidence may be required wherein two more-or-less independent variables must be outside their limits simultaneously to initiate safety action, and the action itself may be something other than scram, such as closing valves for containment isolation or initiation of a sequence of valve and pump operations for emergency core cooling.

Although in principle it would be possible for an output signal other than binary to be required of protection instrumentation, no examples are known to us at present.

3.1 Need for Correct Functioning

It is self-evident that protection instruments must perform their functions correctly and adequately. Not only must something happen when needed (reliability), but what happens must do the job (performance). Unfortunately, these essentials have sometimes been slighted, in our opinion. Necessary upgrading of protection system reliability has not always been accompanied by equally necessary maintenance and, in some cases, upgrading of system performance. It is surely true that both

performance and reliability are essential to the correct functioning of protection equipment.

Without exception, all known reactor accidents in which the protection system did not function correctly involved failure of performance rather than failure of reliability. In no case known to us has random failure of a protection instrument component contributed to a reactor accident. On the other hand, an appreciable number of performance failures have occurred.* We have therefore chosen to give a fairly complete discussion of performance and testing criteria, failure modes, and design precepts. Some of this material should be known to every designer, but the convincing evidence of accident occurrence suggests otherwise.

3.2 Reasons for Performance Failures

Care and foresight are necessary to insure correct functioning (performance) of protection system instruments. Provision of ample margin in the design and diversity of design approach (see Sect. 3.3) are useful in protecting against the unforeseen.

3.2.1 Equipment Functioning Impossible

The protection equipment cannot possibly function if it is, in fact, "guaranteed not to work." An example of this came to light in the HTRE-3 accident, in which a series resistor insured that the current in the ionization-chamber circuit could never be as high as the trip value.³

3.2.2 Equipment Paralyzed by Accident

The protection equipment may be paralyzed (poisoned) or destroyed by the accident that necessitates protection, and although functioning is possible under some circumstances, performance failure can occur if the accident happens in a way not foreseen by the designer. An example is the system of meter relays which operated successfully when tested by

*A good review of incidents, accidents, and failures is given in Chapter 11 of Ref. 2, which should be consulted for chronologies of the various occurrences.

rapid increase of the radiation field but failed in service because a slow increase produced small forces and insufficient mechanical momentum to actuate the electrical contact.⁴

3.2.3 Operation Without Protection

A performance failure may be said to have occurred if the protection equipment is known to have failed, but plant operation is permitted anyway. This is an administrative rather than a design problem and is illustrated by the NRX² and Boris Kidric² accidents.

3.2.4 Consequential Failures

Performance failures may occur if the design and analysis are incomplete and an unknown or undetected causal relationship exists between failures that are hypothesized as independent or even incredible. For example, in the HTRE-3 accident, the thermocouples for shutting down the reactor on high temperature were located in the hottest regions for full-power operation. An unexpected startup accident, in a different configuration, resulted in hot spots elsewhere, so the temperature protection was ineffective.

3.2.5 Interaction Between Protection System and Operation System

Interaction between the operation system and the protection system can produce an accident, and from the same event, cause paralysis of the protection for that accident. This is the worst case of all, since the failure in the operation system, presumably tolerable, produces infallibly the protection system failure and its intolerable consequences. The HTRE-3 accident has this feature also.

3.3 Validity of Instrument Outputs

Having decided (on a basis outside the scope of this report) that certain safety actions are required when certain conditions exist, the protection system designer must relate the outputs of instruments to the desired conditions. In many cases, a direct relationship is unobtainable.

This situation most often occurs regarding fuel and coolant variables in the core. Although neutron and gamma fluxes can be measured as a function of position in the core (usually in the core coolant channels), techniques for measuring fuel center-line temperature, cladding temperature, and local flow velocity are not presently available for in-core use. The value of vital process variables such as these must therefore be inferred from other measurements, together with known or assumed parameters (cross sections, heat transfer coefficients, etc.). The accuracy of knowledge of the unmeasurable variable will vary, depending on the state of knowledge of the links in the chain of inference in addition to the accuracy with which the measurements are made. In this situation, a conservative approach sometimes used is diversity, which is the use of two (or more) different chains of inference, with different measured variables (symptoms) to determine the needed quantity. The use of diversity in protection instruments has the great potential advantage of reducing the chance of unknown systematic errors of measurement and/or inference. The reduction of systematic errors is of sufficient importance that diversity may well be justified in those protection subsystems upon which the public safety is directly dependent.

3.4 Accuracy of Measurements

Margins cost money, and accuracy is therefore a necessary ingredient of protection instruments. Hardly ever is there a significant degree of error in electronic devices. Usually, a margin of 1 or 2% is adequate allowance for deviation of the entire instrument chain from sensor to actuator. The most ubiquitous component of purely instrument error is drift, and a suitable calibration interval can be found to ameliorate the drift error satisfactorily.

Although electronic instrument error can be made arbitrarily small, the overall error of measurement cannot. Unavoidable errors occur in transducers and in the relationship between the transduced variable and the inferred parameter (the validity problem; see Sect. 3.3). The trip level must therefore be set more restrictively to compensate for the possible error, or the safety analysis must take it into account as wider

allowable variations; these are equivalent ideas. Thus the reactor power rating might depend on the overall accuracy attainable in measuring power — obviously a situation with strong economic incentive for improving instrument accuracy.

The accuracy of measurement must be evaluated for the set of conditions under which the protection system is required to function. Many of the adverse circumstances discussed in this report can lead to increased measurement error, although the discussions are in the context of equipment failure. In a way, errors beyond those allowed for constitute a species of failure that is to be guarded against like any other.

3.5 Speed of Accident and Response Time of Instruments

It is self-evident that the protection function must occur soon enough to provide the necessary protection, that is, to avoid the (intolerable) consequences of nonprotection. The speed of the accident and the speed of response needed in the protection instruments are, of course, intimately connected. It therefore seems attractive, sometimes, to slow down the accident rather than to speed up the protection if the two are inconsistent. This is a design approach to be used with considerable caution. The potential problem is that of overlooking some accident mode faster than the one that was "fixed."

It is particularly necessary to check that an unexpectedly (or "spuriously") rapid variation of signals does not paralyze the protection equipment. In a famous example,⁵ the reactor power rose on an unexpectedly rapid excursion as a result of a misplaced control rod used in a previous calibration. Although the trip level was exceeded, the protection function was never initiated. Reports of the accident indicate that the power level trips failed to operate because their trip level was exceeded too rapidly. An excessive delay in response time coupled with amplifier saturation and loss of amplifier output could cause such a failure. Section 3.2.2 cites an example of failure caused by too slow a change.⁴

A minor but annoying aspect of time response is its relationship to instrument noise. Some variables are subject to considerable fluctuation, because of either the nature of the phenomenon itself (turbulent flow)

or the statistical nature of the transducer (neutron flux) or the properties of the instruments (measurement of small temperature differences). The fluctuations are enhanced if a rate signal is required, as for reactor period. It is sometimes necessary in such cases to compromise among speed of response, trip setting, and spurious trips. These variables are not independent. Increased speed of response leads to increased fluctuations due to the greater bandwidth. For the same trip setting, the probability of spurious trips is thus increased. A compensatory change in trip setting will decrease the spurious trip rate, but the safety performance degradation may not be acceptable. Sometimes no satisfactory compromise is possible. This means that a realistic evaluation of the protection performance reveals limitations due to the noisy character of the signal. In the statistical case, at least, the limitation is fundamental to the nature of radiation detectors. In any case, the performance specification must be capable of achievement in the presence of unavoidable fluctuations.

3.6 Functioning Under Accident Conditions

The protection system must function when needed and must not be inhibited by the presence of unforeseen circumstances such as those referred to in Sections 3.2.2 and 3.2.4. Some examples of "unforeseen circumstances" suggested by analysis and by experience are discussed in the following sections.

3.6.1 Effect of Accident on Plant Configuration

It must be recognized that the plant may not be the same under accident conditions as it is normally. This is an obvious fact with respect to the excursion or fault that precipitates the hypothesized accident, but it must also be recognized that other aspects of the plant may not behave as might be assumed. As an example, the relationship of ionization-chamber signals to neutron flux in the core can be altered if the intervening water (say, in the reflector, between thermal shields, etc.) changes markedly in temperature, void fraction, or poison concentration. Moreover, flow patterns may change substantially during the course

of the excursion and lead to further changes in observed readings. Such transients are notorious for causing errors in readings of flow, temperature, and pressure in flowing fluids and in plant conditions inferred from such readings.

Rod motions under accident conditions are likely to change the spatial distribution of neutron flux and power density. In extreme cases, disruption of the core can make such readings meaningless.

The fluid circuits are quite likely to change during an accident. Valve actuation, intentionally via the operation system or the protection system, or unexpectedly due to failures, can send fluids in new directions. Relief valves can introduce leakage in directions that may be known or unknown. Pump operation may be abnormal, and broken pipes will spill and divert fluid flow.

Not all these suggested failures can be predicted nor should all be analyzed. The point to remember is the necessity for justification of each assumption regarding the plant configuration in predicting instrument behavior under accident conditions.

3.6.2 Effect of Accident on Instrument Signals

Since the possibility or likelihood of an unusual plant configuration existing during an accident must be acknowledged, it is necessary to consider the unusual instrument signals that could arise. This is important for several reasons connected with assuring that protection be provided.

The signal magnitude may have an unusual value. The most obvious possibility is overload; that is, variation above the design range of the instrument. It is essential that this unusual signal value not lead to false instrument operation in an unsafe direction. For electronic instruments, this problem is called overloading, or saturation. The requirement is that all input signals outside the "safe range of the variable" must give rise to output signals whose character denotes the nonsafe value of the input signal. In other words, no unsafe value of input signal, no matter how unusual, can be allowed to produce a safe value of output signal. The most common problem is simply that a value of the process variable is too large. It is not always recognized, however, that in

some transients highly abnormal signals may be generated, either spuriously or genuinely. As an example of the care to be taken in this regard, it should be required of current amplifiers for ionization chambers that the output signal remain above the trip level for all currents possible in an accident. As an arbitrary minimum, we suggest that this be tested to at least ten times the trip level. In some reactors, nondestructive neutron-flux transients are possible with peaks up to 10^6 times the trip setting, but this is fortunately not a characteristic of most power reactors.

It is worth noting that most counting-rate systems are worthless for application to protection systems because of their unacceptable overload characteristics. The output signal may reach a maximum and then decrease as the neutron flux increases.

The time variation of the signal may have unusual characteristics under accident conditions. An example of a too-fast accident is given in Section 3.5, and a too-slow one is cited in Section 3.2.2. Another possibility is the "spike": an excursion that somehow returns to safe values before the protection function can be performed. As with overload magnitudes, the most spectacular spikes are associated with neutron-flux excursions. It is not possible to give a general rule regarding spikes. The credible excursions must be analyzed for tolerability of consequences. If required, the time response of the protection instrument must be made fast enough to recognize the spike and to initiate the protection action upon its occurrence. It is fortunate that such fast response is not usually necessary, since with response speed appropriate to fast spikes goes an increased probability of spurious shutdowns arising from instrument noise.

Not only can signals be unusual, they can appear in unusual combinations under accident conditions, and this possibility must be allowed for both in instrument design and in failure analysis.

3.6.3 Instrument Module Behavior in Accident Environment

The vagaries of instrument behavior in the environment associated with accident conditions must not, in general, prevent correct functioning

of protection systems. The effects of unusual process variable magnitudes and rates of change on the input signals to instruments were discussed above (Sect. 3.6.2), but it is also necessary that unusual values of process variables not have a direct adverse effect on instrument components. Clearly, this refers principally to transducers and preamplifiers. Increased temperatures must not melt and increased pressures must not burst the temperature and pressure transducers that initiate protection actions associated with such excursions. Transducer ratings should have adequate overrange margins to accommodate unusual and unexpected variations in the measured variable or the worst accident will be the one for which the reactor is the least protected.

The course of an accident can affect an instrument by changing its physical environment. The temperature, pressure, humidity, etc., of the atmosphere surrounding the instrument can change as a direct result of the accident. Steam can be blown on the instrument or it can be submerged in liquid. An engineered safety feature (e.g., containment spray) could be responsible for wetting many instruments. Components could be shaken, moved, shocked, or burned. Interconnecting tubing and wiring could be severed or crushed. Although some of these results are impossible to predict, it is at least necessary to evaluate the environmental effects of design-basis accidents. Either enough of the necessary protection instruments must survive the ordeal or it must be demonstrable that the plant is protected by something else. As examples, it is only necessary to demonstrate that the primary pressure instruments can survive a pipe break long enough to initiate emergency core cooling, whereas the flow instrumentation necessary to supervise cooling must function throughout the accident, and the external radiation monitors may be needed for months.

A quite different "environmental" factor is the supply of energy for the operation of instruments. The voltage and frequency of an ac supply, or the voltage of a battery bus, or the pressure and cleanliness of the compressed-air supply may vary significantly under accident conditions from their normal behavior. It is, of course, necessary that the protection instruments perform their function in spite of these variations.

One supply variation always evaluated is the loss of the source of energy. It is necessary to consider this eventuality in spite of the precautions taken to avoid it. If more than one source is provided, it is usually required as a minimum that loss of all sources make the protection instruments revert to the safe state, whatever that may be in the plant under consideration. The emphasis in this case is on instrument criteria, since obviously such functions as core cooling cannot be assured if no energy source whatever is available. Decisions regarding pumping power, etc., are outside the scope of this report.

3.7 Functioning Under Special Nonaccident Conditions

A nuclear power plant does not operate at rated conditions throughout its life, and special nonaccident situations must be considered in the design of the protection instruments, since special performance may be required. Some examples of special conditions are the following.

1. Special plant experiments or maneuvers may be performed in which parameters are varied deliberately outside normally permitted limits. If it is necessary to disable protection instruments to perform an experiment, this should be justified by detailed analysis. The loading of developmental or even intentionally defective fuel would be an example of an experiment that might be performed.

2. Refueling, which is a planned and necessary operation, often requires violation of containment.

3. The plant may be operated with equipment, protection or other, known to be inoperative or otherwise unavailable.

4. Initial operation before plant shakedown is completed may present special conditions.

As with other sections of this report, the need for special consideration of operation under special conditions should be obvious, and yet several reactor accidents have occurred because this problem was not adequately considered in the design or in operation. For example, HTRE-3 was in its initial power ascent when it was melted; NRX had special poorly cooled fuel elements at the time of its destruction, and the rod-position indicators were known to be erratic; and EBR-1 was undergoing

a special transient in a region of known positive feedback when it was melted.

The number of accidents that have occurred when the reactor was thought to be shut down is also worth noting. The most important of these was, of course, the SL-1 disaster, but there have been others. In fact, as has been mentioned by Breckon and Collins,⁶ the safest operation mode seems to be steady-state power generation. No serious accident known to us has yet occurred during steady-state power generation.

Most power reactors operate at steady state, at or near rated power, most of the time. However, we must not be lulled into too great a sense of security by their good initial operating records in this relatively safe mode. Since they have so few opportunities to go wrong, it may take many reactor-years of "experience" to gain assurance of genuine demonstrated plant reliability.

3.8 Confirmation of Performance

It is not a simple matter to demonstrate that the protection system has the required performance. Such demonstration is far different from the testing for operability discussed in Section 4.3. Ultimately, the adequacy of performance of a protection system can be established beyond doubt only by its adequate performance in an accident situation. Fortunately, most reactors do not experience accidents, and therefore most protection systems have not been given the ultimate performance test.

