NUREG/CR-3520
BNL-NUREG-51718
Vol. II

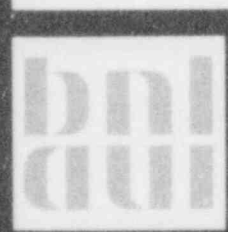
LONG-TERM RESEARCH PLAN FOR HUMAN FACTORS AFFECTING SAFEGUARDS AT NUCLEAR POWER PLANTS

VOLUME II: DEVELOPMENT OF DETAILED ANALYSES

John N. O'Brien and Anthony Fainberg

Date Published — April 1984

ENGINEERING ANALYSIS AND HUMAN FACTORS GROUP
DEPARTMENT OF NUCLEAR ENERGY, BROOKHAVEN NATIONAL LABORATORY
UPTON, LONG ISLAND, NEW YORK 11973



Prepared for the
United States Nuclear Regulatory Commission
Washington, D.C. 20555

NUREG/CR-3520
BNL-NUREG-51718
VOL. II
AN, RS, IS

LONG-TERM RESEARCH PLAN FOR HUMAN FACTORS AFFECTING SAFEGUARDS AT NUCLEAR POWER PLANTS

VOLUME II: DEVELOPMENT OF DETAILED ANALYSES

John N. O'Brien, Anthony Fainberg, Allan Mazur,
Sidney Arenson, Jeff Katzer, and Barbara Settel

Manuscript Completed — January 1984
Manuscript Published — April 1984

ENGINEERING ANALYSIS AND HUMAN FACTORS GROUP
DEPARTMENT OF NUCLEAR ENERGY
BROOKHAVEN NATIONAL LABORATORY
ASSOCIATED UNIVERSITIES, INC.
UPTON, LONG ISLAND, NEW YORK 11973

Prepared for
U.S. NUCLEAR REGULATORY COMMISSION
HUMAN FACTORS AND SAFEGUARDS BRANCH
OFFICE OF NUCLEAR REGULATORY RESEARCH
CONTRACT NO. DE-AC02-76CH00016
FIN NO. A-3260

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
and
National Technical Information Service
Springfield, Virginia 22161

ABSTRACT

This report presents a long-term research plan for addressing human factors which can adversely affect safeguards at nuclear power plants. It was developed in order to prioritize and propose research for NRC in regulating power plant safeguards.

In 1982, the Human Factors Society developed, under NRC contract, a long-term research plan for studying human factors in power plant operations. That plan, published in NUREG/CR-2833, specifically excluded from consideration fuel cycle, waste disposal, health physics, and plant security activities. The purpose of this report is to address human factors in plant security. This research effort did not address human factors associated NRC activities, such as the use of mandatory reporting systems, or areas of research outside of plant operation, such as probabilistic risk assessment (PRA). Instead, it focused on the performance of security activities by safeguards personnel at operating power plants. For the purposes of this research, the terms "safeguards" and "security" can be considered synonymous.

The first task was to identify and rank human factors affecting the quality of nuclear power plant safeguards in terms of their importance. The opinions of over 85 experts were solicited and 28 responses were received. These responses were rigorously analyzed to ascertain what human factors could be considered important to power plant safeguards. In addition, the Safeguards Summary Event List (NUREG-0525) was systematically analyzed for human factors influences. Also, relevant government and industry literature was reviewed. These data sources were then aggregated and an overall importance ranking of human factors issues was developed. This part of the research effort is fully documented and described in Chapter 2 of Volume II.

The second part of this effort involved determining the feasibility of conducting research in the areas found to be important to power plant safeguards. A determination of research feasibility was based on the practicality, usefulness, and acceptability of conducting research and using the results in a regulatory context. This part of the effort is fully documented in Chapter 3 of Volume II.

Research efforts addressing human factors in safeguards were then developed and prioritized according to the importance of human factors areas derived in the first part of the study and the feasibility of research determined in the second part. Research was also grouped to take advantage of common research approaches and data sources where appropriate. Chapter 4 of Volume II details the development of methodological groupings for optimizing resource use.

Four main program elements emerged from the analysis, namely (1) Training and Performance Evaluation, (2) Organizational Factors, (3) Man-Machine Interface, and (4) Trustworthiness and Reliability. Within each program element,

projects are proposed with results and information flowing between program elements where useful. An overall research plan was developed for a 4-year period and it would lead ultimately to regulatory activities including rule-making, regulatory guides, and technical bases for regulatory action. The entire plan is summarized in Volume I of this report.

TABLE OF CONTENTS

Chapter 1

1. INTRODUCTION

Brookhaven National Laboratory was contracted by the Nuclear Regulatory Commission to develop a long-term research plan for studying human factors associated with nuclear power plant safeguards. That plan is presented along with a summary of research performed in Volume I of this report. In Volume II (this volume), all relevant analyses leading to the research plan are fully described.

2. ORGANIZATION OF THIS DOCUMENT

Three different phases of research are presented in this volume. Chapter 2 documents the research which led to the identification and ranking of human factors safeguards issues in terms of their importance to site security. Chapter 3 asesses the feasibility of performing research on the issues identified in Chapter 2. Chapter 4 is an independent review of the open literature aimed at formulating optimal research design for studying human factors issues. These chapters are summarized in Sections 2 and 3 of Volume I.

Summary of Chapter 2

The purpose of this chapter is to identify and rank human factors which affect the quality of safeguards at nuclear power plants. The resulting ranking of human factors is based on a consensus on what human factors present "problems" that NRC should consider in its future research plans.

The method used to arrive at rankings is a consensus method based on expert opinion, analysis of reported safeguards events, and review of relevant literature. In order to access these data sources, an initial list of human factors issues relevant to nuclear power plant safeguards was developed by consulting Brookhaven National Laboratory (BNL) staff, NRC personnel, and contractor organizations. This list contains all human factors which are generally held to affect the performance of safeguards personnel. The term "problem" was then defined as a state of affairs for which there is a consensus that some improvement in the quality of safeguards can be achieved, but appropriate means and/or justification for achieving a solution is lacking. The list of human factors issues was then annotated to provide background on each item. This list was then sent to eighty-five professionals in the nuclear energy safeguards and/or human factors fields. A cover letter explained the project and asked specific inquiries concerning the list. Twenty-three responses were received (32% response rate). Responses were analyzed by topic and empirically and a ranking of human factors issues as problems was developed.

Using the same initial list of human factors affecting nuclear power plant safeguards the safeguard Summary Event List was analyzed, event by event, for the influence of human factors in safeguards responses. Human factors were ranked in terms of their influence on responses. Relevant literature was identified and reviewed. Recommendations for further research or regulatory actions were analyzed in terms of the human factors list and ranked.

A final set of rankings is presented which are held to be a consensus on what human factors pose problems in nuclear power plant safeguards.

CHAPTER 2

IDENTIFICATION AND RANKING OF HUMAN FACTORS AFFECTING SAFEGUARDS AT NUCLEAR POWER PLANTS

John N. O'Brien and Anthony Fainberg

Table of Contents

Chapter 2

1.0 Introduction

The term "human factors" has been used in many contexts concerning nuclear reactor safety, most significantly since the accident at Three Mile Island. However, a common definition of what constitutes human factors is not evident in the accumulated literature. Human factors are defined here as those identifiable factors which are held to affect the performance of personnel in executing their job related responsibilities. These include engineering, personnel, and administrative factors at play in a nuclear power plant. The objective of this first part of the overall human factors in nuclear power plant safeguards project is to systematically enumerate the human factors that should be considered in the protection of nuclear power plants from sabotage and to determine their relative importance.

1.1 Background

The risks from operating nuclear power plants have been examined by NRC by using the techniques of Probabilistic Risk Assessment (PRA). This research has shown that a major factor dictating the risk to society from nuclear power plant operation is how well the personnel taking part in the overall plant organization perform their job tasks.[1] If performance is not optimal, then plant safety may be suboptimal and risk, consequently, higher. Therefore, a large effort has been made to determine how risk is affected by the performance of most personnel in nuclear power plants[2] with the goal of identifying dominant factors and correcting deficiencies. PRA research has shown that human error may often be the dominant factor in the potential for a major reactor accident occurring or being avoided.[3]

Safeguards and security at nuclear power plants have long been viewed as primarily concerned with reducing risk due to operation of these facilities by reducing the probability of radiological sabotage. However, the study of PRA has been aimed almost exclusively at determining human contributions to risk by operational personnel, for instance, human factors concerning the performance of operators in the control room and maintenance personnel in the plant.[4] Human factors affecting risk associated with the behavior of safeguards and security personnel have not been examined in any comparable fashion.

In order to determine which human factors affect risk from safeguards events and to develop a plan for dealing with those risks, a systematic approach is used. An examination of appropriate literature and consultation with industry and government personnel, as well as of event and compliance reports, were used to develop data and a list of those human factors in safeguards that affect risk. Ultimately the contribution of safeguards personnel to overall risk may be assessed, however, that assessment is beyond the scope of this present effort.

The purpose of this chapter is to develop a list of human factors in safeguards and security that may impact risk. In the context of this study, risk is regarded as a threat to health and welfare of the public so that an off-site release of radioactivity is viewed as the consequence of importance (i.e., radiological sabotage) rather than industrial safety. Accordingly, weight is given to those human factors which could most predictably affect the probability of core damage. Human factors affecting overall risk stemming from

transportation of nuclear materials and abuse of fuel cycle facilities are not directly covered in this project because they are outside the statement of work provided by NRC. In addition, fuel cycle facilities and transportation activities do not directly affect risk from reactor operation. However, it is likely that many of the human factors discussed in this report will apply to safeguards for both transportation and fuel cycle facilities.

1.2 Method

In order to identify human factors issues in nuclear power plant safeguards logically, all human factors held to affect the performance of safeguards personnel should be considered. A technique must then be employed to systematically identify those human factors issues which can be considered "problems." While safeguards systems have worked well for many years at many nuclear reactor sites, it is not clear that nuclear power plant safeguards, as they exist today, are optimal given current resources. That is to say, it is unrealistic to accept the lack of significant events as the index of safeguards quality, because of the acknowledged low probability and high consequences of such an event should it occur. Therefore, other indexes must be developed to assess safeguards quality. A "problem" is defined here as a state of affairs for which there is a consensus that some improvement in the quality of safeguards can be achieved, but the appropriate means and/or justification for achieving a solution is lacking. Human factors issues which do not pose problems, as defined here, will not be considered as topics for potential study in the final long-term research plan to be produced by this project.

The process for achieving a consensus on what actually constitutes a set of problems must be sufficiently broad based to take into account several relevant, but diverse data sources. For instance, data referring to actual safeguards events reported by licensees must be considered since these are a partial accounting of the nature of events actually faced by nuclear power plant safeguards personnel. However, the biases attendant upon a required reporting system must be taken into account. The operational safety literature shows, that many Licensee Event Reports (LERs) were classified as equipment failure when, in fact, they were human errors.[5] LERs are those reports required by NRC which pertain to operational safety events that may adversely affect plant safety. Safeguards Event Reports are required for safeguards-related events and can be analyzed similarly. The opinions of professionals can also provide valuable insights into the nature of human factors which adversely affect the performance of safeguards personnel. However, expert opinion alone may not be sufficiently comprehensive or capable of being subject to rigorous analysis unless a scientifically designed survey is used. The vast literature on human factors in personnel performance can also be brought to bear on this consensus process through examining the findings and recommended research in relevant studies. Since recommendations are generally formulated at the completion of a study, they arise, for the most part, from state-of-the-art thinking. Using all of these data sources, a system for setting priorities on the importance of the human factors which are identified as problems can also be developed.

To begin with, an initial attempt to enumerate all human factors that may affect human performance in nuclear power plant safeguards was undertaken. The Office of Nuclear Materials Safety and Safeguards (NMSS) at NRC informally polled their staff and supplied the results for consideration. This list was

statedly not comprehensive and was to be used only as a starting point. In addition, staff suggestions were solicited from more than twenty Brookhaven National Laboratory (BNL) scientists (Engineering Analysis and Human Factors Group and Technical Support Organization for Nuclear Safeguards) and all the results were combined to arrive at an overall initial list. This was then divided into the categories of 1) material control and accounting and 2) physical security.

At fuel cycle facilities strict material control and accounting measures are required to assure that sensitive nuclear materials which are usable in an explosive device or capable of being dispersed as a radiological toxin are kept secure from theft or diversion. At a nuclear power plant no similar threat exists. Studies have shown that new fuel is not a radiological health or safety threat to the public and that spent fuel is not an attractive target for theft, and therefore not very sensitive. Analysis has shown that sabotage aimed at spent fuel is similarly difficult and an unlikely threat to the public health and safety.* At nuclear power plants accounting for spent fuel elements is done by recording identification numbers and location of all elements in storage. Because of the relatively low sensitivity of spent fuel and relatively minimal level of accountancy at nuclear power plants an investigation of human factors affecting material control and accounting should properly be done in the context of fuel cycle facilities. As a result, this report is limited in scope to nuclear power plants so only human factors affecting physical security are considered. The list of material control and accounting human factors are in Appendix A. The resulting list of human factors affecting nuclear power plant safeguards (Table 1) was then considered to be reasonably comprehensive.

Two major considerations dictated the form of the solicitation for comments from safeguards and human factors professionals. First, a scientifically designed survey was considered, but because of administrative requirements and time constraints, the use of a formal scientific survey was ruled out. Second, because the general intent of the required research method is to expand the range of expertise in this analysis to include both professionals from the field of human factors in operational safety and safeguards professionals, a very broad-based solicitation instrument had to be used. Accordingly, it was determined that a discussion paper along with general questions on the discussion paper itself sent to various experts, would be an appropriate, albeit not rigorous, way to gather expert opinion. The results of the expert solicitation, analysis of reported events and an analysis of relevant literature can be combined for an overall ranking of human factors issues in safeguards.

The discussion paper (contained in Appendix B) which accompanied each request for comments was in two parts. First, a general discussion of what physical security at nuclear power plants actually consists of was given. This amounted to a description of the requirements in 10 CFR 73.55 (the section of the Federal Regulations which requires specific safeguards measures for nuclear power plants) along with a discussion of relevant rulemaking actions (from the Federal Register) and SECY (internal NRC) documents. This was provided in the solicitation as a basis for 1) apprising human factors specialists of the types

*"Final Environmental Impact Statement: U.S. Spent Fuel Policy," Vol. 2, U.S. DOE, DOE/EIS-0015, May 1980, pp. 4.112-3; E.E. Voiland et al., "Sabotage Analysis for Spent Fuel at Morris, General Electric Co., NEDM-20682, 1974, p. 7.

of tasks and human performance expected of safeguards personnel, 2) disagreement or consensus among safeguards professionals as to the actual requirements of the regulations, and 3) a contemporary review of existing regulatory actions and issues. The second part of the discussion paper was aimed at summarizing the salient aspects of each human factor. Equal treatment of each factor was attempted in order to minimize bias. To facilitate the use of this list, human factors were grouped under four general headings presented in Table 2. A paragraph on each item described the human factor and its potential effects on security. The reader is referred to the discussion paper in Appendix B for specific descriptions of human factors in nuclear power plant safeguards.

The resulting list which became the basis for the common analysis of the data sources, was developed primarily from expert opinion, reported events, and reviewed literature.

Table 1

Initial List of Human Factors in Nuclear Power Plant Safeguards

Two-Man Rule

Communications

Format and Wording of Contingency Plans

Task Variety/Rotation

Vigilance

Adequate Manpower and Staffing

Self Preservation Manifested as Reluctance

Personnel Screening

Intructional Programs

Safety/Safeguards Interactions

Behavioral Observation

Fitness for Duty

Corporate Attitude

Equipment Induced Error

Maintenance of Equipment and Alarms

Proper Levels of Automation

Reporting Requirements and Analysis

Table 2

Human Factors in Nuclear Power Plant Safeguards Grouping for Discussion Paper and Subsequent Analysis

A. Insider Threat

- A.1 Two-Man Rule
- A.2 Behavioral Observation Programs
- A.3 Trustworthiness
- A.4 Fitness for Duty

B. Organization

- B.1 Boredom Reduction - Vigilance
- B.2 Communication
- B.3 Rotation/Shiftwork/Manpower
- B.4 Corporate Attitude
- B.5 Instruction

C. Response Capabilities

- C.1 Format and Wording of Contingency Plans
- C.2 Self-Preservation and the Use of Deadly Force
- C.3 Coordination Between Operation and Security Staffs

D. Equipment and Facilities - the Man-Machine Interface

- D.1 CAS/SAS Design
- D.2 Maintenance
- D.3 Communications Equipment
- D.4 Environmental Influences on Security

NOTES for Section 1

1. T.G. Ryan, "NRC Human Factors Research on Nuclear Industry Organization and Management: Assumptions, Objectives, and Milestones," Presented at the Tenth Light Water Reactor Safety Research Information Meeting, National Bureau of Standards, Oct. 1982; "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," NRC Report WASH-1400, NUREG-75/014, 1975.

2. A.D. Swain and H.E. Guttmann, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Operations," NUREG/CR-1278, 1980.

3. T.G. Ryan, note 1.

4. See for example: R.A. Kisner and P.R. Frey, "Functions and Operations of Nuclear Power Plant Crews," NUREG/CR-2587, April 1982; S. Baron et al., "An Approach to Modeling Supervisory Control of a Nuclear Power Plant," NUREG/CR-2988, 1982.

5. D.M. Speaker, S.R. Thompson, W.J. Luckas, Jr., "Identification and Analysis of Human Errors Underlying Pump and Valve Related Events Reported by Nuclear Power Plant Licensees," NUREG/CR-2417, 1982.

2.0 Solicitation and Analysis of Comments

Part of the research for this project included solicitation of comments from industry and government experts on the importance of various human factors as they related to quality of nuclear power plant safeguards. It was determined that the short time allowed before the project completion date coupled with the need for administrative clearance from the Office of Management and Budget for a formal survey worked against a scientifically developed survey instrument and rigorous statistical analysis. Instead, as a means of soliciting opinion, the document described in the previous section (contained in Appendix B), which discussed safeguards at nuclear power plants and associated human factors issues, was developed at BNL. This document was reviewed by both safeguard professionals and reactor safety human factors professionals on the BNL research staff. It was then revised to reflect comments and suggestions.

A solicitation for comments was then sent to 85 safeguards and/or human factors professionals from industry, industry organizations and major universities with relevant programs. These individuals were systematically selected from attendance lists of human factors professional meetings and safeguards conferences. An attempt was made to include all major industry organizations and contractors while compiling the mailing list for the solicitation. A brief background of the project was provided and certain questions of interest specified in the cover letter. The reader is referred to Appendix B of this report which contains the letter and solicitation document.

Seven specific areas of inquiry concerning the discussion piece were addressed in the cover letter. They were:

1. Are there human factors/safeguards issues which are not addressed or addressed inadequately?

2. Are any of the issues covered unimportant in your opinion?

3. Are there studies addressing these issues which can be brought to bear in the development of a long-term research plan (i.e., can we avoid reinventing the wheel)?

4. What is the relative importance of these issues with respect to each other?

5. Who else should have provided input to this report now or at subsequent stages?

6. Are any of these issues impractical to study or would they require corrective measures unacceptable to Government or industry?

7. Can any of these issues be "clustered" in order to better study them?

As a result of the informal structure of the inquiry, responses varied with regard to their comprehensiveness and emphasis. Twenty-eight separate responses containing hundreds of comments were received. These comments were analyzed empirically and by topic to assist in ranking the issues.

Typically mail surveys receive a 10 to 20% response rate except where the subject population is very specifically selected to maximize the response rate and follow-up are used. As such, the return rate of 32% (28 of 85) for this solicitation can be considered good. In addition, since responses came from professionals in the field, an analysis of responses can be considered a reliable indicator of what human factors are held to be "problems" and to what extent they are believed to affect the quality of safeguards at nuclear power plants.

2.1 Analysis of Comments by Topic

2.1.1 General Comments by Respondents

It was suggested that the present study cannot be a parallel study to NUREG/CR-2833 ("Critical Human Factors Issues in Nuclear Power Regulation and A Recommended Comprehensive Human Factors Long-Range Plan," August 1982) which was principally a review of prior research costing several million dollars in the area of operational safety. Very little human factors/safeguards work has ever been undertaken except by the Defense Nuclear Agency (DNA) for the Department of Defense (DOD) which was cited as relevant by several commentators. (DNA-sponsored research was examined in order to evaluate its usefulness in regulating, assessing, and improving nuclear power plant safeguards.)

It was suggested that the solicitation instrument was comprehensive, logical, and creative, fairly accurate, and thorough. One comment reflected concern that the investigation was overly broad.

As comments were analyzed it became apparent that the original list of human factors affecting safeguards lacked three items which were often mentioned. First, the lack of a means to accurately evaluate the performance of safeguards personnel was cited repeatedly as a factor contributing to potential deficiencies in safeguards. Evaluations based on actual performance, rather than surrogate determinates (quality of recordkeeping, frequency of patrols, etc.), were suggested as necessary for an accurate evaluation of personnel performance. Second, the notion that safeguards is mainly concerned with intentional acts and not, as in operational safety, unintentional errors was widely refuted. Human error can cause breakdowns in safeguards at least as easily as in operational safety according to several comments and therefore should be considered in this study. Third, the pervasive effect of false and nuisance alarms was mentioned and, as a result, was added to the list. In addition, the category of Instruction was broadened to "Instruction, Training, and Selection" because of the large number of comments combining these factors. Signal detection theory was suggested as a good method to use in judging the integrity of some safeguards measures.

