ALO-1011

ALO--1011

DE84 015912

**AN INTEGRATED APPROACH
TO
ECONOMICAL, RELIABLE, SAFE
NUCLEAR POWER PRODUCTION**

MASTER

Printed June 1982

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use or the results of such use of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Printed in the United States of America

Available from
National Technical Information Service
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

Price: Printed Copy \$11.00; Microfiche \$3.00

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

NOTICE
PORTIONS OF THIS REPORT ARE ILLEGIBLE. It
has been reproduced from the best available
copy to permit the broadest possible avail-
ability.

Distribution Category
UC-78

ALO-1011

AN INTEGRATED APPROACH TO
ECONOMICAL, RELIABLE, SAFE
NUCLEAR POWER PRODUCTION

Prepared by

Combustion Engineering, Inc.
1000 Prospect Hill Road
Windsor, Connecticut 06095

Prepared for

U. S. Department of Energy
Light Water Reactor Safety Technology Management
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sponsored by

U. S. Department of Energy
Division of Nuclear Power Development
Washington, D. C. 20545

Work performed under Sandia Contract No. 68-5149

Submitted: April 1982

Printed: June 1982

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ABSTRACT

An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production is the latest evolution of a concept which originated with the Defense-in-Depth philosophy of the nuclear industry. As Defense-in-Depth provided a framework for viewing physical barriers and equipment redundancy, the Integrated Approach gives a framework for viewing nuclear power production in terms of functions and institutions. In the Integrated Approach, four plant Goals are defined - Normal Operation, Core and Plant Protection, Containment Integrity and Emergency Preparedness - with the attendant Functional and Institutional Classifications that support them. The Integrated Approach provides a systematic perspective that combines the economic objective of reliable power production with the safety objective of consistent, controlled plant operation.

ACKNOWLEDGEMENTS

This report was prepared through the combined efforts of many people in three separate companies: Combustion Engineering, Inc. (C-E), in Windsor, Connecticut, and through subcontracts, International Energy Associates, Ltd. (IEAL), in Washington, D.C., and Technology for Energy Corp. (TEC) in Knoxville, Tennessee.

We are particularly indebted to Messrs. J. D. Griffith and A. C. Millunzi (U.S. Department of Energy) for their continued input and support in the development of this program.

Joseph C. Braun
Project Manager

AN INTEGRATED APPROACH TO
ECONOMICAL, RELIABLE, SAFE
NUCLEAR POWER PRODUCTION

TABLE OF CONTENTS

Title Page.....	i
Abstract.....	iii
Acknowledgements.....	iv
Table of Contents.....	v
List of Tables.....	vii
List of Figures.....	viii
List of Acronyms and Abbreviations.....	ix
Executive Summary.....	ES-1
<u>Section 1: An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production.....</u>	<u>1-1</u>
1.A. Description of the Integrated Approach	
1.A.1 Objectives of the Integrated Approach.....	1-1
1.A.2 Details of the Functional Classification...	1-2
1.A.3 Details of the Institutional Classification	1-6
1.B. Evolution of the Integrated Approach	
1.B.1 Defense-in-Depth/Physical Barriers.....	1-9
1.B.2 The Critical Functions in Aviation/ Aerospace.....	1-9
1.B.3 The Safety Level Concept.....	1-12
1.B.4 An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production....	1-12
<u>Section 2: Demonstration of the Integrated Approach to Economical, Reliable, Safe Nuclear Power Production - Applications.....</u>	<u>2-1</u>
2.A. Application One: Use of the Integrated Approach to Evaluate the Standard Review Plan...	2-1

2.B.	Application Two: How the Integrated Approach Can Be Used to Evaluate Reactor Operating Experience.....	2-5
2.C.	Application Three: Use of the Integrated Approach in the Development of an Economic Risk Assessment Framework.....	2-10
2.D.	Application Four: Use of the Integrated Approach in Operator Training.....	2-21
	<u>Section 3: Other Uses of the Integrated Approach.....</u>	3-1
	References.....	R-1
Appendix A:	Nuclear Power Plant Functional Classification.....	A-1
Appendix B:	Nuclear Power Plant Institutional Classification.....	B-1

LIST OF TABLES

TABLE

1.A-1	Goal Objectives	1-1
1.B-1	Historical Summary of Defense-in-Depth	1-10
2.B-1	Integrated Approach - Significant Features of the TMI Event	2-9
2.C-1	Outage Categorization Matrix (Excluding Refueling) ...	2-14
2.C-2	Performance Enhancement Factors	2-16
2.C-3	Event Type Framework	2-19

LIST OF FIGURES

FIGURE

1.A-1	Functional Classification	1-5
1.A-2	Functional/Institutional Classification Descriptions	1-8
2.B-1	Event Significance	2-7
2.B-2	Interpretation of Significant Events	2-8
2.C-1	Outage Frequency (Per Reactor Year) vs. Outage Duration	2-12
2.C-2	Outage Cost (\$Million/Reactor Year) vs. Outage Duration	2-13

LIST OF ACRONYMS AND ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
AEC	Atomic Energy Commission
ASME	American Society of Mechanical Engineers
BWR	Boiling Water Reactor
C-E	Combustion Engineering, Inc.
CEA	Control Element Assembly
CFR	Code of Federal Regulations
DOE	Department of Energy
DNBR	Departure from Nucleate Boiling Ratio
ECCS	Emergency Core Cooling System
EHC	Electro-Hydraulic Control
ESF	Engineered Safety Feature
GDC	General Design Criterion
GE	General Electric
GPU	General Public Utilities
HPSI	High Pressure Safety Injection
IEAL	International Energy Associates, Limited
INPO	Institute for Nuclear Power Operation
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LWR	Light Water Reactor
MSIV	Main Steam Isolation Valve
NRC	Nuclear Regulatory Commission
NSAC	Nuclear Safety Analysis Center
NSIC	Nuclear Safety Information Center
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PWR	Pressurized Water Reactor
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
SLC	Safety Level Concept
SRP	Standard Review Plan
TEC	Technology for Energy Corporation
TMI	Three Mile Island
TMI-2	Three Mile Island Unit 2
USAEC	United States Atomic Energy Commission

EXECUTIVE SUMMARY

Introduction

This report describes a concept, called "An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production", which was developed as part of a DOE sponsored program to improve the process by which nuclear plants are regulated.

This concept, the "Integrated Approach", consists of an organized listing and classification of the functions and subfunctions needed to produce power in a nuclear plant, along with a listing of the design, construction, operation and maintenance activities that support them. These listings can be used to examine nuclear plants in either a general or a specific way to determine whether all of the necessary functions and activities are being implemented in a satisfactory manner.

This approach deals with both plant economics and safety. It offers several improvements over the current safety philosophy, often called "Defense-in-Depth" (References ES-1 through ES-16), which focuses on high quality design, the assumption of failures, and the assurance of physical barriers to limit the release of radioactivity to the public. The translation of Defense-in-Depth into regulations over the past three decades has tended to produce an excessive number of specific regulations and requirements that appear to lack integration (Reference ES-17). Defense-in-Depth emphasizes the design process (Reference ES-3) and does not relate well to the way in which plants are actually operated.

The Integrated Approach relates better to the temporal sequence of accident events and more correctly reflects the ways in which safety is achieved in the nuclear industry. Specifically, it shows how nuclear power plants are designed, constructed, operated and maintained to achieve the following four Goals and objectives to protect the plant and the public.

- (1) Normal Operation - Maintain or restore the normal operating conditions.
- (2) Core and Plant Protection - Maintain core and plant protection in the event that normal operating conditions cannot be maintained.
- (3) Containment Integrity - Maintain the integrity of containment structures for those low probability events that result in failure to protect the core.
- (4) Emergency Preparedness - Maintain adequate emergency preparedness to protect the health and safety of the public during those extremely low probability events when the integrity of the containment building cannot be maintained.

As a structured approach to Light Water Reactor (LWR) operation, the Integrated Approach provides a framework for developing a more definitive understanding of the areas of responsibility of plant owners and regulators, and a more effective means of communicating with the public on the safety of LWRs. When fully developed, it will provide a better mechanism for the public and others to monitor LWR safety activities. This report does not directly address nuclear plant regulation. However, it describes an approach that can be used to help examine nuclear power plants in a systematic manner. If this approach receives widespread use and acceptance by the industry, it is believed that it will eventually find application in the regulatory process by providing a systematic means of responding to regulatory concerns.

Description of the Integrated Approach

The Integrated Approach is a systematic ordering of the many functions and activities that are implemented to ensure economical, reliable and safe nuclear power production. It describes how the nuclear industry works. Each of the Goals and objectives stated above is achieved through a group of inter-related functions. For example, the Goal of Normal Operation is achieved through all the functions that are required in a plant to produce electric power. The various functions are achieved and maintained through the appropriate design, construction, operation and maintenance of the plant systems and components. Relating the functions necessary to produce economical, reliable, safe nuclear power to the activities required to support those functions is an important feature of the Integrated Approach. It provides a framework from which the various aspects of the nuclear industry can be understood.

The Integrated Approach categorizes the functional and organizational structure of the nuclear industry into systematic groupings (or classifications). These have been identified as the Functional Classification, which deals with the functions, success paths, systems and components within a plant, and the Institutional Classification,

which deals with the general and specific industry activities which are needed to achieve these functions. Each of these classifications is described below.

Functional Classification

The basic idea of the Functional Classification is illustrated in the following figure which shows a "success tree" for any one of the four Goals.

For each Goal, there is a group of functions or sub-functions which are necessary to achieve the objective of that Goal. Each function (or subfunction), in turn, is accomplished through a number of "success paths". A success path consists of a set of systems and components, combined with appropriate human actions, which together accomplish or maintain a function. Human action is shown with a dotted line because it may or may not be present or needed for the operation of a specific system or component.

Please note how "and" and "or" logic symbols are used in this figure. The "and" gate implies that all of the elements below the symbol must be present for success, while the "or" gate indicates that any one of the elements is sufficient to achieve success. For critical safety functions in nuclear plants, there are usually several success paths which can be used to achieve a particular function.

Institutional Classification

The Institutional Classification of the Integrated Approach views the nuclear power process from a different perspective. Whereas the Functional Classification deals with the power plant and its associated hardware, the Institutional Classification focuses on those organizations responsible for designing and constructing the power plant and keeping it operational throughout its lifetime. The Institutional Classification examines the four major industry activities of Design, Construction, Operation and Maintenance, as they pertain to the successful achievement of the objectives of the four Goals. This is shown in the following figure.

As with the Functional Classification, this approach provides continuity from the ultimate goal to the specific procedure or action. There are many specific activities that must be performed in order to design, construct, operate and maintain a nuclear power plant. The characteristics associated with any particular activity indicate how

well the activity is being performed. In the nuclear industry, a series of inter-related checks is established to ensure that significant deficiencies are detected and corrected. The Institutional Classification, developed as part of the Integrated Approach, provides a listing of the specific activities associated with the four general activities of Design, Construction, Operation and Maintenance, and lists the characteristics which are considered to be typical of well run and successful activities.

The importance of the inter-relationship between the Functional Classification and the Institutional Classification cannot be overstated. Good design, construction, operation and maintenance are based on a clear, logical understanding of the many functions, subfunctions and success paths that must be achieved in a power plant.

The Integrated Approach can be used to assist a utility in allocating resources, both financial and human, to achieve the overall objectives of economical, reliable power production while meeting safety requirements. It deals with safety in terms of achieving overall Goals or objectives and can help the utilities and the regulators to determine whether overall safety objectives are being met even though individual power plants and utilities may elect to choose substantially different equipment, methods, techniques and organizational structures to achieve them. The overall Goals can be stated in either a qualitative or quantitative manner.

In addition, the Integrated Approach pays considerable attention to the protection of the utilities' financial investment. This is done through an examination of the first two Goals: Normal Operation and Core and Plant Protection. By attending to these two Goals, utilities not only provide more economical power for their customers, but also protect their investment and economic position while reducing the probability of a serious nuclear accident.