It should be realized that a successful test of some protection systems is difficult to recognize. Logbooks and operating reports are full of "false trips," described with scorn heaped onto the presumed failure of the protection equipment. There is evidence, however, that not all such trips are false. The Boris Kidric, NRX, and ETR accidents all involved, to some degree, "false" trouble information that was ignored by the operator and upon later examination found to be true.² In several cases, flurries of "false" period scrams have later been recognized as arising from genuine short periods.⁷ It therefore seems reasonable to suppose that an unknown number of events have occurred in which a

protection system has performed successfully under (at least potential) accident conditions.

On the other hand, a nonnegligible number of reactor accidents have already been experienced in which the functioning of the protection system was demonstrated to be inadequate. It is therefore of great concern that adequacy of performance be established to the extent possible. This may involve an elaborate testing program. The General Electric Company tests at Moss Landing⁸ of pressure-suppression containment and the ORNL tests of a fast nuclear scram system at the SPERT Facility⁹ are examples of such tests. An ideal test would be conducted with an accident environment (see Sect. 3.6), but this is rarely possible. This subject should receive further study.

As a minimum, it seems prudent to test complete functioning of all protection systems and associated engineered safety features at least once on each reactor. Again, this test is different from the necessary periodic verification of operability, which usually must be done component by component or, at best, subsystem by subsystem during the life of the plant. The complete test referred to usually must be performed, if at all, before the first core loading. After initiation by some suitable signal, the entire protection sequence (scram, auxiliary power, containment isolation, emergency core cooling, for example) proceeds more or less as in an accident. The objective of this test is to determine, to the extent possible, that the system functions as a whole - a determination not available from piecemeal tests.

4. RELIABILITY AND RANDOM FAILURES

The problem of reliability, which is a measure of the probability of functioning of the system, must be considered in addition to the adequacy of the performance of the system (Chap. 3). Since nothing is perfect, all the components, modules, subsystems, etc., and their interconnections, which constitute a protection system are subject to failure. Wires break or touch a grounded conduit or each other; components become open- or short-circuited or change value; batteries lose charge; and instruments die or go berserk. Such failures in the protection system must be allowed for in the design and must be considered in evaluating system reliability.

4.1 Safety and Serviceability

The modes of failure of a protection system can be explained with the use of Table 4.1.

Mode 1 is the normal operating condition of the plant. No protection action is needed, and none is actuated. Mode 4 is the safe shutdown, with the appropriate protection equipment having operated when a genuine need arose.

Modes 2 and 3 represent failure of the protection system. In Mode 3, the protection is absent despite plant variables being outside the safe limits. Protection is needed and is not forthcoming. The plant is in an unsafe situation, and it may be said that the protection system failed

Table 4.1. Modes of Plant and Protection System Operation

| | Protection System Quiescent | Protection System Actuated |
|------------------------------|--------------------------------|--|
| Plant within safe limits | Mode 1: safe | Mode 2: false actuation of protection |
| Plant outside safe limits | Mode 3: unsafe | Mode 4: protected |

unsafely. Mode 2 is opposite to Mode 3. No protective action is called for by the plant conditions, and yet the protection system is actuated. The protection system operated when it was not needed, and it may be said that the protection system failed safely.

For this report, we define reliability as the propensity to be free from failures, safety as the propensity to be free from unsafe failures, and serviceability as the propensity to be free from safe failures. Thus, reliability is a composite of safety and serviceability. Some attempts at numerical definitions of these terms are discussed in Section 4.5.

The need for safety (as defined here) is universally acknowledged. An unsafe failure robs the plant of protection against an event whose consequences are intolerable. This follows from the definition of the protection system given in Sections 2.1 and 2.2. The probability of actual intolerable consequences is compounded from the probability of an unsafe failure and the probability that the protection will be needed. For example, if potentially destructive reactivity excursions are expected once per reactor-year, and if the probability of an unsafe failure of the appropriate protection equipment is 10^{-6} , and if these two probabilities are independent, there is a probability of 4×10^{-5} that in the 40-year life of a reactor a reactivity transient will destroy the plant with intolerable consequences.

The three if's in the preceding sentence are all necessary to the logic. The numbers given are based on an optimistic evaluation of present-day technology. In over 1000 reactor-years of experience, several destructive reactivity excursions have actually occurred¹⁰⁻¹³ in situations where a correctly functioning protection system might have prevented the destruction. However, the protection failure was systematic in all cases, rather than random; that is, it involved inadequacy of performance rather than inadequacy of reliability. The experimental value for the unsafe failure rate due to unreliability is therefore zero, with an uncertainty band between zero and 1×10^{-3} per reactor-year. We suggest that 10^{-6} per parameter-year is a satisfactory goal for the unsafe failure rate due to random causes for the present, since it is so far below the actually experienced rate of destructive accidents involving functional inadequacy of the protection system.

The need for serviceability is economic and psychological, as well as technical. An excessive rate of false protection actuations costs too much and gives rise to an unhealthy (though sometimes justified) attitude of derogation of the protection system by the operating crew. In particular, the fact that the system is too often acting falsely in the direction of safe failures should suggest that something serious is amiss and that the safety of the system may be inadequate, as well as the serviceability. This has in fact been the case in some past experience, but it is not necessarily so. The excessive unserviceability may be caused by trip settings being too close to operating values. The amount of noise suppression and the accuracy realistically obtainable then produce variations in signal that cause the false trips. One cure is to reduce the operating level or to raise the trip level, but the loss in plant performance or protection may not be tolerable. Thus, although poor serviceability is always a problem when it occurs, and may be a symptom of inadequate safety, its cure must not be based solely on improving the serviceability; performance and safety must not be compromised in the process. A false actuation rate as low as one per year in a power plant has been achieved in a few cases, according to operators in utility organizations. This low rate seems to represent a worthwhile goal for power reactors in the future.

A special case of reliability is that of a system whose failure in either direction is intolerable. For such a system, all failures are unsafe, whether they are failures of commission (actuation of a safety feature when it is not needed) or of omission (failure to actuate the protection equipment when needed). In the previous example, the rate of intolerable consequences was 10^{-6} per year on the basis of only failures of omission coupled with the need for protection. In the present situation, the rate of failures of commission must be included in the calculation of the rate of intolerable events. The serviceability would be undefined, since safe failures would not exist. It is difficult to describe a system that meets these requirements. Generally, all power-reactor protection systems have a safe direction in which to fail, so loss of energy, gross disconnection, and environmental catastrophes (most of them, anyway) can be made tolerable, if expensive, events. Reactor

designers and protection system designers should beware of system requirements that exceed the safety and serviceability standards suggested in this section. Such enhanced requirements would imply the need for a system that cannot fail, which is a system that we do not know how to build.

The requirements and achievements of space exploration provide a clue to the potential of present technology for producing the perfectly failure-free system. Many space-vehicle subsystems have no safe direction in which to fail; their departure from the norm induces failure of the mission. Redundancy techniques have not played an appreciable part in unmanned flight, presumably because of the difficulty of repair. Experience with manned flight — where repair is possible in principle — is so far inconclusive. Up to now, the experienced probability that a given launch will fail in achieving its mission has been enormously greater than 10^{-6} . We suggest that this is additional evidence that perfectly failure-free reactor protection systems should not be specified where failure would be intolerable. Rather, the system must be modified so that realizable and realistic protection system performance will provide the necessary safety.

4.2 Quality of Apparatus

The equipment used in a reactor protection system must be of high quality to insure adequate performance and reliability of the system. Modules built for normal industrial service frequently do not possess the reliability necessary for application to protection systems. It is therefore necessary to pay particular attention to quality in acquiring such apparatus.

The problem of establishing and maintaining adequate quality has been studied exhaustively by agencies of the Department of Defense. The well-known "Mil Spec" requirements for construction and quality control constitute one approach to dealing with this problem. However, the small number of reactor protection system modules built per year, and the lack of industry-wide standardization of such components, have so far precluded the establishment of any generally applicable quality standards for reactor protection system components comparable to Mil Specs.

A partial approach to quality in electronic instruments would be to use components (resistors, connectors, wiring techniques, etc.) designed and fabricated to Mil Specs. This is not generally done at the present time. In fact we have seen, in a manufacturer's shop, instruments for Defense Department reactors being built with Mil-Spec components side-by-side with instruments for commercial power reactors and other components not certified to Mil Specs.

The purchase of protection system instrumentation from the lowest bidder on functional specifications has repeatedly resulted in the acquisition of high-priced junk satisfactory neither in performance nor in reliability. The monotonous regularity with which such systems must undergo expensive upgrading programs has proved over and over again that only by lucky accident will such methods result in an adequately safe and serviceable protection system.

There has been an effort on the part of reactor vendors to write instrument specifications in such a way as to promote quality in design and construction. The degree to which this is successful can someday be ascertained by studying instrument reliability data. It is very important that such data be maintained for all protection systems to feed back to manufacturers the proof in service of various techniques in design and manufacture. To date, the data show no trend, presumably because the reactors that have been operating long enough to produce the data have old instruments in them whose reliability tells very little about present-day instruments. Further, the available data indicate strongly that the quality of maintenance is at least as important as the quality of manufacture in determining reliability.

We often see the expressions "nuclear grade" or "safety grade" in reading descriptions of instruments proposed for protection system application. We suggest that these terms have at present very little meaning beyond a vague idea that they hopefully imply a "high" quality and the certainty that they will be expensive. Only after quality standards and specifications have been established will it be possible to purchase instruments of "Protection System Grade" with assurance of obtaining the necessary quality. A definition of such a term, with specifications of

its meaning and means for determining compliance with the specifications, is sorely needed.

4.3 Monitoring and Testing

At least five modes of verification of module and system performance can be identified.

1. Type Testing. The objective of type testing is usually to verify that the module performance is adequate under the various conditions discussed in Sections 3.3 through 3.7. Testing of reliability may be attempted also, but usually the statistical accuracy of the data obtained is poor.

2. Acceptance Testing. The objective of acceptance testing is to insure that each module has the performance and reliability required of its type; that is, that it is correctly manufactured.

3. System Performance Testing. Occasional tests of the entire system, as discussed in Section 3.8, are used to verify system performance.

4. Maintenance. A periodic preventive maintenance program is necessary to insure that the performance and reliability of the system over its entire service life will remain equal to the type specifications.

5. In-Service Testing. The term "in-service testing" is used to denote a program of periodic verification of operability: a simple test to determine whether gross failure has occurred. The objective is to test so frequently that the probability of failure per test interval is small and the probability of system failure due to multiple random failures per test interval is negligible. In-service testing is essential to system reliability. Continuous monitoring of system and/or instrument parameters can substitute for some aspects of in-service testing.

In power reactors, capability must be provided for in-service testing without shutting down the reactor, since the required frequency of testing (see Sect. 4.5) is far greater than the allowable frequency of plant shutdowns. Such in-service testing is economical in the long run because it almost always permits nearly all instrument maintenance to be performed without requiring or prolonging expensive plant outages. Moreover, on-line maintenance has also been described as the safest method,

as well as the most convenient and economical.⁶ One channel can be tested or repaired at a time, returned to service, and its operability verified before the other channels are touched. This technique avoids the situation, all too common with maintenance during outages, in which startup must proceed with many or all channels of protection having been disturbed since the last operation.

The test should be as complete as possible. It should test the entire line of equipment from sensor to actuator over the expected range of variables in as realistic a way as possible. Practical testing regimes meet this objective to various degrees. It has been found possible in some cases to create a local disturbance in the process variable as detected by one of a redundant group of protection sensors for that variable and thus to simulate accident conditions to an extent. However, this is not always possible, and it is often omitted to save money. An electrical (pneumatic, hydraulic) simulation of an input signal is usually used to initiate a test. This should be introduced as near the "front end" of the channel as possible in order to test everything but the transducer properties. The transducer excitation should be monitored.

Testing of the actuator will necessarily be incomplete, since its operation for testing is generally forbidden if it would shut down the plant. (For some engineered safety features, it is possible and profitable to include the actuator in the test.) Some ingenious techniques have been employed that use transients too fast for actuation or magnetic saturation characteristics to extend the testing regime to include a partial test of the actuator.

The test should be sufficiently detailed to find every failure. This is vital because protection systems are composed of groups of redundant devices, the failure of one of which does not induce system failure. Tests of system performance will fail to disclose such a single-device failure, and yet the reliability of the system is predicated on the possibility of finding and rectifying it. The difficulty of testing for single failures varies with system complexity. Systems with logical arrangements whereby many inputs cause many outputs, with (necessarily) redundant logic devices, are especially troublesome in this respect.

The testing method and devices must not constitute hazards in themselves. The test signal must be applied in such a way that the probability of obtaining the protection function if needed during the test is not decreased. Thus, testing schemes that involve disconnecting or disabling the sensor or bypassing the output signal are to be avoided. Circuit rearrangement for testing (connecting the testing signal, changing logic) should not be a requirement; if necessary, circuit rearrangement should be done with switches rather than manipulation of wires under field direction. The abnormal state of the system under test, and its restoration to normal, should be clearly indicated to the plant operator.

The testing procedure and equipment should be incapable of violating channel independence (see Sect. 4.6).

4.4 Redundancy

The quest for quality runs into diminishing returns above a certain quality level, and yet the requirements for reliability are severe. One answer is redundancy, whereby imperfect parts are combined into a system with (in favorable cases) overall reliability enormously improved over that which would seem possible. As an example, consider a high-quality amplifier costing \$1,000 for which the probability of failing to operate when needed (Q) is approximately 10^{-3} .* A redundant system with two such amplifiers, properly tested and arranged so that either could fail without inducing system failure, would have a Q approaching 10^{-6} , which is a big improvement (a factor of 1000) for an outlay of, say, \$5,000 (two amplifiers, plus logic devices, plus testing). The same \$5,000 spent on a single better amplifier would result in at best a small improvement in Q . With present technology, few indeed are the designers who have succeeded in achieving an adequate value of Q in a single device. The use of redundancy is therefore universal in protection systems.

Since the objective is to mitigate the effect of failures of devices, the basic rule of redundancy is that no single failure shall induce system

*The amplifiers are each assumed to have an unsafe failure rate of two per year and to be tested every 8 hr. These numbers are derived in Section 4.5.1.

failure. It is worth remembering that here we are speaking of reliability failures; redundancy is no defense against failures of performance. The "single failure" referred to has, unfortunately, become a major issue of contention in current evaluations of protection instrument systems.* The relevant questions are what constitutes a single failure and which failures must be considered. These questions have no all-inclusive brief answers at present, but the following discussion may be helpful.

The concept of a channel is useful in discussing redundancy. A channel is "An arrangement of components and modules as required to generate a single trip signal A channel loses its identity where single trip signals are combined." (App. B) Thus a flow channel might include a venturi, tubing from the process pipe to the pressure transducers, the transducers, the power supply for the transducers, preamplifiers, one or more amplifiers, one or more function generators (e.g., square-root extractor), one or more trip (bistable) devices, trip setpoint signal generator(s), power supplies for the electronic elements, and perhaps some relays. The channel associates a single trip output, the appropriate one of the various bistables, with the single measurement, however complex, of a system condition. If the trip setpoint depends on, say, reactor temperature and therefore temperature sensors, amplifiers, etc., are included in the channel, it remains a single channel. However, it is also common usage in this last case to speak of "interconnected (single) temperature and (single) flow channels"; this apparent inconsistency causes no difficulty.