2.1.2 Comments on Specific Human Factors Issues

A. The Insider Threat

A.1 Two-Man Rule - In certain secure areas NRC has required in the past that no individual be free to move about alone. This measure assumes that two individuals are less likely to attempt sabotage than a lone individual.

It was pointed out that the NRC has decided the two-man rule will not be required at power reactors in the foreseeable future. This is due to the significant cost and safety impacts to the licensees. Other comments reflected the following concerns: the two-man rule may be appropriate for certain critical areas; a form of supervisory inspection function should be used instead, which will serve the dual purpose of quality control and security; and multiple-man rules are very expensive; and they may not be effective against human reliability breakdowns. One comment expressed concern that a two-man rule may actually dilute responsibility among individuals as shown by some evidence from research in social psychology.

A.2 Behavioral Observation Programs - NRC has considered various programs designed to detect emotional instability in licensee employees. This may be accomplished through observation of subordinates by supervisors who typically refer individual employees to an employee assistance program.

The concern emerged that no satisfactory research or behavioral observation programs currently exist, despite their importance. In some comments it was suggested that this type of research should have very high priority. Union labor was cited as very important in the potential acceptance of a behavioral observation program; and the FAA and Air Force programs were suggested as models. Adverse impacts on employee civil liberties were also cited as a major factor in the design of a program in order to mitigate adverse effects. It was urged that any research in this area should be a follow-up of previous NRC work (e.g., "Behavioral Observation Program for the Nuclear Industry," NUREG/CR-2076).

A.3 Trustworthiness - Complete control of employee actions is not achievable. Instead, some method of assuring individual trustworthiness is needed. Currently, NRC recommends a background investigation and psychological screening of applicants for sensitive positions. The exact nature of an optimal system is still under discussion, however.

According to one comment, this issue has been addressed by many government agencies and in industry because sabotage events are increasingly common. It was pointed out that trustworthiness is determined on the basis of using psychological screening and background investigations which are assumed to be reasonable determinants of future behavior. Concern was expressed over the vagueness of the American National Standards Institute/American Nuclear Society (ANSI/ANS) 3.3 standard currently used to assure trustworthiness of individuals at nuclear power plants. The need to formulate a rigorous classical selection program was cited. It was suggested that NRC fund development and maintenance of a national nuclear security system to include Department of Energy (DOE), NRC, military, and nuclear utility personnel. Job analysis was suggested as a way to assist development of better training in order to directly enhance trustworthiness.

A.4 Fitness for Duty - Some employees in all industries, at times, work in a physical condition which is considered unfit. These conditions may include the results of alcohol and/or drug use, fatigue, illness and other physical or mental states which can affect performance.

Fitness for duty may be affected by shift work and rotation practices, as well as by extraneous factors such as chemical dependences. Appropriate aptitudes, background screening for drug or alcohol abuse, major law violations, and so on, were given as obvious examples. Employee attitudes were cited similarly. Annual or semiannual recertification by a physician or psychologist for all personnel in sensitive positions was suggested. It was pointed out that research in this area may be better combined with the behavioral observation research.

A.5 Human Reliability - People do make mistakes. The issue here is to determine what organizational and systems designs minimize human error. Because human performance is an essential part of most safeguards activities it was added to the original list in this solicitation.

Concern was voiced about the degree to which actual human error could cause deterioration of safeguards. Errors in assessing closed circuit TV imagery, in command and control of security resources, in tactics employed by investigative teams, and in mistaken assumptions about the probable cause of alarm sources are extensively documented according to one comment. Human reliability was suggested as an important area for research. An example of a human reliability issue was made of the lack of required safeguard personnel night qualification with weapons in NRC regulations although threat assessment suggests that intruders are likely to use darkness as a cover. The DOE does require night certification. Thus, the reliability of safeguards personnel at DOE sites and NRC licensees may, particularly in stressful situations, differ at night.

B. Organization

B.1 Boredom and Vigilance - It is well established that human attention will degrade under certain conditions, including long times without stimulus. An individual's ability to maintain proper levels of vigilance and the effects of vigilance deterioration are important to the quality of safeguards.

According to comments, boredom and vigilance are human factors which do respond to training and drills. The frequency of critical events for which security guards are trained may approach zero, and under these circumstances human performance and alertness may not be maintained at sufficiently high levels unless provisions are made for the personnel to exercise their skills against meaningful albeit simulated intrusions. False alarms are also cited as contributing significantly to vigilance deterioration. The integrity of site surveillance was cited both as important in the quality of safeguards and as a condition for which there is no empirical evidence as to whether or not it exists. Further, it was suggested that it may not be appropriate to link boredom and vigilance together. Boredom may also be examined in the light of the types of personnel lost through attrition out of the career. It was pointed out that excellent candidates may be turned off by being strictly overqualified and/or uninformed about the relative importance of their responsibilities as safeguards personnel at a nuclear power plant. Vigilance, as an area of research, has been extensively examined and further research on its causes may be

unnecessary. Instead, research may be better aimed at job structure as well as equipment reliability.

B.2 Organizational Communication - The organization which operates power plants is composed of organizational units which operate in a coordinated fashion to minimize risk to the public. The ability of these units to coordinate normal responsibilities and emergency responses is important to minimizing risks.

Communications among the individuals and organizational subunits can be critical in the integrity of safeguards. Feedback on how well or poorly the security system is working is rarely given to the security subunit. Problems can arise because of poorly defined management and organization structure and their roles in physical security. Research may be better aimed at the role definition problem.

B.3 Rotation/Manpower/Shiftwork - Many of the positions on the safeguards staff of a nuclear power plant require shift work and rotation. The basic issue of manpower refers to over- and understaffing for certain tasks.

Comments tended to indicate a need to study the effects of shiftwork as part of the job structure on guard performance. The potential for attitude conditioning caused by these human factors may be especially important. The Department of Defense (DOD) has sponsored work in this area which should be used. It includes analyses of salary incentives, adequate staffing levels, and advancement opportunities for personnel. Another comment indicates that most classic research focuses on the area of shiftwork for complex tasks, and the literature that is available consists almost entirely of laboratory studies of arbitrary laboratory tasks. Studies aimed directly at security forces at nuclear power plants may also be very expensive. These studies may be effectively combined with those in the boredom and vigilance area.

B.4 Corporate Attitude - The licensee organization as a whole has a characteristic attitude which is rooted in the basic values, norms, and goals of all management and employees. As such, corporate attitude is not limited to those attitudes of management, but includes those reflected by all licensee employees.

Corporate attitude was repeatedly cited as a major, if not the major, factor in dictating the quality of safeguards at nuclear power plants. Corporate attitude, as an issue, includes all aspects of how the safeguards unit is designed, placed, and treated within the organization as a whole. It was pointed out that there is no model of how a guard force should be designed. Some plants use an industrial security model while others use miniaturized army or local police force models. It was asserted that some preferred model must exist. Concern was expressed that without objective evidence of flawed security it was unlikely that security managers would easily accept changes. Conversely, if they are confronted with objective evidence of a deficiency in safeguards, they will usually pursue changes with vigor.

It was pointed out that the productivity and morale of maintenance personnel in nuclear power plants is significantly influenced by security

regulations. If carried to the extreme, maximum security could be achieved, but operational safety effectiveness almost completely degraded.

A problem which, according to comments, should not be underemphasized is the perceived importance of safeguards and the place of security management within the utility management and overall organization hierarchy. While most individual security problems may be solvable with a piecemeal approach, the overall functioning of an effective security organization is best approached from the top down. A management program must be established with security as a top priority to provide the foundation for an effective, integrated security program. It was suggested that a Safeguards and Security Council comprised of division heads, plant management, and security representatives be established at each facility. The council would promote awareness, coordination, and cooperation among these organizational units. Periodic meetings would help assure continuity between safeguards and operational requirements.

Corporate attitude has been suggested as a potential and occasionally manifest source of friction between employees and management. At one site, the difference in management approaches between two separate licensees appears to have caused the one security force, which was subject to authoritarian management, to unionize while the the other security force showed no such inclination.

Guidelines for management and organization which place plant security at the corporate level were suggested. In addition, NRC may consider scrutiny of its own practices in assessing the role of utility management and organization in physical security. Career path and advancement, reflections of corporate attitude, were cited as major contributors to the quality of plant safeguards.

User acceptance of any actions aimed at improving corporate attitude was cited as very important. It was suggested that selected representatives of utilities should be allowed to participate in and review the feasibility and cost effectiveness of resultant programs. The need for rank and file support was suggested as critical to the success of any proposed program.

B.5 Instruction, Training, and Selection - In order to assure optimal individual performance, selection procedures must pick appropriate individuals for each position, and training and instruction programs must prepare them to best handle the tasks they are required to perform.

Instruction, training, and selection were mentioned frequently as critical human factors in safeguards. It was suggested that a standard selection battery and a standard set of norms for security personnel be made available instead of generic guidance. This has been done according to one comment and inquiries as to its effectiveness have been initiated. Qualification, it was asserted, cannot be reliably based on such secondary criteria as how well the individual keeps his log book or subjective appraisals of appearance, trustworthiness, and other traits. Instead, performance-based appraisals must be made. It has been shown that safeguards personnel are often unaware of some of the rather subtle detection and localization problems they may encounter; on the other hand, they quickly learn to cope with these problems once appropriate exercise and feedback systems have been employed. There should be a correlation between

the practical application of emergency techniques and regular training exercises practiced weekly on every shift. The feasibility of increased security audits or drills should be studied. The appropriate level of experience or law enforcement background and training that would enable safeguards personnel to determine the appropriate tactics for dealing with threats should be studied. It may be that training can be used directly in establishing appropriate roles for all levels of security personnel during a security threat.

It was suggested that training should be conducted in such a way as to allow for some type of measurably improved performance. In particular, a criterion of improved performance should include the ability to cope with novel problems, i.e., to extrapolate past experience to new situations.

It was pointed out that considerable research in training theory exists and should be directly applicable to nuclear power plant safeguards personnel. Training programs should be based on job requirements as determined by good behaviorally based job/task analysis. The results of such analysis could also be used in the development of selection training tools.

One comment referred to a site where one license's guard force had undergone a 200-hour basic training program while a second licensee's program lasted only 40 hours. Security officers for both licensees were provided by the same Contract Security Manager and were screened and hired according to the same criteria. The organizational policy of one licensee included adequate training, good labor relations, and management by cooperation; the other's included minimal training (a cost-control measure), authoritarian guard force management, and contract administration through the imposition of penalty clauses. Perhaps as a result, security officers for the second licensee sought and gained a labor union while the first licensee's officers did not. The unionized licensee then compounded its problem by hiring in-house shift supervisors to keep security forces "honest." When the in-house supervisors rejected several officers for reasons other than security or personality aberrations, they were reassigned to the first licensee and, with additional training, performed above average in every case. This is currently being examined to assess its relevance to training as well as corporate attitude.

C. Response Capabilities

C.1 Format and Wording of Contingency Plans - All licensees are required to prepare and submit to NRC for approval contingency plans for safeguards events. Those plans are to be followed during any emergency situation requiring a safeguards personnel response.

It was suggested that a minimum response capability should be defined operationally. The DOD has funded development of a data recording system which can contribute to the capability for measuring response performance. This system could also provide criteria measures necessary for assessing the acceptability of contingency plans and could provide both local management and the NRC with objective data capable of assessing the adequacy of these plans.

Adversary penetration was characterized as the most important and least tractable of all safeguards issues. Improving the capability of a guard

force to identify potential intruders though training is one way to cope with this problem.

It was pointed out that because of a lack of standardization, contingency plans are seldom practiced. It was recommended that exercises should be established which implement some parts of the contingency plans at least quarterly and they should include one full-scale exercise annually.

One comment pointed out that classes of security responses could be established to dictate types, number, and timeline response curves for security personnel. The use of matrices or computer-aided decision making for response selection may be useful.

C.2 Self-Preservation and Use of Deadly Force - Security guards, in particular, can be instantly placed in a position of great personal risk if adversaries are thought to be present on site. The effects of civil and criminal liabilities for improper use of deadly force combined with the personal consequences of not using it when in danger may lead to eroded guard performance.

It was suggested in one comment that the conflict of NRC regulations with various state laws and local ordinances is a major problem, but one that NRC has not been considered in a systematic or generic fashion. On the other hand another comment stated that NRC policy has been based on exhaustive legal research so that further legal analysis is unlikely to alter these policies. However, there may be a need for periodic, realistic exercises under conditions that are not actually life threatening but prepare personnel for decision making under duress.

One comment described the issues of deadly force and self-preservation as overemphasized. They may also be described as decision making problems that can be made very difficult, as in the case of a security guard who, while not fully qualified in the use of weapons at night, may have to decide very quickly on the use of lethal weapons against an individual in darkness. It is likely that untrained personnel will make a less deliberate decision. Training is cited as a good means of coping with those factors that affect the decision making process on whether or not to use deadly force.

It was pointed out that since the arrest powers of a security guard are very limited compared to those of a peace officer (i.e., police or deputized personnel), security guards may be too cautious in performing their duties. If a guard performs an improper arrest, he can be subject to private civil suits brought by the arrested individual. If such a deficiency in performance can be validly demonstrated, it may be addressable through proper training.

The use of duress words/codes, as in the military, to increase covert resistance capability should also be investigated according to one comment.

C.3 Coordination Between Safety and Safeguards - This issue is similar to Organization Communication (B.2), but is unique because operational and security measures may be in direct conflict during an emergency. For instance, in some cases radiological emergencies require a different organizational response from sabo-

tage emergencies, but the distinction may be lost if, for example, a sabotage event escalates into a radiological safety event.

Coordination, it was suggested, plays a large role in determining how well a facility's overall staff can respond to an off-normal situation. The effectiveness of command, control, and communications, including those between the Control Room and Central Alarm Station, are very important, as are communication and coordination with local law enforcement authorities important. Methods of assessing coordination and communication abilities should be developed. Strict lines of authority between the various elements of the plant staff for off-normal situations should be established.

Some comments were directed at normal operations and staff coordination. When card-keys failed, there have been instances of two individuals using the same card key to gain access to protected and vital areas. Restricted access can and does have a marked effect on the productivity and morale of maintenance personnel. It was further mentioned that safeguards issues cannot be taken out of the context of the overall process of operation and nuclear power plant safety. Key operational personnel have been denied access by safeguards personnel because of, among other reasons, poor interpersonal relationships.

According to research presently being conducted there are many cases where timely physical access to manual valves, repair of incorrectly set torque switches on motor operated valves, or restoration of circuit breakers makes the difference between recovering systems and preventing core melt and a major accident. Safeguards access control requirements will play a major role in permitting or preventing such an event.

C.4 Performance Evaluation - When personnel operate in an organization some method of evaluation must be used to assess their performance. Many methods have been used, but the unique nature of safeguards at nuclear power plants (i.e., few if any real events) dictates that special methods be investigated.

It was asserted that no performance based evaluation techniques are used in safeguards and security. There is a need to understand the skill and task structure of guard forces. Assessment techniques need to be developed, perhaps similar to those used by the Department of Defense. What appears to be needed, according to comments, are sensitive, objective measures of all major system functions, including surveillance, intruder detection, localization, interdiction, and apprehension or neutralization. In other words, operationally meaningful system performance criteria need to be developed. Meaningful standards of performance can then be set so that response performance can be measured.

It was suggested that only tools and methodologies designed to determine the effectiveness of implemented human factors measures will truly reveal overall security system operational effectiveness. Performance needs should be analyzed in terms of desired goals, regulatory mandates, and the management/enforcement approach adopted to date by NRC and its licensees.

D. Security Equipment and Facilities

D.1 Central Alarm Station (CAS)/Secondary Alarm Station (SAS) Design - At any operating reactor there is an integrated intrusion alarm system. This system's design can vary depending on the state-of-the-art employed and particular needs at any facility. The quality of the CAS/SAS design (which includes all intrusion alarms and sensors) may be critical to the quality of site security.

It was suggested that security systems and equipment should be subject to the same human engineering review requirements as other plant control stations. Plant security equipment is rarely installed as a system according to comments, but instead a mix of vendors is usually represented in numerous cameras, video monitors, sensors, monitoring systems, and other hardware. The implications are that equipment components are often incompatible and less efficient in terms of cost and operation. A review of currently used systems is in order including consideration of functional requirements and performance specifications (e.g., reliability). Camera misalignment, illumination deficiencies, weather, and environmental factors can seriously degrade site surveillance, permitting adversaries to take advantage of resulting concealment opportunities.

It was pointed out that there are significant man/machine interface problems in military security system equipment which probably exist in industrial security systems as well. In DOD research, very important interface problems have surfaced with respect to surveillance, intruder localization, and command/control which only became apparent in post-exercise analysis of system failures in DOD systems. It has been shown that the machine elements of the system clearly provide the potential for far superior performance to systems which depend on unaided human capabilities.

It was also stated that in some cases security closed circuit TVs have been placed in the middle of the plant control room where operators have to walk around the security guards to perform their tasks. A pilot study to determine if there is a problem and whether a generic solution exists may be usefully undertaken.

D.2 Maintenance - Equipment can always break down regardless of design. For this reason redundant systems are often employed. To minimize dependence on secondary systems, equipment must be maintained. However, the common maintenance of redundant systems has been shown to reduce the integrity of the overall system through common-mode failures. As such, maintenance can play a large role in overall system integrity.

It was suggested that maintenance of physical security systems is an often overlooked human factor that can profoundly affect safeguards. Maintenance records are seldom kept in most industries and even more seldom evaluated. On the other hand, it was also stated that maintenance does not appear to be a significant human factors issue. It may be necessary to establish a means by which the integrity of maintenance procedures can be measured as well as the effectiveness of compensatory actions taken in the event of failure in some physical component of the security system. Dependence on directives

and equipment was called myopic and inadequate since breakdowns are normally discovered after the fact and thus too late to mitigate an event. It was asserted that data on security equipment downtime are available since requirements stipulate that historical records of availability be maintained for alarm, sensor, and access control equipment. It was suggested that a sensitivity study be conducted to determine whether maintenance, in fact, significantly affects the integrity of safeguards.

D.3 Communications Equipment - Safeguards personnel are particularly dependent on equipment to communicate at a site. If personnel or equipment performs inadequately safeguards can be compromised.

Good communications are very important to the security of the site. Objective testing of communications equipment is vitally necessary. Communications equipment can also be used to enhance performance and attitude by establishing and maintaining interpersonal relationships during shifts.

D.4 Environmental Influences - Various factors can affect the performance of personnel, but because safeguards personnel typically operate in many environments (i.e., plant, buildings, around the site terrain, alarm stations, etc.) those influences may have a more profound effect on their performance.

Department of Defense research has shown that failures or inordinate delays in security team response are often associated with an interaction of equipment, procedural, and environmental variables. Environmental variables (terrain, weather, vegetation, physical obstructions, etc.) may not only affect the reliability of security equipment but also the ability of guards to determine whether an unauthorized intrusion has occurred. A knowledgeable adversary, or even a reasonably intelligent one, can take considerable advantage of environmental factors to reduce the likelihood that the intrusion will be detected or increase the likelihood that detection will be delayed. Security personnel are often unaware of the extent to which such factors affect their performance.

It was suggested that the design of isolation zones can lead potential intruders to take certain routes of entry. Design of these zones will cause entry routes to be nonrandom so that some method of predicting the most likely routes of entry should be developed. One comment stated that environmental influences are not a significant human factors issue.

D.5 Nuisance and False Alarms - Any alarm system effective enough to alert the alarm station to the presence of intruders will necessarily be affected by nonthreatening occurrences (e.g. animals, wind, inadvertent personnel stimuli, etc.). The level of nuisance and false alarms may affect the quality of safeguards.

Respondents suggested that the expectancy of an actual intrusion is very low and the expectancy for false alarms is typically quite high. There appear to be no physical security systems where the false or nuisance alarm rate is not of sufficient magnitude to preclude inappropriate expectancies on the part of security personnel. These problems can lead to a deterioration in the vigilance of security personnel.

It was suggested that rigorous use of signal detection theory and human factors research could lead to an understanding of optimal false alarm rates. This is a very significant problem which dictates the need for equipment with tested reliability and a continuing, effective maintenance program - including preventive maintenance.

2.2 Empirical Analysis of Comments

The number, form, and variety of comments received do not allow statistically significant statements concerning the relative importance of issues. However, a rational scheme for empirically ranking issues was developed and applied.

In all, there were 17 human factors issues discussed in the solicitation document. Three were added before the analysis was conducted to capture issues which comments indicated were worthy of consideration but were not included in the original list. These were performance evaluation (C.4), human reliability (A.5), and nuisance and false alarms (D.5).