Uses of the Integrated Approach

In this study, limited application of the Integrated Approach has been made in a number of areas to illustrate its effectiveness. These applications are listed and briefly described as follows:

- Systematic evaluation of the U.S. NRC Standard Review Plan (SRP).

The SRP was reviewed because it covers a broad spectrum of nuclear power plant hardware and activities. This application looked at the SRP both from a quantitative and a qualitative point of view and compared its findings with those of a similar study performed by Sandia National Laboratories in 1980 and 1981 using the methods of Probabilistic Risk Assessment (PRA). The Integrated Approach evaluation, conducted in substantially less time, produced essentially the

same findings as the Sandia report and identified a number of questions and issues which do not naturally emerge from PRA evaluations.

- Evaluation of operating reactor events and experience.

Operating reactor events and experience were examined from the perspective of the Integrated Approach to help identify:

- (1) the significance of various operating reactor events.
- (2) the causal factors which led to those events.

This brief examination indicated that the Integrated Approach can be used to help the industry develop procedures to sort through the substantial amount of operating reactor experience to identify those events which are truly significant in order to find and correct the root causes which lead to them, when cost-beneficial.

- Development of a framework for the assessment of economic risk.

Because nuclear plant outages have such a major effect on the utility's economic position, a brief evaluation using the Integrated Approach was performed to see if it could be used to identify areas where improvements to either the physical plants or to the organizations that support them could bring about more effective plant operation. This study indicated that identification of causal factors could be aided considerably by the use of the Integrated Approach Institutional Classification.

- Operator training.

The Integrated Approach was explained to a number of nuclear plant operators. The Functional Classification helped the operators to better understand the significance of various events and plant conditions. This insight enhanced their ability to identify more success paths that could be used to accomplish major functions (in particular, safety functions) within their plant.

Potential Applications of the Integrated Approach

Some major potential applications of the Integrated Approach developed in this study are listed below in an approximate order of the anticipated return on investment.

- For a specific plant or group of plants, systematically identify the major contributing factors to unplanned outages and help to eliminate them.
- Develop industry procedures for determining the causes and relative significance of plant operation events.
- Aid in the formulation of operating, emergency and maintenance procedures.
- Act as a foundation for improving technical specifications.
- Form a basis for plant auditing procedures and techniques.
- Educate licensed and non-licensed operators, members of management, and maintenance and engineering personnel.
- Form a basis for the performance of functional and task analysis in nuclear plants.
- Develop the basis for large scale research program management.
- Interpret, review and communicate the concepts and procedural practices of Probabilistic Risk Assessment (PRA).

The evolution of the Integrated Approach and the limited applications to date indicate that it is a tool that can be used by the industry for continuous, thorough self-evaluation and experience feedback. The cost of applying the concept need not be great. A general review of a total reactor plant and a listing of general and specific industry activities is contained in this report. More detailed evaluations may be performed if desired to address specific problems or issues.

A typical application to a problem area would start with a survey of the listed functions to determine which were affected. Then, to the extent needed, a description of the systems, components and human actions relevant to those functions would be developed. This description would then be used in any subsequent evaluation or analysis to develop a potential solution to the problem.

If the approach is used to develop an overview of the problem at the beginning of a work effort (e.g., addressing a particular plant safety question or issue), it can increase efficiency by avoiding unnecessary, redundant or conflicting activities.

The Integrated Approach provides great flexibility in application. Because it naturally relates any specific function or activity to all related activities, it is valuable in keeping problems or issues in

perspective. It also suggests alternative ways of performing activities or accomplishing functions that may be quite acceptable for meeting desired goals or objectives. It is offered as a tool for understanding the entire process of nuclear power production. It is hoped that the nuclear industry will examine this tool, use it where it can be of value and contribute to its further development.

AN INTEGRATED APPROACH
TO
ECONOMICAL, RELIABLE, SAFE
NUCLEAR POWER PRODUCTION

SECTION 1: AN INTEGRATED APPROACH TO ECONOMICAL, RELIABLE, SAFE
NUCLEAR POWER PRODUCTION

1.A Description of the Integrated Approach

1.A.1 Objectives of the Integrated Approach

The Integrated Approach is a systematic ordering of the many functions and activities that are implemented to ensure economical, reliable and safe nuclear power production. An extension of the Defense-in-Depth philosophy, the basic premise of the Integrated Approach is that all nuclear power plant equipment and activities can be associated with one of four Goals: Normal Operation, Core and Plant Protection, Containment Integrity and Emergency Preparedness. A Goal is accomplished through a group of inter-related functions assembled to achieve a particular objective. For example, the Normal Operation Goal is accomplished through all the functions that are required to produce electric power under normal plant conditions. Therefore, the objective of normal plant operation is to maintain the capability to produce power. A statement of each of the Goals is presented in Table 1.A-1.

The various functions are achieved and maintained through the appropriate use of plant systems and components which are implemented and sustained through the general industry activities of Design, Construction, Operation and Maintenance. This dual approach of relating the functions necessary to produce economical, reliable and safe power to the activities required to support those functions provides a framework from which the complex aspects of the nuclear industry can be understood.

The following sections will describe the Integrated Approach, first from the functional perspective - the Functional Classification, and then from the general industry activity perspective - the Institutional Classification. The historical development of the Integrated Approach will be briefly discussed. Applications, both previously explored and potential, will be examined. Finally, recommendations for future directions of the Integrated Approach workscope will be presented.

TABLE 1.A-1

<u>Goal</u>	<u>Statement</u>
Normal Operation	Enable the plant to produce power and ensure that it continues to produce power.

TABLE 1.A-1 (continued)

Core and Plant Protection	Protect the core and plant in the event of a transient which might jeopardize them.
Containment Integrity	Maintain the integrity of the containment prior to and during any incident that might give rise to release of radioactivity outside of the plant.
Emergency Preparedness	Minimize the ill effects of a nuclear accident on the population surrounding a nuclear plant.

1.A.2 Details of the Functional Classification

The ultimate goal of a nuclear power plant is the economical, reliable and safe generation of power. The process by which this objective is attained can be examined through application of the Integrated Approach. Each Goal is achieved by maintenance of a group of functions particular to that Goal, and characterized by a general grouping of plant operating conditions. Functions and possibly subfunctions maintain plant conditions within the appropriate bounds by means of success paths. A success path consists of a set of systems and components, coupled with appropriate human actions, which together accomplish a specified function or subfunction. The Functional Classification (functions, subfunctions, success paths, systems and components) directly relates to the physical aspects of the plant and plant operation.

The NORMAL OPERATION Goal is associated with those plant conditions which support continuous production of electricity. It is accomplished through a group of functions whose purpose it is to prevent or avoid imbalances in plant parameters that could cause a change in the plant conditions such that power production would no longer be the primary objective of plant operation. Successful achievement of this Goal is marked by the absence of fuel or component damage that could give rise to an unplanned, extended outage. In the event that it has been necessary to temporarily interrupt power production, the plant is capable of immediate restart.

There are six general functions associated with the Normal Operation Goal (power production plant condition). These functions are:

- Heat Production Control
- Energy Transfer from Heat Source
- Thermal to Mechanical Energy Conversion
- Mechanical to Electrical Energy Conversion
- Electrical Output Control
- Radiation Exposure Control

The CORE AND PLANT PROTECTION Goal is intended to avoid or limit damage to the plant hardware and the reactor core itself. The successful achievement of this Goal is marked by the prevention or cessation of core or plant damage propagation, and the return of the plant to a long term, stable condition. To achieve this result, it is necessary to maintain or restore the following functions:

Core Protection Safety Functions

- Heat Production (Reactivity) Control
- RCS Pressure Control
- RCS Inventory Control
- RCS Heat Removal
- Heat Transfer to Ultimate Heat Sink
- Radiation Exposure Control

Plant Protection Functions

- Protect Heat Production Control
- Protect Energy Transfer from Heat Source Capability
- Protect Thermal to Mechanical Energy Conversion Capability
- Protect Mechanical to Electrical Energy Conversion Capability
- Protect Electrical Output Capability
- Radiation Exposure Control

The core protection safety functions are based on the work documented in Reference 1.A-1.

The six plant protection functions correspond directly to the six general functions associated with the Normal Operation Goal (power production plant condition) noted above. This direct correspondence exists because this study considered plant protection only with respect to protecting the functions required for producing electrical power.

The CONTAINMENT INTEGRITY Goal ensures that radioactive materials remain within specified constraints and are kept away from the general public. This is accomplished by maintenance of containment integrity prior to, during and after any incident that might give rise to the release of radioactive material outside the plant. It has four major safety functions required to achieve its success:

Containment Isolation
Pressure/Temperature Control
Maintenance of Barriers
Radioactivity Control

The EMERGENCY PREPAREDNESS Goal is accomplished through activities whose purpose is to minimize the ill effects of a nuclear accident

in the event that the objectives of the first three Goals are not accomplished. This objective is accomplished by effectively maintaining the following functions:

Contingency Action Planning
Emergency Organization Implementation
Emergency Communications
Radiation and Meteorological Monitoring
Public Response

Each Goal is accomplished by maintaining a series of functions as shown in Figure 1.A-1. The functions and subfunctions are maintained through success paths. Human decisions, either prior (through design) or immediate (through operator action), determine which success paths are used under the various plant conditions. A success path is defined as a set of equipment, physical processes and procedures, combined with appropriate human actions that, together, achieve a particular function or subfunction. The equipment in each success path is that of systems and components that may have some direct human actions associated with their operation. Each function is usually served by more than one success path. Furthermore, a system that comprises part of one success path may, through a different set of human actions, comprise part of another success path and, consequently, contribute to the maintenance of a different function. Thus, one system may serve several functions.

Examination of the "success tree" in Figure 1.A-1 illustrates the importance of human actions - both in selecting success paths and activating systems and components. It is significant to note that the various human actions indicated in the success tree represent different objectives of human behavior. The human actions on the component level are "skill-based" behavior, such as activating a switch or operating a valve. The selection of a success path is the result of "knowledge-based" behavior in that information and experience are factored into the decision making process (Reference 1.A-2).

Four types of success paths are common to all functions:

NORMAL success path(s): a set of equipment, physical processes, procedures and human actions that maintain a function during normal operation. These frequently use "control" grade equipment.

PRINCIPAL success path(s): a set of equipment, physical processes, procedures and human actions that are used to maintain a function when the plant is challenged by a transient. The equipment used in this type of success path is frequently of a higher quality and reliability (e.g., "safety" grade). In these success paths, equipment actuation is often automatic. The human actions required for this case confirm that the equipment is operating properly and that the automatic action was/is appropriate.

FIGURE 1.A-1

FUNCTIONAL CLASSIFICATION

ALTERNATE success path(s): a set of equipment, physical processes, procedures and human actions that can be used to maintain a function given that the principal success path was not completely effective or was unavailable when the function was challenged. These success paths may use a combination of control and safety grade equipment, and usually require some human action to activate them. Alternate success paths usually involve the use of equipment within its design envelope.

EXTRAORDINARY success path(s): a set of equipment, physical processes, procedures and human actions that maintain a function given the unavailability of both the principal and alternate success paths when the function was challenged. These success paths may involve the use of equipment beyond its design envelope.

A compilation of the particular components (pipes, valves, pumps, etc.), combined with the appropriate human actions and procedures that make up the success paths of all required functions, provides a complete, detailed description of how the objective of each Goal is achieved and ultimately how the overall objective of economical, reliable, and safe power production is realized throughout the operating life of the plant. A more detailed description of the nuclear power plant Function Classification is presented in Appendix A.