The usefulness of the channel concept is simply that it is sufficient to consider channel failure, without worrying unduly why the channel might fail. This has not always been recognized. The early literature abounds in detailed discussions on the failure of a given tube or cable. In particular, the old fail-safe controversy belongs in this category. A safe failure is one that trips the channel or at least does not decrease its ability to initiate a trip if one is needed. In any design, some failures are safe and others unsafe. The unsafe failures impair function without

*A committee of IEEE is currently trying to develop a suitable definition of a "single failure."

causing a trip. By careful design, it is possible to increase the ratio of safe failures to unsafe ones. It is impossible to eliminate all potential unsafe failures; it is not even very important how large a group of possible unsafe failures remains, since the class cannot be eliminated. Such details are important in the design of components and channels, but they are not important in evaluating redundancy. There are so many ways for a channel to fail that detailed attention to a (necessarily) small number of such ways is not useful to safety evaluation. We shall therefore assume that a channel can fail in any way at all; that is, in the worst way for the situation under consideration. This being the case, the minimum number of redundant channels is obviously two, since failure of one is assumed possible. The question then becomes, are two channels enough?

From the standpoint of straight-out calculated reactor safety, two channels are indeed enough (see Sect. 3.6), and yet two-channel systems are almost never seen. The reason is that an adequate value of calculated reactor safety is not the only criterion for design. The assumptions in the calculation formulas include frequent ideal testing, but two-channel systems are exceptionally difficult to test. Moreover, the serviceability of such systems may be inadequate. In order to understand the principles underlying their design, it is necessary to consider the probabilistic basis of reliability calculations.

4.5 Probabilistic Calculation of Reliability

The objective of a probabilistic calculation of reliability is to predict the various failure probabilities and failure rates of the protection system. The predictions are based on probabilistic models and are related only to reliability considerations; performance failures are not and cannot be included. For convenience, the various assumptions made in the developments considered in this report are summarized below:

1. Channels are independent.
2. Failure probability is independent of aging, etc.
3. Channel is perfect or failed completely.
4. Testing is perfect, detects all failures.

5. Channels are identical.
6. Repair restores the channel to its original condition.
7. Probability of channel failures per testing interval is small; that is, much less than one.

4.5.1 Simple Redundancy

For a discussion of simple redundancy we assume that N independent channels are arranged so that any one of them can initiate safety action if required. The assumption of independence is discussed at length in Section 4.6. One of its aspects is the above-mentioned ability of any channel to initiate action regardless of the state of the others.

In general, a channel can fail in many ways, and the failure classifications are analogous to the system failure classifications given in Table 4.1. Either the failure is unsafe and leads to decreased ability to initiate safety action if needed, or the failure is safe and safety action ability is unimpaired. Varying degrees of failure (reduced gain, extra noise, burnout, etc.) do not facilitate mathematical analysis, so the further assumption is made that the channel is in one of the following states: (1) no failure, (2) safe failure that caused a spurious trip, (3) unsafe failure and unable to initiate trip if needed.

To evaluate the safety, we calculate the probability, P , that the system will initiate the safety action if required. It is more convenient actually to calculate $Q = 1 - P$, where Q is, of course, the probability that the system will fail unsafely and will not act when needed. The terms used for probability calculations are defined below:

1. For a protection system

F = Figure of merit for safety: $F = 1/Q$

M = Number of coincident channels required to initiate action

N = Number of redundant channels

P = Safety: probability of action if needed

Q = Unsafety: probability of failure $Q = 1 - P$

V = Unserviceability: false actuation rate

2. For a channel

r = Repair time

u = Unsafe failure rate

v = Safe failure rate

w = Testing interval

The concept of testing is essential to a realistic evaluation of P or Q . If the equipment is not tested, after a sufficiently long delay the probability that failure has occurred is unity. The 30- or 40-year lifetime of a nuclear power plant is far longer than the mean time to failure of even the best protection instruments. Therefore, to achieve a low value of Q it is necessary to postulate a testing program that detects all unsafe channel failures. Safe failures announce themselves and need no testing. Moreover, they have no significance in the calculation of P .

For each channel, a failure rate must be established. The usual assumption is that this rate does not vary with the age of the equipment. Some of the many publications on reliability are misleading in this respect; they describe various "wear-in" and "wear-out" curves for which the failure rate is not uniform with time and then give results based on a constant rate that is more tractable mathematically. The equations in this report are based on the failure rate being uniform in time.

For the calculations, we start with a channel known (by test) to be in working order at time $t = 0$. In an initial small time interval, Δt , the probability that the channel fails (the channel is in working order at the beginning of the interval, failed at the end) is $u \Delta t$, where u is the (uniform) unsafe-failure rate of the channel. Such a failure, occurring at time t , would incapacitate the channel at least until the next test. If w is the testing interval, the postulated failure would endure for a time equal to $w - t$.

The failure probability during a finite time lasting from $t = 0$ to $t = T$ is only approximately uT , since the probability of failure during Δt is the joint probability that the channel was working at t and that it was not working at $t + \Delta t$. Let $x(t)$ be the probability that the channel is in working order at time t ; $x(0) = 1$. Then

$$x(t + \Delta t) = x(t) - u x(t) \Delta t,$$

which for infinitesimal Δt , as Δt approaches dt , gives the equation

$$\frac{dx(t)}{dt} = -u x(t) ,$$

whose solution is

$$x(t) = e^{-ut} .$$

The failure probability during time T is just $1 - x(t)$ which is given by

$$1 - x(t) = 1 - e^{-ut} .$$

For uT sufficiently small,

$$1 - x(t) \approx 1 - (1 - uT) = uT .$$

We will assume uT to be small, and therefore the probability of failure during a testing interval w is very small.

The single failure does not incapacitate the system because $N - 1$ other channels remain. To calculate Q , the system failure probability, we must (for this simple case) calculate the probability that all the channels fail. To do this, we calculate the average time per testing interval that the system is failed, which is equal to Qw .

We start with all N channels in working order at $t = 0$. At time t , the probability that any $N - 1$ channels have failed is $N(ut)^{N-1}$. The factor N is the number of combinations of $N - 1$ failed channels among N channels. It should be noted that use has been made of the hypothesis of channel independence to permit the joint probability of failure of several channels to be set equal to the product of the individual failure probabilities.

As before, the probability that the last channel fails in dt is $u dt$, and the unprotected time is $w - t$. The desired average is therefore

$$Qw = \int_0^w u dt (w - t)N(ut)^{N-1} ,$$

which gives

$$Q = \frac{1}{N + 1} (uw)^N .$$

It is customary to speak of a figure of merit, given by

$$F = \frac{1}{Q},$$

so the result is

$$F = \frac{N + 1}{(uw)^N}.$$

It is evident that for small values of the product uw , increasing N results in a large increase in F . As an example, consider a channel unsafe failure rate u of 2 per year and a testing interval w of 8 hr. Simple calculations yield

| <u>N</u> | <u>F</u> |
|----------|-------------|
| 1 | 1,095 |
| 2 | 900,000 |
| 3 | 660,000,000 |

Care is needed in interpreting the meaning of large values of F . For $w = 8$ hr, the expected value of the time unprotected following system failure and before the next test is 4 hr, since the failure is equally probable at any time during the interval. By contrast, the predicted average unprotected time over the 40-year life of the plant, for $N = 3$, is about 2 sec. The averaging process is therefore being performed on an extremely small population of failures and has little meaning for a single reactor. An unprotected time of 4 hr for an $N = 3$ system would be expected every $4 \times 660,000,000$ hr, which amounts to about 300,000 years, or approximately 8000 reactor lifetimes. Alternatively, an ensemble of 300,000 reactors would be expected to have one unsafe protection system failure per year. This is the true meaning of the large value of F for $N = 3$; to say that it implies an average unprotected time of 1/20 sec per year is misleading and self-deluding, although mathematically correct.

To calculate the unserviceability of the system of redundant channels, we let v be the safe failure rate of a channel. In the simply

redundant system, the false actuation rate is then

$$V = Nv .$$

For small values of v and uw , the improvement in safety brought about by increasing N usually outweighs the much smaller price in increased V . It should be noted that in some systems, v and uw are not small enough for this to be true.

4.5.2 Coincidence

It is often desired to arrange redundant channels of protection instruments so that the safety action is initiated when a coincidence of M channel trips occurs. The principal usefulness of coincidence is to facilitate on-line testing. Coincidence is also thought by some to be useful in reducing false scrams, but the evidence is not presently conclusive.¹⁴

For a system of N independent channels arranged so that an M -fold coincidence will initiate safety action, arguments similar to those in Section 4.5.1 give

$$Q_W = \int_0^W u dt (w - t) \frac{N!}{(M - 1)! (N - M)!} (ut)^{N-M} ,$$

whose solution is

$$Q = \frac{N!}{(N - M + 2)! (M - 1)!} (uw)^{N-M+1} .$$

The simple redundancy of Section 4.5.1 is just the case for $M = 1$. The equation for Q then reduces to the form previously given. The principal effect of coincidence on Q is to decrease the power to which uw is raised by the amount by which M exceeds unity. For $N - M$ greater than or equal to 2, the practical effect is small because Q is exceedingly small (see Sect. 4.5.1).

Coincidence has a marked effect on the calculated value of the false actuation rate. To apply probability theory, it is assumed that some channels trip falsely, and then the probability that this number reaches

M before the failed channels can be repaired is calculated. The testing interval is not significant here, since a safe failure announces itself and does not require a test for its disclosure. The relevant time interval is the repair time, r , the delay between the occurrence (and instantaneous disclosure) of the failure and the moment when the channel trip is cleared. It might be suspected that the reactor operator would try to reset the trip no matter what its cause, but we shall here assume that the "repair" puts the channel back into operating condition, "as good as new."

For a single channel in which a safe failure occurs at $t = 0$ and lasts until $t = r$, the probability that another given channel will fail safely during this time is (approximately) vr , and the probability that $M - 1$ given channels will fail during this time is $(vr)^{M-1}$. The expected rate at which this particular M -fold coincidence of safe failures will occur is therefore $v(vr)^{M-1}$. Such coincidences can happen in $N! / [(N - M)! (M - 1)!]$ ways (permutations). The expected false actuation rate is therefore

$$V = \frac{N!}{(N - M)! (M - 1)!} v(vr)^{M-1} .$$

Again, for $M = 1$ the formula reduces to that for simple redundancy.

Some numerical examples are given in Table 4.2. It is evident that from the standpoint of reliability calculations based on probability theory, simple arrangements of high-quality channels are adequate in both safety and serviceability. Moderate changes in the channel parameters (r , u , v , and w) would not change this conclusion, but large changes might. For example, changing the testing interval, w , from 8 hr to one year would increase Q for a two-out-of-three system to four from its Table 4.2 value of 3×10^{-6} . This absurd value of four for the "unprotected fraction" arises from the postulated average rate of two unsafe failures per year per channel; a testing interval of one year is utterly incompatible with such a failure rate. It should be remembered that the formulas given here apply only where the numerical value of uw is small compared with unity.

Table 4.2. Numerical Examples of Probability Calculations of Reliability^a

Premises:^b $r = 1$ hr = repair time
 $u = 2$ per year = unsafe failure rate
 $v = 2$ per year = safe failure rate
 $w = 8$ hr = testing interval

| N, Number of Redundant Channels | M, Number of Coincident Channels Required to Initiate Action | Q, Probability of Failure | V, False Actuation Rate (number per year) |
|---------------------------------|--|---------------------------|---|
| 1 | 1 | 1×10^{-3} | 2 |
| 2 | 1 | 1×10^{-6} | 4 |
| | 2 | 2×10^{-3} | 0.001 |
| 3 | 1 | 1.5×10^{-9} | 6 |
| | 2 | 3×10^{-6} | 0.003 |
| 4 | 1 | 2×10^{-12} | 8 |
| | 2 | 6×10^{-9} | 0.006 |

^aThe values of Q and V are approximate.

^bThese parameter values are based on experience of the authors and others.

It is our belief that although such calculations as these should be performed and are valuable in pointing out vulnerable components to the designer, the true reliability of a protection system is dependent on events not considered in statistical theories of the kind outlined. Human operator errors, bad setup or maintenance procedures, and channel interactions are examples of such nonstatistical occurrences not in the theory. One goal of statistical reliability calculations ought therefore to be to predict such low system failures rates that random component failure of the types considered can be neglected as a cause of system failure.

In actual reactors, more than one parameter is involved with most protection functions, and it is important to know how to combine the probabilities of safe or unsafe failures associated with different

parameters. Such a combination would be needed to give an overall figure of merit or false actuation rate for the protection system.

For safety, an overall Q can be calculated as the sum of the Q 's for each parameter associated with a given function. Thus there would be values for reactor scram, containment isolation, etc. This method overestimates Q and hence underestimates safety because many potential accidents are protected against by two or more parameters. In this case, loss of protection for one parameter (temperature, for example) is partly compensated by protection for another (high neutron flux). The interrelationships are ordinarily too complex for calculation, so the overall Q can be calculated as indicated above.

For serviceability, the false actuation rates for the various parameters are simply added.

More complex arrangements than M-out-of-N coincidence are feasible and sometimes practicable. Their probability analyses are performed along the same lines as are described in this section.

Two types of coincidence logic, called here general and local coincidence, are illustrated in Fig. 4.1. They have different logical functions, different safe and unsafe failure rates, and different construction problems. Local coincidence is often specified on the basis of its lower predicted false actuation rate, but our experience has been that this rate can be made satisfactory for either type of system and that the general coincidence arrangement is much easier to test properly than the local arrangement.

4.5.3 Safety or Danger in Numbers

A further example of the application of reliability calculations to protection-system analysis is Epler's evaluation of control rods and isolation valves.¹⁵ For a reactor with ten shutdown control rods connected to a protection instrument system, we will suppose that the instrument system has a nominal F of 10^6 or Q of 10^{-6} — a value easily attainable. In considering the control rods, the usual situation is that inserting any one will stop whatever is going on, at least for a while. If this is so, the rods are a one-out-of-ten system with $Q = (uw)^{10}/11$. If the

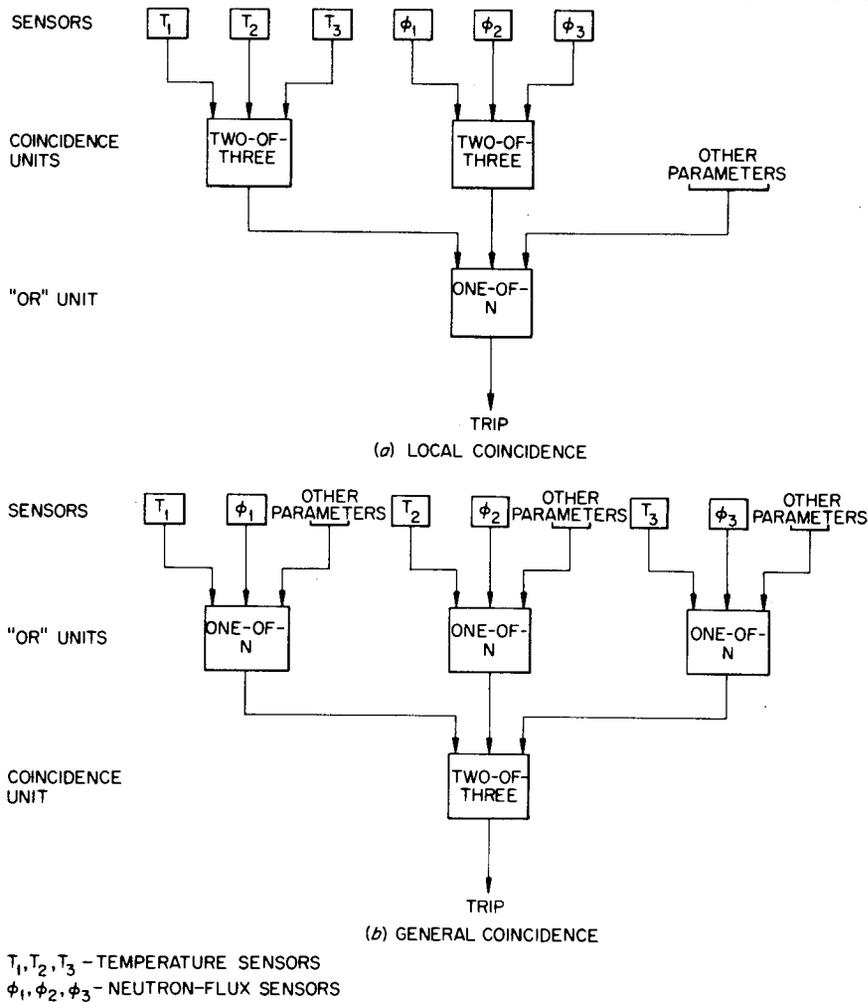


Fig. 4.1. Types of Coincidence Logic.

rod system is to be as good as the instrumentation, $Q = 10^{-6}$ and $uw = 0.32$. Almost anybody can build rods with a uw of 0.32.