Each comment was reviewed and rated for how it perceived each human factor. A five-point liekert-type scale was used to assign a value to each cell and a data matrix was generated. The scale used was -2 (not important at all), -1 (relatively unimportant), 0 (neutral or unmentioned), +1 (relatively important) and +2 (very important). The assignment of cell values was necessarily somewhat subjective. To minimize rater bias, each issue was indexed in each comment by two separate judges (one operational safety professional and one safeguards professional) so that the initial review was made as objective as reasonably possible. Both independent ratings of each response were then cross-compared with a third judge (a methodological social scientist) and a final rating was determined for each cell. Because five comments did not mention any issues, but instead asked to be kept aware of progress in this project and others arrived too late for this analysis only eighteen comments are included in the analysis. The data matrix and results are in Tables 3 and 4.

Table 3. Data Matrix

Responses	A-1	A-2	A-3	A-4	A-5	B-1	B-2	B-3	B-4	B-5	C-1	C-2	C-3	C-4	D-1	D-2	D-3	D-4	D-5	=1
A	1	0	2	0	0	0	2	0	2	2	1	2	0	1	2	2	0	2	0	19
B	0	0	0	0	1	0	0	1	2	2	0	0	1	1	1	0	1	0	0	10
C	0	0	0	0	1	0	0	0	0	2	2	0	0	0	0	0	0	0	0	5
D	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	0	15
E	0	0	0	0	0	0	0	0	2	2	0	0	1	2	2	0	0	0	2	11
F	0	0	0	0	0	2	0	0	0	2	2	0	0	0	0	0	0	0	0	6
G	0	2	2	0	2	0	0	0	0	0	0	2	0	2	0	0	0	0	0	10
H	1	2	0	1	0	2	0	0	2	2	2	2	0	0	2	0	0	2	0	18
I	0	0	0	0	2	0	0	2	0	1	1	0	0	2	0	0	0	0	0	8
J	0	0	0	0	0	0	0	0	2	0	0	0	2	0	0	0	0	0	0	4
K	2	0	2	0	2	0	0	0	0	0	2	0	1	0	0	0	0	0	0	9
L	2	0	2	2	0	1	2	2	1	2	2	1	1	0	2	2	1	2	0	25
M	-2	1	2	0	0	2	1	1	1	1	2	-2	2	0	1	-2	1	-2	0	7
N	0	0	0	0	2	0	0	0	0	0	2	1	0	2	0	0	0	0	0	7
O	1	2	2	1	0	-1	2	-1	1	2	1	1	1	1	2	2	1	0	0	18
P	1	2	1	1	2	1	0	1	2	2	2	1	0	2	0	2	2	0	0	22
Q	0	0	2	2	0	-2	2	0	2	2	0	-2	2	0	1	2	2	1	2	16
R	0	2	0	1	1	0	0	0	2	2	0	1	0	2	0	0	0	0	0	10
TOTAL	6	13	16	8	15	8	12	7	22	27	22	9	14	18	16	11	11	7	6	248

Scale: +2 - Very important
+1 - Important
0 - Neutral/Unmentioned
-1 - Unimportant
-2 - Not important at all

Table 4

Importance Ranking of Human Factors Issues in Nuclear Power Plant Safeguards As Derived from Comments

Ranked Issue	Weight	% of Total Weight
1. Instruction, Training, and Selection (B.5)	27	11
2. Format and Wording of Contingency Plans (C.1)	22	8
Corporate Attitude (B.4)	22	8
4. Performance Evaluation* (C.4)	18	7
5. CAS/SAS Design (D.1)	16	6
Trustworthiness (A.3)	16	6
7. Human Reliability* (A.5)	15	6
8. Coordination Between Safety and Safeguards (C.3)	14	6
9. Behavioral Observation Programs (A.2)	13	5
10. Organizational Communication (B.2)	12	5
11. Maintenance (D.2)	11	4
12. Communications Equipment (D.3)	11	3
13. Self Preservation and Deadly Force (C.2)	9	3
14. Boredom and Vigilance (B.1)	8	3
Fitness for Duty (A.4)	8	3
16. Rotation/Man Power/Shiftwork (B.3)	7	3
Environmental Influences (D.4)	7	3
18. Two-Man Rule (A.1)	6	2
Nuisance and False Alarms* (D.R)	6	2
	248	

*Added subseq nt to receiving comments.

3.0 Safeguards Summary Event List (SSEL) NUREG-0525

The SSEL was used to examine the frequency and impact of human factors in various safeguards events reported to NRC by licensees. The SSEL is an NRC publication which contains brief summaries of safeguards-related events reported to NRC and is intended to provide a broad perspective on the nature of safeguards incidents in the licensed nuclear industry. Events reported (both routine and unusual) are placed among several categories of events in the SSEL which is completely updated and reissued annually. The analysis presented here is from data in the SSEL (Revision 4) on events which occurred over the 5½-year period between 1976 and the first half of 1981. While the SSEL does not represent a complete data base such an analysis can be useful. However, the results of this analysis taken alone may be an overly broad conclusion based on extrapolation of limited data.

The first category in the SSEL is "Bomb-Related Events," which involves explosives and incendiary devices or materials and related threats. This category is split into two subcategories, one involving actual bombs and the other in which no such device was discovered. The second major category of events in the SSEL is "Intrusion Events," which includes incidents of attempted or actual penetration of a facility's barriers or safeguards systems. "Missing and/or Allegedly Stolen" is the third category and includes events in which licensed material was stolen, alleged to be stolen, misplaced, found missing or inadvertently disposed of. Category four is "Transportation-Related Events," where licensed material was misrouted, involved in an accident, or lost during transportation. "Vandalism" is the fifth category including any acts which involve low-level destructive or harrassing activities directed against the licensee. "Arson," the sixth category, includes intentional acts involving incendiary materials resulting in serious damage. The seventh category, "Firearms-Related Events", describes discharge, discovery, or loss of firearms at or near licensed facilities. "Sabotage," the eighth category, includes deliberate acts directed against a licensee which culminate in direct or in-direct danger to the public. The last category, "Miscellaneous Events," includes all reported events which do not fit in any of the first eight categories.

These categories are analyzed in order to identify those events involving human factors which are more frequent and/or more serious than others. Judgments concerning the relative effects of human factors are then made. (Judgments were first made by one judge, then a validity check was carried out by another.) It must be noted, however, that event-reporting requirements have changed over the last several years so that judgments about trends and variations cannot be rigorously made, but rather read from an overview of these data as they have been collected.

3.1 Bomb-Related Events

The bomb-related events against nuclear reactors are, by far, the most frequent of reported safeguards-related events. In all, 296 of the 410 reactor-related events during the 1976 - mid 1981 period involved bombs or bomb threats. Only six events reported to NRC actually involved an explosive or incendiary device, and of these only two occurred during the period for which these statistics were compiled (the other four occurred before 1976). In no case did use of a device pose a direct threat to the public.

A detailed analysis of the SSEL data and other available information concerning bomb-related events was conducted by Mazur* using data from 1969 until the first half of 1980. There were 37 bomb threats during that period. From 1969 to 1975, 64% of these threats were directed against reactor facilities as opposed to other licensed facilities such as fuel cycle and waste facilities. After 1975, 91% were directed against reactors.

Threats nearly always come by phone and approximately 80% were from male callers. Most calls went directly to the target (the licensee), but occasionally also went to local law enforcement, news media, and offices of corporations associated with the target facilities. About 10% of the calls can be attributed to employees because they came from a phone on site rather than through the main switchboard.

Mazur's work was directed at investigating the correlation between bomb threats against nuclear facilities and media coverage of the nuclear power issue. Using article events from the Reader's Guide to Periodic Literature, trend data obtained from Television Evening News Covers Nuclear Energy: A Ten Year Perspective by the Media Institute, column inches listed in the New York Times Index, and the number of pages on the Three Mile Island Accident in Time and Newsweek, it was found that the occurrence of bomb threats against licensed facilities shows a remarkable correspondence with media coverage of nuclear power. Although Mazur does not give a definitive interpretation of the data, the close correspondence of media coverage indicates that some measure of "normal" bomb threats frequency could be predicted using these media coverage indexes.

3.2 Intrusion Events

During the period 1976 through June 1981 35 intrusion events occurred, all at reactor sites. This represents 8% of all reactor-related events. These 35 events can be broken down into three general categories: (1) those potentially or actually involving an unauthorized knowledgeable insider, (2) those involving outside intruders and guard force response, and (3) those involving clear false alarms or warnings. There were 16 events in the first category indicating the unauthorized presence of knowledgeable insiders. They range from inspectors or reporters gaining unauthorized access to restricted areas, including vital areas and control rooms, to the sighting of an individual scaling the perimeter fence in a certain area and a check of all personnel there revealing that only authorized individuals (i.e., knowledgeable insiders) are present. There were 17 events due to outside intruders which resulted in subsequent guard force response. These ranged from intoxicated individuals ramming the fence or gate with an automobile to a hunter approaching the perimeter and individuals seeking help after a boating accident. Interestingly, 5 of these 17 response events involved intoxicated individuals. This may indicate a need to include methods of dealing with intoxicated individuals in training. Two events involved false alarms--those being a hoax and a rumor--both threats of intrusion.

*A. Mazur, "Bomb Threats and the Mass Media: Evidence for a Theory of Suggestion," American Sociological Review, June 1982, pp. 407-411.

Intrusion events listed in the SSEL were analyzed in order to ascertain which human factors came into play most frequently. Each reported intrusion event was examined and scored so that all intrusion events could be included. Each event was scored by whether or not each human factor was or was not involved. Criteria used to indicate the presence of a human factors concern in an intrusion event are:

A.1 Two-Man Rule - where a lone authorized individual was found to be, or thought to be, responsible for the event.

A.2 Behavioral Observation Programs - where authorized individuals actually committed some act indicating that a behavioral observation program may have been desirable.

A.3 Trustworthiness - where an individual or individuals gained undetected, unauthorized entry to the facility and where unauthorized individuals were detected after entry. The reason these are both included is that the distinction between them is not clear from a reading of some events.

A.4 Fitness for Duty - where an authorized individual was found to be unfit for duty.

A.5 Human Reliability - where the performance of safeguards personnel was a dominant factor in the success or failure of a response by the security force.

B.1 Boredom/Vigilance - where deterioration of vigilance did contribute or could have contributed to faulty security.

B.2 Organizational Communication - where the security force was not adequately informed of events such as the presence of inspectors or emergency personnel.

B.3 Rotation/Manpower/Shiftwork - where these factors had a direct effect on the response of the security force.

B.4 Corporate Attitude - where an event involved or was influenced by some aspect of employee or employer attitude.

B.5 Instruction, Training, and Selection - where some aspect of security force performance indicated the use of or need for better performance and/or training in a response.

C.1 Format and Wording of Contingency Plans - where contingency plans were, or were supposed to be, the basis for a response.

C.2 Self-Preservation and the Use of Deadly Force - where it can be shown that consideration of these human factors affected guard performance.

C.3 Coordination Between Staffs - where security personnel had to interact with other staff elements.

C.4 Performance Evaluation - where performance was or needed to be measured.

D.1 CAS/SAS Design - where the intrusion system was or was not activated or did or did not contribute to an event.

D.2 Maintenance - where security equipment was found to be compromised or not useful.

D.3 Communications Equipment - where any communications equipment was used during or subsequent to an event.

D.4 Environmental Influences - where some environmental influence had an effect on the response or contributed to an event.

D.5 Nuisance and False Alarms - where an alarm was disregarded or misinterpreted for any reason.

The results of applying these criteria to each intrusion event in the SSEL are presented in Tables 5 and 6. Of the 35 events analyzed, 26 (74%) involved human reliability as a dominant factor in security responses. This indicates that the reliability of safeguards personnel to successfully execute their tasks is very important in assuring optimal site security. Twenty-five events (69%) involved the use or supposed use of contingency plans, which is evidence of the pervasive nature of contingency planning in properly responding to safeguards events involving intrusions. Identifying the appropriate format for contingency plans in order to facilitate their use during off-normal events seems to be important if their use will improve safeguards. Twenty events (55%) involved activities for which training is drawn upon or a lack of proper response could be attributed to training. Having the proper safeguards personnel and whether or not they are adequately trained bear strongly on the quality of safeguards at licensed facilities. Boredom and viligance as human factors contributed or could have contributed to the quality of response in 18 events (51%). The effects of vigilance deterioration may cause site security to degrade, but the manner in which that may occur is not now understood. Communications equipment was used in 18 of the 35 events reported (51%). This indicates the need for high-quality and well-maintained communications equipment and personnel well trained with its use during an emergency situation. The issue of trustworthiness arose 15 times (42%) and there were many cases of violated access controls. Examples of these violations ranged from NRC inspectors gaining unauthorized access to vital areas to maintenance workers using common card-keys. The design of CAS/SAS and its intrusion alarm system were involved in 13 events (37%). Corporate attitude, coordination between staffs, and environmental influences each were factors in 11 intrusion events (31%). Organizational communication was involved in nine events (25%) and the need for or use of performance evaluation was present in 5 events (14%).

As a percent of total events all of the above issues are important ranging from human reliability in 74% of all reported events to performance evaluation in 8%. It must be noted, however, that the nature of the data, that is what events are and are not reported, can bias these percentages to a significant degree. With that caveat, these percentages are reasonable indicators of the pervasive influence of human factors on the quality of safeguards at nuclear power plants.

Table 5

Events from SSEL

Human Factors Issues

	1976										1977		1978					1979			1980												1981	Total
	1	2	3	4	5	6	7	8	9	10	1	2	1	2	3	4	5	1	2	3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	1	35
A.1																	x					x				x										3
A.2																																				0
A.3				x							x		x	x			x	x		x	x	x	x	x		x				x	x		x			15
A.4																															x					1
A.5	x			x		x	x	x	x	x	x	x	x	x		x	x	x	x	x		x	x				x	x	x	x	x	x		x	x	26
B.1	x			x			x	x			x	x	x		x		x	x		x	x	x	x		x	x	x						x			18
B.2			x	x							x		x	x		x					x			x						x							9
B.3											x																										1
B.4	x												x			x	x			x	x	x	x	x		x					x						11
B.5	x			x		x	x	x	x	x	x	x	x	x	x	x		x	x	x		x	x							x					x		20
C.1	x	x			x	x	x	x	x	x	x				x	x	x		x	x	x		x		x	x	x	x	x		x	x	x	x			25
C.2						x																															1
C.3											x	x		x			x				x	x	x	x		x	x				x						11
C.4				x							x	x		x						x																	5
D.1										x		x	x	x	x		x	x			x	x			x		x		x				x				13
D.2																																					0
D.3					x		x	x	x	x		x			x	x	x		x				x		x		x	x	x		x	x			x		18
D.4							x	x	x			x				x				x		x	x			x		x	x								11
D.5																																					

Table 6

Ranking of Human Factors Issues for Intrusion Events

	Number of Events	% of Total Events	% of Total Score
1. Human Reliability (A.5)	26	74%	14
2. Format and Wording of Contingency Plans (C.1)	25	69	13
3. Instruction, Training and Selection (B.5)	20	55	11
4. Boredom and Vigilance (B.1)	18	51	10
Communications Equipment (D.3)	18	51	10
6. Trustworthiness/Access Controls (A.3)	15	42	8
7. CAS/SAS Design (D.1)	13	37	7
8. Corporate Attitude (B.4)	11	31	6
Coordination Between Staffs (C.3)	11	31	6
Environmental Influences (D.4)	11	31	6
11. Communication (B.2)	9	25	5
12. Performance Evaluation (C.4)	5	14	3
13. Two-Man Rule (A.1)	3	8	2
14. Fitness for Duty (A.4)	1	2	1
Rotation/ManPower/Shiftwork (B.3)	1	2	1
Self Preservation and Deadly Force (C.2)	1	2	1
	188		

3.3. Missing/Allegedly Stolen

There were 121 missing/allegedly stolen events between 1976 and the first half of 1981. Virtually all of these events occurred at research reactors and fuel cycle facilities, whereas only two occurred at power reactors. This is because no nuclear material on site at a power reactor can be easily misplaced or stolen. New fuel comes in large bundles too heavy to be moved without special equipment, and spent (used) fuel is so highly radioactive that it is considered "self-protecting." The start-up neutron source is burned up in the reactor during the startup so it cannot be removed or misplaced. Therefore, further consideration of events in this category was not undertaken.

3.4. Transportation

There were 43 transportation related events. Thirty-three involved events listed under missing/allegedly stolen. Three events involved normal mishaps such as shipping a low level waste container to the incorrect disposal site. Two involved drivers violating access controls such as covertly bringing a sleeping child through the security gate in the truck cab. Two events involved gunfire on a truck. Two involved material lost in transport, e.g., a set of sources falling overboard off a transport ship. In only one case did an individual improperly transport material. Since transportation of nuclear materials is not within the scope of this report it is given no further consideration.

3.5. Vandalism

There were 22 vandalism events during the period under consideration, all but one at power reactor sites. Of these, 8 were attributable to insiders. Nine events involved unknown individuals, but the descriptions of most of these events leave the direct impression that insiders were involved although that has not been conclusively shown. Only 2 events involved outsiders -- one an anti-nuclear protestor and one children.

Vandalism events are not as diverse i nature as intrusion events, since normally they are discovered after the fact. It can only be deduced that the breakdown in security associated with these events indicates some type of weakness in safeguards and that knowledgeable insiders contribute to many events. Twelve events involved sites under construction or where fuel was not on site. This indicates that most (12 of 20) events occurred when personnel movements were not as closely controlled as under normal operating conditions. The results of an analysis of these using modified criteria events are presented in Table 7.

Criteria used to indicate the presence of an event condition (i.e., human factors) in each SSEL vandalism event were:

Actual Safety-Related Threat - where fuel was present on site , actual plant safety depended upon or could possibly have depended on the object which was vandalized.

Insider Possible - where a knowledgeable insider could have played a role in the event. If it was impossible to assume the greater likelihood of an insider over an intruder, then this condition was not deemed present.

Table 7

Analysis of Vandalism Events from SSEL

Event Conditions	1978		1979							1980								1981					Total
	1	2	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	1	2	3	4	5	
Actual Safety Related Threat									x	x	x					x						x	5
Insider Possible						x		x		x		x	x		x				x	x	x		9
Insider Probable		x	x	x	x				x		x					x						x	8
Alarm		x		x					x	x													4
Under Construction/ No Fuel or Site	x	x	x			x		x			x			x	x				x	x	x		12
Compromised Locks				x	x			x		x		x										x	6
Outsider Intruders	x						x																2

Insider Probable - where there was direct evidence that a knowledgable insider was involved in the event.

Alarm - where an alarm was or can be assumed to be relevant to the event such that an alarm should have indicated the presence of an intruder.

Under Construction/No Fuel On Site - where the reactor was being built or unfueled so that no radiological threat to the public was possible.

Compromised Locks - where a lock was compromised or where such compromise would be necessary for the event to have occurred.

Outsiders - where direct evidence exists that outside intruders committed the event.

These conditions were used to analyze vandalism events instead of the full list of human factors because of the lack of substantial diversity among them.

3.6. Arson

There were only five arson-related events during the period of interest, all at power reactor sites. There were no suspects in any of these events, but, as with vandalism, it is reasonable to conclude that some, if not all, of these events involved knowledgeable insiders.

3.7. Firearms-Related Events

There were 19 firearm-related events during the period of interest, 15 occurring at power reactors. Of these 19 events, 6 involved authorized insiders, 5 lost weapons or illegal possession, 2 accidental discharges by guards, 3 guards being fired on or returning fire, and two were hoaxes and 1 was a guard committing suicide.

3.8. Sabotage

There were no sabotage events reported in the SSEL.

4.0 Literature and Studies on Human Factors and Safeguards

Having examined expert opinion and reported safeguards events a remaining consideration is the relevant literature. Several comments stated that research in many areas of interest has already been undertaken. In addition, research which is recommended by studies already completed should receive explicit consideration in the development of a long-term research plan.

In this chapter, studies which have been undertaken by government agencies, government contractors, and industry organizations are reviewed. A brief description of the objective, method, and results of each study is given along with the recommendations received for further research. A more broad based literature review is presented in Chapter 4.

Beyond using expert opinion and past history of safeguards-related events to project human factors issues, it is also necessary to look at the research and studies that have already been done in this field. There is a sizable body of literature on work in the area during the past few years, both government agency-sponsored work and academic studies. The results of our survey of this literature are presented in the following sections.

4.1 Government and Contractor Studies

In this section, studies which have been undertaken by government agencies, government contractors, and industry organizations are reviewed. For each work covered, brief descriptions of the objective, methods, and results are given. In addition, the recommendations made by the authors for further paths of research are presented. At the end of the section, a matrix, similar to that in Figure 2 above, is shown, with recommendations grouped under the same headings used in Table 2.

The selection of studies and reports gathered here should not be construed as exhaustive. Nevertheless, the sample is representative and large enough to draw some tentative conclusions as to which human factors topics are likely to be productive as subjects for future research according to government and contractor experts.

4.1.1 People-Related Problem Survey: Method, Analysis, and Results, G. Spies et al., U.S. N.R.C., NUREG-0768, March 1981.

This report contains the results of an investigation by the Safeguards Division in the Office of Nuclear Materials Safety and Safeguards of the U.S. Nuclear Regulatory Commission to uncover possible problems relating to human factors which could affect security in NRC-licensed facilities. The method used was to interview security personnel at 36 facilities, and, in addition, to consult with law enforcement officials and others defined by this report (see p. 1 of the report).