1.A.3 Details of the Institutional Classification

In the Integrated Approach, each Goal is accomplished by maintaining the required functions. These functions are brought into being and supported by the general industry activities of Design, Construction, Operation and Maintenance. For each of these general industry activities, specific activities can be identified. Each specific activity possesses characteristics whose presence is indicative of how well the activity is being carried out. For example, in the general activity of Operation, there is a specific activity of "training operators". A characteristic of good operator training is the use of actual "hands-on" experience with systems and components. A detailed breakdown of the characteristics of the general and specific activities is given in Appendix B.

The importance of these characteristics was highlighted in an earlier segment of this study when significant nuclear plant events were reviewed using the Institutional Classification. It was found that the absence of key characteristics has sometimes been a source of problems in nuclear plant operation. For example, the absence of the key characteristic of "careful review of procedures, work efforts and records" (in the specific activity of checking maintenance) has resulted in events involving valve and circuit breaker misalignments which can lead to degraded operating conditions.

Figure 1.A-2 presents the success tree of Figure 1.A-1 in terms of each of the four Goals. The functions of each are supported by the four general industry activities of Design, Construction, Operation and Maintenance. Each of the four industry activities has specific activities, characteristics and specifications associated with them.

For each Goal, it is important that the designer identify and understand the specific functions and the success paths that maintain those functions. For the plant to be operated safely at all times, the operator must also understand these functions, the success paths that are intended by design to maintain them and the human actions that are required to support each. Consequently, the specific activities and characteristics associated with the general activity of Operation are different from those specific to Design.

The general activities of Construction and Maintenance also have their own sets of specific activities and characteristics. These two industry activities deal primarily with the hardware of systems and components, while Design and Operation deal with systems, components, success paths, functions, Goals, and the human and hardware interaction necessary to achieve safe and effective power production.

FIGURE 1.A-2

1.B Evolution of the Integrated Approach

1.B.1 Defense-in-Depth/Physical Barriers

The idea of the Integrated Approach originated from the concept of Defense-in-Depth which has been an integral part of the nuclear industry since its inception. It is based on the idea of designing and building plants to high standards and backing up that original action with built-in safety features to account for accidents and unforeseen situations. In 1973, the Atomic Energy Commission (AEC) described Defense-in-Depth in WASH-1250 (Reference 1.B-1) as follows:

- Design to high standards.
- Assume failures and provide safety systems.
- Provide alternate safety pathways, based on assumed failures of the safety systems.

The Defense-in-Depth concepts which have been widely reported in the literature (References 1.B-2 through 1.B-17) discuss the ideas of levels of activities and multiple physical barriers to protect the public from the consequences of a severe accident in a nuclear power plant.

Table 1.B-1 presents a historical summary of references to Defense-in-Depth up through the forerunner of the Integrated Approach, the Safety Level Concept (Reference 1.B-18). In general, the references described a "layered" approach to Defense-in-Depth in which a failure of protective layer 1 was accommodated by successful achievement of layer 2, a failure of layers 1 and 2 was accommodated by achievement of layer 3, etc. The numbers in Table 1.B-1 indicate the number of Defense-in-Depth layers addressed in each reference and correlate each layer with the corresponding Goals of the Integrated Approach.

1.B.2 The Critical Functions in Aviation/Aerospace

The aviation and aerospace industries go to great lengths in the design, construction, operation and maintenance of air- and space-crafts to prevent the loss of specific critical functions and to halt the propagation of damage or equipment failures that would keep these critical functions from being maintained. International Energy Associates, Ltd. (Washington, D.C.), under subcontract to C-E, performed a review of the critical functions in the aviation/aerospace industry. Five examples of critical functions associated with commercial aviation and aerospace are:

Propulsion Control
Flight (Attitude) Control
Navigation (Orbit) Control
Communications (Telemetry)
Environment Control

TABLE 1.B-1

HISTORICAL SUMMARY OF DEFENSE IN DEPTH

Source	Normal Operation (Engineering and Quality Assurance)	Core & Plant Protection (Protective and Safety Systems)		Containment Integrity (Engineered Safeguards and DBA Analysis)	Emergency Preparedness (Public Protection)	Barriers
U.S. AEC 1971 Hanauer	1	2		3	NM	Accomplish DID by use of multiple barriers
10 CFR 50 1971 Interim Policy Statement	1	2		NM (Not Mentioned)		NM
U.S. AEC 1973 WASH-1250	1	2		3	NM	NM
AIF 1974 Grey	1	2	3	4	NM	Multiple barriers
Text 1975 LaMarsh	1	2		3		Multiple barriers
C-E 1975 Dietrich	1	2	3	4	NM	NM
Nuclear Safety 1976 Moeller/Selby	1	2		3	4	NM
U.S. NRC 1976 Telford	1	2		3	NM	Multiple barriers
Text 1977 Lewis	1	2	3		NM	NM
W 1977 Arnold	1	2		3	NM	NM
U.S. NRC 1979 Hendrie	1	2		3	NM	Multiple physical barriers
U.S. NRC 1979 NUREG-578 NUREG-585	1		2		3	Diversity, redundancy, multiple barriers
U.S. NRC 1979 NUREG-553	1	2		3	4	NM
G-E/U.S. DOE 1979 ALO-66	1	2	3		4	Levels of assurance
NSAC 1980 Breen	1	2		3		NM
ACRS 1980 Okrent	1	2		3	4	NM
Safety Level Concept	1	2		3	4	Multiple physical barriers

Investigation of the commercial aviation and aerospace industries suggests that these industries, of necessity, have less safety margin built into their products, that is, the hardware, than the nuclear industry. Consequently, these industries focus greater attention on operational and procedural details. In comparison, the nuclear industry, having greater margins of "hardware safety", has tended to place less emphasis on operating practices.

The 1967 fire in the Apollo I spacecraft forced a thorough review of all aerospace industry practices and led to many improvements, both in the hardware of spacecraft and in the procedures and practices associated with their design, construction, operation and maintenance. The accident at Three Mile Island has had much the same impact on the nuclear industry in that the industry was forced to re-examine its fundamental practices and concepts of safety. From this re-examination, new approaches and thinking have evolved.

Specific aerospace accidents were evaluated to compare fundamental aviation and aerospace safety concepts to the Safety Level Concept (SLC) and to examine the lessons learned from these accidents. In addition, this effort examined the fundamental safety concepts of the Military Airlift Command (MAC) and compared these to commercial aviation. The following aviation and aerospace findings have significant implications to the nuclear power industry (Reference 1.B-19).

- NASA, the airlines, the military and the nuclear industry have similar safety objectives, strategies and approaches, although there are differences in the language used by these industries.
- Significant numbers of aerospace, aviation and maritime accidents are caused by human error. Therefore, sound human engineering should be emphasized in the prevention and mitigation of accidents.
- Typical causes of catastrophic accidents are component or subsystem failures that were not fully recognized by the operators (pilots, astronauts, reactor operators, etc.), and which eventually challenged the safety systems and operators.
- The failure to provide the operator with quality information rather than a quantity of raw data is viewed as a failure of the man-machine interface.
- Improper maintenance can render Safety Levels and activities useless and the overall system configuration unsafe.
- The ramifications of both maintenance and operational procedures must be fully understood by all parties involved to prevent system challenges.

1.B.3 The Safety Level Concept

Since the original concepts of Defense-in-Depth were conceived, U.S. industry has gained considerable experience, both from the operation of the early nuclear plants that have been constructed and from other technologies, most notably, aviation and aerospace. In addition, the expansion of data processing technology has made the computer an important tool for sorting and categorizing the many events which occur in nuclear power plants. It is also capable of performing complex calculations in which the probabilities of various events are computed (Probabilistic Risk Assessment).

The Safety Level Concept (SLC) (Phase I of the Sandia Safety Study, Reference 1.B-18) arose from the desire to systematize the Defense-in-Depth concept so that the methods and techniques of the aviation industry, operating reactor experience and recent analytical techniques could be incorporated into it. In the SLC, the Safety Levels were related to the historical "physical" barriers of fuel, primary system boundary, containment building and physical distance that have been viewed to separate the public from fission products within the reactor.

1.B.4 An Integrated Approach to Economical, Reliable, Safe Nuclear Power Production

The Integrated Approach also is related to the "physical" barriers. However, the Integrated Approach considers not only the protection of life and health, but also the economic factors associated with a nuclear plant. These include the capital investment of the plant as well as the factors associated with the continuous, reliable generation of power. The Integrated Approach is a logical extension of Defense-in-Depth and the SLC that embraces all aspects of the nuclear power industry. The structured framework of the Integrated Approach provides a logical and consistent method for working with many of the important areas, whether financial or safety related, of the process of nuclear power production.

SECTION 2: DEMONSTRATION OF THE INTEGRATED APPROACH TO ECONOMICAL, RELIABLE, SAFE NUCLEAR POWER PRODUCTION - APPLICATIONS

2.A Application One: Use of the Integrated Approach to Evaluate the Standard Review Plan

The following application was performed by the Technology for Energy Corporation (TEC) under subcontract to Combustion Engineering, Inc. Its purpose was to evaluate the Standard Review Plan (SRP) as described in NUREG-75/087 (Reference 2.A-1). There are several reasons why this application was chosen for demonstration. First, the SRP is intended to be a comprehensive document, addressing all aspects of nuclear plant safety and nuclear plant design, construction, operation and maintenance. Second, a previous evaluation of the SRP had been performed by Sandia National Laboratories (SNL) (Reference 2.A-2) using Probabilistic Risk Assessment (PRA) and comparison could be made between results of the PRA evaluation and those of the Integrated Approach evaluation. Third, the Integrated Approach could provide insights which were not provided by the PRA study. In particular, PRA tends to focus on the Functional Classification where the Integrated Approach addresses both the Functional and Institutional Classifications. Finally, the SNL study (the result of rather extensive and deliberate effort) could be used as a "benchmark" against which the evaluations of the Integrated Approach could be compared.

The TEC study examined the SRP from both a quantitative and a qualitative perspective. For the quantitative study, the earlier work of SNL, "Second Interim Report - Value Impact Assessment of Regulatory Review Units" (Reference 2.A-2), hereafter called the SNL STUDY, was used as a point of reference. The SNL STUDY used PRA as a basis for determining the relative significance or safety importance of various SRP sections. The Nuclear Regulatory Commission (NRC) provided information to SNL regarding the relative amount of time spent reviewing various SRP sections. SNL then made a comparison of the time spent on a particular SRP section relative to the safety importance of that section. If one assumes that the quality of a review is in some way related to the time spent conducting that review, then one would hope that the greatest amount of time would be spent reviewing those sections which have the greatest safety significance. SNL then proceeded to develop tables comparing the relative time spent on individual SRP sections with the safety importance. Approximately one-half of the systems examined were given an appropriate amount of review time, that is, high importance systems were given high review times and low importance systems were given low review times. There were, however, some cases where systems of high safety importance were given a low review time and, conversely, some cases where systems of a relative low importance were given high review times.

The Integrated Approach study conducted by TEC uses the SNL work in two ways. First, the evaluations performed by SNL using PRA to establish the relative safety significance of various SRP sections were used as a "benchmark" against which Integrated Approach evaluations of the

relative safety significance of the same sections could be compared. Second, the TEC study evaluated the relative time spent on various SRP sections and looked also at the "quality" of various SRP sections. The "quality" measures used to evaluate the SRP are closely related to overall systems integration and attention to interface details as well as design, construction and maintenance requirements, as would be indicated by both the Functional and Institutional Classifications of the Integrated Approach.

A relatively simple interrogation procedure was developed to determine the relative safety importance of a particular SRP section. That procedure consists of asking the following questions:

What is the maximum number of Goals (Levels) affected by this particular SRP section?

For any Goal (Level), what is the maximum number of functions affected by this particular SRP section?

For any particular function, what is the maximum number of success path types impacted by this section of the SRP (normal, principal, alternate or extraordinary)?