Next we will consider that in this same reactor a system of ten ventilating ducts must be closed under accident conditions. Again, we will assume that the protection instrumentation to do this has a Q of 10^{-6} . If the valve system is also to have a Q of 10^{-6} , and one valve is provided for each duct, this is a ten-out-of-ten system, for which $Q = 10^{-6} = 5 uw$; uw must therefore be less than 2×10^{-7} . For ventilation valves, w is certainly no less than one week, so this requires that u be less than 10^{-5} per year. This is an impossible condition with present technology, so

we postulate two valves in series in each duct. This is not a ten-out-of-twenty system, since there are some combinations of ten failed valves that let the containment system leak. Rather, it is considered a ten-out-of-ten combination of one-out-of-two subsystems.

The probability of failure of a ten-out-of-ten combination of identical subsystems is approximately $10Q$, where Q is now the probability of failure of a single subsystem. Therefore Q for each subsystem of two valves in series must be 10^{-7} , which leads to a value of uw of about 5×10^{-4} . Here, u and w , respectively, are the unsafe failure rate and testing interval of the individual valves. For $w = 1$ week, u must be 0.025 per year, and the valves must have a mean time between failures of 40 years. These would be very good valves, but perhaps not beyond possibility.

It is worth noting that the ten control rods give safety in numbers, while the ten ventilating ducts give danger in numbers. Nobody would really be satisfied with the operation of rods for which uw was 0.32, and yet the resulting safety is adequate. On the other hand, a uw of 5×10^{-4} is required of each of the valves. An important distinction is that an inadequate value of uw for the valves would not show up in plant operating troubles the way rod difficulties would.

4.5.4 The Meaning of Operating Experience

It might be supposed that statistical analysis of reactor operating experience would yield useful data regarding component and system failure rates. This has indeed been true with regard to serviceability. Although the early studies¹⁴ showed poor agreement between predictions and observations, better results have been obtained recently.^{16,17} The U.K. group has been able to predict component and system failure rates consistent with their observational predictions that are based on a careful and searching analysis of the relevance and validity of their input data. It is worth noting that these researchers found it necessary to include much more input information than the commonly used electronic component failure rates.

With regard to safety, the present situation is not at all clear. Operation of a few plants for a few years without finding unsafe

protection system failures may give almost no information regarding the protection system, except that its serviceability is adequate if the system does not suffer an unacceptable false actuation rate. Calculations can be made to determine how many reactor years of operation are required to show, with a given confidence limit, that a particular system reliability has been achieved.¹⁸ The result is a function of the testing interval and the number of unsafe failures that occur. For example, these calculations for a two-out-of-three system indicate that approximately one year of operation without an unsafe failure is necessary to show that a system failure probability of 10^{-6} is being achieved with a confidence limit of 95% for a testing interval of 8 hr. Actually, testing intervals presently used in power-reactor protection systems are reckoned in weeks, rather than hours, and some components, such as detectors and actuators, are tested annually. The above calculations for a testing interval of two weeks indicate that operation without a failure for approximately 50 years is needed to demonstrate a Q of 10^{-6} with a confidence limit of 95%. If unsafe failures occur, the operating time must be increased. In all likelihood, far more reactor-years of operation will be required than will accrue before this report is obsolete. Even when — or if — adequate statistical evidence becomes available to establish that the in-service unsafe failure rate is satisfactorily low, confirmation of performance will still be required.

4.6 Channel Independence

The application of redundancy to the design of protection systems and their evaluation depends critically on the assumption that the redundant channels are independent. Any interaction introduces the possibility that a single event could incapacitate more than one channel. In that case, the idea that the working channel could make up for the unavailability of the failed channel would be incorrect, since operability of any channel would be suspect. In probabilistic terms, this means that the probability of failure of all N channels in time t would be not $(ut)^N$, but instead it would be more like Zut , where Z is an interaction coefficient

that gives the conditional probability that the first failure will propagate to the remaining $N - 1$ channels.

A simple numerical example illustrates the devastating effect of a small amount of interaction. Consider the two-out-of-three system of Table 4.2, for which Q was originally 3×10^{-6} . In order for interaction-type failures to contribute no more than random failures to the loss of safety, Z_{uw} must be no greater than $(uw)^2$, since $(uw)^2$ is the probability of system failure from random failures. Thus, the requirement is that Z be 10^{-3} or less, approximately. Thus, an interaction probability of 10^{-3} increases the system failure probability by about a factor of 2. Clearly, interaction to what seems to be a negligible extent has a large effect on the probability of failure of the system. Moreover, it must be noted that interaction between channels allows a single failure, whether random or nonrandom, to affect the entire system. We emphasize that nonrandom failures are not treated in reliability theory and that a nonrandom externally caused failure may have a high probability of producing system failure.

On the other hand, complete independence is unattainable. The redundant channels reside in the same reactor, indeed in the same subsystem and process stream. They share the same reactor core, building, and control room. They are afflicted with the same natural disasters (hurricanes, earthquakes, etc.) and, inevitably, the same human caretakers. It must therefore be acknowledged that efforts to achieve channel independence are doomed not to succeed completely. However, the serious effect of a small amount of interdependence justifies much attention to its elimination where possible.

4.6.1 Interdependence Arising from Common Elements

The most obvious source of channel interdependence is the presence of elements common to more than one channel. Examples abound. The simplest, not often seen now, is the use of a single detector, amplifier, or the like for two or more channels of protection. Less obvious, but no less serious, is the use of logic elements (AND gates, OR gates, relays, circuit breakers) that are not redundant. That logic elements must be common to several channels is acknowledged; if two-out-of-three

channels are to initiate protection, the two-out-of-three logic must receive input signals from three channels and must thus be a kind of common element. This fact is recognized in the definition of a channel: "The channel loses its identity where trip signals are combined." On the other hand, failure of the logic portion of the protection system must not be allowed to inhibit safety action. The logic subsystems must therefore be designed with the same quality, redundancy, testability, etc., as the information channels connected to them. It is usually not possible to separate the logic elements into channels, so the no-single-failure criterion is more difficult to apply, the presence of a common element constituting an Achilles' heel is more difficult to detect, and testing to find the first failure is more difficult to perform.

In some designs, all the safety devices are connected to a single bus, power to which is supplied by multiple sources through some sort of logic circuit. This single bus is a common element whose failure (connection to a battery, for instance) would cause the entire protection system to fail. The example most often seen is connection of all control-rod magnet (clutch, trip, etc.) coils to a common bus. In principle, it should be possible to design a single-bus system adequately so that no single failure would inhibit the safety action. In practice, however, single-bus designs leave much to be desired, and they are generally very difficult to test adequately. Provisions needed to counter postulated failures encumber the systems to the point where they are more complex than the multiple systems whose "complexity" was originally avoided by choosing the single-bus design. Our present opinion is that single-bus designs should be avoided.

Another sort of common element is a power source used for more than one channel. Although systems almost invariably fail safely upon total loss of electrical energy, this is not always the case for the loss of a single supply. Common bias regulators are notorious examples of such interdependence. High voltage as well as low must be considered.

Yet another example of a common element is a mode switch. Many protection systems must operate in different ways for different operating regimes: startup, low power, base loaded, load following, special testing, one or more heat-removal systems out of service, refueling; that is,

for various nonstandard or multiple-standard sets of conditions. Switching protection system modes to correspond to plant operating regimes is often done manually under administrative control. (The consequences of failure — having selected the wrong mode — must be considered but are outside the scope of this discussion.) This switch is a potential common element, since in general many channels or interconnections intended to be independent are brought together in the switch. It is important that this convergence not compromise channel independence, even if the switch should break in an unexpected way. Separate switch sections with plenty of distance between them are part of the answer.

The testing equipment can be a common element compromising channel independence. This is most obvious in testers of the octopus type with tentacles reaching into every corner of the protection system to inject test signals and to sense test responses. Such a machine inevitably provides potential for cross connecting supposedly independent channels. It is a difficult and frustrating chore to find, eliminate, and demonstrate the absence of channel interdependence from this source. At the other end of the spectrum, a simple tester in the form of a single box connected in turn to various channels cannot give rise to direct interconnections between channels. Rather, an interdependence can occur via a failure in such a tester, or a mistake in the procedure used by the man applying it, with the result that there is incorrect adjustment of all channels to which it is successively connected. Experience with this kind of failure has been rather widespread; dependence should not be placed wholly on a single tester.

4.6.2 Interdependence Arising from Common Environment

To the extent that protection systems and components are vulnerable to extremes in environment, so will channels be interdependent if they are affected by the same environmental influences. The interdependence is enhanced by proximity of the different channels, enhanced further by their sharing the same box (cabinet, rack, chassis, conduit, penetration), and enhanced still further by any possibility that trouble in one channel (overheating, leaking) can cause trouble in another. The only real safeguards are distance and physical barriers.

5. RELATIONSHIP BETWEEN PROTECTION AND OPERATION SYSTEMS

As defined in Section 1, the operation system makes the plant do what is wanted; the protection system stops the plant if it does something not wanted. The operation system should therefore prevent excursions, while the protection system should suppress them or mitigate their consequences in the event the operation system does not prevent them. Interaction between these two systems has an important effect on the required reliability of both systems.

5.1 Interaction Between Need for Protection and Failure Probability

In Sections 4.1 and 4.5, we stated our belief that an appropriate goal for a protection system is a calculated probability no greater than 10^{-6} that the system will fail to function when needed. Experience with some protection systems has strongly suggested the achievability and adequacy of this goal, although the evidence is not extensive enough to be conclusive. That 10^{-6} is an adequately small calculated failure probability is based on several premises. First, it is assumed that failures are random and that the probability of failure is uniform over the life of the plant. Second, it is assumed that a genuine need for protection system action occurs rather seldomly. So far as we know, this is in agreement with the available evidence. It is a necessary assumption, since if the protection system had to function once per hour, a failure probability of 10^{-6} per try would give an average unprotected failure rate of about one every hundred reactor-years, or a 40% chance that a reactor would experience some sort of unprotected accident during its 40-year lifetime. Third, it is assumed that the need for protection and the likelihood of protection being available are independent. This assumption is essential to any evaluation based on probability of success or failure of the protection system. If there is any possibility that the need for protection can cause a lack of protection, probability analysis is meaningless, since in this case the failure events are not random. The unprotected accident rate under such conditions would be the rate at

which events occurred that needed protection, multiplied by an interaction coefficient that would relate need to failure of the protection system. In Section 4.6 there is a numerical illustration of the effect of a slight interaction on the computed failure probability. Stated another way, it is not possible with interaction to multiply a low rate of events that need protection by a low probability of failure where protection is needed to obtain an acceptable, extremely low, rate of occurrence of unprotected accidents.

The operation system is of concern in this connection because it can induce events for which protection is needed and because it has a potential for interaction with the protection system. Thus, the possibility exists that interaction between the two systems could invalidate the design basis of the protection system.

5.2 Role of Operation System in Need for Protection

The operation system can induce events for which protection system action is needed. The classical example is the neutron-flux servo system that withdraws the regulating rod and initiates a reactivity transient. Other examples of controller failure are the level regulator on the SPERT-3 pressurizer and the volume control system for the MTR head tank, but controllers are not the only type of operation instrument whose failure can require protection system action. The human operator is a regulator capable of complex control actions, which he performs on the basis of information received principally from operation instruments. He has available an almost infinite variety of correct and incorrect actions he can make. Any operation instrument, therefore, whose incorrect reading or action will cause the human operator to act (correctly, on the basis of information available) so as to require a protection function is in the class of instruments whose failure induces need for protection. It is evident from the variety of operation instruments and the prevalence of manual control under administrative procedures in nuclear power plants that the operation system has large potential for invoking the need for protection system action.

It is worth noting, because it is sometimes forgotten, that any potential requirement for protection action as a result of failure of the protection system is an invitation to catastrophe.

5.3 The Consequences of Interdependence

The likelihood that operation system failure can result in conditions that require protection system action, the need for safety, and the pernicious effect on safety of interaction between protection and operation systems lead to the criterion that interactions between the protection system and the operation system shall be minimized. The objective is to avoid the possibility that a single cause can initiate an event needing protection and then negate the protection and let the excursion proceed while the protection system stands approvingly by.

The subject of interaction between operation and protection systems is not academic. The HTRE-3 core was melted because a failure in an element common to the neutron-flux servo and the neutron-flux protection was inadequately designed; failure of the common element to perform correctly induced the accident and paralyzed the protection. The SPERT-3 pressurizer broke, partly because the level control and the level protection used the same sensor.¹⁹ Misoperation of NRX controls caused an excursion and deactivated the shutdown system.¹¹ At Hanford and at WTR, rod withdrawal by the operator based on instrument readings during an accident made the consequences worse. Many other instructive examples with more tolerable consequences are hidden in logbooks; perhaps something can some day be learned without waiting for human or property damage, but for the present, learning seems to occur largely via punishment.

If nonnegligible interaction between the operation system and the protection system were to be permitted, a showing of adequate protection would have to be based on a low frequency of need for protection. Demonstration that events needing protection would occur at a rate tolerable for such a situation has not yet been attempted. For a numerical example, consider a goal of 10^{-6} unprotected accidents per reactor-year, together with an acceptance of a known interaction coefficient of 10^{-3} . To achieve the goal, events requiring protection would have to occur at a rate of

less than 10^{-3} per reactor-year. It would be extremely difficult to show that such a low rate was in fact not exceeded. Verification that the need for protection occurred at a rate less than 10^{-3} per reactor-year would require at least 1000 reactor-years of operation for a confidence level of 66% and 6900 reactor-years for 99.9%.¹⁸ It will be a long time before a high degree of confidence in a low rate is possible. Lacking experimental evidence, an attempt might be made to demonstrate by analysis that such a low rate would exist, but assurance at the required confidence level would be hard to achieve. To date, in fact, the difficulty of making such an analysis has been prohibitive.

5.4 Modes of Interdependence

Interdependence between the protection system of a reactor and its operation system can arise in a variety of ways. Interaction between channels of instrumentation was discussed previously in Section 3.2.5. The sources of channel interaction described there for protection channels apply to interaction between the protection system and the operation system.