Much of the report's evidence is somewhat anecdotal in nature. Examples of the effects of corporate attitude on security figured prominently. Other concerns were security officer selection and training, security management, security force morale, and human compensatory measures for inadequate equipment. A list of recommendations was produced after an analysis of the sur-

vey and interviews. Some of these recommendations deal with the regulatory process, including some suggestions for modifications and additions to NRC regulations. These are listed below.

1. Communications with licensees during rule making. It is proposed that seminars dealing with security matters be given for licensees, and that better routine communications be established between NRC and licensees. Also, the clarification of the licensing roles of NMSS and NRR would be helpful.

2. Licensees should be allowed to test any new part of a proposed improvement on the physical protection system for effectiveness, without being irrevocably committed to it in advance.

3. Modifications are suggested in the NRC rulemaking process, particularly regarding implementation schedules and increased visibility for guidance and acceptance criteria.

4. NRC should help licensees in their contacts with Local Law Enforcement Agencies, if necessary.

5. NRC should provide licensees with information on the state of the art in security equipment, as regards improvements and modifications.

6. Prolonged human-based compensatory measures for periods when equipment is unavailable should be discouraged.

7. Inspectors should oversee possible human factors problems more closely than is now the case.

8. The authority of licensee security managers should be regulated by the NRC, basically to strengthen their influence within the organization of the licensee.

9. Overtime should be limited for security personnel, both because effectiveness is reduced and because morale may be negatively affected.

10. Non-security-related duties should be restricted because of the bad effect on morale.

11. The terms "guard" and "watchman" should be replaced in the regulations by more authoritative sounding words.

12. Field tests of security force should be devised and used to develop a capability to evaluate the effectiveness of the force.

13. There should be some kind of nationwide licensing of security officers and managers to assure some kind of uniformity among licensees.

It should be remarked that some of the data analysis and reduction which are used to justify the above conclusions are not completely rigorous. Appendix A of the report contains the results of the above-mentioned survey, presented in the form of contingency tables. The security force morale is examined for independence from many sociological variables using a chi-square

test. In several cases, the results are insignificant, as noted by the authors of the report. In at least one case, however, involving the correlation of security force morale with non-security duties, the data clearly show an inverse correlation, which escaped the author's attention. The chi-square test can only show independence between variables; it cannot show whether the correlation is positive or negative or how great the correlating is. The conclusion reflected in 10 above is, therefore, not justified by the data presented in the report.

4.1.2. Standards for Psychological Assessment of Nuclear Facility Personnel, F.D. Frank et al., Assessment Designs Inc., NUREG/CR-2075, July 1981.

The purpose of this report is to detail the development of standards for the assessment of emotional instability in applicants for nuclear facility positions. It also addresses the issue of on-the-job behavioral reliability to a limited extent, but is principally aimed at the selection system administered before an applicant is actually hired.

The methodology used to conduct this research is rigorous in that the breadth of the investigation is comprehensive and feedback mechanisms were included as the study progressed to refine its findings. It follows six steps beginning with site visits and interviews aimed at assembling a job analysis for security guards and supervisors. Then a literature search was conducted to identify instruments capable of measuring emotional instability. On the basis of those instruments identified as potentially useful tentative standard criteria were developed. A panel of experts was then assembled including subject matter experts on the nuclear industry with specific expertise including psychometrics; clinical, industrial, physiological, and counseling psychology; psychiatry; and law. The expert panel provided inputs in order to redefine the standard criteria to more closely reflect the nuclear industry. Using the redefined standard criteria, those measurement instruments identified previously were reevaluated and those most applicable to a nuclear facility were identified. In addition, additional research needs are identified.

The findings of the report indicate that because emotional instability is multidimensional no single instrument is sufficient to measure its presence. The predictive validity of instruments aimed at behaviorally oriented measurement of on-the-job emotional instability was found to be very weak. This led to the conclusion that those instruments shown to be valid and of use in the selection system should be required. Specific instruments which were recommended from among over 15 considered include the Minnesota Multiphase Personality Inventory, the Sixteen Personality Factors Questionnaire, situational simulations, and the clinical interview.

Specific caveats and qualifications accompany the report's conclusions. A major consideration is that of the employees' rights to confidentiality and appeals. To fully assure these rights, the report advocates that only qualified professionals be used in psychological assessment and that standard criteria applying to positions of differing sensitivity be developed from methods shown to be valid. Standards for instruments and professionals are extensively covered in separate chapters of the report.

Among the specific recommendations made in the report are:

1. Criterion-oriented validity studies using multidimensional, multiple regression methods aimed at determining the predictive value of indicators. It is recommended that rigorous scientific method be applied in order to screen out moderator variables and internal bias.

2. Content and construct validity studies on those indicators found effective, including consideration of task congruency between job task elements and tasks associated with various measurement instruments as well as between convergent and discriminant validity indexes.

3. Studies to identify and account for false positives found during assessments.

4. Studies aimed at determining intra- and inter-rater reliability for those instruments selected.

5. Research on the effects of career path and compensation plans opportunities on the pool of applicants.

6. Research on the effects of compensation plans and job rotation on the incidence of on-the-job emotional instability.

4.1.3 Behavioral Reliability Program for the Nuclear Industry
J.C. Buchanan et al., Personnel Decisions, Inc.,
NUREG/CR-2075, July 1981.

A program for promoting behavioral reliability at nuclear plants has been developed in great detail. The study begins with a survey of the field of behavioral observation, as applied to personnel reliability. Prior and current work in the field are reviewed. Next, the pathologies of emotional disorders applicable to those in a working environment are described. The rates of incidence and the potential causes of the disorders are presented.

Methodologies for early detection of behavioral instability are given. These include interviews, objective techniques (tests), projective techniques, observation of behavior, and establishment of a set of criteria for determining behavioral instability.

In order to establish standards for a behavioral reliability program, site visits to nuclear plans were conducted and interviews were held with personnel at many levels at the sites. Expert opinion was solicited from psychologists and lawyers, as well as from some union representatives. Finally, a training workshop was held for supervisory personnel from some participating utilities, and the workshop was evaluated by the authors for how effectively it trained the participants in observation of behavior which could be a precursor to unreliability. The program would include professional assistance for those employees with apparent problems, to aid in resolving them.

This report is summarized in Appendix B of the "People-Related" study covered in Section 4.1.1.

This report states that there are potential problems with the approach of asking supervisors to, in effect, "spy" on employees to avoid behavioral problems on the job. It is not clear that such a program would meet with acceptance on the part of the general work force, who could well resent the interference of the company into their personal lives. The approach, if implemented, would have to be done very tactfully and carefully, with worker participation and accord at all levels. There is also the danger that supervisors, being trained in what to look for, would be able to mask their own aberrant behavior before their own supervisors. Finally, there could be a massive disregard and evasion of the program on the part of all personnel, if those concerned are not convinced of its utility.

The study recommends:

1. a workshop and training program incorporated into management training;

2. a sharing of techniques and results among facilities so that the industry may benefit overall from a steady improvement in developing these training and complementary programs for behavioral observation.

4.1.4 Stress and Duress Monitoring at NRC Licensed Facilities, A. Fainberg, Brookhaven National Laboratory, NUREG/CR-1031, September 1979

This report investigates the hardware possibilities for stress monitoring of employees by the employer to assure fitness for duty. The capabilities of various techniques are discussed, including voice stress analysis, observation of metabolism indicators (e.g., blood pressure, pulse rate), and skin secretions. Also considered were various techniques to allow duress monitoring of individual members of a guard force during an emergency situation, such as an attack on or the capture of an individual guard. In the case of stress, it was found that none of the techniques were sufficiently developed to provide a reasonable barrier against admission of employees to the plant who may be temporarily unfit for duty. As for the duress monitors, several techniques were found to be feasible, although some needed more development.

4.1.5 The Role of Security Clearances and Personnel Reliability Programs in Protecting Against Insider Threats, R.W. Perry et al., Battelle Human Affairs Research Centers, B-HARC-411-018, July 1979.

The report discusses the effectiveness of security clearances and personnel reliability programs in protecting against insider threats to any facilities with Special Nuclear Material. It concludes that security clearances are aimed at "loyalty" and questions of national security and are thus less sensitive to many insider threats. Redesigning of clearance criteria would be necessary to render clearances reasonably effective in predicting threats from employees of screening them out.

Personnel reliability programs are aimed at detecting deteriorating behavior or other signs which could indicate a future threat from a given individual. They have in the past, however, been directed at safety and accident prob-

lems rather than malevolent acts. Problems beyond this are ambiguous criteria for determining unreliability and capabilities of nonprofessional observers in applying unreliability criteria (normally, work supervisors would fill this role). The report recommends that personnel reliability programs be developed to protect against insider acts, rather than to rely too strongly on security clearances. This study was presumably a reason for the later detailed report which developed a behavioral reliability program for the US NRC, mentioned above. (Section 4.1.3). The same caveats noted in that section apply here, as well.

4.1.6 A Review of Selected Methods for Protecting Against Sabotage by an Insider, L. Goldman and P. Lobner, SAI, NUREG/CR-2643, August 1982

This report is mainly a compendium and detailed study of hardware and procedural methods of preventing and protecting against insider sabotage. Analyses of safeguards material control and physical security systems are made, using such computer-based techniques as SAI's MAIT and Generic Sabotage Fault Tree. Then, fixes are suggested, such as separation of duties on a spatial or temporal basis, n-man rules, and so on. The report is a useful description of the ways of dealing with insider sabotage, using current safeguards technologies. Recommended improvements include:

1. procedural modifications, which are relatively easy to implement;

2. modifications in hardware and sensor monitoring;

3. response plans for sabotage.

4.1.7 A Method for Determining the Susceptibility of a Facility to Sensor System Nullification by Insiders, D. Boozer and R. Worell, Sandia National Laboratories, SAND-77-1916C, 1977.

This study is a report on the development of a computer study of the levels of collusion necessary between insider adversaries to defeat a sensor system protecting a nuclear facility. No recommendations are made.

4.1.8 The Insider Threat to Secure Facilities: Data Analysis, J.M. Heineke and Associates, NUREG/CR-1234, June 1980

This study investigates data of insider crimes in three areas of concern: banks, computers, and drug manufacturing. With banks, the major crimes are fraud and embezzlement. With computers, in addition to theft of services, manipulation of accounting data was a prime concern. In the drug industry, diversion of drugs by employees, usually for resale on the black market, is importa , and, in fact, is closely analogous to problems of diversion of nuclear materials. Analogies are also drawn between the other crimes and problems of safeguards in the nuclear industry. One conclusion is that many drugs are "lost" in transit (i.e., stolen). A clear warning is inherent for the nuclear industry: safeguards are not always as effective during transportation as at a fixed site. Another was that increasing the severity of the charges, as a measure of the level of law enforcement in the drug field, has a deterrent effect. Increasing the number of perfunctory penalties, as opposed to fewer but more se-

vere penalties, may actually encourage illegal activities. Finally, it is held that economics is an important determining factor in the level of crimes, and that this may have ominous implications for the nuclear industry, considering the potential value on the black market of special nuclear materials.

Beyond these comments, no specific recommendations were made, and it is a matter of conjecture as to how close the analogy really is to the nuclear industry; in fact, since there is no established theft industry in the nuclear field as there is in other fields, there is some question as to the relevance of, say, increasing the number of arrests as a palliative.

4.1.9 Nuclear Power Plant Perimeter Intrusion Alarm Systems
E-Systems, Inc., EPRI-NR-2355, April 1982

This report extends the NRC sabotage design basis threat and makes recommendations as to performance standards to improve the response time of a guard force to an external assault by improving the perimeter intrusion alarm system. It suggests that guard force disposition and logistics be aimed at making a rapid response to an intrusion. Further, layering and signal processing techniques for reducing false and nuisance alarms are suggested. Beyond this, the report consists of a detailed analysis of the state of the art of perimeter detection. A baseline system is suggested, along with costs and reliability testing methods.

4.1.10 Potential Threat to Licensed Nuclear Activities from Insiders (Insider Study), S.A. Mullen et al., US NRC, NUREG-0703, July 1980.

This report gives the results of a study made of past insider theft and sabotage incidents at nuclear and nonnuclear facilities. Nonnuclear industries were surveyed as well, since the database for incidents in the nuclear industry is relatively small. An attempt was made to choose those industries where an analog to safeguards exists. As a result of the survey, typical profiles of insider thieves and saboteurs were developed. Additionally, conclusions were drawn with respect to detecting and preventing insider malevolence.

Detection

1. Employees can have an important role in detecting abnormalities resulting from criminal acts; security awareness programs and a good management/security employee relationship would be helpful.

2. Inventory manipulations might be more detectable during periods of enforced absence (mandatory vacations, for example) when cover-up action would be impossible.

3. Audits, inventories, and inspections, particularly if frequent and unannounced, are successful detectors of diversions.

4. Informants account for 20% of theft detections; an anonymous informant program might be useful for licensees. The Atomic Weapons and Special Nuclear Materials Rewards Act offers rewards to informers on theft of SNM; publicity of these rewards could be of help.

5. Relative to transportation of material, close accountability of transactions and of shipper/receiver differences is indicated. Close cooperation between licensee and local law enforcement authorities would also be useful in promoting outsider awareness of any improprieties.

Prevention

1. Screening is an effective control strategy, at least for preventing conspiracies to commit theft. This may be in disagreement with the conclusions of Section 4.1.5, above.

2. Clearances can reduce the likelihood of infiltration by terrorist and criminal elements. They can also reduce the probability that persons who misrepresent their histories, persons with a history of criminal or pathological behavior, or those susceptible to coercion or blackmail will be hired.

3. A behavioral observation program could be useful if a baseline of behavior for each employee is established at hiring time, if supervisory personnel are properly trained in this sort of observation, and if the program's criteria are applied equitably and unambiguously.

4. Psychological assessments could be of some use but are dangerous in terms of possible misuse and potential demoralizing effect on the work force.

5. The use of all of the above four techniques cannot substitute for "strict internal procedural controls."

6. Useful activities by the management of nuclear facilities would include: a) maintenance of a good rapport with the workforce; b) support and help for the security division; and c) encouragement of a healthy awareness among employees regarding safeguards against the insider threat.

7. Frequent internal inspections are the most effective technique to guard against successful internal storage.

8. A "dynamic and multifaceted program" is the best posture against the insider threat in the nuclear industry.

4.1.11 Stress and Duress Detection for NRC-Licensed Facilities: A Constitutional and Regulatory Analysis, John N. O'Brien, Brookhaven National Laboratory, NUREG/CR-1032, Sept. 1979

This report is a companion report to NUREG/CR-1031 (Section 4.1.4, above) which examined the physical and technical aspects of remote methods for establishing fitness-for-duty by stress detection and the well-being of

patrolling guards by duress sensors. This report analyzes administrative and legal problems associated with implementation of these systems.

Legal requirements for access control at licensed facilities are described and likely legal challenges analyzed. Issues covered are: 1) extension of public employee rights to licensee employees, 2) search and seizure, 3) general personal search laws, 4) self-incrimination, 5) right to privacy, 6) tortious intrusion, and 7) analogies to the FAA antihijacking program. Methods of stress detection examined in light of these issues are 1) voice stress analysis, 2) skin secretions, and 3) biophysical monitoring.

Conclusions drawn concerning duress detection center around the consideration that guards who are "wired" to the central alarm station should be subject to monitoring aimed mainly at seeking an indication of duress. The use of duress monitors may have a detrimental effect if used to "check up" on safeguards personnel and their continuous activities.

Appendices included contain discussions of Equal Opportunity law and union concerns in addition to a detailed discussion of each legel are cited above. No recommendations for further research are made.

4.1.12 Reactor Facility Threat and Tactical Response Procedures, J.J. Cadwell et al., Brookhaven National Laboratory, Oct. 1979

The purpose of this report is to provide recommendations to NRC licensees of nuclear power plants for the guard force initial reaction to alarms, for the threat analysis, and for the guard mobilization and tactical response to a threat. Specific procedures are given for each of the 32 representative alarm postulated in the report.

The initial reactions recommended consist of combinations of circuit inquiry of alarm electronics to check operability, CCTV monitoring, sending a guard to inspect and assess the alarm, query of redundant alarms, waiting on-alert for the next alarm, and requesting visual observation from a guard already in place.

Each alarm was classified according to the degree of seriousness as Class A (clearly a threat of substantial magnitude), Class B (clearly a threat), Class C (real possibility of a threat - degree unknown), and Class D (potentially a threat - likelihood low). The 13 alarms in Classes A and B are considered alarms credible on their face such that no threat assessment is required before guard mobilization and tactical response begins. However, as a parallel activity while the mobilization and tactical response is taking place, an alarm assessment and threat level determination technique is recommended. This means that threat analysis techniques are given for all 32 alarms, even though 13 alarms are considered powerful enough to cause immediate guard mobilization without waiting for a threat level determination. The technique recommended avoids the procedure of calling for maximum effort by the entire guard force for each type of alarm every time an alarm is sounded. A list of information required for the security supervisor's threat analysis is given for each alarm. This list includes techniques for obtaining this information, such as "view the intruder while a guard is held in reserve out of view of the

intruder" and typical information to obtain such as number of intruders, ages, arms, demeanor, direction of travel, and so on.

Once a threat is confirmed, the nature of the threat is used to dictate a guard mobilization and tactical response. Guard response to intruders is developed by considering the regulatory requirements, the legal restraints, and the techniques which the guards may use to respond to intrusions. Guard actions necessary to protect the facility against sabotage are also developed. General recommendations and schematic diagrams are given for the seven sample tactical responses. Response scenarios are covered comprehensively and discussed extensively for each alarm.

Some methods of surveying barriers are provided in Appendix B. Recommended barrier-survey methods consist of combinations of guard visual inspection, CCTV, and passive alarms. The primary recommendations are that guards on barrier patrol not be given other duties which would degrade the barrier patrol and that these patrols be at random times.

4.1.13 The White-Collar Challenge to Nuclear Safeguards, Herbert Edelhertz and Marilyn Walsh, Lexington, Mass., 1978.

The authors start from the beginning in assessing the white-collar threat to the commercial nuclear energy industry. The first obstacle is the inapplicability of empirical analysis relied upon so heavily in other contexts of nuclear regulation. The dependence of both the probability of failure and the consequences on deliberate human action combined with the questionable availability of basic data concerning the effectiveness of specific safeguards systems dilutes the value of such analysis.

Instead, the study uses the descriptive method in an exhaustively examination of the concept of white-collar crime, aiming at pinpointing potential safeguards vulnerabilities rather than ferreting out problem areas in current regulations. The approach taken is to integrate the body of knowledge developed in the area of white-collar crime with nuclear regulation. Particular vulnerabilities of nuclear facilities to criminal activities by management personnel in those facilities are not specifically examined in this study.

The approach, first, gives a general description of the accepted definitions and background of white-collar crime as it is understood today. The operating characteristics of the white-collar criminal are discussed in detail using recent studies on the general topic to form an integrated and workable concept of white-collar crime. Then the book sets out to develop, through general scenarios, the concept of crime in the nuclear energy industry. The motivations and opportunities for nuclear theft are examined, but only in a general way. Finally, the general aspects of nuclear safeguards regulation which may be applicable to coping with the threat of white-collar crime are scrutinized to reveal how safeguards research should be shaped to deal most efficiently with the problem.

The study makes several important points. First, the existence of a market for illicitly obtained nuclear materials may foster an impetus for nuclear white-collar crime which does not exist currently. The authors maintain that increased worldwide proliferation of nuclear energy along with increasing

constraints on legitimate markets will undoubedly foster such a market. Secondly, safeguards threats have, up to now, received selective attention in an arbitrary manner. In fact, there are strong arguments for suggesting that current safeguards regulation is off base, considering past experience. Much attention is given to the overt or terrorist threats to nuclear facilities and materials, while covert threats receive relatively little regulatory attention. However, no armed adversary assault has been made to date and it is not possible to state with complete confidence how likely and/or imminent such an assault may be. While the same argument can be made concerning white-collar crime, it is important to note that no one can state with complete confidence that a white-collar adversary action has not taken place to date.

This book is useful for those initiating regulatory research in this urgent and important area of nuclear safeguards. It must be borne in mind by the safeguards professional that the book is not meant to suggest safeguards measures but rather to construct a workable framework for examining this difficult problem through the discipline of white-collar crime research.

4.2 Summary and Analysis of Literature

A preliminary reduction of recommendations found in the literature to matrix form is presented in Table 8. Table 9 contains the derived ranking. The same method used in the analysis of comments was used except that ratings where compiled by individual reviewers with an independent validity check.