On this relatively simple basis, point values were assigned to various SRP sections. Point values typically ranged from two to three on the low end to twelve to thirteen on the high end. On this basis then, any number of SRP sections could be assigned a point value. The SRP sections were rated using this procedure and ranked with the highest point value corresponding to highest safety importance. This simple Integrated Approach ranking was then compared to the ranking obtained using PRA. The agreement between the two ranking techniques was remarkably good. A technique known as the Spearman Rank Correlation Coefficient was used and a relative correlation of ninety-two percent was obtained between the PRA ranking and the Integrated Approach ranking (Reference 2.A-3). This high correlation indicates the potential use of the Integrated Approach.

The Functional Classification contains many of the basic physical assumptions that are present in PRA. In particular, examination of the four Goals (Levels) shows the following:

<u>Integrated Approach</u>	<u>PRA</u>
Normal Operation	Tied to the frequency of initiating events. The more attention that is paid to preserving normal operation, the lower the frequency of initiating events.

Core and Plant Protection

Tied to the probability that if an initiating event occurs, the appropriate actions will be taken and equipment utilized to minimize propagation of damage and, in particular, minimize damage to the reactor core.

Containment Integrity

PRA studies indicate that, in order for serious consequences to occur to the public, not only must core damage occur, but containment integrity must be violated in some way.

Emergency Preparedness

After a failure to keep the core from melting and the failure of the containment, PRA calculates the consequences of an accident to the public by considering the amount of radioactivity released and the dose that will be received by various members of the public.

As illustrated above, the more Goals (Levels) affected by a particular system (or SRP section), the greater the chances of a common cause failure. Similarly, the more functions within the one Goal (Level) that are affected by a particular system (or SRP section), the more vulnerable that Goal (Level) is to failure of that system; hence, the more safety importance that system has. Finally, the more success paths affected by a particular system (or SRP section), the more a particular function depends on the effectiveness of that particular system (or section). From the above, we see that the Functional Classification alone can be a very helpful tool in evaluating the relative safety importance of systems within a nuclear plant. Additional information about this study may be obtained from Reference 2.A-3.

While the Functional Classification of the Integrated Approach was used alone in a quantitative sense to establish the relative importance of SRP sections, both the Functional and Institutional Classifications were used to evaluate the "quality" of various SRP sections. This was done in the following manner.

Initially, a series of sixty-eight questions was developed, based on a careful review of both the Functional and Institutional Classifications. These questions were expressed so that they would have a "yes" or "no" answer. The point value assigned to each answer was "yes" equals 1.0 or "no" equals 0.0. In addition, a partial point value was assigned for answers which were not clearly "yes" or "no" answers. For example, a value of 0.25 was assigned for an answer that

was given as "maybe", a value of 0.50 was given if an answer to a question could be "to some extent", and a value of 0.75 was assigned if an answer of "probably" could be given. Thus, a procedure emerged for evaluating the degree or extent to which a particular SRP section agreed with the Integrated Approach. If the answers to all sixty-eight questions were "yes", then a point value of sixty-eight could be assigned to a particular section and if the answers to all questions were "no", then a point value of zero could be assigned to that section. Since partial point values could be assigned for questions answered with "maybe", "to some extent" or "probably", fractional credit could be assigned to the answer for any one question.

Approximately twenty-five SRP sections were interrogated using the procedure outlined above. The highest score obtained for any section examined was twenty-three points and the lowest score obtained was two points.

Comparison can be made between the Integrated Approach and the SNL STUDY results. Where the SNL STUDY used time spent on an SRP section as a measure of the quality of the SRP review, the Integrated Approach used the extent or degree of agreement with the Integrated Approach as an indicator of the relative review quality of an SRP section. Clearly, one does not expect to require SRP sections to be in perfect agreement with the Integrated Approach. This is particularly true since, in general, the SRP does not emphasize the overall systematic approach taken by the Integrated Approach. However, one would hope that those systems (or SRP sections) with a high safety importance are reviewed with greater care than those with a lower value. If these systems (or sections) were reviewed in a manner consistent with the Integrated Approach, there would be considerable attention paid to the functional aspects (Goals, functions, success paths, the impact of human actions/errors, system interfacing requirements, systems integration, system performance under normal and faulted conditions, design requirements) and the institutional aspects (Design, Construction, Operation and Maintenance requirements, as well as those systems and organizational activities which were established to ensure their successful implementation). Consequently, since more of these features would need to be addressed under such systems, it is expected that more time would be spent reviewing these particular systems.

2.B Application Two: How the Integrated Approach Can Be Used to Evaluate Reactor Operating Experience

The Integrated Approach can be used in operating experience evaluation programs to determine the significance of events and to identify their causes. Significance can be determined by examining the number of Goals affected, the number of functions affected, the number of success paths available to maintain each function, and the availability and reliability of these remaining success paths (Figure 2.B-1). Operator impact on event significance could be assessed by asking:

- How would the event have proceeded had there been no operator action or if the operator had erred at a critical point in the sequence of events?

The causes of an event could be established by asking (Figure 2.B-2):

- Which general industry activities contributed to this event?
- For each general activity, which specific activities contributed to this event?
- Which characteristics of these specific activities were weak or absent?

These techniques offer a means of analyzing nuclear power plant experience to identify key activities (and their corresponding characteristics) whose presence or absence determines how a plant is to achieve its goals. The Integrated Approach permits analyses to proceed beyond determining the hardware or human error causes of events to the identification of possible institutional weaknesses which may underly many nuclear industry problems. This also suggests that a systematic review at a nuclear power plant, whose management intentionally sought to determine whether these key activities and their characteristics were present, could identify areas where improvements could be made to reduce the number of incidents.

A particular advantage of the Integrated Approach is the systematic method it offers for analyzing complex events. For example, a matrix showing the four Goals and the four industry activities of the Integrated Approach can be constructed. Various elements of the event being analyzed can then be placed in the matrix according to the Goal and activity that each element affects. The elements can then be further evaluated to identify the specific activities and key characteristics whose weakness or absence contributed to this aspect of the event. The first step of such a process was performed during an earlier phase of the development of the Integrated Approach. Various elements of the TMI accident as reported in "Nuclear Accident and Recovery at Three Mile Island" (the "Hart" report, Reference 2.B-1) were placed in the Goal/industry activity matrix as shown in Table

2.B-1. Further evaluation of each element as outlined above would reveal the fundamental causes of these aspects of the accident. Significantly, many of the major recommendations arising from investigations of the TMI accident affected institutional features of the nuclear industry. The Integrated Approach can provide a systematic technique for assessing these features in the evaluation of complex events.

FIGURE 2.B-1

EVENT SIGNIFICANCE

How many Goals were affected?

How many functions affected?

For each function:

- How many success paths remaining?
- What is reliability of remaining success paths?

* Human action:

No Operator Action?

Operator Error?

How frequently does this occur?

TABLE 2.B-1

INTEGRATED APPROACH

SIGNIFICANT FEATURES OF THE TMI EVENT
(Quotes from the "HART" report)

	Design	Construction	Operation	Maintenance
NORMAL OPERATION	<p>"... insufficient attention to human factors ..."</p> <p>"... lack of direct indicator to show whether the ... (PORV) was open or closed ..."</p>		<p>"... TMI ... personnel did not have ... guidance, based on similar accidents ..."</p> <p>"Had the utility closed the block valve, as required by ... Technical Specifications, the loss-of-coolant accident ... would not have occurred."</p>	<p>"... it was known ... that one or more valves on ... the pressurizer had been leaking ... for more than six months ... Statements of ... personnel indicated they had become accustomed to the elevated temperature readings."</p>
CORE & PLANT PROTECTION	<p>"... 1200 alarms, of which several hundred went off in the first minutes ..."</p> <p>"... insufficient attention to human factors ..."</p> <p>"... Instrumentation ... could not provide indication for the extreme conditions ..."</p> <p>"... computer printer ... became severely backlogged ..."</p> <p>"... 'candy-cane' curve trapped steam ..."</p>		<p>"... they throttled HPI before determining there was a loss-of-coolant accident ..."</p> <p>"... emergency procedures ... were vague, confusing, incomplete ..."</p> <p>"... key readings of temperature in the core were rejected ..."</p>	<p>"A radiation monitor did not sound ... it may have been miscalibrated."</p>
CONTAINMENT INTEGRITY	<p>"... failure of the containment ... to seal ... on initiation of high pressure injection ..."</p> <p>"... inability to seal off the pathways between the auxiliary building and the environment ..."</p>		<p>"... missed, misinterpreted or discounted critical information ... an example was the response to the hydrogen burn in the containment at 1:50 p.m. ..."</p>	
EMERGENCY PREPAREDNESS	<p>"Offsite radiation monitoring ... was both disorganized and insufficient ..."</p> <p>"... no procedure ... for participation by the reactor-vendor, the NRC or the architect-engineer in assessing plant conditions."</p> <p>"... severe communications difficulties ..."</p>		<p>"... lack of coordination among the utility, the NRC and the State ..."</p> <p>"... State did not have enough technically qualified staff ..."</p>	<p>"... (NRC had insufficient drills ...) ..."</p>

FIGURE 2.B-2

INTERPRETATION OF SIGNIFICANT EVENTS

2.C Application Three: Use of the Integrated Approach in the Development of an Economic Risk Assessment Framework

A major hindrance to the resurgence of the nuclear power industry is the perception that this option presents a significant financial risk. Prior to TMI, this perception resulted from the ever-increasing licensing requirements and schedule slippages that, when coupled with rising inflation, doubled or quadrupled original cost estimates. The fact that nuclear power plants required large capital investments at a time when utilities had trouble raising capital increased the perception that nuclear power was too costly. After TMI, this perception was reinforced as it became obvious that a nuclear plant was not only costly to build but could also be very costly to operate. To counter this perception, or at least to put it in the proper perspective, the economic risk associated with nuclear power must be quantified. This application was undertaken to determine a framework in which the economic risk of nuclear power could be evaluated. Reference 2.C-1 provides additional details of the economic risk evaluation.

Economic risk is defined as the product of the occurrence frequency of an event and the consequences of the event expressed in dollars or in units readily convertible to dollars. This definition divides the risk analysis into two relatively independent calculations; the first, to determine the frequency of event occurrence and, the second, to determine the event consequences.

Of the two, estimating the frequency of occurrence presents the more difficult problem. For large, complex entities like a nuclear power plant, there is an almost infinite number of possible events. Therefore, before useful frequencies can be calculated, the almost infinite number of events must be grouped into a manageable number of event types. How the event types are defined will, to a large degree, determine the usefulness (and the complexity) of the risk analysis.

Once the event types are defined, the frequency of occurrence for a particular event type can be determined by one of two methods. First, the expected frequency of a particular event type can be estimated from the observed frequency of similar events that have already occurred. Second, a reliability analysis can be performed using historical system or component failure data to predict event type frequencies.

After event type frequencies are determined, the event type consequences must be found. As with event type frequencies, the method used to predict event consequences is dependent on whether sufficient historical event data exists.

The U.S. nuclear power industry has accumulated some 500 reactor years of experience, including almost 300 PWR years. This experience base will allow most event type frequencies to be determined by the first method. However, the experience base is too small to determine the

frequencies and consequences of events having a frequency on the order of less than once per 100 reactor years. The very high consequence events having probabilities between 10^{-2} and 10^{-6} per reactor year cause many utility executives to be concerned with the potential financial risk of the nuclear power option. Thus, any economic risk treatment of nuclear power must include not only the risks from high and moderate frequency events but also from the low frequency-high consequence events.

In an economic risk reduction program, it would be natural to examine first those events which pose the greatest economic risk. Therefore, the first segment of this economic risk analysis attempted to identify the event types for which the economic risk is greatest. The C-E Reliability Data Base was used for this purpose.