It is also worthwhile to refer to Section 4.6 for a discussion of the impossibility of complete separation of channels. In the same spirit, it must be acknowledged that the protection system of a nuclear power plant occupies the same microuniverse as the operation system of that plant; that is, the same containment building, control room, primary process system, reactor core, operating staff, and so on. It is certainly impossible, in this larger sense, to provide complete isolation of these two systems from each other. The subject of this section is therefore the elimination of removable interdependence, both intentional and unintentional.

5.4.1 Common Elements

The use of a single instrument module for more than one protection-system channel is now almost never seen, and yet many designs currently in use incorporate modules - channels, in fact - that serve both protection and operation systems. An example frequently encountered is the use of a detector, an amplifier, and an action generator, together with

the appropriate power supplies, to furnish signals to controllers (operation) and to trips (protection). There is no way of disguising that these common elements provide interdependence between the operation system and the protection system. Sometimes an "isolation amplifier" is used to avoid propagation of the most obvious failures from one system to the other, but most of the interdependence remains. If the detector, or the amplifier, or a power supply, or any other common element, including the isolation amplifier, should fail, this failure would affect both the operation system and the protection system.

Three defenses of this arrangement have been offered. The first, that failure is sufficiently unlikely that the system safety is adequate in spite of interdependence, has been utterly and (we hope) finally discredited. The second defense is the observation that for some combinations of protection and operation instruments no conceivable failure of the operation component involved can result in a situation requiring action of the protection component involved. To the extent that this can be proved, both initially and throughout reactor lifetime, the particular interdependence could be acceptable. A hypothetical example is the instrument system used to measure and control the pressure of a sealed containment enclosure. The operation component is used principally to provide a pressure differential between the inside of the containment structure and the outside and thus to provide a means for surveillance of the leakage rate. The protection action might be to initiate reactor shutdown, emergency cooling, and isolation of process piping if an increase in containment system pressure should indicate the presence of a serious leak of potentially radioactive fluids. It might be demonstrable that no failure whatever of the instrument measuring containment leakage rate could induce a substantial leak of radioactive fluid, in which case no real interdependence of operation system and protection system would in fact exist. The application of this defense is discussed further in Section 5.1.1.

The third defense, which is the one usually brought forward, is based on redundancy and the improbability of simultaneous failures. Total failure of a channel with both operation and protection functions would not

negate all protection. Other redundant channels of protection system instruments would remain available if needed to cope with the event induced by the operation system failure or with any other need for protection system action. This point of view is recognized in the IEEE Criteria (App. B), which require extra redundancy where protection channels are used for operation functions. The objective seems to be that upon total failure of all equipment used for the operation function (including equipment common to the protection and operation systems), the remaining protection equipment shall have the redundancy specified for a protection system standing alone. Our present view is that this approach is not very rewarding (see Sect. 5.5).

It often occurs that the elements which actually perform the protection function are also used for operation functions. The most obvious example is the reactivity control rods, which are used for control and safety. Other examples are emergency coolers that are also used for normal cooling or during normal shutdown, electrical buses used for vital loads that include operation and protection functions, and charging or feedwater pumps used for emergency core cooling. In some cases, the advantages of this mode of protection-operation interdependence outweigh the disadvantages, but the potential for systematic failure of protection as a result of the interaction must be thoroughly analyzed in all cases.

5.4.2 Interdependence Arising from Operational Use of Protection Instruments

An insidious form of interdependence arises as a result of the use of protection instruments for operation purposes. As a simple example, consider a test reactor with the usual scram on high neutron flux. In many such reactors, the readings of the flux-measuring instruments are prominently displayed to the operator. This is legitimate, since the measured or apparent values of all protection parameters may be needed quickly in analyzing unusual situations. On the other hand, use of these displayed values as the primary operating variables can cause, and has caused, a variety of problems affecting the protection action of this instrumentation:

1. There is a tendency for the operators to demand accuracy beyond what is needed for safety in order to improve operations. The resulting "improvement" may degrade safety through additional complication, better smoothing with poorer time response, or increased adjustment frequency with correspondingly increased chance of gross maladjustment.

2. Redundant measurements of a single parameter always disagree to a certain extent, and neutron-flux instruments are notorious offenders in this regard. The use of these instruments to operate the plant creates a demand that they agree - a requirement unrelated to protection requirements. Adjustments not needed for protection are added, and used frequently, with results potentially deleterious for the protection action.

3. Finally, if the operator is sufficiently seduced by these read-outs, a failure in the protection instruments can induce him to initiate an increase in power, the protection for which has just been reduced or lost.

There have been several instances of the above problems in test reactors.⁷ The extension to nuclear power plants is evident, though complex.

5.4.3 Use of Protection System Signals for Quasi-Protection Functions in the Operation System*

In Section 2.4 we mentioned that instruments are often installed whose function it is to avoid protection action by forestalling it with a less drastic preventive action. A classic example from test-reactor technology relates to the high-flux scram. To forestall the scram, the rods are inserted with their drive motors if the reactor power exceeds a preset value lower than the scram point but higher than normal operating power. The motor-driven insertion produces a slight decrease in power (the insertion stops when the power decreases below the preset value) and is reversible. The cost of operation is minimal - orders of magnitude smaller than the cost of a scram. Moreover, such instruments can be installed in echelon; for example, they can block rod withdrawal if

*We are greatly indebted to Mr. J. S. Moore of the Westinghouse Electric Corporation for an enlightening discussion of this subject. Mr. Moore should not be held responsible for our conclusions, however.

the power exceeds another set point lower than the preset value for motor-driven insertion but still higher than normal operating power. In this way, the most probable cause of a power increase would be inhibited before it would cause trouble.

Avoidance of protection action is an operation function, since the protection action, however expensive, is by definition tolerable. (The action under discussion merely avoids a tolerable event.) However, it is convenient to use the redundant signals from the protection system instruments to initiate these quasi-protection actions, even though they are truly operation and not protection functions. To what extent is this use of protection equipment for an operation function justified?

Quasi-protection functions fall into two classes. Functions in the first class cannot induce any situations requiring protection action. The examples given fall into this class. Motor-driven rod insertion or blocking of rod withdrawal can be annoying, can limit the available power, and can even cause plant shutdown (if caught by xenon, for example), but it is difficult to imagine their provoking any excursions or other need for protection system action. We see no reason to forbid the use of signals from the protection system for such functions.

The second class of quasi-protection functions is different in that successful action can provoke the need for protection system action. An example is to be found in a pressurizer control system, where the charging flow is valved off if the level gets too high in order to prevent overfilling and having to relieve the primary system. On the other hand, shutting off the charging because of a spurious signal would have potential for requiring not only reactor shutdown but perhaps activation of engineered safety features as well. It seems evident in this example that the level instrumentation can, by its malfunction, initiate an excursion (the decrease in level caused by valving off the charging flow) which the same system would then be called upon to sense (low level) in calling for protection action - a clear case of interdependence if the same instrumentation is used for both level functions.

It therefore appears that the use of protection signals for quasi-protection-operation functions can be acceptable or not, depending upon

the circumstances, and that each such proposed use must be considered on its merits.

5.4.4 Identical Devices for Protection and Operation

We caution against merely separating the protection and operation systems and using identical instruments in both systems. Identical elements may be subject to simultaneous failures as the result of a single event. Such failures can be brought about by external events or environmental factors. This class of failures we call "common disasters."

A recent study of common disasters in instrument systems indicates that their rate of occurrence may be ten times the rate at which the co-existent independent failures of two redundant channels²⁰ will cause a system to fail. The coexistent failure rate from independent failures can always be decreased by increasing the number of channels or by decreasing the testing interval, but common disaster rate for identical channels of instruments is determined by nonrandom external events and cannot be so reduced.

Some typical external events or environmental factors are listed below:

1. changes in characteristics of the reactor plant; for example, flooding a beam hole with water and thus affecting the neutron attenuation to all neutron detectors;
2. unrecognized dependence on a common element; for example, a single desiccant system serving dry air to all coaxial cables for the protection and operation systems;
3. disabling by the accident being guarded against; for example, the high ionization current from the power burst of a pulse reactor destroying the field-effect transistors in the amplifiers of all the neutron-detecting channels;
4. communication error (or human error); for example, typed instrument settings posted on or near the related instruments, in an effort to improve maintenance procedures, but with the typed numbers in error and all identical instruments being incorrectly adjusted.

A possible solution to the common disaster situation is the use of diversity. Instruments of different types and based on different principles should be less susceptible to a common environmental factor. Diversity must be carefully planned and applied. The probability that diversity will prevent an accident may not be very good when such diversity is not expressly designed for this purpose. In some cases, it may be that one device is far superior to all others for a specific job. In such a situation, an attempt should be made to limit the use of identical units to that one device and to evaluate thoroughly its failure modes.

5.5 The Case for Independence

The basic justification for independence of protection and operation systems, in our opinion, is the relative ease with which the protection function can be assured with independence and the great difficulty of realizing such assurance with interdependence. We have found it easier to separate the systems than to assure that their interactions are harmless. We believe it to be easier to maintain independence than to insure, for the lifetime of the plant, that deliberate changes or inadvertent alteration of the operation system will not adversely affect the protection function. We acknowledge the controversial nature of this subject and that there are some arguments in favor of the contrary viewpoint. We also acknowledge, as discussed in Sections 4.6 and 5.4, the unattainability of complete independence.

The dismal list of accidents caused by design errors, and the much larger list of design errors caught before they caused accidents, lead us to believe that design errors will continue to occur. We believe further that independence of operation and protection is one of the best defenses against the possibility that a design error may cause an unprotected accident.

Failure of a control function of the operation system is a possible cause of the need for a protection function. Our concern is that the instruments in the protection system that are expected to provide this protection function will fail from the same event that caused loss of control. The instruments in the channels that provide a particular

protection function and the instruments in the channels whose failure will cause the need for the particular protection function should not be identical.

It is easy to show, with probability analyses of the type illustrated in Chapter 4, that system failures, whether linked to interdependence or not, arising from random component faults can be neglected. We are concerned with systematic, nonrandom, concurrent faults in protection and operation systems that may lead to potential accidents not considered in probability calculations.

5.5.1 Independence of Function in Spite of Interdependence of Equipment

As we stated in Section 5.4.1, interdependence of operation and protection systems can, in principle, be justified either by lack of real interaction of function or by provision of extra redundancy. Also, in that section we gave a hypothetical example of acceptable sharing of protection and operation system components. The basis was the impossibility that failure of the operational equipment could ever, under any circumstances, lead to a situation in which protection action would be needed. Therefore, sharing of equipment (common elements) between the protection system and the operation system could not lead to interaction between the two systems. It would be difficult to prove conclusively this lack of functional interaction, and the problem of insuring that this lack of interaction could and would be maintained throughout the life of the plant would be even more difficult. Operators are not designers, and operators in charge of the plant at the end of its 40-year life are not the ones who may have discussed protection problems with the designers at the beginning. Subtle considerations are likely to be forgotten or ignored. It is easy to forget that plant protection was originally based on the impossibility that failure of certain operation instruments could result in a need for protection system functioning. For these reasons, we believe that only in exceptional cases should operation-protection interdependence be designed on the basis that failure of the operation function cannot involve the need for protection.

5.5.2 Extra Redundancy

Inclusion of extra protection system redundancy has recently been proposed* as an antidote for operation-protection interdependence, particularly for interaction due to common elements. No complete design with this feature has yet been built and operated, so perhaps our comments are premature. Nevertheless, we see some hazards in this approach.

As we understand it, the proposal calls for sufficient redundancy that if all equipment used for operation should fail, the remaining instrumentation would constitute a protection system whose redundancy (and other features) would be satisfactory. In principle, therefore, failure of all elements common to the operation system and the protection system would be tolerable. This appears to satisfy the criterion for inclusion of such equipment in the operation system, and yet it is also used for protection by providing "extra" redundancy. The question arises whether this extra redundancy is in the direction of increased safety.

The use of redundancy to improve system safety is strongly dependent on the independence of the redundant channels (see Sect. 4.6). The possibility of interaction between protection channels is always present. In the case at hand, however, use of the extra channels for both operation and protection opens the way for interdependence between the protection channels not used for operation and the operation system proper via the dual-purpose channels. We believe that this interdependence reduces the overall safety of the system. The protection channels not used for operation are required to be adequate in all respects, including redundancy. The probability of random failure is therefore negligibly low without the extra redundancy, which therefore buys nothing usable in probability (see Sect. 4.5.1). We suggest that extra redundancy is a specious remedy for a curable disease. Instead, the common elements should be eliminated and the protection system made independent of the operation system.

5.5.3 The Benefits of Interdependence

Those with a viewpoint antithetical to ours hold that interdependence is not only allowable but provides benefits to safety and serviceability.

*By IEEE; see Appendix B.

We shall attempt to summarize the arguments in favor of this view, but we must acknowledge our bias in favor of independence of the protection system and the operation system.

It is suggested that the distinction between protection system and operation system is not useful. Since the operation system must prevent excursions of plant variables outside their limits, and the protection system must suppress such excursions in the unlikely event they occur or mitigate their consequences, both systems are important to plant safety and both systems are supposed to work. Both systems are designed not to fail by using the best techniques available for the job, and both systems are built with modules of high quality. It is said therefore that it is necessary to treat only the "plant instrumentation and control system," which is a single entity with many parts and is called in this review the control system for brevity.

The control system, according to this view, is designed and built "all of a piece"; that is, interactions between channels and functional interactions are considered on their merits. Whatever redundancy or other features may be necessary to insure protection where needed are incorporated into the channels. Recently, design proposals have tended to include extra redundancy (see Sect. 5.5.2) where equipment is used for both control and protection, with one channel only (perhaps selectable among several) being used for the controller. In other examples, an average of the signals from several channels is computed by the controller. Modes of failure are considered for each channel, with channel independence usually assumed. Testing provisions vary widely. The stated objective is to provide adequate control and protection by using redundancy, testing, and monitoring, coupled with especially good, foresighted design to accomplish the result.

A stated benefit of this approach is the continual use of the protection equipment. In order to control the plant, the operator must use, often, the equipment on which he also relies for protection of the plant. Instead of standing idle, waiting for a once-a-year or once-a-million-years command to function, the protection instruments have frequent or continuous surveillance by the operator. Moreover, failure is announced

when it occurs by the incorrect control signal that arises. In fact, testing of the protection instruments may not be necessary because of the continuous monitoring involved with the control function.

Another stated benefit of this approach is economy, not just in money. Fewer detectors are needed, but more important, fewer penetrations of the shielding and the primary system are required to accommodate the detectors. There is an overall saving in the amount of instrumentation, the control room is less cluttered, and the readouts are fewer in number. The whole system is easier to understand. Further, the customer saves money in initial cost and in maintenance expenses.

The effect of "extra redundancy" on this last item is not yet known, but we suggest that these savings would be eliminated because of the extra equipment that would be needed.

5.5.4 The Benefits of Independence

To the reader who has followed the argument up to this point, it will be evident that we favor independence of the protection system and the operation system from each other for reasons associated with the evils and pitfalls that we believe are inherent in interdependence. On the other hand, there are positive aspects to separation of the operation system from the protection system.

The separated systems are easier to design. Independence permits designing the protection system for protection and the operation system for operation. The protection system must have redundancy and channel independence and be capable of being tested in order to satisfy the requirements for protecting against undue hazard to the health and safety of the public. The operation system can be optimized for ease and economy of operation, or in any other way, with inclusion of each feature decided upon by using engineering analysis of cost and benefits. The current trend toward use of digital computers for operation functions could be in this direction, with use of the computer made possible by its independence from the protection system.