Table 8

Partial Analysis of Government Literature

	A	A2	A3	A4	A5	B1	B2	B3	B4	B5	C1	C2	C3	C4	D1	D2	D3	D4	D5
NUREG-0768 People-Related	0	0	0	0	0	0	+2	+2	0	0	0	+2	0	0	0	0	0	0	+1
NUREG/CR-2076	0	+2	+2	+2	0	0	0	0	0	+2	0	0	0	0	0	0	0	0	0
NUREG/CR-1031	0	0	0	-1	0	0	0	0	0	0	0	0	0	0	0	0	+2	0	0
B-HARC-411-018	0	+2	+2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NUREG/CR-2643	0	0	0	0	0	0	0	+2	0	0	0	0	0	0	0	+2	+2	0	+2
NUREG/CR-1234	0	0	0	0	0	0	0	0	0	+1	0	0	0	0	0	0	0	0	0
EPRI-NR-2355	0	0	0	0	0	0	0	0	0	0	0	+2	0	0	+2	+2	+2	+2	+2
NUREG-0703	0	+1	+2	0	+1	0	0	+1	+2	0	+2	0	+2	0	0	0	0	0	0
SAND-77-1916C	0	0	0	0	0	0	0	+2	0	0	0	0	0	0	0	0	0	0	0
NUREG/CR-1032	0	0	0	0	0	0	0	+1	+2	0	0	0	0	0	0	0	+2	0	0
BNL-NUREG/24850	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
NUREG/CR-2217	0	0	+2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
"White Collar Challenge..."	0	+2	+2	+2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Scale

+2
+1
0 Neutral or unmentioned
-1
-2

Table 9

Importance Ranking of Human Factors Issues in Nuclear Power Plant Safeguards Derived from Literature

	Issue	Weight	% of Total Weight
1.	Trustworthiness (A.3)	10	14
	Commuications Equipment (D.3)	10	14
3.	Shiftwork/Rotation (B.3)	8	11
4.	Behavioral Observation (A.2)	7	10
5.	False Alarms (D.5)	5	7
6.	Attitude (B.4)	4	5
	Contigency Plans (C.1)	4	5
	Use of Force (C.2)	4	5
	Maintenance (D.2)	4	5
10.	Fitness-for-duty (A.4)	3	4
	Instruction and Training (B.5)	3	4
	CAS/SAS Design (D.1)	3	4
	Environmental Influences (D.4)	3	4
14.	Organizational Communications (B.2)	2	3
	Staff Coordination (C.3)	2	3
15.	Human Reliability (A.5)	1	1
16.	Two-man Rule (A.1)	0	0
	Vigilance (B.1)	0	0
	Performance Evaluation (C.4)	0	0
		73	

5.0 Conclusions and Summary

This chapter has arrived at three sets of data, summarized in tables 4, 6, and 9. Each Table displays a ranking of the human factors issues developed as part of this task. The ranking is in terms of need for research and development with a view to usefulness for safeguards at nuclear power plants. Each table of priority ranking arises from a different source; each has been produced with its own set of biases. The expert opinions are shaped, to some degree, by the initial set of human factors issues submitted as part of the letter of solicitation (see Appendix B); it is true that some additional issues were drawn out of the expert responses (since those arose spontaneously they should receive more weight--they are indicated by asterisk in Table 4), but most were originally suggested in the solicitation. There is also a bias arising from the natural tendency of experts to emphasize those areas in which they are working. This effect should, however, be canceled if a large number (18) of opinions are used.

In analyzing the other two sources of information, the set of issues assembled by the authors and supplemented by the expert responses was used as a framework for classification. The classification of actual history - past safeguards-related events - has its own particular problems. In this case, it is not always easy to assign areas of deficiency for a given incident. As an example, an event may indicate poor security force response, but it could be unclear whether such a problem shows failures in performance evaluation, training and qualification, man-machine interface, other factors, or a combination thereof. This difficulty in assigning events to particular human factors may be compensated to a degree by reasoned judgment on the part of the raters. Nevertheless, a bias against some factors for which events are difficult to classify may exist.

For this part of an overall ranking only intrusion events are used because they cover the broadest range of events reported and generally indicate a manifestation of safeguards actions.

In a literature search a different sort of bias may occur. Researchers will generally emphasize the areas in which they themselves are working. The overall result will be a set of discovered human factors problems which represent an aggregate of current research directions. These may or may not be the directions to support most heavily in the future.

It is hoped that, to some degree, adding the fractional occurrences for each issue from each of the three techniques will tend to reduce the biases inherent in each technique alone. The combined rankings are presented in Table 10a. First, the straight, nonweighted approach is given for combining data. As a type of sensitivity test, we show, in Tables 10b, c, and d the results obtained by weighting experts, then events, and finally literature by a factor of 2. Stressing one of the techniques at the expense of the others does not radically change rankings (with a few exceptions). It is seen, for example, that B.5 (Instruction, Training, and Selection), C.1 (Format and Wording of Contingency Plans) and A.3 (Trustworthiness) remain highly ranked.

From these analysis an action plan will be developed from which an overall, long-term research plan can be established.

Table 10a

COMBINED RANKING

	Issue	Combined Weight
1.	A3 - Trustworthiness	28
2.	D3 - Communications Equipment	27
3.	B5 - Instruction, Training, Selection	26
4.	C1 - Format of Contingency Plans	26
5.	A5 - Human Reliability	21
6.	B4 - Corporate Attitude	19
7.	D1 - CAS/SAS	17
8.	A2 - Behaviorial Observation	15
	B3 - Rotation/Manpower/Shiftwork	15
	C3 - Staff Coordination	15

Table 10b

Combined Ranking - Expert Comments Weighted by Factor 2

	Issue	Combined Weight
1.	B5 - Instruction, Training, Selection	37
2.	A3 - Trustworthiness	34
	C1 - Format of Contingency Plans	34
4.	D3 - Communications Equipment	30
5.	A5 - Human Reliability	27
	B4 - Corporate Attitude	27
7.	D1 - CAS/SAS	23
8.	C3 - Staff Coordination	21
9.	A2 - Behavioral Observation	20
10.	B2 - Communication within Corporation	18
11.	B3 - Rotation/Manpower/Shiftwork	18

Table 10c

Combined Ranking - Events Weighted by Factor 2

	Issue	Combined Weight
1.	C1 - Format of Contingency Plans	39
2.	B5 - Instruction, Training, Selection	37
	D3 - Communications Equipment	37
4.	A3 - Trustworthiness	36
5.	A5 - Human Reliability	35
6.	B4 - Corporate Attitude	25
7.	D1 - CAS/SAS	24
8.	B1 - Boredom and Vigilance	23
9.	C3 - Staff Coordination	21
10.	D4 - Environmental Influence	19

Table 10d

Combined Ranking - Literature Weighted by Factor 2

	Issue	Combined Weight
1.	A3 - Trustworthiness	42
2.	D3 - Communications Equipment	42
3.	C1 - Format of Contingency Plans	31
4.	B5 - Instruction, Training, Selection	40
5.	B3 - Rotation/Manpower/Shiftwork	26
6.	A2 - Behavioral Observation	25
7.	B4 - Corporate Attitude	24
8.	A5 - Human Reliability	22
9.	D1 - CAS/SAS	21
10.	C3 - Staff Coordination	18

Appendix A

Human Factors in Material Control and Accounting

- Manual Data Entry
- Estimation Techniques
- Sampling Procedures
- Calibration Procedures
- Personnel Systems
- Licensee "Self Test"

Appendix B

Solicitation Letter and Discussion Paper

BROOKHAVEN NATIONAL LABORATORY
ASSOCIATED UNIVERSITIES, INC.
Upton, Long Island, New York 11973
(516) 282
FTS 666 3698

October 25, 1982

Dear

As you know, there has been a great deal of interest how human factors affect nuclear power plant operations since the Three Mile Island (TMI) accident in March of 1979. During the last two years, the Nuclear Regulatory Commission (NRC) staff has been reorganized to accommodate this surge of interest by establishing the Division of Human Factors Safety in the Office of Nuclear Reactor Regulation and the Human Factors Branch in the Office of Nuclear Regulatory Research (RES). Both of these new entities have established programs designed to integrate human factors research and findings with operational regulations and guidance.

In 1980, the Human Factors Society (HFS) was contracted by the Human Factors Branch to develop a long-term research plan for NRC. In August 1982 their report was published (NUREG/CR-2833) including a critique of current human factors research programs and recommendations for improving NRC staffing in key positions. The HFS report specifically excluded safeguards and security problems.

Also this past August the Safeguards Branch of RES contracted Brookhaven National Laboratory to produce a long-term (5-7 year) plan for conducting research on human factors in nuclear power plant safeguards. We are currently in the process of developing that plan.

This study of human factors in safeguards does not directly benefit from the multitude of information developed on operational safety and human factors which came as a result of the TMI accident. Instead, an initial complication of safeguards/human factors issues must be developed. The objective of the overall program is to develop and prioritize 10-15 research programs which NRC can effectively undertake. As a result, the initial effort of identifying and generally assessing safeguards/human factors issues in the power plant context is important.

Enclosed is a discussion on human factors/safeguards issues which may be appropriate for NRC to address in research. The importance of each issue is being weighed at this stage in the project. Their amenability to meaningful research and practicality of the expected results will be considered in the next stage. It is, however, very important not to overlook critical issues and equally important not to overemphasize issues of minor significance.

As a member of the nuclear energy community, any comments you have regarding this discussion would be very helpful. Keep in mind that this study does not consider safeguards for transportation or fuel cycle facilities, although comments on these activities in terms of human factors will certainly be appreciated.

Specific questions about the enclosed discussion are:

1) Are there human factors/safeguards issues which are not addressed or addressed inadequately?

2) Are any of the issues covered unimportant in your opinion?

3) Are there studies addressing these issues which can be brought to bear in developing a long-term research plan (i.e., can we avoid reinventing the wheel?)

4) What is the relative importance of these issues with respect to each other?

5) Who else should have input to this report now or at subsequent stages?

6) Are any of these issues impractical to study or would they require corrective measures unacceptable to Government or industry?

7) Can any of these issues be "clustered" in order to more effectively study them?

Comments should be sent to me at Brookhaven. Thank you for your time and interest. Your input is appreciated and will be used in this study.

Sincerely,

John N. O'Brien, Associate Scientist
Engineering Analysis and Human
Factors Group

JNO'B:jf
enclosure

Human Factors in Nuclear Power Plant Safeguards

The human factors aspects of operational safety in nuclear power plants have been extensively examined during the past 4 years. No such activity has yet been undertaken in safeguards. Brookhaven National Laboratory (BNL) has been contracted by the Nuclear Regulatory Commission (NRC) to develop a 5-7 year research plan for integrating human factors work into research and development in safeguards regulation. This program is sponsored by the Safeguards Branch of The Office of Nuclear Regulatory Research.

The first task involves identification of "safeguards-related facilities, equipment and activities which are impacted by or asociated with human factors, and asess whether there is a need for research in any of these areas." The task goes on to require a survey of "appropriate NRC and industry staff and organizations, investigating reports of safeguard accident/events, and other relevant documents and reports" in order to complete that task. This program is aimed only at power plants and excludes fuel cycle facilities and transportation of nuclear materials.

As a first step toward completion of this task, this description of safeguards requirements and activities will be used. The Office of Nuclear Materials Safety and Safeguards (NMSS) has supplied a list of human factors safeguards issues developed inernally by NMSS staff. That list was used to develop this docuent in addition to suggestions from BNL and NRC staff.

This discussion is aimed mainly at the physical security aspects of safeguards at nuclear power plants. By and large, material control and accounting activities are limited at power plants because the only nuclear materials present are the fuel and a few items such as the isotopic neutron source for start-up which is consumed during the start-up. New fuel cannot be used in any way as an explosive or toxicological threat. Spent fuel contains some plutonium which could be reprocessed to produce fissionable plutonium which can be used both for explosives and as a toxin. However, spent fuel is highly radioactive and very difficult to move so that the act of clandestinely reprocessing it is not a credible threat. In fact, the most serious safeguards threat facing a utility licensee is that of sabotage and not theft or diversion of nuclear materials.

I. PROTECTION OF NUCLEAR POWER PLANTS FROM SABOTAGE

The Code of Federal Regulations contains requirements for safeguarding nuclear powerplants. In particular, 10 CFR 73.55 details NRC requirements. These requirements are outlined below. There are several applicable regulatory guides and proposed rules. In addition, a revised ANSI/ANS standard for security for nuclear power plant has been issued (ANSI/ANS-3.3-1982).

The physical protection in place at power plants is designed to protect against the design basis threat of radiological sabotage as described in 10 CFR 73.1(a) which states:

> (1) Radiological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment: (A) well-trained

(including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and (ii) An internal threat of an insider, including an employee (in any position).

The definitions of the terms used in this requirement are given in 10 CFR 73.2, and should be referred to if any are unfamiliar.

The standard of administrative review for determining adequacy of safeguards is similar to that used for safety determinations; namely that the licensee "provide high assurance that activities involving special nuclear materials are not inimical to the common defense and security, and do not constitute an unreasoanble risk to the public health and safety."

The regulations require licensees to establish a "security organization" which may be a contract organization. However, the licensee is always ultimately responsible for site security, all records and reports must be available to NRC, and the security organization must demonstrate its ability to carry out the provisions of the licensee's security plans. At least one full-time member of the security organization with authority to direct security activities must be on site at all times. A licensee management system is required "to provide for the development, revision, implementation, and enforcement of security procedures." Security procedures, which are required for an operating license, document the structure of the security organization and detail the duties of guards (security officers), watchmen, and other responsible individuals.

The licensee is not permitted to hire individuals for its security force unless they are qualified under the "general criteria for security personnel" in 10 CFR 73, Appendix B. These criteria include employment suitability and qualification (education, criminal records, age, prior experience, physical fitness, vision, hearing, diseases, addictions, mental alertness, emotional stability, behavioral observation, and requalification), general training (security knowledge including tactics, knowledge of facility and plans, and over ninety other categories of knowledge) and weapons training and qualification. Two current regulatory activities have direct bearing on these requirements. A new rule on "fitness for duty" has been proposed (covered later) and a rule on "trustworthiness" is currently under internal review by the NRC staff and not presently available for comment. Each licensee security employee must be requalified every 12 months under current regulations.

The licensee is required to establish physical barriers and defensible spaces around vital equipment. These take the form of a "vital area" within a "protected area" surrounded by an "isolation zone." Vital equipment is defined as:

"any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public public health and safety following such failure, destruction or release are also considered to be vital."

Vital equipment, which is so designated according to a method, is to be located only in a vital area which in turn is within a protected area. The issue of what constitutes vital equipment may not be in step with the current trend in operational safety to reclassify "non-safety" equipment as "important to safety" when it has been shown to impact risk. Since physical barriers surround vital and protected areas, access to vital equipment requires passage through at least two barriers. An isolation zone must be maintained around the perimeter of any protected area such that the activities of people on either side of the perimeter can be observed in the event of an intrusion. In addition, the reactor control room must be subject to positive access control and completely bullet proof.

The licensee is required to control all points of access into any protected area. Entrants are to be searched for firearms, explosives, and incendiary devices. The security officer ultimately in charge of controlling access through any access control point must be isolated within a locked, bullet-resisting structure. All packages and vehicles entering a protected area must also be searched. This search can be done by remote means (e.g., magneto-meter) or physical means (e.g., pat-down search). Licensee vehicles are to be limited in their use and are to remain in the protected area except for operational, maintenance, repair, security, and emergency purposes.

NRC has proposed rules which would require the mandatory use of remote search equipment for employee searches and pat-down searches of all visitors (45 Fed. Reg. 79492, Dec. 1, 1980). Regular employees would not need to be subject to routine pat-down searches.

A numbered picture-badge system is required for all individuals authorized for unescorted access to protected areas. For all others, an escort must be used and a badge indicating the need for an escort msut be worn by the unauthorized individual at all times.

Access to vital areas is required to be highly restricted. For instance, access for the purpose of general familiarization and other non-work related activities cannot be authorized. All unoccupied vital areas must be locked and equipped with intrusion alarms. Access hatches and doors to the reactor containment are to be alarmed and equipped with locks of "substantial construction to offer penetration resistance and impede both surreptitious and forced entry." All keys, locks, combinations, and related equipment are to be controlled and changed whenever there is any evidence of compromise or termination of an employee under adverse circumstances. There may have been very little consideration of human factors such as moral, efficiency, attitudes, and operations/safety coordiation in arriving at these requirements.

NRC has proposed rules (45 Fed. Reg. 15937, March 12, 1980) which would require that access to vital areas be allowed to authorized personnel only for a

specific task to be undertaken. If any authorized individual does not need to enter a vital area, then access would not be allowed. Current licensee practice is to grant blanket access authorizations to individuals with limited control on specific need for access.

The licensee is required to maintain a "continuously manned central alarm station (CAS) located within the protected area and.., at least one other continuously manned (secondary alarm) station (SAS)." The interior of the CAS cannot be visible from the perimeter of the protected area and is not to be used for any operational activities which could potentially interfere with alarm response functions. All alarms must be self-checking and indicate the type and location of any break or malfunction. The CAS is, itself, considered a vital area.

Each security officer is required to carry communications equipment capable of continuous communication with the CAS and SAS which, in turn, are required to be capable of telephone and radio communciation with other personnel and local law enforcement agencies. All communications equipment must be operable from independent power sources. The reliability of communcations equipment has been questioned by several sources including EPRI (EPRI NP-1567).

The licensee is required to establish test and maintenance procedures for all security related equipment. For example, each intrusion alarm must be tested a minimum of once every seven days and all communciations equipment tested at the beginning of every shift. Redundancy in security equipment is required:

> "The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures."

In addition, it is required that all alarms be maintained in operable conditions at all times. While this is not possible, it indicates that all maintenance procedures be of high integrity and repair activities carried out immediately. The revised ANSI/ANS security standard suggests that complete security equipment maintenance records should be kept for five years.

A annual internal review of all security procedures, testing and maintenance programs, local law enforcement response plans, and the effectiveness of the physical protection system is required. The individuals conducting the review must be independent of both management and security supervision. The review itself must be documented and delivered to licensee management at least one level higher than that having day-to-day responsibility for plant operations. These reviews are to be kept available for NRC inspection for a minimum of five years.

The licensee is required to be capable of minimum response capability as outlined in the regulations. "Safeguards contingency plans" are required and the necessary contents are outlined in 10 CFR 73, Appendix C. The licensee must also establish and fully document liaison with local law enforcement agencies. At least ten armed, trained personnel must be onsite at all times including at least five uniformed security officers. Some licensees have trained and armed

non-security (operational) personnel for the purpose of meeting this requirement while minimizing the number of uniformed security officers needed.

If an intrusion does occur the licensee is required to determine the existence of the threat, assess its extent, and neutralize it if necessary. Security officers are required to "interpose themselves between vital areas and... any adversary attempting entry for the purpose of radiological sabotage..." and simultaneously inform the local law enforcement agencies of the threat and request assistance. The level of force authorized by NRC to prevent radiological sabotage is:

> "force sufficient to counter the force directed at him (the responding officer) including the use of deadly force when the guard or other armed response person has a reasonable belief it is necessary in self-defense or in the defense of others.

The ANSI/ANS security standard suggests that all policies on the use of force be consistent with all federal, state and local laws. In some states, because of the "retreat requirement" in the face of deadly force, interposition may not be allowable under state law.

The CAS is required to have remote means of detection and assessment of threats, such as closed circuit (CC) TV, in order to minimize security personnel exposure to dangerous threats.

II. HUMAN FACTORS AND SAFEGUARDS

The security organization is charged with detering, detecting, and defeating any adversary action against the plant. The perceived adversary threats include external (e.g., armed terrorists), internal (e.g., authorized insider) and combinations (e.g., authorized insiders subject to terrorist extortion). Security considerations surrounding the transportation and processing of nuclear materials are not covered under the current work scope, but this study should seek to accommodate their eventual inclusion.

Human factors problems in security differ to a degree from operational safety human factors problems. First, operational safety assumes that personnel will respond only in ways intended to return the plant to safe operating conditions. The range of human failure is broader for security since "intentional failure" must be considered. In other words, error is not the only case of human failure in safeguards, so the study of human factors in security is not simply an analysis of making mistakes and assessing their effects on risk.

Second, the consequence of a core melt (the top end operational safety event) is an additional step away from a safeguards event for the purpose of risk analysis. In operational safety it is less difficult to link human actions with the top event than in safeguards where an event may or may not lead to an operational safety event. It is probably not possible to defensibly place most safeguards events into the typical fault tree much less assign any type of probability for their influence on the integrity of the reactor core. While risk analysis is not useful some reliability methods may be of use, however.

Third, there has been a significant lack of data on safeguards events due to both poor collection techniques and the infrequency of events. The Licensee Event Reporting system has been deficient in reporting human errors in safeguards activities. Inspection and enforcement records are more instructive, but still generally deficient for any rigorous analysis. In addition, the events which do infrequently occur tend to be varied to the extent that particular types of events or trends do not readily surface.

Fourth, the man-machine interface in safeguards is limited compared to that of operational safety. A failure of all safeguards related equipment at a reactor site would not necessarily result in an accident of any kind. Safeguards equipment is mainly sampling and measuring devices for material control and accounting (MCA) and physical security equipment such as barriers and alarms for protection of the plant from adversaries. At a reactor site MCA activities amount to keeping track of fresh and spent fuel in the storage areas and reactor core. In addition, radioactive materials, such as the start-up source, must be accounted for and secured. There are no materials on site at a nuclear power reactor which can be readily used to fabricate an explosive or dispersal (toxicological) device. Physical security equipment includes alarms, locks, closed circuit TVs, doorway monitors, card-key systems, and individual equipment and arms. A central alarm station (CAS) is far less complicated than a reactor control room, but more importantly, the CAS does not "control" anything. Rather, it "coordinates" the movements of security officers around the site. The "front line" of control is the individual officers themselves, not the "operators" in the CAS. A typical man-machine interface problem in safeguards occurs when an alarm malfunctions or a method of circumventing a security system is discovered. The failure of a safeguards "machine" usually means only that a method for monitoring the integrity of the site is compromised. It is less likely in safeguards than operations safety that a signal in the CAS could be misinterpreted to the degree that it causes an action which directly threatens the safety of the plant. However, CAS and SAS design can effect the performance of the security force if not designed with sound human factors design practices in mind. For instance, a high false alarm rate could cause CAS personnel to disregard what may be an actual intrusion.