Three thousand PWR outages (excluding refueling) during the period January, 1961 through August, 1980 were examined. This review encompassed 260 reactor years of commercial operating experience. For this portion of the analysis, event types were defined on the basis of outage duration. The total risk of operating a nuclear power plant does not vary as a function of how event types are defined. However, the total risk will be apportioned differently depending on event type definitions. The occurrence frequency of events producing outages of each duration was determined from the data base. Short term replacement power costs were used to compute the economic consequences of outages of various durations in terms of dollars per plant year. Finally, the occurrence frequency of outages of each duration was multiplied by the corresponding economic consequences to compute the economic risk. The results are shown in Figures 2.C-1 and 2.C-2 and Table 2.C-1.

Figure 2.C-1 shows the occurrence frequency of outages of various durations along with examples of the events causing the outages. Figure 2.C-2 shows the cost (based on short term replacement power costs) in dollars per reactor year of outages of each duration. The product of occurrence frequency and economic consequences in Figures 2.C-1 and 2.C-2 is shown in the bottom line of Table 2.C-1. The figures in this line show the economic risk associated with outages of each duration and indicate that the greatest risk is associated with events producing outages lasting from one month to one year. The table also contains examples of events causing outages of each duration, the occurrence frequency of such events, and the cost of each resulting outage. Analysis results such as these can be used to set priorities for the detailed examination of events within an event type framework developed using the Integrated Approach as discussed below.

The event types for this segment of the economic risk analysis were defined using a matrix of the four Goals (Normal Operation, Core and Plant Protection, Containment Integrity and Emergency Preparedness) and the four general industry activities (Design, Construction, Operation and Maintenance) of the Integrated Approach. Within each of the general activities, a more detailed definition of event types can be

FIGURE 2.C-1

OUTAGE FREQUENCY (PER REACTOR YEAR)

VS. OUTAGE DURATION

FIGURE 2.C-2
OUTAGE COST (\$MILLION/REACTOR YEAR)
VS. OUTAGE DURATION

TABLE 2.C-1

OUTAGE CATEGORIZATION MATRIX
(EXCLUDING REFUELING)

Characteristic	Outage Duration					
	<One Day	One Day to One Week	One Week to One Month	One Mo. to One Year	One Year to Five Years	Five Years to Plant Loss
Cause Category (Examples)	Scrams Trans.	Minor Equip. Repair	Reg. Req. Chem. Problems	Major Equip. Problems	Reg. Req.	Major Core Damage
Experience (Examples)	Reactor/Turbine Trips	RCP Seal Leak CRDM Repair	Inspect SG Tubes Turbine Repair	Retube Cond. Modify Turbine	TMI-1	TMI-2 Class 9
Incidents/Plant Year	7.7	2.7	1.0	0.3	10^{-2}	10^{-4}
\$/Incident	200K	1.5M	8M	40M	400M	2-8B
\$Risk/Plant Year	1.5M	4.0M	8M	12M	4.0M	0.2-0.8M

developed by using Performance Enhancement Factors (PEF). PEF's are those characteristics which, if present, might have reduced the probability of occurrence of an event. A set of PEF's was developed using the specific activities and characteristics of the Institutional Classification and is shown in Table 2.C-2. As an example of placing an event into an event type category, consider a transient caused by mis-operation of switchyard breakers due to poor arrangement of the breaker controls. The event would be placed in the Goal/Industry Activity matrix in the element corresponding to the Goal of Normal Operation and the general industry activity of Design. The event could be further categorized within this matrix element by the PEF of Human Factors - use of good human engineering practices in the design of systems and components.

Approximately 200 outages from two sources of data, Licensee Event Reports (LERs) and the EPRI Limiting Factor Analysis (LFA), were used to evaluate the event type framework. Summarized by percentage of total outage hours, Table 2.C-3 identifies the predominant PEFs which, had they been present, could have prevented the outage. This information can suggest areas where greater emphasis could be placed to prevent similar outages from occurring.

A properly constructed economic risk analysis can direct attention to areas where cost and risk reduction efforts can be most fruitful. It can also be used to evaluate the financial value of proposed changes before they are made.

TABLE 2.C-2

PERFORMANCE ENHANCEMENT FACTORS

Design Related Performance Enhancement Factors

1. OPERATING CONDITIONS: Full range of operating conditions identified and met. Consideration given to the full range of conditions the system or component may be operated under and still function as required. Must also consider all external environmental conditions to which the system or component may be exposed. Consideration given to potential system imbalances and failures, the use of multiple success paths, and the use of passive or self-actuating components when possible. Design should also incorporate a fail-safe and self-protection philosophy.
2. DESIGN CONSIDERATION: Design consideration for operation, maintenance, repair and testing of systems and components during their lifetime. Consideration given to corrective and preventive maintenance requirements, status monitoring, and system or component isolation capability.
3. STANDARDS AND CODES: Need for strict adherence to current standards and codes during the design process. Also involves use of current state of the art technology.
4. HUMAN FACTORS: Use of good human engineering practices in the design of systems and components. Attention given to possible human actions that may take place in the use of equipment or systems. Consideration also given to the need for prioritized information to the operator during accident monitoring.
5. REVIEW AND DOCUMENTATION: Review process that is independent of the design process and conducted by qualified personnel. Also considers the complete documentation and retrievability of the design process.

Construction Related Performance Enhancement Factors

1. PROCEDURES: Use of current standards, codes, procedures and practices that directly affect the construction of a plant or manufacture of systems or equipment used during construction. Procedures should also ensure review and documentation of the construction process.
2. PLANNING: Consideration given to the overall sequence of events as well as the processes and procedures used in the construction and manufacturing process.

TABLE 2.C-2 (Continued)

3. EQUIPMENT: Consideration given to the equipment used in the construction of a plant or manufacture of systems or components used in construction.
4. MATERIAL: Consideration given to the material used in the construction of a plant or manufacture of systems or components used in construction. Consideration given to obtaining the specified material in a timely manner.
5. TRAINING: Consideration given to the training of construction or manufacturing personnel. Includes training on equipment use, procedures, and material procurement.

Operation Related Performance Enhancement Factors

1. PROCEDURES: Attention given to procedure clarity, completeness, format, detail and ability to handle problems that may occur. Where possible, procedures should include the use of checklists and address required review and documentation.
2. QUALIFICATION/TRAINING: Consideration given to initial and continuous training and qualification of personnel to respond to both normal and abnormal situations. Training program should stress the safe operation of systems and equipment in a manner that minimizes risk to the public. Emphasis on experience feedback as an integral part of the training program is necessary.
3. STAFFING: Consideration given to the size of the plant staff necessary to ensure safe operation of the facility.
4. ENVIRONMENT: Developing an environment that is free of distractions to the operator. The environment should be conducive to ensuring the adequate readiness and performance capability of systems and equipment.
5. COMMUNICATION: Consideration given to information flow to and from operators and plant personnel at all levels. Includes both written and verbal communication.
6. LINES OF RESPONSIBILITY: Facility's "chain-of-command" authority defined and used. The roles and responsibilities of personnel during normal plant operation as well as in the event of an accident are defined and understood.

TABLE 2.C-2 (Continued)

Maintenance Related Performance Enhancement Factors

1. PROCEDURES: Attention given to procedure clarity, completeness, format, detail and ability to handle problems. Where possible, procedures should include the use of checklists and address required review and documentation.
2. QUALIFICATION/TRAINING: Consideration given to the training of maintenance personnel in the disassembly, repair, assembly and testing of equipment and components. Emphasis on the need to anticipate the consequences of maintenance action and potential effect on safe plant operation is required as part of the training process.
3. EQUIPMENT: Consideration given to the use of the proper tools and test equipment while conducting maintenance activities.
4. SCHEDULING: Consideration given to scheduling of maintenance activities to minimize the impact on plant operations and the potential risk to the public. Consideration also given to anticipating component natural end-of-life and prevention of excessive component testing.

TABLE 2.C-3 (PART A)

EVENT TYPE FRAMEWORK
(LICENSEE EVENT REPORTS)

		Goals					
Industry Activity	Performance Enhancement Factors	Normal Oper.	Core and Plant Prot.	Cont. Intg.	Emer. Prep.	Totals	
Design	Operating Conditions	9	10	11	----	29	
	Design Considerations	<1	3	<1	----	5	
	Standards and Codes	<1	8	1	----	9	58
	Human Factors	<1	<1	----	----	<1	
	Review and Documentation	<1	15	----	----	15	
Const.	Procedures Planning	<1	1	<1	----	1	
	Equipment	----	----	----	----	----	
	Material	6	2	<1	----	8	10
	Training	<1	1	----	----	1	
Oper.	Procedures Qualification and Training	<1	2	10	----	12	
	Staffing	<1	2	9	----	11	
	Environment	----	----	----	----	----	24
	Communications Lines of Responsibility	<1	<1	----	----	1	
Maint.	Procedures Qualification and Training	1	2	1	----	4	
	Equipment	1	1	----	----	2	
	Scheduling	<1	----	----	----	<1	8
		1	1	----	----	2	
Totals		19	48	33	----	100	100

TABLE 2.C-3 (PART B)

**EVENT TYPE FRAMEWORK
(EPRI LIMITING FACTOR ANALYSIS)**

		Goals					
Industry Activity	Performance Enhancement Factors	Normal Oper.	Core and Plant Prot.	Cont. Intg.	Emer. Prep.	Totals	
Design	Operating Conditions	25	4	----	----	29	
	Design Considerations	11	----	----	----	11	
	Standards and Codes	----	4	----	----	4	46
	Human Factors Review and Documentation	2	<1	----	----	2	
		----	----	----	----	----	
Const.	Procedures Planning	2	----	----	----	2	
	Equipment	----	----	----	----	----	
	Material	1	----	----	----	1	15
	Training	11	----	----	----	11	
Oper.		1	----	----	----	1	
	Procedures Qualification and Training Staffing	7	<1	----	----	7	
		<1	<1	----	----	1	
		----	----	----	----	----	
Maint.	Environment Communications Lines of Responsibility	----	----	----	----	----	8
		<1	<1	----	----	<1	
		----	----	----	----	----	
		----	----	----	----	----	
Totals	Procedures Qualification and Training	7	2	2	----	11	
	Equipment Scheduling	5	2	2	----	8	31
		1	----	----	----	1	
		11	----	----	----	11	
Totals		84	12	4	----	100	100

2.D Application Four: Use of the Integrated Approach in Operator Training

It is postulated that the Integrated Approach would help nuclear plant operators evaluate the relative safety importance of various conditions and system lineups that would occur in a reactor plant. To test this idea, an experiment was formulated and performed. This compared the results of plant personnel event analysis, before and after exposure to the Integrated Approach, with the result of a sophisticated risk calculation computer program.

As part of a separate contract with the Nuclear Safety Analysis Center (NSAC), a very detailed and comprehensive computerized method, SIEVE (SIGNificant EVENT Evaluation, Reference 2.D-1), has been developed which calculates the change in risk (measured in terms of core damage probabilities) in a nuclear plant associated with the particular system lineups, failures of components or human errors. SIEVE utilizes a detailed systems description of the reactor plant. When a failure is postulated, the program simulates that failure and calculates the change in probability of having a core melt based on the single failure or combination of failures described to it. Hence, it is possible, given a number of different events, to interrogate the computer and establish the relative importance of each event. The importance in this case is measured by the increase in probability of core damage or core melt that would result from the occurrence of the event which is described.

Two groups of students were scheduled to receive lectures on the Integrated Approach. Before and after each lecture, a group of six events was presented to the students. The students were asked to rank the events by what they perceived to be their safety significance. The six events were also programmed into SIEVE to quantitatively determine the relative significance. The intent was to utilize the computer significance predictions as "truth" and compare the students' ability to predict importance.

Analysis of the results of the test indicate a small positive effect on event significance ranking of prior exposure to Integrated Approach methodology. The test was limited in scope and should be interpreted as indicative of possible trends only. The details of the experimental design limit validity of extension of these results to more general conclusions.