6. THE ROLE OF THE HUMAN OPERATOR IN PLANT PROTECTION

Given an automatic, redundant, tested protection system with demonstrated performance and reliability, what role in plant protection is played by the human operator? A few low-power reactors have been arranged to run unattended, but a nearly universal rule requires the presence of one or more operators. Are these people important to plant protection? Is their function necessary to safety? Can they make a positive contribution to protection? Or, can the human operator be detrimental to protection? The answer to each of these questions can be affirmative under some circumstances.

Humans are complicated beings and are not very well understood. The same man can, on different days, be alert, intelligent, and wise or dull, stupid, and irresolute. The plant protection system is therefore made independent of human caprice in its operation. On the other hand, the human brain is a computer far more complex than anything yet built of electronic components, and surely the memory, reasoning, and decision-making capability of the human operator should be exploited for protection. The methods of doing this are considered in the following sections.

6.1 Human Surveillance

Perhaps the most important role of the human operator is his constant surveillance of the plant. Human monitoring is far more subtle and flexible than any manufactured monitoring system, but it is less speedy and reliable. To make maximum use of both schemes should be the objective. Accordingly, the operator should have all the information he needs to assess the condition of the plant and its protection system. This information should be displayed clearly and as concisely as possible. The use of data-loggers and computers seems to be a worthwhile step in the correct direction.

With good information, an alert operator can "smell a rat" and thus detect plant abnormalities before protection is needed. Moreover, unforeseen combinations of circumstances can perhaps be perceived even in situations wherein no protection system action is provided for. The

vigilance of the operator thus provides a guard, slow maybe and incomplete, against unprotected excursions occurring in unexpected ways. The successes of such vigilance are buried in logbooks; failures are displayed in accident reports.² Operators at NRX and WTR failed to read the signs correctly and aggravated accidents by incorrect actions. The operator at ETR decided that the ¹⁶N monitor was giving a false indication of trouble.* The operators at ORR studied the reactor power fluctuations and then increased the power anyway. For each such incident, there have surely been many situations in which correct action by an alert operator forestalled unacceptable consequences.

The operator is the protection system designer's friend, no matter how many stories seem to demonstrate the contrary. It is the operator who provides, day in and day out, the surveillance essential to correct operation of the instruments. The designer who recognizes this role of the operator will give him easily comprehended displays to make the correct interpretation of the readings routine. Instrument systems whose displays keep secrets from the operator invite misinterpretation of the readings they do provide, misoperation, and eventual inclusion in accident reports. It is especially important that the designer foresee the operator's need for information under unusual circumstances, including accident and postaccident situations.

The operator should have available, possibly in a computer memory, complete information regarding the status of his protection system. Any components known not to be in working order should be so indicated in an obvious manner. The readings of all detectors of safety parameters should be available, and thus it is preferable to use analog equipment rather than process-operated binary devices (switches) from which the operator can learn little if something goes wrong or behaves unexpectedly.

In some designs, the necessary periodic in-service testing of the protection system is arranged so that the plant operator can perform the

*The instrument was "known to be erratic and unreliable," and accordingly its indication was not believed. This points up the futility of providing poorly functioning instrumentation, which might actually be worse than having none.

test himself. This is preferable in principle to the presently more usual technique of requiring an instrument technician or engineer, or a small army of them, to do the testing. The preferred method involves the operator directly and explicitly in the surveillance and testing of the plant protection system. His understanding of that system and concern for it are thereby greatly enhanced. We well remember several occasions in our own experience when informed and alert operators were able to report clearly and accurately on unusual occurrences in protection systems because of their detailed knowledge of them through surveillance experience. We also recall even better the instances in which operator ignorance made valid information unobtainable and evaluation impossible.

6.2 Manual Initiation or Inhibition of Protection Action

The protection system for the first reactor consisted of a man with an axe to cut a rope holding a safety rod when and if he decided (or was told) that a dangerous situation impended. Today this seems primitive and even a bit laughable, and yet the need for manual actuation remains a feature of some protection systems.

The first, and perhaps the original, justification for strictly manual actuation was the possible independence from the vagaries of gadgets of all kinds. To achieve this, the safety action was carried out directly with human fingers. Other examples were dropping of boron-steel balls into the ORNL Graphite Reactor, manual opening of the last-ditch dump valve on NRX, and handwheel-operated rod insertion on early reactors in the U.K. This manual approach is not now used. For one thing, it is more difficult to accomplish anything useful on large reactors; one man-power is not enough. Also, perhaps people now trust certain classes of gadgets more than they used to.

This does not mean that the manual scram switch nor manual actuation of any other protection function should be eliminated. These are facilities essential to the operator in performing his surveillance functions and in acting intelligently on his overall view of how the plant is operating. Intervening equipment between the manually operated switch and the protection function should be minimized and should meet applicable

protection system criteria, such as immunity from single component failures. In addition, the manual facility should be as nearly independent as possible from the automatic protection equipment.

As stated above, manual initiation of protection action is not very often used in present-day technology and is not very often justifiable. The usual reason given for manual operation is a compelling need for the operator's judgment. We encourage exploitation of human judgment, particularly in surveillance, but we question whether such judgment should be employed on the spot in protection decisions. Our chief concern is that the need for judgment may imply intolerability of the consequences of protection action, and thus the need for perfectly failure-free systems (see Sect. 4.1). It seems to us unreasonable to expect (and require) an operator to make, in a few minutes or even seconds, a decision the designer was unwilling or unable to incorporate in the protection system, even after the expenditure of many man-years of design effort. Such a decision by the operator would require information on which he could rely; that is, redundant information. Would it not be better to design, build, and test an adequately redundant protection subsystem to use the same information automatically to perform the required action? We think so, in most cases. If the consequences of this action are so disruptive or expensive as to be almost intolerable, something is awry in the plant design. Shifting the onus onto the poor operator may reduce the probability of expensive false action, but it is not a good way to obtain the needed protection. This point of view, which we think is mistaken, is illustrated in the control room of a power reactor that must remain nameless. The main control panel is dominated by a large sign, lettered "THOU SHALT NOT SCRAM." The reader can imagine the emotional pressures on a luckless operator in that plant who sees a combination of readings which indicate to him the need for a manual shutdown.

It is necessary, of course, that manual initiation of all protection functions be available to the operator so that he will not be helpless in the presence of an indicated need to initiate protection.

One set of circumstances in which we believe manual initiation of protection action would be justified could occur during the aftermath of

an incident or an accident. After the immediate, automatic, protection system response to signals indicating plant abnormalities, the course of the accident, if an accident ensued, would not be especially predictable. That is, although a conservative analysis may have been made to demonstrate tolerability of the worst possible course of events, the actual sequence in any particular incident could proceed in a variety of ways. The choices are likely to be unforeseeable, and the supporting design information may be unknown. It is therefore prudent to plan for automatic initial protection system action to be followed by a choice of alternatives. One example of such a choice is the mode of operation of engineered safety features, such as cooling with high-pressure pumps or depressurizing to use low-pressure pumps. For such a choice to be meaningful the operator must have sufficient information and sufficient time for reasonable exercise of human judgment.

The information needed by the operator to make choices under accident conditions is likely to be more extensive than was foreseen by the designer. The operator will need assurance that his information is valid, and redundancy is necessary for this assurance. Diversity, too, is especially desirable because under accident conditions some variables may seem to have unbelievable values. The operator must in addition keep track of some variables that normally are of little or no concern to him. He must also know just what his protection systems are doing and what else may need to be done.

An example of the need for correct information is to be found in the various inadequate and incorrect responses made by load dispatchers during the blackout in November 1965 in the northeastern portion of the U.S. It is clear from the vantage point of hindsight that too much was required of these people too quickly and that the information available to them was inadequate. In particular, the unforeseen widespread loss of voltage and frequency control caused the instruments to read falsely, so valid information was unavailable when it was most needed.²¹

All the information available must be comprehended by the operator, and this takes time. For a decision of any real complexity, many minutes are required. Simpler decisions might well be automated in order to leave the operator free to concentrate on the complicated questions.

In cases where information must be gathered outside the control room and evaluated, even more time is required - up to 1 hr may be needed.

A variant sometimes encountered is the availability of manual inhibition or delay of an action that otherwise would be automatic. This is actually preferable to manual initiation, since in this case the protection action would take place unless the operator deliberately stopped it. The requisites for this operator decision are the same as for others discussed in this section - enough information and enough time for judgment.

6.3 Other Manual Operations Affecting Safety

In this section, we discuss what is probably the most difficult problem of all related to the role of the operator in plant protection. In large manually operated plants (and all large plants presently proposed are mainly manually operated), the operator makes many decisions and initiates many actions that have some bearing on safety. An example, already discussed in Section 2.2, is control-rod manipulation. The obvious mistakes - overpower, overtemperature - are protected against by trips and forestalled by other means (e.g., rod block). However, more subtle problems abound. Correct rod sequencing is important in large reactors to avoid hot spots and also to insure sufficient shutdown capability. In general, the protection systems do not detect the existence of hot spots or the loss of shutdown margin. In-core instrumentation can reveal flux irregularities, but calculation and/or judgment are required to decide whether these indicate hot spots. Shutdown margin can be inferred from rod position. Other problems of the same class are limitation of the potential reactivity worth of a single rod and spatial feedback due to xenon buildup. The situation with respect to all these potential problems can be determined from instrument readings with more or less calculation and inference. To date, these inferences are not used as protection system inputs, and yet incorrect operator action can cause hot spots, or infringe on needed shutdown margin, or create a rod with too high worth, or aggravate a spatial fluctuation.

This is a gray area that is neither clearly part of protection nor obviously part of operation. The consequences of such operator errors

can be pretty bad — in fact, on the borderline of tolerability. The necessary judgments and inferences are complex, time-consuming, and difficult. At the present stage of reactor and protection system evolution, no clear answer can be stated for this class of problems. Application of on-line computers to these problems is increasing — to the benefit of the quality of information available to the operator, but large digital computers are not yet part of protection systems, and many questions must be answered before they will be. The current rapid increase in the number, power, power density, size, and complexity of power reactors demands an improvement in measurements of the kind discussed here, with concomitant improvements in associated protection system techniques.

6.4 Administrative Control of Protection Systems

Although the preceding sections may seem to treat the protection system as immutable, such is not the case. The system must undergo operation, testing, maintenance, and change. This must be done under administrative control to prevent intentional disturbances. It will always be possible, with planning, to disable as much of the protection function as may be needed for the legitimate ends foreseen above, so unauthorized tampering can be prevented only administratively.

It is almost self-evident that control of access to the protection system is the first line of defense against unauthorized tampering. Control of access is, of course, also the prime defense against intentional sabotage, a subject not treated in this report. The tampering discussed here is directed toward legitimate ends; whether or not it is dangerous depends on circumstances.

Access control can be accomplished by locks and keys, or by surveillance, or both. It is our experience that operators are justifiably more comfortable where they can see the instruments without leaving their posts. The technician with his head in an instrument case can be queried as to what he is doing so that everyone knows what is going on. In large systems, this facility for constant surveillance may be difficult to provide.

Any manipulations of the protection system required routinely should be accomplished by the reactor operator or under his immediate supervision and control. Examples are changing ranges and withdrawing nuclear detectors. The designer should beware of "special conditions" requiring special protection that must be specially accomplished. The NRX accident¹¹ should demonstrate the dangers in such requirements. The operator should always be able to determine easily the state of his protection system, particularly if it is in some such "special" configuration. Instruments out of service, under test, or being repaired should also be clearly indicated to him.

The periodic testing required of redundant channels should be done with the knowledge of the operator and under his control. Any other testing, for example, special tests to trouble-shoot a failure whose exact location is unknown, must be closely controlled to insure that no loss of protection results from the testing procedure.

Changes in the protection system are a potential source of much trouble with respect to both protection functions and plant reliability. The most elementary change is one-for-one replacement of a component, as during maintenance. The necessity for checking the status of the replacement unit is usually well understood.

Operation with some protection equipment known not to be in working order constitutes a change, in that the system is not operating as designed. For a system with sufficient redundancy, the extra cost of the originally installed "spare" is compensated by the value of the additional plant availability thereby achieved. The adequacy of the channels remaining in working order should be demonstrable by calculation and testing, as appropriate. It is also necessary that the equipment in use be independent of the failed components to an acceptable degree.

Design improvements are probably the most radical changes for a protection system. While we do not wish to derogate progress, we have found that design changes are difficult and require large amounts of effort by engineering and administrative personnel. The changes must in many cases be checked and tested with the same or greater care as that used in an original design. Compatibility with the many constraints imposed by

existing equipment and practices must be assured, as well as conformance with original, or revised, plant design bases and accident analyses. After administrative review and approval, the change must be clearly understood by the operators before its implementation. A formal set of procedures is essential to orderly administrative control of changes.

7. CONCLUSIONS

7.1 Lack of Information

Our study of protection system design has been greatly hampered by lack of authoritative information. The technical literature on the subject is essentially void. Only a few papers exist on the statistics of system failures. We found not a single reference in the public domain that gave design bases or assumptions for any of the approaches used. The manufacturers sometimes have prepared an internal report or specification related to this subject in various degrees, and sketchy justifications may be found in various safety analysis reports (SAR's). Because of space limitations and because of the context of support for a license application inherent in an SAR, the information therein is too general to fill the need for high-quality technical information.

The lack of a developed technical literature is evidence of the technical immaturity of the protection system field. A report such as the present one is not an adequate substitute for reports by the workers in the field that give their professional colleagues details of their discoveries and designs. Publication is time-consuming and expensive and could present a controllable risk of divulging company secrets, but it is indispensable to progress in technology.

The lack of technical information on protection system design is complemented by an equal lack of information on protection system performance. We learn by our successes and mistakes, and so long as these are concealed in logbooks, the lessons are confined to the people who experienced them. It is embarrassing to publish one's failures, but presently even the successes remain untold. Some recent efforts by the AEC, while laudible, will not by themselves result in adequate dissemination of power reactor protection system experience.^{22,23}

7.2 Design Criteria

Until very recently, no generally accepted criteria existed for protection system design. Now the just-approved (1968) "IEEE Criteria for

Nuclear Power Plant Protection Systems" have appeared and a start has been made. These Criteria are reproduced as Appendix B to this report.

It is important to distinguish between standards, codes, and regulations. All of them contain criteria. A standard (in the United States) expresses an industry consensus. It may contain standard definitions, standard test methods, or (as in the IEEE Criteria) standard design requirements. Codes and regulations are rules with the force of law -- administrative or legislative. Examples are building codes, the National Electrical Code, and the ASME Boiler Code. The enforcement may be quasi-judicial, as in the case of the National Electrical Code, which is administered by the Board of Underwriters, as well as having been enacted into law in some jurisdictions.

A standard is not a code. It may be that a code develops out of a standard, as did some building codes and the Boiler Code, but in many cases, the conditions necessary for industry consensus in adopting a standard make the resulting product unsuitable for a code.

The IEEE Criteria "establish minimum requirements ... for functional performance and reliability" of protection systems. They contain many clauses of great value, but they are couched in general terms, and some of them are almost platitudes. Most important of all, the criteria have not yet been applied to actual designs; that is, they have not been meaningfully interpreted with regard to requirements of actual reactors.