The following categories of safeguards human factors issues are derived mainly from the list provided to RES by NMSS for this study. Each item is briefly described.

A. The Insider Threat

It seems generally accepted in the safeguards field that the threat posed by authorized individuals (insiders) who turn bad and sabotage the facility is more serious than that posed by outside intruders. In fact, the insider threat has been and is a subject of debate within the safeguards community. This was not the case until the last several years so that most safeguards requirements are still aimed at outside intruders. The typical response to the insider threat has been similar to those measures aimed at intruders, for example, preventing access to authorize individuals unless a guard is present to unlock the area. Several studies of the insider issue have been made. However, these studies have generally viewed the insider as in intruder so solutions generally stress obstructing the insider rather than dealing with the causes or prevention of the

ma'evolence. Several specific safeguards regulatory issues stem from the insider threat.

1. Two-man Rule - In early safeguards regulatory development most emphasis was put on MCA and very little concern was paid to physical security, which was left to the licensees to conduct as normal industrial security. In order to optimize the performance of MCA workers they were sometimes required to work in pairs, both to assure the quality of the measurements taken and assure that materials which were to be transferred from one inventory area to another were, in fact, transferred. When the insider was recognized as a sabotage threat it was assumed that people in pairs would be less likely to take malevolent actions than individuals by themselves. As a result of this unproven assumption, the two-man rule was adopted for some physical security purposes. The usefulness of the two-man rule is currently a subject of discussion in the safeguards community. It is noteworthy that the presence of two individuals is relied on in the banking industry to foster honesty.

2. Behavioral Observation Programs - It has been widely recognized that good people can turn bad. The decision to sabotage a facility can be made for various reasons, of which many can manifest after a period of employment (e.g., disgrunted by promotion passover, marital or personal stress, psychosis, blackmail). In order to identify employees who may potentially become threats, NRC has considered requiring licensees to establish behavioral observation programs. The optimal mix of relevant considerations such as methodological validity, civil liberties concerns, and effects on employee attitudes and motivation has not been systematically examined.

3. Trustworthiness - All employees in sensitive positions must undergo some form of security check. At this time, licensees are required to apply ANSI/ANS standard 3.3 (or its equivalent) which deals with the fitness of employees. The ANSI/ANS standard is fairly vague containing only a requirement for written personality tests administered by licensed psychologists so these programs are not uniform. At times licensees have been unable to acquire information on applicants about their criminal records or, in some cases, even past employment. NRC has been unable to require federal security clearances for plant personnel because, among other things, nuclear power plant security it is not considered a matter of national security "under the law". In order to compel standard federal security clearances, the information to be protected must concern a matter which could threaten the national security (i.e., the existence of the Federal Government). The NRC staff is currently reviewing a proposed rule on trustworthiness they intend to send to the commission in the next few months. Once this proposed rule is made available, it can be analyzed for human factors significance. There is a paucity of literature or research on assessing the trustworthiness of individuals.

4. Fitness for Duty - The number of drug-related security incidents at nuclear power plants has increased substantially during the past three years. As a result, the NRC staff has developed a proposed rule (SECY-82-196) which would require NRC licensed utilities "to establish and implement adequate written procedures to assure that personnel with unescorted access to protected areas are not under the influence of drugs or alcohol or not otherwise unfit for duty." The term "otherwise unfit for duty" is meant to include fatigue, stress, illness, and temporary physical impairments. The actual constitution of such

a set of procedures would be left to the licensee, although NRC may choose to provide guidance in the form of NUREG documents or Regulatory Guides.

B. MANAGEMENT AND ORGANIZATION

Early safeguards regulation developed primarily from an MCA standpoint because physical security at a nuclear power plant was considered normal industrial security which should properly be left to the licensee. During the early 1970's, significant physical security requirements were added to those for MCA. Physical security requirements underwent a further "upgrade" in the late 1970's and presently constitute the majority of safeguards requirements at nuclear reactors. This developmental pattern rarely included a comprehensive approach to nuclear power plant safeguards management, which was left mainly to security managers hired or contracted by the licensee. As a result, management techniques for power plant security have been derived largely from police, military, and industrial security sciences. The shortcomings of such techniques for civilian nuclear power plant protection have been dealt with by adjustment rather than any comprehensive approach. Several issues important to safeguard management have been suggested and they are described below.

1. Boredom Reduction - Vigilance - Safeguards personnel are mainly physical security oriented at a nuclear power plant. In the classic sense, the vigilance problem is similar in both safeguards and operational safety in that individuals must maintain attention focussed on detecting a rare event - an abnormality at the facility. An operator must maintain vigilance over indicators of many plant conditions, as well as being aware of annunciators. At the CAS, a security officer may have to maintain vigilance over many indicators of site security (e.g., CCTV), as well as annunciators (e.g., perimeter alarms). An officer on patrol must maintain a sufficient level of concentration throughout his rounds to notice veiled threats. Vigiliance may be a more important problem in safeguards however, since, in a relative sense, events are far less frequent and the preceived likelihood and consequences of an event are often far less than in operational safety.

2. Communication - The type of communciation channels used within the overall operating organization are very important in dictating the ultimate safety of plant operation. The security organization is administratively separate from the overall organization, but there must be good communication between and within suborganizations in spite of the administrative isolation of the security organization. In the nuclear power plant context many suborganizations, including health-physics, maintenance, operation, quality control, and management must effectively communicate with the security suborganization to minimize risk of operation.

3. Rotation/Shiftwork/Manpower - These are classic management issues in any organizational endeavor. In most contexts, these issues are settled according to productivity measures and constrained by labor laws and practices. Performance in the context of nuclear power plant operation, while not measurable strictly in terms of productivity, can be assessed using techniques such as surrogate variable measurement. There has been some work done in the operational safety field dealing with these issues, but this work to date has not been very instructive. The literature from the management discipline of organizational

behavior contains many studies on these issues, but it has rarely been used by safeguards or operational authorities.

4. Corporate Attitude - Truly good security can only occur where the entire organization at a plant views it as very important. For instance, the general lack of any financial incentive for security upgrading may tend to lessen the overall commitment of corporate management toward security. A lack of commitment by upper management can manifest itself in unexpected, but simple ways. For example, if security is a high priority within the overall organization, then all personnel will be aware to look for the "hole-in-the-fence". Otherwise, a "that's security's job" type of organizational attitude may emerge making good site security far more difficult, if not impossible, to attain. Every individual from the highest corporate officer to part-time custodians must be highly and sincerely committed to good security for optimal plant protection. Methods for dealing with this problem have been elusive because of NRC resistance to regulating the management aspects of plant security and operation. However, because of the general recognition that management deficiencies contributed to the severity of the TMI accident, that resistance seems to be generally breaking down.

5. Instruction - The requirements for assessing and training safeguards personnel in order to qualify for employment under NRC regulations are loosely outlined in the 10 CFR Part 73, Appendix B, and in Reg. Guide 1.8. These requirements, which include a wide range of concerns including physical and mental suitability, weapons qualification, and security expertise, have been developed in a generally ad hoc manner as needs seemed to dictate. No general, comprehensive assessment of these requirements has been undertaken, and evidence has surfaced (e.g. drug use, sleeping on duty) that security personnel performance has not been wholly acceptable. This is not to indict security personnel generally, but rather to question the selection and qualification techniques currently used.

C. RESPONSE CAPABILITIES

As in operational safety, safeguards regulation is aimed at assuring as effective response to events which do occur, as well as avoiding them to begin with. If an intruder does activate an alarm, the proper CAS response is similar to that of a control room operator. The difference is that the actual manifestation of the response is usually human instead of mechanical. For instance, a security officer is dispatched to visually inspect the alarmed area instead of a train of valves being realigned. This adds another level to the interaction of humans with the integrity of the plant. It also provides a very good level of feedback from the "system" since security officers can answer questions about the status of the system by observation - valves cannot articulate a description of the situation for the control room. This occasionally necessitates complex control room diagnostics not generally necessary in a security response.

1. Format and Wording of Contingency Plans - All nuclear power plant licensees are required to have contingency plans to deal with potential security threats. Guidance for preparing contingency plans is given in 10 CFR 73.55, Appendix C. The goals of these plans are: 1) to organize a licensee response, 2) provide for predetermined, structured responses, 3) insure integration in an overall response, and 4) achieve a measurable response capability. An accept-

able contingency plan must contain 1) predetermined decisions and actions, identification of data, criteria, procedure, and mechanisms necessary to effect decisions and actions, and 2) designation of individuals accountable for response decisions. Licensees submit contingency plans which are then classified and retained by the security organization and NRC. When a security event occurs at a site (e.g., an alarm goes off and an intruder is found), NRC compares the actual licensee response which must be reported to NRC by the licensee to that contained in the contingency plan. If they are inconsistent, punitive or corrective action may be taken. It is possible that the format and wording of contingency plans could be improved in light of experience gained since contingency plan regulations have only been recently promulgatged. There is also a problem when the reality of a situation dictates that the security plan procedures may not be optimal or appropriate.

2. Self-Presevation and the Use of Deadly Force - When a security officer responds to an alarm or incident, it is always possible that he will enter a life-threatening situation. In an instant, an officer can be confronted with many contradictory objectives. For instance, if an officer were confronted with a hostile intruder, the officer may have to use force. The use of force puts an officer in great personal risk, but probably lowers the level of risk to the palnt. If deadly force is necessary (and it is not really clear in all situations when it is necessary of justifiable), then the officer may be risking his life. Self-preservation is the tendency for an officer under duress to maximize his own safety as opposed to that of the facility. This is a particularly sensitive area when considering the regulatory requirement for interposition of security officers between an armed adversary and the plant during an assault. The officer must also be wary of using deadly force because unjustified use of deadly force can result in subjecting the officer and the licensee to criminal and civil charges up to and including murder. The effects of the deadly force and self-preservation issues on security force performance are not well understood.

3. Coordination Between Operational and Security Staffs - Sabatoge of a nuclear power plant can take many forms and originate from many sources. As a result, it is not possible to postulate sufficiently detailed procedures for handling all possible security events. Instead of having extensive and detailed procedures, generic planning for security events is adjusted to specific situations by the officer in charge of security at the time of the incident. When a security breach occurs, it is important for the operational staff to be capable of dealing with potentially damaged equipment. This could be made significantly more difficult if an insider with operational knowledge were manipulating the situation to mislead the control room operators. Another problem area in staff coordination was demonstrated by the breakdown of security which occured during the Three Mile Island accident. At that time, access controls were not fully in force and officers were sometimes relegated to support functions. Lastly, if an all-out assault did take place and some safety systems were damaged, a high degree of communication, cooperation, and understanding would have to exist between all elements of the suborganizational staffs to keep the plant in a safe mode.

D. EQUIPMENT AND FACILITIES - THE MAN-MACHINE INTERFACE

Unlike the operational staff of a nuclear power plant the security staff does not maintain a highly dynamic electrical generating system. Instead the security staff monitors the site for any indication of a security breach. In order to deter, detect, and defeat potential adversaries many types of equipment are used. In a sense, however, security equipment usually substitutes for what could be purely human functions. For instance, alarms and CCTV substitute for the presence of officers to monitor an area, arms substitute for use of human force, doorway monitors substitute for pat-down searches of individuals, I.D. cards substitute for personal knowledge of authorized individuals, and card-keys substitute for a stationed officer at an access way. Most equipment functions in security can be taken over by security officers, but the number of officers and skill necessary can become excessive. As a result, security equipment is used mainly to increase the efficiency of the security force by freeing humans to serve those functions which cannot be reliably served by an equipment substitute. This, however, does not mean that man-equipment interfaces do not present potential for increased risks which are not necessary or could be improved on.

1. CAS/SAS Design - There is very little guidance available for licensees to design their central and secondary alarm stations (CAS and SAS). The level of performance required for alarms is dictated in 10 CFR 73.50 (GSA Interim Federal Specification W-A-00450B (GSA-FSS)), but beyond that licensees are relatively free to design their own alarms stations. There has been less attention paid to alarm station design than control room design, but the relative simplicity of the alarm station may allow a greater level of improvement if it is warranted. In addition, it is not clear that security personnal would be sufficiently competent to perform in an SAS if under duress. The CAS and SAS are not required to be similar.

2. Maintenance - it is impossible to presently assess the level and effect of down-time associated with security equipment, but there is reason to believe it is not insignificant. While licensees are required to have maintenance programs, with possible exception of examining internal security reviews there is no way of acquiring equipment reliability data. Maintenance of security equipment includes testing alarms, cleaning and repairing weapons, checking communciations equipment, and assuring the ready availability of personal equipment such as riot control gear. No comprehensive review of security equipment relaibility and maintenance has yet been undertaken by NRC. Perhaps such a review could capitalize and the development of the FRANTIC program which is designed to track equipment reliability.

3. Communications Equipment - At any reactor site, an on-site CAS is required along with a SAS in case the CAS is seized or otherwise compromised. At any time ten armed personnel are on duty performing various functions such as checking alarms and monitors, observing performance of operational activities (eg. fuel shipment arrivals) locking and unlocking vital areas, escorting guests and unauthorized workers, routine patrols, among others. Some armed, trained personnel may be operational employees. Sophisticated communication systems, both wire and wireless, are required by NRC. The major concern in designing regulatory requirements for communications abilities was to keep adversaries from

being capable of easily disabling communications. Secondary conerns were the ease of use of the system during an emergency and overall efficacy of the total system.

4. Environmental Influences on Security - The ultimate bottom line in site security is the capability of the security officers to physically carry out responses to threats. This capability can be influenced by environental factors such as illumination, noise, radiation, and physical terrain. It is important to recognized that a nuclear power reactor site is an industrial production site with all attendant activities. For instance, it is not unusual to find low-level waste contained in steel drums piled near the reactor, roped off and placarded for radioactivity. Will a security officer search among these drums for a suspected intruder despite the radiation warning? If an intruder is suspected to be in the turbine building the noise level may make apprehensive more difficult. If the terrain around the perimeter is not level it will require more effort to visually inspect the isolation zone. All of these factors contribute to the integrity of site security and their affects have not been comprehensively examined.

III. CONCLUSIONS

The types of human factors regulatory issues associated with safeguarding nuclear power plants are similar in some respects to operational safety human factors issues and very different in others. Where the gains made in operational safety research can be of use in resolving safeguards regulatory issues, the substance of that research should be made available to those regulating safeguards. This will require identification of relevant research and reformating it for safeguards needs. Where safeguards issues are sufficiently unique, other areas of human performance analysis, such as ascertaining the causes of personnel malevolence, will be appropriate for investigation.

The ultimate product of this study will be 10 to 15 project descriptions for research in safeguards related human factors areas. These project descriptions must be prioritized and include a statement of objectives, recommended research methodology, and anticipated products. The final report is due April 30, 1983.

CHAPTER 3

FEASIBILITY OF RESEARCH APPROACHES FOR EXAMINING HUMAN FACTORS AFFECTING NUCLEAR POWER PLANT SAFEGUARDS

John N. O'Brien and Anthony Fainberg

Table of Contents

Chapter 3

Table of Contents (Cont'd)

Chapter 3

Tables

CHAPTER 3

ABSTRACT

This chapter details an effort to assess the feasibility of conducting research on human factors which affect nuclear power plant safeguards. The prior chapter identified and ranked human factors issues in terms of their importance to safeguards. This chapter examines the same set of human factors issues identified in Chapter 2 in terms of research feasibility.

Section 1 describes the method used to assess the feasibility of research on various human factors issues. Each human factors issue is assigned index values according to the practicality, usefulness, and acceptibility of research in each area. Index values were assigned according to the criteria set forth in this section.

Section 2 is an analysis of each human factor including a background statement which details the state-of-affairs and state-of-knowledge about each human factor and the reasons for assignment of specific index values. These index values were then integrated to form a final ranking of human factors in terms of research feasibility.

Section 3 is an integration of research into groups according to common research approaches and other similar characteristics. Groupings are developed according to methodological perspectives in order to minimize resource requirements needed for study.

The results of this chapter will be integrated with the rankings of human factors in terms of importance to develop an integrated long-term research plan presented in Volume I to be considered by the Nuclear Regulatory Commission.

1.0. Introduction

1.1. Purpose

The purpose of this chapter is to determine and rank the feasibility of conducting research on each of the safeguards-related human factors identified in Chapter 2 which ranked the human factors presented in Table 1 by importance. The rankings which resulted are in Appendix B. They reflect a professional consensus on what human factors need to be addressed (and are therefore "important") in nuclear power plant safeguards, integrated with supporting analysis from actuarial data (i.e., reported events) and a review of relevant literature. The product of this chapter is a ranking of those same human factors ranked in Chapter 2 according to the feasibility of researching them. In addition, research approaches are grouped to minimize resource requirements by taking advantage of similar research methods. The two rankings, from Chapter 2 and from this chapter, will be integrated to formulate a set of prioritized human factors research projects in a long-term research plan.

1.2. Feasibility Ranking Method

There are three central considerations which must be examined in assessing the feasibility of researching human factors affecting nuclear power plant safeguards. These considerations are the 1) practicality, 2) usefulness and 3) acceptability of conducting research and employing the potential findings. Since different research approaches to the same research problem may entail different considerations, alternative approaches available must be included in the analysis as well.

A systematic analysis of these three considerations was conducted. A data matrix was developed for integrating these considerations (Table 3) and a final ranking in terms of the feasibility of researching these safeguards-related human factors was arrived at (Table 4).

In order to conduct this analysis specific attributes of practicality, usefulness, and acceptability were assigned index values of 1, 2, or 3. Each index is scaled to reflect higher feasibility with higher scores. As such research which is highly desirable would have an average score approaching 3. The assignment of values was made by reason and judgement as well as actual data when available. Because these values are best judgements, this approach is characterized as an "open-judgement" process rather than a rigorous empirical approach which was not considered feasible.

The index values which were assigned for each research approach considered for each human factor are cost, time required, data availability, equipment availability, regulatory need, risk reduction, and acceptability. Using this approach, analyses of the resulting data matrix can be made so as to vary weights given to the various attributes considered. In that way, if the reader has a particular perception of the relative importance of each attribute, an analysis can be easily performed by assigning weights. A summary of index values is presented in Table 2.

1.2.1. Research Approaches

Frequently a research problem can be approached using more than one research method. For instance, in some cases there are existing data which can be analyzed and applied to a problem. However, those data may not be as applicable as others developed in an experiment designed to directly model the problem of interest. In some cases studies of analogous problems have been conducted in non-nuclear contexts and academic studies. In that case, results can be extrapolated to the research problem of interest. Other times, more research must be done to better formulate the problem. Descriptions of these research approaches are given in the following section.

1.2.1.1. Experimentation

An experiment can be characterized as a means of collecting primary (i.e., new) data concerning an identified research problem. The means for collecting appropriate data involve either a controlled environment designed to model the situation in which specific human factors of interest come into play or by observation of the actual situation of interest itself. For most safeguards situations, some form of experimental modeling must be used because of the relative infrequency of appropriate events and difficulty with arranging direct observation. The aim of proper experimental design management is to minimize the biases in the model which can make the results less transferable to the real situation of interest. As a result, the better the information available, the better the design and management.

Any activity which involves an exercise or activity to collect new data on a human factors of interest is characterized as "Experimental" in this chapter.

1.2.1.2. Data Analysis

Frequently data are available which can be brought to bear on a specific research problem. Many data sources exist which are used for many purposes. These include Licensee Event Reports, the Safeguards Summary Event List, inspection and enforcement reports, license applications and files, licensee records required to be on file by NRC, security data from DOD, DOE and DNA, previous NRC reports and industry studies.

In some cases, a research problem can be meaningfully approached using data developed for some other purpose. It is also important to recognize that NRC and the licensees have extensive documentation which was often collected without specific purpose, but rather to be available as a regulatory reference or for future research. The main advantage of using existing data is that it eliminates the need for experimentation which can be both expensive and intrusive. The main disadvantage is the potential biases on existing data because it was collected for other purposes which may make analyses less transferable to the situation of interest. Any research approach which involves identifying and analyzing existing data from government or nuclear industry sources will be considered "Data Analysis."

Table 1

Safeguards-Related Human Factors Identified in Chapter 2

A. Insider Threat
   - A.1. Two-Man Rule
   - A.2. Behavioral Observation Programs
   - A.3. Trustworthiness
   - A.4. Fitness for Duty
   - A.5. Human Reliability

B. Organization
   - B.1. Vigilance
   - B.2. Organizational Communication
   - B.3. Shiftwork/Manpower
   - B.4. Corporate Attitudes
   - B.5. Training and Instruction

C. Response Capabilities
   - C.1. Format and Wording of Contingency Plans
   - C.2. Deadly Force and Self Preservation
   - C.3. Safeguards/Operational Staff Coordination
   - C.4. Performance Evaluation

D. Equipment and Facilities - The Man-Machine Interface
   - D.1. Central and Secondary Alarm Station Design
   - D.2. Maintenance
   - D.3. Communications Equipment
   - D.4. Environmental Influences
   - D.5. False and Nuisance Alarms

1.2.1.3. Extrapolation

The influences of human factors on personnel performance generally operate in a far broader context than that of government or nuclear industry activities. For instance, the effects of shiftwork have been extensively studied in terms of how they affect human performance. The resulting findings may be of use in the nuclear safeguards context. Other studies on human factors performed outside the nuclear context include, for example, many aimed at understanding the roles of individuals in small, mission-oriented groups. However, the applicability of these studies to nuclear safeguards is not as clear as those studies examining shiftwork.