SECTION 3: OTHER USES AND APPLICATIONS OF THE INTEGRATED APPROACH

In addition to those applications identified in SECTION 2, the following provides a list of other possible applications of the Integrated Approach.

- Operating, Emergency and Maintenance Procedures - A systematic review of plant procedures using both the Functional and Institutional Classifications can provide substantial improvements in these procedures. Review of a procedure from a functional standpoint could ensure that critical functions are always maintained during execution of the procedure. Operational and maintenance personnel could be made more cognizant of potential problem areas by presenting plant conditions in terms of available and non-available functions and success paths.
- Technical Specifications - The Integrated Approach can be used as a basis for evaluating and upgrading Technical Specifications (nuclear plant operational readiness requirements). Such an effort could produce simpler, more comprehensive and logical Technical Specifications by addressing the functional aspects of plant operation under all plant conditions. It also could use the Institutional Classification to assure that human organizations are properly maintained in support of the Goals and functions.
- Plant Auditing Procedures and Techniques - Those individuals and organizations that are charged with the responsibility of performing safety or economic audits of plant operations could use both the Functional and Institutional Classifications as a basis for performing these audits. This would ensure a certain degree of completeness and balance in the auditing process. Furthermore, the Integrated Approach can identify potential interactions where the absence of certain features at one Goal, function or success path could be accommodated by additional features in another area. This is particularly true at the success path level. Compensation for a perceived weakness in one success path could be accommodated through alternate independent success paths to achieve a particular function. The systematic nature of the Integrated Approach can provide the audit team with a well-structured framework on which to base the audit format as well as the generation of more constructive recommendations for improvements.
- Training of Licensed and Non-Licensed Operators, Management, Maintenance, and Engineering Personnel - A clear understanding of both the Functional and Institutional Classifications by all major nuclear industry parties could enhance the safety, reliability, and economics of nuclear power production. This is particularly true of those individuals who are directly associated with the operation of nuclear power plants. It is valuable for these individuals to understand the overall relationship of the various systems, and the significance of human actions. In particular, it is very important for operating personnel and management to have simple

"rules of thumb" with which to make judgements about the relative safety importance of certain actions and activities without exaggerating or underestimating the importance of either. The Integrated Approach techniques are valuable for this purpose. In addition, an overall understanding of the plant through the use of the Functional Classification can aid in planning and scheduling maintenance, repairs, and modifications. A good understanding of the Institutional Classification can assist operators and management in locating potential shortcomings in tasks prior to action execution. If operators, management and engineering staff are aware that particular tasks, systems or components are essential to plant safety, they can dedicate an appropriate level of attention to the systems and components.

- Functional and Task Analysis - A great deal of emphasis is presently being placed on using functional and task analyses to evaluate tasks in a power plant which are performed by machines and by humans. In the task analysis phase, identification is made of what the human operator is specifically required to do in order to satisfy the functions. Task analysis has proven to be a very valuable tool in identifying the skill and knowledge requirements for individual operators, shift crews and plant personnel. Through analysis of all the tasks that a person must complete in order to do his job well, it becomes possible to develop training programs which are specifically geared toward imparting the required skills. The Integrated Approach is valuable in such an endeavor because it provides an overview that helps ensure training programs and staffing objectives are established such that all required plant functions are properly maintained during normal, abnormal, and emergency conditions.
- Basis for Large Scale Research Programs - Large scale research programs emphasizing improvements in aspects of nuclear power plant operation could be reviewed in terms of the Functional and Institutional Classifications from the point of view of completeness and balance. This type of application is similar in approach to the review of the NRC Standard Review Plan described earlier. A systematic, functionally oriented review of any large research program, supported by insight gained from institutional reviews of industry needs, could help assure efficient use of research funds and resources.
- Interpretation, Review and Communication of Probabilistic Risk Assessment (PRA) - The principles and practices used in PRA are complex in usage and interpretation. The Integrated Approach is a useful tool in communication of PRA-based findings to decision makers, executives and legislators, as well as the general public. For example, serious accidents of the type analyzed by reports such as WASH-1400 are simply represented as a loss of all four Goals.

programs which are specifically geared toward imparting the required skills. The Integrated Approach is valuable in such an endeavor because it provides an overview that helps ensure training programs and staffing objectives are established such that all required plant functions are properly maintained during normal, abnormal, and emergency conditions.

- Basis for Large Scale Research Programs - Large scale research programs emphasizing improvements in aspects of nuclear power plant operation could be reviewed in terms of the Functional and Institutional Classifications from the point of view of completeness and balance. This type of application is similar in approach to the review of the NRC Standard Review Plan described earlier. A systematic, functionally oriented review of any large research program, supported by insight gained from institutional reviews of industry needs, could help assure efficient use of research funds and resources.
- Interpretation, Review and Communication of Probabilistic Risk Assessment (PRA) - The principles and practices used in PRA are complex in usage and interpretation. The Integrated Approach is a useful tool in communication of PRA-based findings to decision makers, executives and legislators, as well as the general public. For example, serious accidents of the type analyzed by reports such as WASH-1400 are simply represented as a loss of all four Goals.

REFERENCES

EXECUTIVE SUMMARY

- ES-1 Hanauer, S. W./Morris, P. A., "Technical Safety Issues for Large Nuclear Power Plants", Proceedings of the Fourth International Conference on the Peaceful Uses of Atomic Energy, Geneva, September 1971, Page 1
- ES-2 Federal Register, Volume 39, Number 3, page 1001, part 50, "Licensing of Production and Utilities Facilities"
- ES-3 WASH-1250, "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities", Washington, D.C., U.S. Atomic Energy Commission, July 1973
- ES-4 Grey, J., "Nuclear Power Safety", New York, Atomic Industrial Forum, Inc., 1974, Page 8
- ES-5 Lamarsh, J. R., "Introduction to Nuclear Engineering", Reading, Massachusetts, Addison-Wesley Publishing Company, 1975, Page 500
- ES-6 Hetrick, D. L., Proceedings of the American Nuclear Society National Topical Meeting, Washington D.C., American Nuclear Society, 1975: Dietrich, J. R./Stathopoulos, A., "Protection of the PWR Against Loss of Coolant Effects", Page 243
- ES-7 Moeller, D. W./Selby, J. M., "Planning for Nuclear Emergencies", Nuclear Safety, (January-February, 1976), 1-8, Page 1
- ES-8 Rust, J. H./Weaver, L. E. (Editors), Nuclear Power Safety, New York, Pergamon Press, Inc., 1976: Telford, J. T., "Current Problems in Reactor Safety", Page 351
- ES-9 Lewis, E. E., "Nuclear Power Reactor Safety", New York, Wiley Interscience, 1977, Page 97
- ES-10 International Atomic Energy Agency, Nuclear Power and Its Fuel Cycle, Volume 5, May 2-13, 1977: Arnold, W. H., "Safety Considerations of PWRs", Page 270
- ES-11 Rogovin, M., "Three Mile Island, A Report to the Commissioners and to the Public", Volume 2, Part 1, Washington, D.C., Nuclear Regulatory Commission, January 24, 1980, Page 14
- ES-12 NUREG-0585, "TMI-2 Lessons Learned Task Force Final Report", U.S. Nuclear Regulatory Commission, October 1979, Page 3-3

- ES-13 Salomon, S. N., "Beyond Defense-in-Depth", Washington, D.C., U.S. Nuclear Regulatory Commission, NUREG-0553, October 1979, page I-1
- ES-14 El-Sheikh, K. A., "Methodology for the Selection of LWR Safety R&D Progress", ARSD-00027, Springfield, Virginia, National Information Service, November 1979, Page 6
- ES-15 Breen, R. J., "Defense-in-Depth Approach to Safety in Light of TMI-2", Presented at American Nuclear Society 26th Meeting, Las Vegas, Nevada, June 10, 1980, Pages 1 and 2
- ES-16 Inside NRC, Volume 2, Number 21, October 20, 1980, Page 5
- ES-17 NUREG-0839, A Survey by Senior NRC Management to Obtain Viewpoints on the Safety Impact of Regulatory Activities from Representative Utilities Operating and Constructing Nuclear Power Plants, U.S. Nuclear Regulatory Commission, August, 1981, page 4

REFERENCES

TEXT

- 1.A-1 Corcoran, W. R., et al, "The Critical Safety Functions and Plant Operation", Nuclear Technology, Volume 55, December, 1981
- 1.A-2 Goodstein, L. P./Rasmussen, J., "The Use of Man-Machine Design Criteria in Computerized Control Rooms", RISO National Laboratory, DK-4000, Roskilde, Denmark
- 1.B-1 WASH-1250, "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities", Washington, D.C., U.S. Atomic Energy Commission, July 1973
- 1.B-2 Hanauer, S. W./Morris, P. A., "Technical Safety Issues for Large Nuclear Power Plants", Proceedings of the Fourth International Conference on the Peaceful Uses of Atomic Energy, Geneva, September 1971, Page 1
- 1.B-3 Federal Register, Volume 39, Number 3, Page 1001, Part 50, "Licensing of Production of Utilities Facilities"
- 1.B-4 WASH-1250, "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities", Washington, D.C., U.S. Atomic Energy Commission, July 1973
- 1.B-5 Grey, J., "Nuclear Power Safety", New York, Atomic Industrial Forum, Inc., 1974, Page 8
- 1.B-6 Lamarsh, J. R., "Introduction to Nuclear Engineering", Reading, Massachusetts, Addison-Wesley Publishing Company, 1975, Page 500
- 1.B-7 Hetrick, D. L., Proceedings of the American Nuclear Society National Topical Meeting, Washington D.C., American Nuclear Society, 1975: Dietrich, J. R./Stathopoulos, A., "Protection of the PWR Against Loss of Coolant Effects", Page 243
- 1.B-8 Moeller, D. W./Selby, J. M., "Planning for Nuclear Emergencies", Nuclear Safety, (January-February, 1976), 1-8, Page 1
- 1.B-9 Rust, J. H./Weaver, L. E. (Editors), Nuclear Power Safety, New York, Pergamon Press, Inc., 1976: Telford, J. T., "Current Problems in Reactor Safety", Page 351
- 1.B-10 Lewis, E. E., "Nuclear Power Reactor Safety", New York, Wiley Interscience, 1977, Page 97

- 1.B-11 International Atomic Energy Agency, Nuclear Power and Its Fuel Cycle, Volume 5, May 2-13, 1977: Arnold, W. H., "Safety Considerations of PWRs", Page 270
- 1.B-12 Rogovin, M., "Three Mile Island, A Report to the Commissioners and to the Public", Volume 2, Part 1, Washington, D.C., Nuclear Regulatory Commission, January 24, 1980, Page 14
- 1.B-13 NUREG-0585, "TMI-2 Lessons Learned Task Force Final Report", U.S. Nuclear Regulatory Commission, October 1979, Page 3-3
- 1.B-14 Salomon, S. N., "Beyond Defense-in-Depth", Washington, D.C., U.S. Nuclear Regulatory Commission, NUREG-0553, October 1979, page I-1
- 1.B-15 El-Sheikh, K. A., "Methodology for the Selection of LWR Safety R&D Progress", ARSD-00027, Springfield, Virginia, National Information Service, November 1979, Page 6
- 1.B-16 Breen, R. J., "Defense-in-Depth Approach to Safety in Light of TMI-2", Presented at American Nuclear Society 26th Meeting, Las Vegas, Nevada, June 10, 1980, Pages 1 and 2
- 1.B-17 Inside NRC, Volume 2, Number 21, October 20, 1980, Page 5
- 1.B-18 "The Safety Level Concept and Its Application to Light Water Power Reactors - Final Draft", Combustion Engineering, Inc./International Energy Associates, Ltd./Technology for Energy Corporation, as Prepared for the U.S. DOE, June 1, 1981
- 1.B-19 "Analysis of Aerospace and Aviation Safety Concepts and Their Potential Application to Nuclear Safety - Final Draft", International Energy Associates, Ltd, for Combustion Engineering, Inc., October 21, 1980
- 2.A-1 U.S. NRC, NUREG-75/087, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", Revision 2, U.S. Government Printing Office, 1979
- 2.A-2 Sandia National Laboratories, "Second Interim Report - Value Impact Assessment of Regulatory Review Units", SNL, July 13, 1980
- 2.A-3 "The Assessment of the Standard Review Plan Using the Levels of Protection Concept - Final Draft", Technology for Energy Corporation, Report Number R-81-038, under Subcontract to Combustion Engineering, Inc., September 25, 1981
- 2.B-1 Subcommittee on Nuclear Regulation, "Nuclear Accident and Recovery at Three Mile Island", U.S. Senate, Serial 96-14, June 1980