We have not presented a detailed evaluation of the IEEE Criteria in this report, since we prefer to make use of other channels of communication to attempt to influence a few clauses that are at variance with the precepts of this report. (The reader will recognize that Paragraphs 4.2, 4.3, 4.7, and 4.11 of the Criteria may not be consistent with our ideas.) Whatever their faults may be, the Criteria represent, in our opinion, a substantial step toward establishing adequate protection system design. It will be necessary to watch carefully the initial interpretations with regard to actual design features in order to evaluate the "real" meaning of this document.

Criteria are still needed in the following areas:

1. diversity of instruments and variables in critical areas, particularly for initiation of emergency core cooling,
2. allowable and prohibited interdependence of the protection system and the operation system,
3. instrument quality,
4. allowable and prohibited interdependence of reactor scram protection systems and various engineered safety protection systems.

7.3 Reliability

The present theory and practice of reliability evaluation depend almost entirely on assumptions made to render the mathematics tractable (see Sect. 4.5.1). These assumptions are known to be incorrect: failures are not independent; testing is not perfect; failures do not occur only in the neat modes postulated. Moreover, the basic failure-rate data needed for evaluation are very inadequately known. Research in this area is urgently needed.

On the other hand, reliability is not everything. Protection depends also on adequate performance and independence of redundant parts.

8. RECOMMENDATIONS

8.1 Protection Instruments

A study should be undertaken of protection instruments, that is, the hardware used in carrying out the system designs discussed in this report. Only the hardware protects the reactor and the public; paper designs are only essential preludes to functioning systems. Design principles should be reviewed in a report of similar depth to the present one. The matter of quality standards is of particular concern.

8.2 Criteria

More nearly complete, more detailed, and clear system design criteria are urgently needed. In particular, the areas delineated in Section 7.2 (diversity, protection-operation interaction, quality standards, function interaction) should be treated. The criteria should be sufficiently definitive that compliance, or noncompliance, can be unequivocally determined.

8.3 Determination of Safe Conditions

Research and development is needed on methods for directly measuring safety parameters, particularly in the core. Examples are fuel temperature, local flow, and local heat flux.

8.4 Performance Testing

The performance of more protection systems should be determined experimentally under simulated accident conditions that are as realistic as possible (see Sect. 3.6). It would also be worthwhile to review the available data, both from experiments conducted for the purpose and from successful protection system functioning when needed in operating reactors.

8.5 Reliability

Research and development are needed in both the theory and the data for reliability predictions. Reliability theory needs to be more nearly consistent with the real world. Aging should be incorporated into failure-rate predictions. The formulation should provide for the widely different testing often used on different parts of a channel (sensors, once per year; electronics, once per second). A realistic method should be devised for coping with interdependence.

Existing methods for collecting reliability data are generally inadequate and should be improved with regard to their relevance to in-service conditions and their validity. As an example, a number of test rod drops in unacceptably long times, followed by repair and acceptable performance, has been logged and reported as "Test OK."²⁴ Inferences drawn from this log entry cannot be valid regarding the reliability of these rods dropping in acceptably short times. Additionally, it is essential that successful protection system operation be reported, as well as the failures.

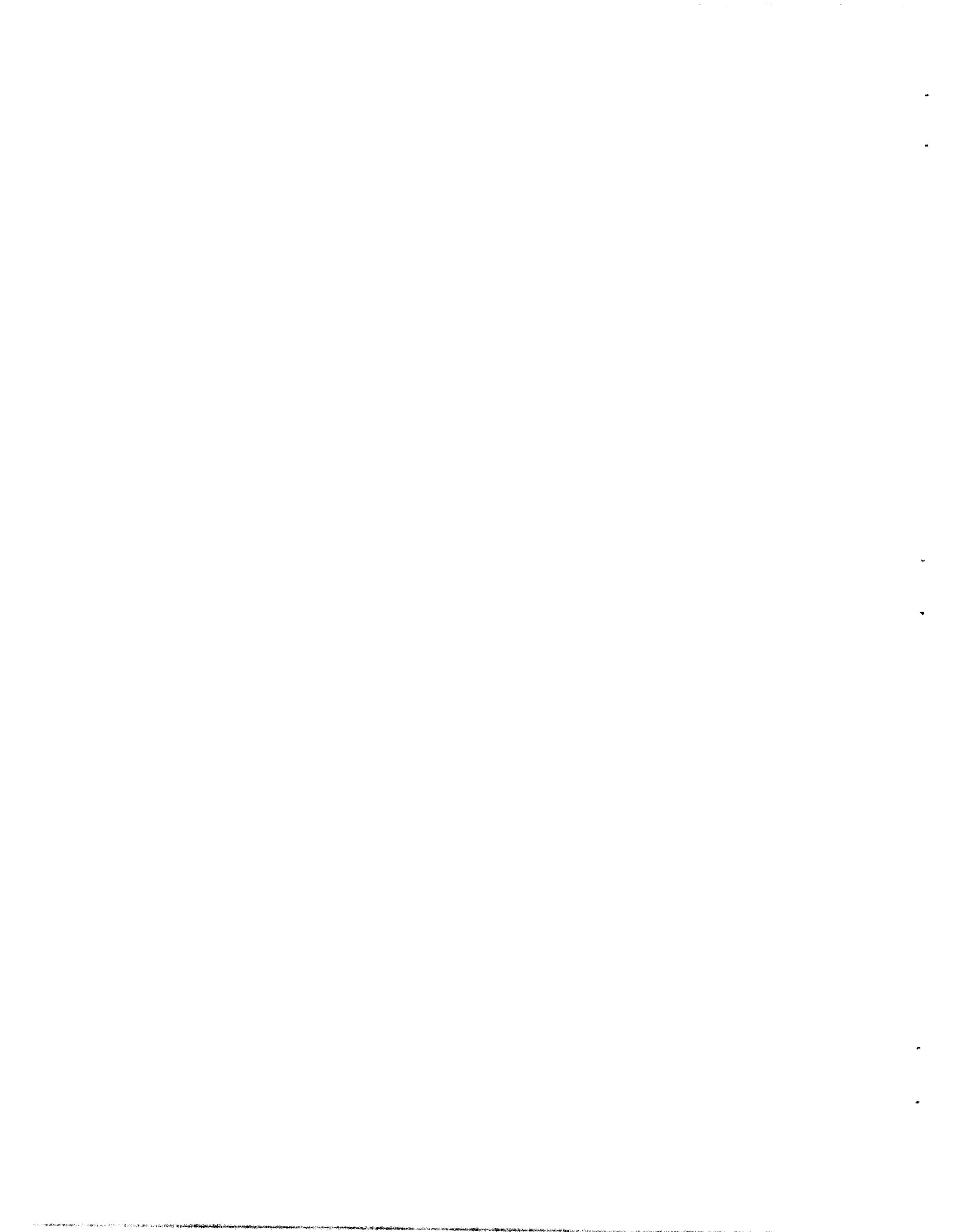
8.6 Publication

As discussed in Section 7.1, the protection system technology is handicapped by the lack of good information. More and better publications will be essential to orderly development.

REFERENCES

1. Principles of Nuclear Reactor Instrumentation, Publication 231, International Electrotechnical Commission, Geneva, Switzerland, 1967.
2. T. J. Thompson and J. G. Beckerley (Eds.), The Technology of Nuclear Reactor Safety, Vol. 1, Reactor Physics and Control, MIT Press, Cambridge, Mass., 1964.
3. E. P. Epler, HTRE-3 Excursion, Nucl. Safety, 1(2): 57-59 (December 1959).
4. C. S. Walker, Experience with NRX and NRU Safety Systems, Nucl. Safety, 4(2): 70-72 (December 1962).
5. E. P. Epler, Failure of Alize-I Reactor Safety System, Nucl. Safety, 5(2): 172-174 (Winter 1963-1964).
6. D. G. Breckon and J. H. Collins, Control and Safety in the Operation of the NRX and NRU Reactors, Canadian Report AECL-1486, Atomic Energy of Canada Limited, April 1962.
7. Private communications from various plant operating personnel.
8. Bodega Bay Preliminary Safeguards Analysis Report, General Electric tests at Moss Landing of pressure-suppression system.
9. J. R. Tallackson et al., Performance Tests of the Oak Ridge National Laboratory Fast Safety System, Trans. Amer. Nucl. Soc., 3(2): 428 (1960).
10. H. B. Smets, A Review of Nuclear Incidents, in Reactor Safety and Hazards Evaluation Techniques, Symposium Proceedings, Vienna, 1962, Vol. 1, pp. 89-110, International Atomic Energy Agency, Vienna, 1962 (STI/PUB/57).
11. T. J. Thompson, Accidents and Destructive Tests, in The Technology of Nuclear Reactor Safety, Vol. 1, Reactor Physics and Control, MIT Press, Cambridge, Mass., 1964.
12. E. P. Epler, Operating Experience with Coincident vs Noncoincident Reactor Safety Systems, USAEC Report ORNL-TM-738, Oak Ridge National Laboratory, Dec. 12, 1963.
13. W. R. Stratton, A Review of Criticality Accidents, Chapter 11 in Progress in Nuclear Energy, Ser. IV, Vol. 3, Technology, Engineering and Safety, Pergamon Press, New York, 1960.
14. M. A. Schultz, Reactor Safety Instrumentation, Nucl. Safety, 4(2): 1-13 (December 1962).

15. E. P. Epler, Failure Probability of Engineered Safeguards, Oct. 5, 1964, unpublished.
16. J. F. Ablitt, Contribution of Systematic Incident Evaluation to the Achievement of Reactor Safety, Nucl. Safety, 7(3): 279-292 (Spring 1966).
17. A. R. Eames, Reliability Assessment of Protective Equipments for Nuclear Installations, British Report AHSB-(S)-R-99, 1965.
18. I. M. Jacobs, Reliability of Engineered Safety Features as a Function of Testing Frequency, Nucl. Safety, 9(4): 303-312 (July-Aug. 1968).
19. R. E. Heffner et al., SPERT-III Pressurizer Vessel Failure, USAEC Report IDO-16743, Phillips Petroleum Company, Jan. 29, 1962.
20. E. P. Epler, Identical Systems for Protection and Control, Nucl. Safety, 10(1) (Jan.-Feb. 1969), in preparation.
21. Federal Power Commission, Major Power Failure Investigation, An Interim Report, November 1966.
22. B. J. Garrick, W. C. Gekler, and H. P. Pomrehn, An Analysis of Nuclear Power Plant Operating and Safety Experience, USAEC Report HN-185, Vols. I and II, Holmes & Narver, Dec. 15, 1966.
23. USAEC Division of Operational Safety, Operating Experiences, Reactor Safety Bulletins.
24. Anonymous, personal communication to the authors.



APPENDICES



Appendix A

NOMENCLATURE

1. Note on Terminology

The arts of reactor protection system design and evaluation are hampered by the lack of a universally accepted terminology. Perhaps this was inevitable as a consequence of the diverse technological backgrounds of the workers and writers in the field. Different manufacturers, laboratories, and regulatory bodies may all use different words to describe the same concept or function; in some groups, the terminology is not even internally consistent.

The USASI Glossary¹ does not include the terms necessary to understand a detailed discussion of protection system design. Evidently such terms were thought too specialized for a general compilation. Recent draft glossaries from the International Standards Organization (ISO)² and the International Electrotechnical Commission (IEC)³ also fail to supply the terms for reactor protection systems. A recent IEEE draft of Criteria for Nuclear Power Plant Protection Systems⁴ (App. B) defines seven terms explicitly, and by implication in its text, many other terms are defined to a degree.

The most orderly set of terms and definitions is to be found in the publications and drafts of Technical Subcommittee 45A (Reactor Instrumentation) of the IEC.⁵⁻⁸ Unfortunately, these represent international compromises and are therefore not in full agreement with American practice.

In the list that follows, the various terms and definitions used in this report are given, together with their origins, if they were obtained from the above-referenced sources.

2. Glossary

2.1 Systems

Protection System (IEEE 1.0)* - For purposes of these Criteria, the nuclear power plant protection system encompasses all electrical and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those trip signals associated with the protective function. These signals include those that actuate reactor trip and that, in the event of a serious reactor accident, actuate engineered safeguards such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning.

Protection System (IEC 231A:5.1.1)** (provisional definition) - All circuits and assemblies which act to prevent the reactor conditions from exceeding safe limits or to reduce the consequences of their being exceeded. The protection system includes the safety shutdown system and where provided, the containment isolation system, the system which initiates emergency cooling, etc.

It is evident that the above two definitions are equivalent. Some component systems are also defined in IEC 231A.

Safety Shutdown System (IEC 231A:5.1.2) (provisional) - That part of a protection system which initiates a rapid shutdown of the reactor (also referred to as "reactor trip" or "scram").

This is evidently the classical "safety system" or "scram system" of early reactors.

In the following four definitions, the operative word is "safety." These systems can be part of the protection system under suitable conditions. In American practice, they are usually not part of the protection system.

Safety Interlock System (IEC 231A:5.1.3) (provisional) - That part of a protection system which permits certain operations affecting reactor safety only when prescribed conditions exist.

Safety Power Cutback System (Programmed Action Safety System) (IEC 231A:5.1.4) (provisional) - That part of a

*IEEE references are paragraph numbers in Reference 4.

**IEC references are given as follows: publication number: clause number.

protection system which controls a decrease of power according to a program, down to a value which is not necessarily zero.

Other words, such as "setback," "reverse," "runback," and the like have also been used.

Safety Alarm (IEC 231A:5.1.5) (provisional) - An alarm function which calls for necessary protective action by the operator.

Safety Alarm System (IEC 231A:5.1.7) (provisional) - The totality of all safety alarms.

The inclusion of alarms, plus operator action, in a protective system is a controversial matter that is discussed in the text.

By contrast,

Operation Instrument System - Instruments and controls not included in the protection system.

2.2 Hierarchy of Apparatus

The most complete set of terms comes from the IEC:

Apparatus (IEC 181:105.005) - A general term used in this Recommendation for designating assemblies, sub-assemblies, basic function units, detectors, etc., in a title or text of general scope, when it is not practical to specify them more precisely. However, because of its lack of precision and varying interpretations, its use is deprecated in the definition of assemblies, sub-assemblies, basic function units, detectors, etc.

Example: "Apparatus wiring."

Equipment (IEC 181:105.010) - An association of assemblies associated to attain a determined final objective.

Example: Failed element detection and localization equipment (of a nuclear reactor).

Assembly (IEC 181:105.015) - A well-defined set of members necessary and sufficient to achieve a specified total function.

Example: A power-measuring assembly based on the neutron flux density may consist of a detector, a linear pulse amplifier and a scaler.

This definition is applied to protection-system apparatus.

Safety Monitoring Assembly (IEC 231A:5.1.8) (provisional) - A monitoring assembly used for reactor safety. A safety monitoring assembly typically comprises the sensor, signal processing and discriminating sub-assemblies (which

convert an analogue signal into an on-off signal), intermediate cabling and output circuit.

Example: A thermocouple feeding into a temperature trip amplifier with a relay output stage.

Note: Several safety monitoring assemblies may be used for each parameter to provide the necessary redundancy.

Evidently, this term is the same as

Channel (IEEE 2.2) - An arrangement of components and modules as required to generate a single protective action signal when required by plant condition. A channel loses its identity where single action signals are combined.

Smaller units are defined by IEEE:

Module (IEEE 2.3) - Any assembly of interconnected components which constitutes an identifiable device, instrument or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Components (IEEE 2.4) - Items from which the system is assembled (e.g., resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

2.3 Actions and Functions

Protective Function (IEEE 2.6) - A system protective action which results from the protective action of the channels monitoring a particular plant condition.