Whenever data from one setting is being used to understand another, the biases and conditions which bear on the accuracy of extrapolating the results must be examined and evaluated. Extrapolation is most useful if a rational and systematic attempt is made to minimize inherent biases. Any research approach which involves using data or other information from contexts besides those related to nuclear and government contexts is characterized in this chapter as an "Extrapolation" method.

1.2.1.4. Further Research Formulation

The level of effort for this overall project is not adequate to fully address all of the methodological problems which would arise in a uniform level of development of research feasibility considerations for each human factor. As shown in Section 2, some subjects are more methodologically developed than others. In some cases further development of issues is still needed to optimally formulate an effective and meaningful research approach. Any research approach which involves or requires significant further methodological development is characterized as "Further Research Formulation" in this chapter.

1.2.2. Practicality

Different research problems and methods entail different costs, time, and constraints. In order for research to be practical it must be within the resources available for the overall study of human factors affecting safeguards. It is not likely that resources available for this type of research will be sufficient to comprehensively study all or even most of the human factors found to be important in Chapter 2 so that a means of assessing the relative practicality of researching these human factors must be used.

An assessment of the practicality of research involves its costs, time required, and the availability of needed data and equipment. It must be recognized that this is a difficult area to study quantitatively. Therefore, it must be reiterated that the analysis which is presented here is more of an open judgement process than a rigorous empirical analysis. The principal reasons for different rankings can be tracked through the process and the source of differences identified.

1.2.2.1. Cost

For any research approach an estimate can be made of the probable costs. These costs are estimated in staff-years of research personnel effort

(staff-year = $100,000) in this report and do not include NRC administrative and oversight costs. Equipment costs can also be estimated for projects involving use of special equipment.

According to NRC staff, a reasonable size (substantial, but not overly large) project involves about one staff-year of effort ($100,000). As such, costs are split into three regimes for the purpose of this analysis. These are 0 - $75,000, 75,000 to 200,000, and over $200,000 per year. These are assigned cost indexes of 3, 2 and 1 respectively reflecting the relative costs of proposed research approaches.

1.2.2.2. Time Required

Projects may take more than one year to complete in which case they are called "multiyear projects." Priority is given to those projects which will yield timely results. Estimates of time necessary to complete projects can be made based on time required for similar research. It is assumed that NRC would prefer results and products on a fiscal year basis so that time requirements are divided into three regimes. These are one-half to one year, one to two years, and three and more years. The assigned time indexes are 3, 2, and 1 respectively.

1.2.2.3. Data Availability

For any research approach, the data (i.e., information) required to conduct the research may or may not be easily available. If required data will be difficult to obtain, then that research approach will be less practical. A judgment can be made for any specific research approach and research problem as to the availability of required data. This consideration includes data necessary to properly design and manage an experiment as well as for data analysis or extrapolation. The three regimes which data availability is divided into are, easily available from known sources or already obtained, obtainable through identifiable sources but will need to be collected, and not easily identifiable or obtainable. These are assigned data availability indexes of 3, 2 and 1 respectively.

1.2.2.4. Equipment Availability

Certain research approaches involve special or unique equipment which must be used to conduct the project. While the cost of the equipment is factored into the cost index, if it is difficult to obtain, in spite of cost, it will be less practical to conduct the research. The three regimes of equipment availability are, easily available, some significant procurement activity necessary, and not easily available. The equipment availability indexes are then 3, 2 and 1 for each respectively. If no equipment is required, an index of 3 is assigned to prevent a systematic bias against projects not requiring equipment.

1.2.3. Usefulness

The usefulness of any research will be a measure of two principal factors. These are the near and medium-term needs of NRC for a technical basis for regulatory actions and the potential for risk reduction stemming from research results.

1.2.3.1. Regulatory Needs

NRC has certain research interests which at any given time are more important than others. For instance, NRC has announced that it is about to publish an Insider Rule Package and Fitness-For-Duty rule. With regulatory compliance programs coming into place over the next several years, studying their effectiveness could not be currently undertaken and expected to yield useful results. Instead, NRC may wish to examine these systems once in place (i.e., three to five years hence) so relevant data for analysis can be collected. (It should be noted that for those data to be optimally collected, some mechanism could be established earlier.) Other issues are more timely with regard to NRC needs. For instance, licensees have recently made efforts to reduce complexity and detail in their Contingency Plans. NRC may wish to have technical guidance in evaluating the newer, simpler plans. This could be done by investigating the usefulness of new formats capable of simplifying and reducing ambiguity concerning selection and presentation of appropriate response tactics for complex situations.

The three regimes of regulatory need are currently needed, potentially useful, and no current regulatory need. These are assigned regulatory need indexes of 3, 2 and 1.

1.2.3.2. Risk Reduction

The ultimate goal of all NRC regulatory activity is to assure the health and safety of the public so that negative impacts stemming from operation of a nuclear power plant are minimized through regulation to acceptable levels. As such, some estimation of expected risk reduction from an improvement in safeguards must be made. This determinant should distinguish between research projects which will probably have a negligible effect on risk from those that can potentially reduce risk. As such three regimes, probable risk reduction, possible risk reduction, negligible risk reduction can be estimated for each human factor given some improvement in performance. These correspond to risk reduction indexes 3, 2, and 1 respectively.

1.2.4. Acceptability

1.2.4.1 Industry Interests

It is important, in terms of practicality, that research conducted on human factors and safeguards entail methods and yield results which are not actively opposed by licensees and/or their employees. In some instances, industry has requested better regulation or guidance (e.g., uniform and transferable access authorization programs) and, in others, a stated opposition to certain types of rules (e.g. routine pat-down searches, two-man rules in radioactively contaminated areas). As a measure of acceptability the three regimes are requested or desired by industry, tacit acceptance by industry, and opposed by industry. These are assigned acceptability indexes of 3, 2, and 1.

1.3. Grouping of Research Approaches

After the human factors are ranked according to the feasibility of research (Section 2.0), they will be grouped methodologically in order to take advantage

of common research approaches to similar problems (Section 3.0). It must be recognized that the human factors which are identified and analyzed in Section 2.0 are not strictly research topics, but rather a set of issues to be addressed in research. As a result, estimates made with regard to practicality, usefulness, and acceptability are not made with a view toward an overall research plan but, instead, to address each human factor separately. By doing so, sources of consensus and disagreement concerning each human factor can be isolated among all those human factors considered and addressed in a systematic manner. An overall research plan will address these issues in a manner which integrates many research measurement and analysis techniques with different goals into single projects to minimize resource requirements.

Table 2

Feasibility Index Measures

Research Approaches -	A - Experimental	
	B - Data Analysis	
	C - Extrapolation	
	D - Further Research Formulation	
Practicality		
Cost	3 - 0-$75,000 2 - $75,000-200,000 1 - over $200,000	
Time	3 - ½ year to 1 year 2 - one to two years 1 - more than two years	
Data Availability	3 - easily available or already obtained 2 - obtainable but must be collected 1 - not easily available	
Equipment Availability	3 - easily available or not needed 2 - significant procurement necessary 1 - not easily available	
Usefulness		
Regulatory Needs	3 - currently needed 2 - potentially useful 1 - no current regulatory need	
Risk Reduction	3 - probable risk reduction 2 - possible risk reduction 1 - negligible risk reduction	
Acceptability		
Industry	3 - requested or desired by industry 2 - tacit acceptance by industry 1 - opposition by industry	

2.0 Analysis of Individual Human Factors Research Feasibility

This section examines each human factors issue identified in Chapter 2 in order to assess the feasibility of conducting research. Feasibility indexes are assigned according to the criteria set forth in the previous section. Each human factor is first discussed with regard to the nature of its effect on nuclear power plant security and the state of knowledge concerning those effects. There are many areas that overlap among the human factors examined so that the feasibility indexes are not to be taken as completely reflective of those which would arise in an overall comprehensive program. Instead analysis has shown that many of these human factors issues are related and can be studied concurrently using common methods.

2.1 Two-Man Rule

2.1.1. Background

Recently, the NRC has decided that the two-man rule will not be required for vital areas at nuclear power plants for safety and cost reasons.[1] In radiation areas the two-man rule can be argued to be unsafe and at odds with NRC policy concerning exposures. This could terminate consideration of this option, however, the topic may be worthy of some further consideration for selected research. This could be undertaken to determine whether there are possible uses of the rule which would add significantly to safeguards quality and have a minimal negative impact on the licensee.

The suggestion that implementation of the rule may even have the effect of degrading safeguards capability at power plants is of interest;[2] if this is found to be true, the option could immediately be rejected.

The existence of several sophisticated systems analysis methodologies,[3] which have already been used to evaluate the effectiveness of safeguards at DOE nuclear facilities and nuclear power plants, leads to the suggestion that it would be useful to use such techniques to determine the incremental increase in safeguards protection which could be achieved by selectively instituting a two-man rule in power plants. This could be done by examining areas individually where a two-man rule may be appropriate. It should be noted that the threat which is to be guarded against is radiological sabotage by an insider, not the diversion of special nuclear material. That fact may have an impact on the need for a two-man rule since sabotage is probably a more overt act than diversion. It would be necessary to rigorously determine whether the incremental increase would be worth the interference with facility operation as well as the additional costs and exposures, incurred. If the results of such an analysis indicate that the two-man rule does not merit consideration, no further findings would be necessary. However, no such rigorous analysis has been located.

Another question concerns the possible utility of using the two-man rule to improve response capabilities in areas dealing with guard force deployment or safety related matters. The former alternative is more appropriately discussed in the section dealing with contingency plans (2.11) and the latter goes beyond the scope of the present study which deals with safeguards.

2.1.2. Research Approach

2.1.2.1. Data Analysis and Experimental

Computer simulations of facilities, organizational structure, and resultant vulnerabilities are feasible and, in fact, have been performed for several nuclear power plants and DOE production plants. These can reveal weaknesses in safeguards effectiveness which may be closed by application of the two man rule. Much recent work in this regard has been done where integrated safeguards systems are designed using the two-man rule.[4] In principle, if the two man rule works as it is supposed to, gaps would be narrowed or closed. However, additional work needs to be done to ascertain whether it would, indeed, be likely that the written rule would be adhered to in practice, and what its value actually is given the other human factors involved. A field test conducted as an experiment (or as an inspection activity) would be an appropriate means for assuring that a rule of this sort would be correctly and usefully implemented after its value has been shown.

2.1.3. Practicality

2.1.3.1. Cost - Since licensees have already conducted surveys of their facilities in order to assign vital area designations those same data can be used to identify areas where a two-man rule may be appropriate. Criteria for determining where the two-man rule may be desirable must be developed and the the utility of the two-man rule verified. Such analysis would take 1 to 2 staff years and therefore is assigned a cost index of 2. If an experiment is needed to verify use then the cost may be slightly higher.

2.1.3.2. Time Required - If a data analysis is conducted with negative results for the usefulness of the two-man rule, it could be done in less than one year. If an experiment is needed to validate its usefulness then it may take longer, however, not significantly so a time index of 3 is assigned.

2.1.3.3. Data Availability - The data needed to analyze areas for their potential for using a two-man rule must be collected so a data availability index of 2 is assigned. NRC may have more ready access to this information than a contractor.

2.1.3.4. Equipment Availability - No equipment, except possibly easily available computer equipment and software would be needed so that an equipment availability index of 3 is assigned.

2.1.4. Usefulness

2.1.4.1. Regulatory Needs - To an extent, this has already been evaluated implicitly in the NRC decision to no longer require the rule at power plants. Therefore, a need index of 1 is appropriate.

2.1.4.2. Risk Reduction - If the two-man rule could be reasonably applied, some potential reduction in vulnerability may result. Since the data analysis would reveal that, a risk reduction index of 2 is assigned.

2.1.5. Acceptance

2.1.5.1. Industry Interests - The industry has and would continue to oppose imposition of the two-man rule, because of high costs so an acceptance index of 1 is assigned.

2.1.6. Summary of Index Values

	Data Analysis and Experimental
Practicality	
Cost	2
Time	3
Data Availability	2
Equipment Availability	3
Usefulness	
Regulatory Needs	1
Risk Decrement	2
Acceptance	
Industry Interests	1

References

1. Chapter 2, p. 9.

2. For examples of how small groups can actually diffuse responsibility see, McConnell, J.C. Understanding Human Behavior, 2nd Edition, NY: Holt, Rinehart, and Winston, 1977, 647-648; Darley, J.M. and Latane', B. "Bystander Intervention in Emergencies: Diffusion of Responsibility." Journal of Personality and Social Psychology, 8, 1968, 377-383; Latane', B. and Darley, J.M. "Group Inhibition of Bystander Intervention in Emergencies." Journal of Personality and Social Psychology, 10, 1968, 215-221; Latane', B. and Rodin J. "A Lady in Distress: Inhibiting Effects of Friends and Strangers on Bystander Intervention." Journal of Experimental Social Psychology, 5, 1969, 198-199; Piliavin, I.M., rodin, J. and Piliavin, J. "Good Samaritanism: An Under ground Phenomenon?" Journal of Personality and Social Psychology, 13, 1969, 289-299.

3. For example, Lewis Goldman and Peter Lobner, "A Review of Selected Methods for Protecting Against Sabotage by an Insider," NUREG/CR-2643, August 1982.

4. A. Winblad, et al., "An Integrated Sabotage Protection System Concept," SAND 82-2963C, April, 1983; P. Lobner, "Damage Control and Design Changes as Elements of an Integrated Sabotage Protection System," presented at ANS Power Plant Security Workshop, April 25, 1983; Also NUREG/CR-2585, SAND 82-7011, May 1982; L.A. Goldman et al., "A Review of Selected Methods for Protecting Against Sabotage by an Insider," NUREG/CR-2643, SAND-82-7031, August 1982.

2.2. Behavioral Observation Programs

2.2.1. Background

The idea of instituting behavioral observation techniques at the supervisor level and above as a means of protecting organizations, and more specifically, protecting nuclear power plants, has already been studied by NRC in some detail;[1] a discussion and summary of the conclusions of this study has been given reference 2. The theoretical aspects of the topic have been studied as well, and it is not likely that further theoretical work is needed at this point. Privately communicated opinions on the topic[3] have not been optimistic as to the practicality of using behavioral observation techniques exercised by facility supervisors in predicting the wide range of anti-social behavior which could be detrimental to the facility.

Nevertheless, it is clear from the literature[4], and the recent burgeoning interest in the field of behavioral observation and assessment, that a considerable number of experts in the field of behavioral psychology do believe that behavioral observation could provide useful information and reduce risk.

Because of NRC's recent proposal to require facilities to establish and document a behavioral observation program[5] there will be a need for critria and measures to assess their adequacy. Appropriate measures have not been developed.

2.2.2. Research Approach

2.2.2.1. Experimental or Data Analysis - It appears logical to suggest a test which could measure the effectiveness of such a program. A suggested behavioral observation program such as that put forth in reference 1 could be put into place at a nuclear power plant. Such a test need not be rigorous, but rather aimed at making more informed judgements about effectiveness. If there is some difficulty in obtaining the agreement of a licensee for collecting data on a field test of such program, it might be possible to make the test at an analogous DOE contractor site or facility. However, since several utilities already have such programs the data may be available without an experiment. Acquisition of licensee data concerning the effectiveness of their programs would be worth while. Such data would be necessary to establish criteria and measures by which the usefulness and effectiveness of the test program could be assessed.

2.2.3. Practicality

2.2.3.1. Cost - The scope of a test program will require trained social scientists and security experts to examine data collection and conduct analyses. In terms of staff years, it is estimated that the total effort to develop criteria, measures and findings regarding effectiveness will be great, meriting an assignment an index of 1 if programs are to be implemented requiring experimentation. However, if data can be made available from existing programs a higher index would be appropriate.

2.2.3.2. Time - It is estimated that the time for implementation and analysis of such a program would be on the order of one to two years, justifying an index of 2.

2.2.3.3. Data Availability - Large amounts of data will have to be taken and analyzed to set up a proper experiment. There is no intrinsic problem in this once the experiment is set up, but a great deal of effort will be required to set up an experiment with appropriate measures. If data are available it will have to be collected so a data availability index of 2 is assigned.

2.2.3.4. Equipment Availability - No special equipment need be procured for this experiment beyond those normally used in the field of behavioral science. An index of 3 is assigned.

2.2.4. Acceptability

2.2.4.1. Regulatory Need - If it can be shown that the impact of a behavioral observation program on safeguards personnel performance or likelihood of insider malevolence is significant, the need for and value of appropriate regulations would then be indicated. The Insider Rule package about to be announced by NRC includes guidance requiring establishment and documentation of a behavioral observation program.[5] There will be a need to assess the adequacy of programs submitted to NRC. As such, a regulatory need index of 3 is assigned.

2.2.4.2. Risk Reduction - There is little question that a probable risk reduction would be attained if behavioral observation programs were successful in reducing the threat from malevolent insiders: personnel who, for one reason or another are not trustworthy, reliable, or are temporarily unfit for duty. There is, in fact, a strong overlap with these human factors and they can be studied together. Because of the significance of an insider threat against a plant, a risk reduction index is assigned a value of 3.

2.2.5. Acceptance

2.2.5.1. Industry Interests - Industry has commented it needs guidance on behavioral observation programs rather than rules.[6] Since the Insider Rule Package addresses these programs it is assumed that industry would actively oppose additional measures warranting an acceptance index of 1.

2.2.6. Summary of Index Values

	Experiment or Data Analysis
Practicality	
Cost	1
Time	2
Data Availability	2
Equipment Availability	3
Usefulness	
Regulatory Needs	3
Risk Reduction	3
Acceptance	
Industry Interests	1

References for Section 2.2

1. J.C. Buchanan, et al., "Behavioral Reliability Program for the Nuclear Industry", Personnel Decisions, Inc., NUREG/CR-2076, July 1981.

2. Chapter 2, pp. 33-34.

3. R. Mackie, private communication (1983).

4. F.D. Frank, et al., "Standards for Psychological Assessment of Nuclear Facility Personnel," NUREG/CR-2075, July 1981; L.B. Beam, "Utility Problems in Meeting Security Requirements at Nuclear Power Plants," presented at ANS Power Plant Security Workshop, April 25, 1983; Buchanron, Note 1; S.L. Davis, "Utility Considerations in Emotional Stability Monitoring for Nuclear Plant Personnel," presented at 7th Annual Symposium in the Role of Behavioral Science in Physical Security, Defense Nuclear Agency, DNA-TR-82-13 November 17, 1982.

5. G.W. McCorkle, "The NRC 'Insider Rule'," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

6. Private correspondence, Atomic Industrial Form, May 2, 1983.

2.3. Trustworthiness

2.3.1. Background

NRC has long sought a solution to the problems posed by threats from knowledgeable insiders. Strict access controls were first required at reactors in the mid-1970s due to the growing recognition of the "insider threat". The development of access controls also included consideration of intruder threats. Access controls include all on-site measures, both procedural and mechanical, aimed at restricting human access to areas containing equipment critical to the safe operation of the plant. Those physical security measures aimed specifically at outside intruders, such as perimeter fences and isolation zones (areas just outside the perimeter fence), are not considered access controls for this discussion on trustworthiness.

Access controls include manned access points, pat-down searches of personnel, magnetometer searches, card-key doorways, vehicle searches, numbered picture badges, escort requirements, internal alarms and closed circuit TV, lock changes subsequent to employee termination, and tamper indicating security equipment. All of these measures which restrict access to vital equipment can potentially impact safety if expeditious access is necessitated by an accident sequence. As such, a policy of lessening access controls where trustworthiness can be established has emerged and is being considered.

NRC has also sought to minimize insider threats by promulgating administrative personnel selection requirements which include the use of psychological assessment and background investigations as measures of trustworthiness. If personnel can be considered more trustworthy, less access controls are necessary.[1] NRC Regulatory Guide 1.17 cites the ANSI-N-18.17 standard as a reference for satisfying NRC personnel selection regulatory requirements (both were published in 1973). In 1977 new regulatory requirements for physical security at power plants were published (10 CFR 73.55). As a result, ANSI-N-18.17 was superseded by ANSI/ANS-3.3 in 1982. The new standard was designed to conform with the 1977 regulations. (For a discussion of the background and explanation of these federal regulations and industry standards see Appendix A.)