- 2.C-1 "An Integrated Approach to the Economic Risk Analysis at Nuclear Power Plant Operation", Combustion Engineering, Inc., as Prepared for U. S. DOE, Final Report to be Issued
- 2.D-1 "Operational Experience Evaluation Using Safety Function Fault Trees", Combustion Engineering, Inc., under Contract to Electric Power Research Institute, Project Number R102-2, Final Report to be Issued

APPENDIX A

NUCLEAR POWER PLANT FUNCTIONAL CLASSIFICATION

TABLE OF CONTENTS

1.0	INTRODUCTION	A-1
2.0	FUNCTIONAL CLASSIFICATION	A-1
	REFERENCES	A-5

LIST OF FIGURES

FIGURE A1	GENERAL FUNCTIONAL CLASSIFICATION
FIGURE A2	FUNCTIONAL CLASSIFICATION

APPENDIX A

NUCLEAR POWER PLANT FUNCTIONAL CLASSIFICATION

1.0 Introduction

Nuclear power plants are designed to accommodate a broad spectrum of operating conditions. It is possible to perform a systematic, detailed examination of nuclear power plants under various operating conditions on a functional basis. In essence, the plant conditions associated with the Integrated Approach to Economical, Reliable, Safe Nuclear Power can be identified and the functions that must be maintained under these conditions defined. The plant systems, components and operator actions that maintain these functions are then determined and categorized accordingly. This appendix describes a proposed method that, with some additional development, could produce a complete Functional Classification of nuclear plant systems and components and the human actions associated with their use. The Integrated Approach provides a detailed framework into which the functions, success paths, systems, components and human actions can be placed. In this way, a complete picture is produced of how each Goal, and its objective, is achieved, thus achieving the ultimate objective of economical, reliable and safe nuclear power production.

2.0 Functional Classification: Details of Decomposition

The proposed method for constructing the complete Functional Classification of nuclear plant systems, components and associated human actions is presented in general terms in Figure A1. The top elevation of the diagram is the ultimate goal of "economical, reliable and safe nuclear power production". The next layer of detail in the decomposition presents the four Goals of the Integrated Approach. Each Goal has its own particular objective which, when taken together, address the needs of the ultimate objective at the first elevation. As the decomposition is carried to the next stage, the general plant conditions for each Goal are defined. Functions and subfunctions can then be assigned to each of the plant conditions for the Goals. Finally, the success paths that achieve the functions are identified for each of the functions and subfunctions. When the classification is taken to the most detailed decomposition, every component and each operator action is placed into the framework. This then provides a complete description of how each function can be maintained and how the functions achieve the objectives of the Goals.

Figure A2, sheets 1 through 18, depict the work performed to date. It should be noted that this study did not attempt to construct a complete set of success paths for all functions. Rather, the Functional Classification was developed in sufficient detail to illustrate its method of construction and to serve as a starting point for further refinement and development in areas that will be discussed below.

As shown on sheet 1, the ultimate objective of nuclear power plant operation is defined to be economical, reliable, safe nuclear power production. The four Goals are then noted, along with their specific objectives. The plant conditions encompassed by each Goal are shown next. The plant conditions under Normal Operation are those defined in the Standard Technical Specifications. Under Core and Plant Protection, "core damage controlled" refers to conditions in which applicable core damage criteria have been met. "Plant damage controlled" refers to conditions in which the minimum required functional capability of equipment in the success paths for power production is maintained. This definition was employed because this study considered plant protection only with respect to protecting the functions required for electrical energy production. "Radiation exposure controlled" under Containment Integrity refers to post-event conditions in which applicable radiological exposure criteria have been met. "Conditions meet response plan activation criteria" under Emergency Preparedness is self-explanatory.

The breakdown from plant conditions through success paths is shown on sheets 2 through 18. This decomposition has been carried out to the detail of subfunctions for each plant condition. To provide examples of how the complete Functional Classification would be constructed, the breakdown was carried out to the success path level for selected functions and subfunctions in each Goal. These examples are shown on the following sheets:

Sheets 8 through 10 - Normal Operation
Sheets 11 through 15 - Core and Plant Protection
Sheets 16 through 17 - Containment Integrity
Sheet 18 - Emergency Preparedness

A complete Functional Classification would show all success paths in each success path class (normal, principal, alternate and extraordinary) for each function and subfunction. Sheet 12 provides an example of the Functional Classification developed to the extent of showing the principal success path and one alternate success path for a subfunction.

The listing of components in each success path was done using only generic terms such as "pumps, tanks, valves, etc.". Construction of the complete Functional Classification would clearly require specific component identification. Similarly, required operator actions are treated modularly by showing "human action" entering into the success paths. Human action would encompass choosing the success path to be used and performing those tasks needed to line up and operate the components of the success path. These actions would also have to be specifically identified in a complete Functional Classification.

The set of functions and subfunctions defined for each plant condition is clearly not unique. Other functions could be defined as a

consequence of differing individual judgement. Optimizing the set of functions and subfunctions is a possible area of refinement on the initial work reported here.

As noted previously, this study considered plant protection only with respect to protecting the functions associated with power production. A more complete treatment of plant protection could constitute an additional area of further development.

Section 3 discussed applications of this Functional Classification to operator training and preparation of procedures. With respect to such operator-oriented uses, it is interesting to note that the Functional Classification is consistent with concepts developed by human factors specialists. References A-1 and A-2 address human factors considerations and describe the concepts of behavior types, field of attention, and level of abstraction.

The behavior types discussed are skill-based behavior, rule-based behavior and knowledge-based behavior. In brief, skill-based behavior consists essentially of automatic responses to recognized conditions. Rule-based behavior involves the use of prescribed procedures invoked in response to a recognized condition. Knowledge-based behavior occurs "...when skills and rules are neither available nor adequate..." and involves "...causal and functional reasoning based on a knowledge of the functional properties of the system including the potential means for, and effects of, making corrective changes in order to counter an undesirable state or trend..." (Reference A-1). The Functional Classification described here is clearly an asset in assisting the operator in dealing with unforeseen circumstances that require knowledge-based behavior responses.

The concepts of field of attention and level of abstraction are related. As the level of abstraction increases, the operator's field of attention broadens. As the level of abstraction decreases, the operator's field of attention narrows. Reference A-1 provides an illustration of this relationship:

"For example, in the initial phases of a diagnostic, the coverage would be wide and the detail probably restricted to the most critical primary parameters. In the final portion, where a corrective action is identified, the coverage would be limited, and detail concentrated on the location and operation of the selected control."

Reference A-1 defines six levels of abstraction. Consideration of objectives and values comprises the highest abstraction level and deals with the purposes and objectives of systems or functions. The levels proceed down through various forms of functional reasoning to the level of physical function, the second lowest level of abstraction. Physical function involves considering how parts and components work,

how they are connected, and how they interact. The lowest level of abstraction is physical form which relates to the appearance and location of parts and components.

The structure of the Functional Classification parallels these levels of abstraction. It begins with an ultimate objective, proceeds through the specific objectives of the Goals, to functions and subfunctions and, finally, to the systems, components, and human actions which support the functions and subfunctions. Its detail increases as the level of abstraction decreases. The structure of the Functional Classification appears to present information in a manner consistent with human thought and evaluation processes.

REFERENCES

- A-1 Goodstein, L. P./Rasmussen, J., "The Use of Man-Machine System Design Criteria in Computerized Control Rooms", Riso National Laboratory, DK-4000 Roskilde, Denmark
- A-2 Rasmussen, J., "On the Structure of Knowledge - A Morphology of Mental Models in a Man-Machine System Context", Riso-M-2192, Riso National Laboratory, DK-4000 Roskilde, Denmark, November 1979

GENERAL FUNCTIONAL CLASSIFICATION METHOD

Figure A.1

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 1)

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 2)

NORMAL OPERATION

PLANT CONDITION: REFUELING

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 3)

NORMAL OPERATION

PLANT CONDITION: REFUELING

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 4)

NORMAL OPERATION

PLANT CONDITION: COLD SHUTDOWN

PLANT CONDITION

FUNCTION

SUBFUNCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 5)

NORMAL OPERATION

PLANT CONDITION: HOT SHUTDOWN

PLANT CONDITION

FUNCTION

SUBFUNCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 6)

NORMAL OPERATION

PLANT CONDITION: HOT STANDBY

PLANT CONDITION

FUNCTION

SUBFUNCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 7)

NORMAL OPERATION

PLANT CONDITION: START-UP

PLANT CONDITION

FUNCTION

SUBFUNCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 8)

NORMAL OPERATION

PLANT CONDITION: POWER PRODUCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 9)

NORMAL OPERATION

PLANT CONDITION: POWER PRODUCTION

FUNCTION

A-18

SUBFUNCTION

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 10)

NORMAL OPERATION
PLANT CONDITION: POWER PRODUCTION

SHEET 9

HEAT
REMOVAL
CONTROL

CORE HEAT
REMOVAL

RCS
INVENTORY
CONTROL

CHEMICAL
AND VOLUME
CONTROL
SYSTEM

REACTOR
COOLANT
SYSTEM

RCS
PRESSURE
CONTROL

REACTOR
COOLANT
PRESSURIZING
SYSTEM

REACTOR
COOLANT
SYSTEM

HEAT TRANSFER
TO SECONDARY

REACTOR
VESSEL
PIPING
STEAM
GENERATOR
TUBES
REACTOR
COOLANT
PUMPS
INSTRUMENTATION
HUMAN
ACTION

MAIN STEAM
SYSTEM

STEAM
GENERATORS
PIPING
VALVES
INSTRUMENTATION

CONDENSATE
& FEEDWATER
SYSTEM

PUMPS
TANKS
CONDENSERS
HEATERS
POLISHERS
VALVES
INSTRUMENTATION

HEAT TRANSFER
TO ULTIMATE
HEAT SINK

MAIN
CIRCULATING
WATER SYSTEM

PUMPS
VALVES
PIPING
CONDENSER
TUBES
COOLING
TOWERS,
RIVER, OCEAN,
ETC
INSTRUMENTATION

HUMAN
ACTION

FUNCTION

SUBFUNCTION

TYPICAL
SUCCESS
PATH

TYPICAL
COMPONENTS

A-19

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 11)

CORE AND PLANT PROTECTION

PLANT CONDITION: CORE DAMAGE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 12)

CORE AND PLANT PROTECTION

PLANT CONDITION: CORE DAMAGE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 13)

CORE AND PLANT PROTECTION

PLANT CONDITION: PLANT DAMAGE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 14)

CORE AND PLANT PROTECTION

PLANT CONDITION: PLANT DAMAGE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 15)

CORE AND PLANT PROTECTION

PLANT CONDITION: PLANT DAMAGE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 16)

CONTAINMENT

PLANT CONDITION: RADIATION RELEASE CONTROLLED

FUNCTION

SUBFUNCTIONS

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 17)

CONTAINMENT

PLANT CONDITION: RADIATION RELEASE CONTROLLED

FUNCTIONAL CLASSIFICATION

Figure A.2 (Sheet 18)

EMERGENCY PREPAREDNESS

A-27

APPENDIX B

NUCLEAR POWER PLANT INSTITUTIONAL CLASSIFICATION

TABLE OF CONTENTS

1.0	INTRODUCTION	B-1
2.0	INSTITUTIONAL CLASSIFICATION	B-1

LIST OF FIGURES

FIGURE B1	INSTITUTIONAL CLASSIFICATION
-----------	------------------------------

APPENDIX B

NUCLEAR POWER PLANT INSTITUTIONAL CLASSIFICATION

1.0 Introduction

Achieving the ultimate objective of economical, reliable, safe production of nuclear power is the result of a complex process involving many activities performed by numerous organizations. This appendix describes the use of the Integrated Approach to Economical, Reliable, Safe Nuclear Power to generate an Institutional Classification that assists in systematically examining in detail the many aspects of this complex process.