Protective Action (IEEE 2.5) - An action initiated by the protection system when a limit is exceeded. A protective action can be at channel or system level.

Trip (IEC 231A:5.1.15) (provisional) - Switching of a device with two stable states from its normal state to its abnormal state, hence:

a. Safety monitoring assembly trip

Switching of one or more bistable output signals (e.g., alarm, cut-back, scram) of a safety monitoring assembly; also called channel trip.

b. Safety logic assembly trip

Switching to its abnormal state of the output signal or signals of a safety logic assembly.

Trip Level (IEC 231A:5.1.16) (provisional) - That value of a parameter at which protective action is initiated.

Trip Margin (IEC 231A:5.1.17) (provisional) - The difference between the value of a parameter and a trip level associated with that parameter.

Reactor Trip (Scram) (IEC 231A:5.1.18) (provisional) - Actuation of the safety mechanism(s) of a reactor to effect rapid shut-down.

Reset (IEC 231A:5.1.19) (provisional) - Switching of a bistable system or component from its abnormal state to its normal state.

Operational By-pass (IEC 231A:5.1.20) (provisional) - A deliberate inhibition for operational reasons of the action of a part of the protection system performing a specific function.

Example: A short circuit may be applied across the contacts of a relay at the output of a safety monitoring assembly.

Reliability. The propensity to be free from failures.

Safety. The propensity to be free from unsafe failures.

Serviceability. The propensity to be free from safe failures.

Safe Failure (IEC 231A:5.1.12) (provisional) - A failure in the protection system which increases the probability of appropriate safety action should an abnormal condition arise on the reactor.

Unsafe Failure (IEC 231A:5.1.13) (provisional) - A failure which reduces the probability of appropriate safety action by the protection system should an abnormal condition arise on the reactor.

Spurious Shutdown (IEC 231A:5.1.14) (provisional) - A shut-down initiated when there is no abnormal condition on the reactor. It may arise as a result of one or more safe failures in the protection system.

References

1. USA Standard Glossary of Terms in Nuclear Science and Technology, N1.1-1967, Revision of N1.1-1957, Approved October 16, 1967, United States of America Standards Institute, New York, New York, 1967.
2. International Nuclear Glossary - ISO/TC85/SC1/WG1, Unpublished memorandum, Circa 1965.

3. Revision of the First Edition (1938) of the International Electrotechnical Vocabulary; Group 26: Nuclear Power Plants for Electric Energy Generation; Second Draft Prepared by the French Electrotechnical Committee, IEC-1 (26) (Central Office) 238, International Electrotechnical Commission, Geneva, Switzerland, September 1964.
4. Proposed IEEE Criteria for Nuclear Power Plant Protection Systems (for trial use) No. 279, Institute of Electrical and Electronics Engineers, Nuclear Science Group, Standards Committee.
5. Index of Electrical Measuring Apparatus Used in Connection with Ionizing Radiation, Publication 181, International Electrotechnical Commission, Geneva, Switzerland, 1964.
6. General Characteristics of Nuclear Reactor Instrumentation, Publication 232, International Electrotechnical Commission, Geneva, Switzerland, 1966.
7. Principles of Nuclear Reactor Instrumentation, Publication 231, International Electrotechnical Commission, Geneva, Switzerland, 1967.
8. Principles of Nuclear Power Instrumentation; Chapter 5: Protective Systems, to be issued as Publication 231A, International Electrotechnical Commission; present draft available as 45A (Central Office) 8, Geneva, Switzerland, 1967.

APPENDIX B



IEEE

No. 279

AUGUST 1968

Proposed
IEEE Criteria for
**NUCLEAR POWER PLANT
PROTECTION SYSTEMS**

(Effective August 30, 1968)

IEEE No. 279



PUBLISHED BY

345 EAST 47 STREET, NEW YORK, N. Y. 10017

FOREWORD

(This Foreword is not a part of the Proposed IEEE Criteria for Nuclear Power Plant Protection Systems.)

The functional performance and reliability of power reactor protection systems is a matter of concern for manufacturers, for users, and for those who are responsible for licensing and regulating reactor facilities. With the increased volume of nuclear power generation plants planned or being designed, attention has focused on criteria and standards as mechanisms for promoting safe design practice and for evaluating the performance and reliability of proposed systems. These criteria are an industry consensus of an acceptable approach to assessing the adequacy of protection system functional performance and reliability in meeting design requirements.

The Institute of Electrical and Electronics Engineers (IEEE) undertook the development of these Criteria in 1964 at the request of ASA Sectional Committee N6, Reactor Safety Standards. In September of that year the Standards Committee of the Nuclear Science Group initiated work on the project. An initial draft appeared in March, 1965, and went through seven revisions before a satisfactory consensus was achieved.

Early in 1966, the working group responsible for generating these Criteria was made a subcommittee of the Reactors and Reactor Controls Committee of the IEEE Nuclear Science Group. Unanimous subcommittee approval for the proposed Criteria was obtained in June, 1966, and in the Nuclear Science Group Standards Committee in September, 1966. In addition, the proposed Criteria have been widely reviewed by other interested persons, both within and outside of the Nuclear Science Group.

The user of these Criteria should be aware that a full national consensus, which would permit their adoption in their present form by the United States of America Standards Institute, does not yet exist. This is basically because of a feeling in some quarters that paragraph 4.7 should be more stringent in its requirements for separation of control and protection functions. On January 1, 1968, the subcommittee was reconstituted as the Nuclear Science Group Standards Committee, and as such it will continue its efforts to improve these Criteria in future editions.

Subcommittees within the present Nuclear Science Group Standards Committee are preparing a number of supporting Standards and Guides that will interpret the intent of the Protection System Criteria and otherwise enhance their usefulness. This work includes, but is not necessarily limited to, the following subject areas:

- (1) Application of the Single Failure Criterion,
- (2) Equipment Qualifications Testing,
- (3) Periodic Testing,
- (4) Numerical Reliability Analysis Techniques.

The Nuclear Science Group Standards Committee invites comments on and suggestions for additional material that should be included in the Criteria and in the supporting documents. Comments and recommendations should be addressed to

C. S. Walker
Oak Ridge National Laboratory
P. O. Box Y
Oak Ridge, Tenn. 37830

with copies to

J. C. Russ
General Electric Company
APED - M/C 622
175 Curtner Avenue
San Jose, Calif. 95125

and

J. J. Anderson
IEEE Standards Committee
The Institute of Electrical and Electronics Engineers, Inc.
345 East 47 Street
New York, N. Y. 10017

Members of the subcommittee participating in the generation of the criteria at the time of final subcommittee approval were:

| | |
|-----------------|----------------|
| J. C. Russ | L. H. Horn |
| J. F. Bates | L. M. Johnson |
| S. J. Ditto | V. A. Moore |
| J. Forster | D. G. Pitcher |
| L. E. Fort | D. F. Sullivan |
| J. M. Gallagher | C. S. Walker |
| A. Hirsch | |

© Copyright 1968 by The Institute of Electrical and Electronics Engineers, Inc.

This publication may be reproduced, without change, in part or in its entirety, provided that notice of its copyright by the IEEE is included.

CONTENTS

| | <i>Page</i> |
|--|-------------|
| 1. Scope | 3 |
| 2. Definitions | 3 |
| 2.1 System | 3 |
| 2.2 Channel | 3 |
| 2.3 Module | 3 |
| 2.4 Components | 3 |
| 2.5 Protective Action | 3 |
| 2.6 Protective Function | 3 |
| 2.7 Type Tests | 3 |
| 3. Design Basis | 3 |
| 4. Requirements | 3 |
| 4.1 General Functional Requirement | 4 |
| 4.2 Single Failure Criterion | 4 |
| 4.3 Quality of Components and Modules | 4 |
| 4.4 Equipment Qualification | 4 |
| 4.5 Channel Integrity | 4 |
| 4.6 Channel Independence | 4 |
| 4.7 Control and Protection System Interaction | 4 |
| 4.8 Derivation of System Inputs | 4 |
| 4.9 Capability for Sensor Checks | 4 |
| 4.10 Capability for Test and Calibration | 4 |
| 4.11 Channel Bypass or Removal from Operation | 4 |
| 4.12 Operating Bypasses | 4 |
| 4.13 Indication of Bypasses | 4 |
| 4.14 Access to Means for Bypassing | 5 |
| 4.15 Multiple Set Points | 5 |
| 4.16 Completion of Protective Action Once It Is Initiated | 5 |
| 4.17 Manual Actuation | 5 |
| 4.18 Access to Set Point Adjustments, Calibration, and Test Points | 5 |
| 4.19 Identification of Protective Actions | 5 |
| 4.20 Information Read-Out | 5 |
| 4.21 System Repair | 5 |

•
•

•
•

•
•

Proposed IEEE Criteria for
NUCLEAR POWER PLANT PROTECTION SYSTEMS

1. SCOPE

These Criteria establish minimum requirements for the safety-related functional performance and reliability of protection systems for stationary, land-based nuclear reactors producing steam for electric power generation. Fulfillment of these requirements does not necessarily fully establish the adequacy of protective system functional performance and reliability. On the other hand, omission of any of these requirements will, in most instances, be an indication of system inadequacy. For purposes of these Criteria, the nuclear power plant protection system encompasses all electric and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protective function. These signals include those that actuate reactor trip and that, in the event of a serious reactor accident, actuate engineered safeguards such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning.

2. DEFINITIONS

The definitions in this Section establish the meanings of words in the context of their use in these Criteria.

2.1 System. Where not otherwise qualified, the word "system" refers to the nuclear power plant protection system, as defined in the scope section of these Criteria.

2.2 Channel. An arrangement of components and modules as required to generate a single protective action signal when required by a plant condition. A channel loses its identity where single action signals are combined.

2.3 Module. Any assembly of interconnected components which constitutes an identifiable device, instrument or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

2.4 Components. Items from which the system is assembled (e.g., resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc.).

2.5 Protective Action. An action initiated by the protection system when a limit is exceeded. A protective action can be at channel or system level.

2.6 Protective Function. A system protective action which results from the protective action of the channels monitoring a particular plant condition.

2.7 Type Tests. Tests made on one or more units to verify adequacy of design.

3. DESIGN BASIS

A specific protection system design basis shall be provided for each nuclear power plant. The information thus provided shall be available, as needed, for making judgments on system functional adequacy.

The design basis shall document as a minimum, the following:

- (a) the plant conditions which require protective action;
- (b) the plant variables (e.g., neutron flux, coolant flow, pressure, etc.) that are required to be monitored in order to provide protective actions;
- (c) the minimum number and location of the sensors required to monitor adequately, for protective function purposes, those plant variables listed in 3(b) that have a spatial dependence;
- (d) prudent operational limits for each variable listed in 3(b) in each applicable reactor operation mode;
- (e) the margin, with appropriate interpretive information, between each operational limit and the level considered to mark the onset of unsafe conditions;
- (f) the levels that, when reached, will require protective system action;
- (g) the range of transient and steady-state conditions of both the energy supply and the environment (e.g., voltage, frequency, temperature, humidity, pressure, vibration, etc.) during normal, abnormal, and accident circumstances throughout which the system must perform;
- (h) the malfunctions, accidents, or other unusual events (e.g., fire, explosion, missiles, lightning, flood, earthquake, wind, etc.) which could physically damage protection system components or could cause environmental changes leading to functional degradation of system performance, and for which provisions must be incorporated to retain necessary protection system action;
- (i) minimum performance requirements including the following:
 - 1) system response times;
 - 2) system accuracies;
 - 3) ranges (normal, abnormal and accident conditions) of the magnitudes and rates of change of sensed variables to be accommodated until proper conclusion of the protection system action is assured.

Note: The development of the specific information to be used in fulfillment of the above requirements is not within the scope of these Criteria. The development of standard criteria and requirements relating to the determination of such design basis information as unsafe conditions requiring protective functions, plant variables to be monitored, operational limits, margins, set points, etc., are under consideration in American Nuclear Society Standards Subcommittee 4.

4. REQUIREMENTS

4.1 General Functional Requirement. The nuclear power plant protection system shall, with precision and reliability, automatically initiate appropriate protective action whenever a plant condition monitored by the system reaches a preset level. This requirement applies for the full range of conditions and performance enumerated in 3(g), 3(h), and 3(i).

4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protection system action when required.

Note: "Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a "single failure" even though several transistor failures result. Mechanical damage to a mode switch would be a "single failure" although several channels might become involved.

4.3 Quality of Components and Modules. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

4.4 Equipment Qualification. Type test data or reasonable engineering extrapolation based on test data shall be available to verify that equipment that must operate to provide protection system action will meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.

Note: Attention is directed particularly to the requirements of 3(g) and 3(i).

4.5 Channel Integrity. All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents.

Note: See especially the requirements documented in response to 3(f), 3(g), 3(h), and (i).

4.6 Channel Independence. Channels that provide signals for the same plant protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.

4.7 Control and Protection System Interaction. Where a plant condition that requires protective action can be brought on by a failure or malfunction of the control system, and the same failure or malfunction prevents proper action of a protection system channel or channels designed to protect against the resultant unsafe condition,

the remaining portions of the protection system shall independently meet the requirements of paragraphs 4.1 and 4.2.

4.8 Derivation of System Inputs. To the extent feasible and practical, protection system inputs shall be derived from signals which are direct measures of the desired variables.

4.9 Capability for Sensor Checks. Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.

This may be accomplished in various ways, for example:

- (a) by perturbing the monitored variable; or
- (b) within the constraints of paragraph 4.11, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable; or
- (c) by cross checking between channels that bear a known relationship to each other and that have read-outs available.

4.10 Capability for Test and Calibration. Capability shall be provided for testing and calibrating channels and the devices used to derive the final system output signal from the various channel signals. For those parts of the system where the required interval between testing will be less than the normal time interval between plant shutdowns, there shall be capability for testing during power operation.

4.11 Channel Bypass or Removal from Operation. The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective function. During such operation the active parts of the system shall of themselves continue to meet the single failure criterion.

Exception: "One-out-of-two" systems are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated. For example, the bypass time interval required for a test, calibration, or maintenance operation could be shown to be so short that the probability of failure of the active channel would be commensurate with the probability of failure of the "one-out-of-two" system during its normal interval between tests.

4.12 Operating Bypasses. Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and must be designed in accordance with these Criteria.

4.13 Indication of Bypasses. If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.

4.14 Access to Means for Bypassing. The design shall permit the administrative control of the means for manually bypassing channels or protective functions.

4.15 Multiple Set Points. Where it is necessary to change to a more restrictive protective action set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used. The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these Criteria regarding performance and reliability.

4.16 Completion of Protective Action Once It Is Initiated. The protection system shall be so designed that, once initiated, a protection system action shall go to completion. Return to operation shall require subsequent deliberate operator action.

4.17 Manual Actuation. Means shall be provided for manual initiation of protection system action. Failure in an automatic protection circuit shall not prevent the manual actuation of protective functions. Manual actuation shall require the operation of a minimum of equipment.

4.18 Access to Set Point Adjustments, Calibration, and Test Points. The design shall permit the administrative control of access to all protective action set point adjustments, module calibration adjustments, and test points.

4.19 Identification of Protective Actions. Protective actions shall be indicated and identified down to the channel level.

4.20 Information Read-Out. The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to plant safety. The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications confusing to the operator.

4.21 System Repair. The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.