2.0 Institutional Classification

As explained in Section 1.A.1, the process by which the ultimate objective of economical, reliable and safe production of nuclear power is attained can be examined by application of the Integrated Approach.

Each Goal is associated with a specific objective which is achieved by maintenance of a group of functions. The functions, plant systems, and components through which they are maintained come into being and are supported by the general industry activities of Design, Construction, Operation, and Maintenance. Specific activities associated with each general activity can be identified. Each specific activity possesses characteristics whose presence is indicative of how well the activity is being conducted.

The Integrated Approach Institutional Classification is shown in Figure B1. Sheet 1 shows its overall structure. The ultimate objective of economical, reliable and safe production of nuclear power is shown at the left. The Goals are shown supporting the ultimate objective. The four general industry activities of Design, Construction, Operation, and Maintenance, encompassed by each Goal, are shown next. The specific activities associated with each general activity are then listed. As noted above, each specific activity possesses certain characteristics. These characteristics are shown on sheets 2 through 6. The Institutional activities and their associated characteristics produce the detailed specifications and criteria to which nuclear power plants are designed, constructed, operated, and maintained.

Under the heading "CHARACTERISTICS" on sheets 2 through 6, the specific characteristics may be read in a sentence in the following manner: the specific activity shown at left "is" or "is characterized by" the following characteristics. For example, on sheet 2, the first item may be read as follows: the specific activity of "developing criteria" is based on defined objectives.

The compilation of activities and characteristics shown on Figure B1 is primarily intended to be an illustration of how the Integrated Approach would be used. The development of a comprehensive set of specific activities and characteristics would involve an industry-wide effort with the participation of experts from many different fields.

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 1 of 6)

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 2 of 6)

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 3 of 6)

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 4 of 6)

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 5 of 6)

B-10

Office of Nuclear Power Systems, (9)
NE-540, US Department of Energy,
Mail Stop B-107
Washington, DC 20545
Attn: J. H. Carlson (5)
D. Giessing, Light Water
Reactor Technology Team
J. D. Griffith, Acting
Director
A. C. Millunzi, Director,
Safety Research &
Development
J. Yevick, Safety Research
& Development

G. Brockett
Intermountain Technologies, Inc.
P. O. Box 1604
Idaho Falls, ID 83401

Paul Boehnert (5)
ACRS
US Nuclear Regulatory Commission
H. Street Offices
Mail Stop H-1016
Washington, DC 20555

T. E. Murley, Director
Regional Operations & Generic
Requirements
US Nuclear Regulatory Commission
Mail Stop MNBB-6113
Washington, DC 20555

George Knighton, Branch Chief
Research & Standards Coordination
Branch
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Washington, DC 20555

Steve Hanauer
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Washington, DC 20555

R. Minogue, Director
Office of Nuclear Regulatory Research
Mail Stop 1130SS
US Nuclear Regulatory Commission
Washington, DC 20555

Ashok Thadani, Chief
Reliability and Risk Assessment
Branch
Division of Safety Technology
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Mail Stop 216
Washington, DC 20555

Gary Burdick
Division of Risk Analysis
Office of Nuclear Regulatory
Research
US Nuclear Regulatory Commission
Mail Stop 1130SS
Washington, DC 20555

Dr. Robert C. Axtmann
School of Engineering and
Applied Science
Princeton University
Princeton, NJ 08544

Mr. Myer Bender
9524 Twelve Trees Lane
Knoxville, TN 37922

Dr. Max W. Carbon, Chairman
Nuclear Engineering Department
Engineering Research Building
University of Wisconsin
Madison, WI 53706

Mr. Jesse C. Ebersole
103 Newell Lane
Oak Ridge, TN 37830

Mr. Harold Etherington
84 Lighthouse Drive
Jupiter, FL 33458

Dr. William Kerr
Department of Nuclear Engineering
Phoenix Laboratory - North Campus
University of Michigan
Ann Arbor, MI 48109

Dr. Harold W. Lewis
Department of Physics - Rm. 6114
University of California
Santa Barbara, CA 93106

Dr. Carson Mark
Los Alamos Scientific Laboratory
Theoretical Division
P. O. Box 1663 - MS 210
Los Alamos, NM 87545

Mr. William M. Mathis
455 Mainmast Court
Richland, WA 99352

Dr. Dade W. Moeller, Head
Environmental Health Sciences Dept.
School of Public Health
Harvard University
665 Huntington Avenue
Boston, MA 02115

Dr. David Okrent
Energy and Kinetics Department
5532 Boelter Hall
School of Engineering & Applied
Science
University of California
Los Angeles, CA 90024

Dr. Milton S. Plesset
California Institute of Technology
104-44
Pasadena, CA 91109

Mr. Jeremiah J. Ray
819 Lantern Lane
Langhorne, PA 19047

Dr. Paul G. Shewmon
2477 Lytham Road
Columbus, OH 43220

Dr. Chester P. Siess
805 Hamilton Drive
Champaign, IL 61820

Mr. David A. Ward
E. I. du Pont de Nemours & Company
Savannah River Laboratory
Building 773-A, A-219
Aiken, SC 29808

Brookhaven National Laboratory (3)
Upton, NY 11973
Attn: J. L. Boccio
H. Kouts
W. Kato

US Department of Energy
Idaho Operations Office
550 Second Street
Idaho Falls, ID 83401
Attn: R. Tiller

Idaho National Engineering (4)
Laboratory
EG&G Idaho, Inc.
P. O. Box 1625
Idaho Falls, ID 83415
Attn: H. Zeille
F. Balkovetz
R. French
L. Leach

Los Alamos Scientific Laboratory (4)
P. O. Box 1663
Los Alamos, NM 87545
Attn: J. Boudreau
R. Waller
B. Washburn
R. Pryor

Oak Ridge National Laboratory (6)
P. O. Box X
Oak Ridge, TN 37830
Attn: D. Trauger
R. K. Kibbe
R. Kisner
J. L. Anderson
L. Oakes
W. Harms

Oak Ridge National Laboratory (2)
USNRD
P. O. Box TC
Oak Ridge, TN 37830
Attn: J. Pidkowicz
T. Lindemer

Tennessee Valley Authority
520 Edney Bldg.
Chattanooga, TN 37401
Attn: C. R. Farreau

Tennessee Valley Authority
400 Commerce Avenue
Knoxville, TN 37902
Attn: J. Raulston

Westinghouse Electric Corp. (3)
P. O. Box 355
Pittsburgh, PA 15230
Attn: R. Slember
J. Cohen
P. Rahe

Westinghouse Electric Corp.
Power Systems
P. O. Box 355
Pittsburgh, PA 15230
Attn: D. Richardson

Westinghouse Electric Corp.
P. O. Box 598
Pittsburgh, PA 15239
Attn: J. H. Murphy

Boston Edison Company
RFD #1, Rocky Hill Road
Plymouth, MA 02360
Attn: W. Armstrong

Commonwealth Edison (2)
P. O. Box 767, Rm 35FN West
Chicago, IL 60690
Attn: G. Klopp
C. Reed

Duke Power Company (6)
P. O. Box 33189
Charlotte, NC 28242
Attn: W. Coley
W. Rasin
R. Summit
B. Logan
J. Gaertner
J. Elliott

Georgia Power Company (5)
230 Peachtree Street
Atlanta, GA 30302
Attn: J. Beckham
W. Burns
P. Springer
S. Hart
G. Bockhold

Institute of Nuclear Power (8)
Operations
1820 Water Place
Atlanta, GA 30339
Attn: P. Dietz
D. Fadden
T. Hinson
E. P. Wilkinson
E. Zebroski
K. Straam
A. Weyrauch
E. L. Thomas

Northeast Utilities Services
P. O. Box 270
Hartford, CT 06002
Attn: R. Wells

Philadelphia Electric Co.
2301 Market Street
Philadelphia, PA 19001
Attn: V. Boyer

Georgia Institute of Technology (4)
Engineering Experimental Station
Computer Science & Technology
Laboratory
Atlanta, GA
Attn: J. A. Mahaffey
D. Grace
J. Scovill
F. Cain

Massachusetts Institute of (3)
Technology
77 Massachusetts Avenue
Cambridge, MA 02139
Attn: N. C. Rasmussen
N. E. Todreas
W. D. Hinkle

University of California (2)
Chemical, Nuclear, and
Thermal Engineering
5532 Boelter Hall
Los Angeles, CA 90024
Attn: W. Kastenberg
D. Okrent

Combustion Engineering Inc. (9)
Nuclear Power Systems Division
1000 Prospect Hill Road
Windsor, CT 06095
Attn: F. Bevilacqua
W. R. Corcoran
J. D. Crawford
E. Hewitt
T. Kettles
M. F. Reisinger
G. Schukei
C. H. Meijer
J. Braun

Energy Incorporated
515 West Harrison
Suite 220
Kent, WA 98031
Attn: Lawrence L. Conradi

Electric Power Research Institute (7)
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, CA 94303
Attn: I. Wall
A. Long
W. Lowenstein
R. Duffy
D. Worledge
J. Taylor
D. Rossin

General Electric Co. (4)
Nuclear Engineering Division
175 Curtner Avenue
San Jose, CA 95125
Attn: G. Sherwood
M. Lyons
H. Stone
R. Mullee

International Energy Associates (2)
2600 Virginia Avenue NW
Washington, DC 20037
Attn: M. Elliot
L. Kenworthy

Pickard, Lowe & Garrick (3)
17840 Skypary Blvd.
Irvine, CA 92714
Attn: J. Garrett
K. Fleming
A. Kelley, Jr.

Sargent & Lundy (2)
55 East Monroe
Chicago, IL 60603
Attn: N. Weber
R. Hammersley

Science Applications Inc.
5 Palo Alto Square
Palo Alto, CA 94304
Attn: R. L. Ritzman

Stone & Webster Engineering Corp.
245 Summer Street
Boston, MA 02107
Attn: M. Rosen

Stone & Webster Engineering Corp. (2)
1875 Eye Street NW
Suite 550
Washington, DC 20006
Attn: A. Giambusso
C. F. Grochmal

Technology for Energy Corp. (3)
10770 Dutchtown Road
Knoxville, TN 37922
Attn: S. Asselin
T. Buhl
T. Tyler

Nuclear and Geosciences Division
US Department of Energy
Albuquerque Operations Office
Albuquerque, NM 87185
Attn: D. L. Krenz, Director
R. L. Clark

J. Harbour
Atomic Safety & Licensing
Board Panel
US Nuclear Regulatory Commission
Mail Stop EW-450
Washington, DC 20555

9400 A. W. Snyder
9410 D. J. McCloskey
9420 J. V. Walker
9440 D. A. Dahlgren
9441 M. Berman
9442 W. A. VonRieseemann
9443 A. R. DuCharme
9443 P. Shea (20)
9443 N. H. Clark
9443 P. O. Strom
9443 P. Yarrington (50)
9444 S. L. Thompson
9445 L. O. Crop
9450 J. A. Reuscher
3141 L. J. Erickson (5)
3151 W. L. Garner

INSTITUTIONAL CLASSIFICATION

Figure B.1 (Sheet 6 of 6)

B-11/B-12