The means for assessing trustworthiness are a psychological assessment and a background investigation. A backgrouind investigation, according to the forthcoming Insider Rule Package will require licensees to verify an applicant's true identity, and then investigate his employment, educational, credit, military and criminal history, in addition to obtaining personnel reference checks. If this check reveals involvement with acts of sabotage, falsification of the application, any illness affecting judgement, habitual criminal tendencies, or use of controlled substances or alcohol to excess, no authorization is to be granted. A psychological test may not end up being in the proposed rules as a firm requirement.[2] This is presumably due to the need for further development of regulatory policy on phychological testing, although substantial research has already been conducted.[3] It should be noted that an NRC-sponsored study found that the typical insider saboteur (in other industries) was usually motivated by psychological problems, disgruntlement or revenge early in job tenure.[4] This indicates the critical nature of an initial review of job applicants for trustworthiness. Industry has voiced concern that criminal records cannot be examined in some states due to privacy laws (in Massachusetts, for example, such access

is specifically allowed by law while in New York it is not). Industry has requested that NRC propose legislation that would allow all licensees access to applicants' criminal records and, further, that NRC develop guidance for a plan to train evaluators how to make proper judgements.[5]

Many utilities already practice some form of psychological evaluation as recommended in ANSI/ANS 3.3. Some claim great success and total legal compliance.[6] In addition, many security systems at nuclear power plants are being upgraded to include software capable of locating all personnel anywhere in the protected area on a real-time basis.[7] Access controls of this type that are less restrictive can improve site security without downgrading access to safety equipment.

2.3.2. Research Approach

2.3.2.1. Data Analysis - Data on historical occurrences of security breaches which happened in spite of trustworthiness measures are available. For instance, cross comparisons of facilities with differing policies could be undertaken. This area has has been analyzed to some limited extent; however a larger scale effort may be appropriate. The objective would be to establish that certain policies result in better assurances of trustworthiness than others.

2.3.2.2. Extrapolation - As in data analysis, extrapolation from other fields has been already undertaken. Industries such as banking and pharmaceuticals have been studied, but the biases in the data due to the different nature of the threat have made data of questionable applicability. Better methods of extrapolation could be developed although the results may still be less than accurate for the nuclear industry.

2.3.2.3. Further Research Formulation - There will be issues which are not addressed by the Insider Rule Package. For example, how to adequately deal with access authorization for outside contractor personnel. Since the new TMI-related requirements imposed by NRC were instituted, a need for hundreds of contractor personnel to have access to vital and protected areas has surfaced. The best way to handle access for temporary site personnel could be investigated along with other areas not covered by the Insider Rule Package. In addition, optimal data collection methods could be formulated now to assist in future analyses by collecting useful data in a meaningful form as it evolves.

2.3.3. Practicality

2.3.3.1. Cost - Data analysis may be costly depending on whether or not good data can be located. Most data which presently exist are not easily reducible and analysis could easily take several staff-years of effort. If data were available (e.g., in the future) then analysis could be conducted more easily. This suggests that a data collection system should be set up as soon as practical. A cost index of 2 is assigned in anticipation of better data being available in the future. Extrapolation has already been conducted in several studies and further work, beyond that done to date, could be costly and is likewise assigned a cost index of 2. Further research formulation aimed at identifying and addressing those problems not addressed by new regulations could

be done very cost effectively (less than one-staff year) and is therefore assigned a cost index of 3.

2.3.3.2. Time Required

To collect the data necessary for an advance in this area by data analysis would take one to two years so a time index of 2 is assigned. For extrapolation less time would be required so a time index of 3 is assigned. Further research formulation could also be completed within one year and is assigned an index of 3.

2.3.3.3. Data Availability

Data analysis could not be easily performed because applicable data do not presently exist due to the imminent release of new regulatory requirements. Since these requirements will change trustworthiness programs to a great extent, historical data may not be applicable. Therefore, a data availability index of 1 is assigned. For extrapolation, data are more readily available but must still be collected so an index of 2 is assigned. For further research formulation data needed will be available from the rulemaking proceeding on the insider rules and can be analyzed to isolate issues not treated so that a data availability index of 3 is assigned.

2.3.3.4. Equipment Availability

None of the research approaches discussed requires equipment so an index of 3 is assigned.

2.3.4. Usefulness

2.3.4.1. NRC Regulatory Needs - Since NRC has gone through extensive staff-level negotiations on the new insider rules it is very doubtful that further data analysis is needed by NRC on these issues at this time so a regulatory need index of 1 is assigned. Extrapolation is likewise not useful so that a index of 1 is also assigned. Further research formulation aimed at those issues not addressed in new rules and at means for collecting usable data from programs being implemented could be of great use to NRC and is, therefore, assigned a value of 3.

2.3.4.2. Risk Reduction

Trustworthiness of individuals is a problem which has been shown to affect the safe operation of power plants. Therefore, since there is some possible risk reduction, an index of 2 is assigned. This index could be arguably higher.

2.3.5. Acceptability

2.3.5.1. Industry Interest

Industry has indicated a need for guidance in these areas. However, further data analysis or extrapolation is not as useful to industry as a method for addressing special problems such as those posed by contractor personnel.

Therefore, data analysis and extrapolation are each assigned an acceptability index of 2 and further research formulation, especially aimed at providing instructions for evaluators and guidance on contractor personnel, an index of 3.

2.3.6. Summary of Index Values

	Data Analysis	Extrapolation	Further Research Formulation
Practicality			
Cost	2	2	3
Time	2	3	3
Data Av.	1	2	3
Equipment Av.	3	3	3
Usefulness			
Regulatory Needs	1	1	3
Risk Reduction	2	2	2
Acceptability			
Industry Interests	2	2	3

References for 2.3

1. L.B. Bean, "Utility Problems in Meeting Security Requirements at Nuclear Power Plants," presented at the AWS workshop on Power Plant security April 25, 1983.

2. G.W. McCorkle, "The NRC 'Insider Rule'," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

3. F.D. Frank, "Standards for Psychological Assessment of Nuclear Facility Personnel," NUREG/CR-2075, July, 1981.

4. G.W. McCorkle, "The NRC Threat Assessment Program," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

5. Private Correspondence, Atomic Industrial Forum, May 2, 1983.

6. E. Gary Baker, "A Psychologically Developed System for unescorted Access of Vendor and Owner Applicants," presented at ANS Workshop on Power Plant Security, April 25, 1983; E.R. MacCormack, "Nuclear Power Plant Protection Against the Insider Development of Personnel Screening Programs," presented at ANS Workshop on Power Plant Security, April 25, 1983.

7. G.M. Gurican, "A Combined Security and RE&M System Operational Experience at the D.C. Cook Nuclear Plant," presented at the ANS Workshop at Power Plant Safeguards, April 25, 1983.

2.4. Fitness for Duty

2.4.1. Background

This topic involves a number of different safeguards concerns. From the point of view of the ability of an employee to reliably fulfill his safeguards-related functions, it would be desirable to assure that he is not impaired (i.e. using drugs, consuming alcohol, suffering acute psychological stress) on a routine basis. This problem is similar to the corresponding human factors concerns for safety-related operational personnel. More deep seated problems (i.e. physiological disorders, chronic psychological stress) could be monitored on a longer term basis by a behavioral observation program (section 2.2).

There is another dimension of concern on the subject of fitness for duty. It deals with the insider threat. One would like to ascertain that employees, particularly those with access to vital areas, do not intend, for reasons of job dissatisfaction, ideology, extortion or any other motivations, to damage the facility through actions of sabotage, or by attempting to aid others in sabotage attempts. It has been assumed in some past research that when such activity is being carried out, the potential perpetrators will be highly stressed. The question is, whether such stress is amenable to detection in ways which are constitutionally acceptable, and acceptable to employees and employee unions. Some studies have been made of the feasibility of detecting stress among employees from both the technical and the legal perspectives.[1] At the time of those works, it appeared that technical means were not yet reliable, and that there were serious legal problems with at least some of the proposed methods. It is technically possible to detect many drugs in body fluids, so that the first part of the fitness for duty problem may be technically tractable; however, there may still be legal and personnel problems.

NRC is currently developing a "Fitness for Duty" rule which has been proposed. These rules once officially published will define means for meeting requirements for assessing fitness for duty at nuclear power plants.[2] This rule is being proposed because of the substantial increase of reported drug-related employee incidents at power plants. Instead of integrating that rulemaking with the Access Authorization Rule (10 CFR 73.56 part of the Insider Rule Package) the seriousness of the problem led NRC to separate regulatory actions.

The proposed rule would require licensed facilities to establish, document, and implement procedures to assure that personnel with unescorted access to the protected area of the facility are not unfit for duty. The exact form of these procedures is left to the licensees. The Commission will seek public comment on: 1) the establishment of specific fitness criteria for nuclear plant personnel (not just safeguards personnel), 2) specific methods of implementation including the use of breath tests, background investigations, psychological tests, behavioral observation programs, employee awareness programs, employee assistance programs, among others and 3) limiting the scope of the rule to unescorted access to vital areas.[3] As such, it is clear that NRC has yet to decide these issues. The NRC Office of Inspection and Enforcement has published a report titled "Survey of Industry and Government Programs to Combat Drug and Alcohol Abuse" (NUREG-0903) to assist licensees in setting up their programs.

It is worth noting that many human factors besides fitness are opened to comment in this rulemaking which may be a very constructive source of information.

2.4.2. Research Approach

2.4.2.1. Data Analysis - NRC must develop a means for assessing the adequacy of programs submitted to NRC for review. Work in this area should include a review of the current feasibility of technical methods of detecting stress and chemical addictions in an individual, as well as a legal review of the implications of the various control methods suggested. Next, the problem of implementation of such a program in the field must be dealt with, involving either more review of data, or extrapolation of similar experiences in other industries or situations where similar control over personnel has either been instituted, or where there have been attempts to do so. It is anticipated that the main methodology needed on this human factor will be the data analysis approach, including discussions with representatives of organizations where such attempts to control fitness for duty have been successful. Since NRC is going to publish the fitness for duty rule such an analysis should be aimed at providing regulatory guidance for meeting the new regulatory requirements as well as establishing assessment criteria.

2.4.3. Practicality

2.4.3.1. Cost - The necessary data analysis could be performed using two staff-years of effort, covering all the needs discussed in the above section including time to gather all relevant data. This results in the assignment of an index of 2 for the cost.

2.4.3.2. Time - An estimate for the amount of time needed for an evaluation is from one to two years. Even though several (technical, legal, human and organizational matters) areas need to be further explored, these could run in parallel using expertise from the appropriate different fields. This results in an index of 2. This index will be higher after data from programs going into place become available.

2.4.3.3. Data Availability - The data on methods shown to be effective in other contexts may be easily available, however data on the nuclear power industry is not. Once fitness for duty programs are put into place at utilities, data concerning the effectiveness of there programs will be available. Some measure of effectiveness must be developed to assess these programs. The Edison Electric Institute has developed a model drug abuse program which will be ready in late 1983.[5] As a result a data availability index of 2 is assigned and expected to rise in the future.

2.4.3.4. Equipment Availability - In order to implement a program, state-of-the-art equipment for determining fitness will be needed. Costs may not be high, but some equipment availability currently appears problematic. An index of 2 is assigned.

2.4.4. Usefulness

2.4.4.1. Regulatory Need - Since the fitness for duty rule is about to be proposed, NRC would have little need for extensive research except that

aimed at to assessing the adequacy of licensee programs submitted for review. Therefore, an index of 2 is assigned.

2.4.4.2. Risk Reduction - The insider threat or the possibility of negligence on duty due to drug- or stress-related problems must be regarded as significant. Indeed, on the latter matter, there have been numerous examples of personnel at power plants being on duty, but unfit to function reliably. If this problem could be successfully countered, this would be a significant contribution to improving safeguards. A risk reduction index of 3 is assigned.

2.4.5. Acceptance

2.4.5.1. Industry Interests - If a satisfactory means of assuring fitness could be found, one would anticipate industry acceptance, especially as it would help assure reliability of employees without causing employee and union problems, leading to improved operations. An index of 3 is therefore assigned. It is doubtful, however, that industry would accept a program which intrudes on employee civil liberties or rights or would cause a deterioration in employee attitude.

2.4.6. Summary of Index Values

	Data Analysis
Practicality	
Cost	2
Time	2
Data Availability	2
Equipment Availability	2
Usefulness	
Regulatory Need	2
Risk Reduction	3
Acceptance	
Industry Interests	3

References for Section 2.4

1. J.N. O'Brien, "Stress Duress: Detection for NRC-licenses Facilities: A Constitutional and Regulatory Analysis," NUREG/CR-1032, Sept. 1979; A. Fainberg, "Stress and Duress Monitoring at NRC-Licensed Facilities," NUREG/CR-1031, Brookhaven National Laboratory, Sept. 1979.

2. "Proposed Rulemaking Requiring Fitness for Duty for Personnel with Unescorted Access to Protected Areas", SECY-82-196, May 18, 1982; 47 Fed. Reg. 33980, Aug. 5, 1982.

3. Id.

4. Private Correspondence, Atomic Industrial Forum, May 2, 1983.

5. Id.

2.5. Human Reliability

2.5.1. Background

Since the accident at Three Mile Island the issue of how reliable humans actually are has received substantial attention. It has been shown that human reliability breakdowns (i.e., errors) can profoundly affect the quality of a response directed at recovery of safety systems. For instance, safety equipment must be reliably maintained, calibrated and tested at periodic intervals. Faulty maintenance can cause common-mode failures of redundant equipment as recently happened at the Salem plant. (In that case adequate procedures were not in place so that no maintenance of redundant circuit breakers occurred.) At Three Mile Island, operators did not correctly diagnose the problem until hours had gone by because of the interplay of equipment failures and inadequate procedures. Similar types of human reliability breakdowns have been identified in PRA research as dominant risk contributors.

In the context of nuclear power plant safeguards, the reliability of humans in executing their tasks can be viewed as a major determinant of the quality of security. Human reliability can be viewed as those factors affecting physical response capabilities, mental preparedness, the man-machine interface, and awareness.

2.5.1.1. Physical Response Capabilities

In 1978 the Department of Energy implemented medical and physical fitness standards for U.S. DOE Security Inspectors. Because of the lack of information validating the legitimacy of using the standard adapted (i.e., "Police Officer's Agility Test" used by many police departments), the requirements were permanently suspended in 1980. DOE then undertook a study to determine what physical qualifications could be used to best assure the physical reliability of personnel in executing their job-related duties. The results of that study were announced as DOE policy in 1982.[1]

The study attempting to validate physical fitness requirements involved visits to over fifty offices and sites where data were collected pertaining to safeguards job tasks and their relative physical demands. It was determined that the most physically demanding duties would occur during a hostile act against the facility. It was assumed, then that personnel shown capable of executing duties involving "defensive combatics" could reliably execute lesser tasks. (Defensive combatics is a term expressly defined in the study and is exclusive of offensive combatics.) The objective of the study was to select and validate measures of physical fitness that would constitute reasonable assurance of reliability in performance of defensive combatics.

A sample of DOE Security Inspectors (Guards) was selected and analyzed demographically (i.e., sex, age, etc.). A battery of sample qualification tasks were then conducted including 1-mile run, ½-mile run, 40-yard prone-to-running dash, 80-yard shuttle run, and the 40-yard agility run. Approximately 70 personnel were tested in each of these qualification tasks for ability and speed.

The MILES system (described in Sec. 2.14) was used to simulate the execution of defensive combatics activities in a systematic manner for each sub-

ject. After practice trials, subjects were monitored for heart rate and breathing while executing defensive combatics tactics. By statistically comparing the data from simulated tactics and qualification tasks it was determined that for defensive combatics the best single prediction of physical reliability was the ½-mile run and the best combination to be the ½-mile run and the 40-yard dash.

Threshold scores were determined using the criteria that the test should produce no false negatives (disqualifying actually qualifiable personnel) regardless of the number of false positives. The findings of the report are that guards should be able to run the ½-mile run in 4:40 minutes and the 40-yard dash in 8.2 seconds in order to assure physical reliability. This report appears to offer a partial basis for NRC determinations of adequacy for the Training and Qualification Plan required for an Operating License.

2.5.1.2. Mental Preparedness

In order for safeguards personnel to perform reliably they must be prepared to understand and execute what may be complex tasks. Mental preparedness includes the necessary knowledge and competence to carry out these tasks effectively.

While it is relatively straightforward to determine criteria for physical fitness requirements it is very difficult to determine such criteria for mental preparedness. Drills and subsequent evaluations have been shown to be very effective for improving personnel reliability by increasing mental preparedness.[2] The degree of mental preparedness which can be achieved is largely dependent on training and instruction which is covered in section 2.10.

2.5.1.3. Man-Machine Interface

This area of human reliability is addressed in the CAS/SAS design section (2.15).

2.5.1.4. Awareness

Personnel who are acutely aware of the importance of security in the overall risk of operating a nuclear power plant will more likely maintain a high awareness of security. Awareness is a trait of attitude and organizational climate and culture which is covered in section 2.9.

2.5.2. Research Approach

2.5.2.1. Experimental - Approaches similar to that used in the study of physical fitness requirements can be used to verify requirements. The relationship between mental preparedness and awareness to specific requirements may be very difficult to establish, however, criteria for the man-machine interface may be developed by using ergonomic data from operational safety research and experiments aimed at the security environment.

2.5.2.2. Data Analysis

A sensitivity study aimed at identifying situations where human reliability is crucial to safeguards quality would reveal the contexts in which special measures aimed at assuring reliability may be warranted. Where human reliability is backed up or checked by technical or administrative measures no research need be done. Issues identified as crucial could then be made the basis for further study or recommendations.

2.5.2.3. Extrapolation

Although human reliability has been extensively studied in terms of operational safety, no comparable studies of safeguards personnel exists. As such, data from operational studies could be "extrapolated" and applied to safeguards problems. (This may be considered another form of data analysis as well.)

2.5.3. Practicality

2.5.3.1. Cost

An experimental approach aimed at establishing standards for human reliability across the board could be very costly. Unless a data analysis takes place to identify crucial tasks the cost index must be 1. However, since such a data analysis is considered likely an index of 2 is assigned. Extrapolation of human reliability data from nuclear safety research could involve a large effort so an index of 2 is appropriate.

2.5.3.2. Time

An appropriate study of human reliability must be conducted over a long period of time to assure optimal results. A proper approach would involve a data analysis sensitivity study with experiments and extrapolation to follow. As such a time index of 1 is assigned. If only data analysis is performed a time index of 2 is appropriate.

2.5.3.3. Data Availability

Data on human reliability has been generated in large volume in the operational safety field. The particular applicability of these data must yet be determined however, because of the extensive availability of human reliability data an index of 3 is assigned.

2.5.3.4. Equipment Availability

Equipment may have to be procured for an experimental approach warranting an index of 2. No equipment would be necessary for a data analysis or extrapolation so an index of 3 is assigned.

2.5.4. Usefulness

2.5.4.1. Regulatory Need

Human reliability has been pointed out as an important factor in the quality of safeguards. As a result, a regulatory need index of 2 is assigned in light of the potential usefulness of information generated.

2.5.4.2. Risk Reduction

The demonstrated ability of human unreliability to affect site safeguards indicates that a probable risk reduction can be attained warranting an index of 3.

2.5.5. Acceptance

2.5.5.1. Industry Interests

Industry would not object to a program aimed at assessing the safeguards impact of human reliability and subsequent study of those tasks deemed sensitive. Therefore an acceptance index of 2 is assigned.

2.5.6. Summary of Index Values

	Data Analysis Only	Data Analysis and Experimental	Extrapolation
Practicality			
Cost	2	2	2
Time	2	1	1
Data Availability	3	3	3
Equipment Availability	2	3	3
Usefulness			
Regulatory Need	2	2	2
Risk Reduction	3	3	3
Acceptability			
Industry Interests	2	2	2

References for Section 2.5

1. W.D. Telfair, et al., "United States Department of Energy Physical Standards Validation Study," Sept. 30, 1982, Referenced in W.D. Telfair, "Validation of Physical Fitness Standards," presented at ANS Conference on Power Plant Security, April 25, 1983.

2. R. Kindilien and R.K. Harper, "Practical Implementation of Security at Nuclear Power Plants - Impacts on Costs, Operations and Safety: Practical Armed Response Training for Commerical Nuclear Facilities," presented at ANS Workshop on Power Plant Security, April 25, 1983; SSORA, HFR, L.D. Chapman, et al., "Tactical Improvement and Security Force Evaluation Program," presented at ANS Workshop, April 25, 1983.

2.6. Boredom and Vigilance

2.6.1. Background

A large number of studies have been made since the Second World War to determine the ability of personnel to respond correctly to infrequent alarms while having to maintain vigilance for hours at a time. Sonar and radar operators are prime examples of such personnel who must perform duties of this kind. There have been many such efforts[1]. However, little if any experimental work has been done on the problem of vigilance of guard force personnel at nuclear plants, although similar efforts have been made at other types of protected facilities using guard forces. Significant work on reducing the need for human vigilance through automated compensatory measures is currently under investigation by the Defense Nuclear Agency.[2]

2.6.2. Research Approach

2.6.2.1. Experimental - Although much work has been done in other industries and services,[3] little scientific work has yet been done on the problems of boredom and vigilance at nuclear plants. Pilot experimental work along these lines at one or two facilities may be appropriate, in order to probe similarities and differences relative to other situations already examined. The SSORA system described in Section 2.14 will reveal some vigilance sensitivities in site security.

2.6.2.2. Data Analysis - There may be useful boredom and vigilance information already available from past safeguards-related incidents and from normal operations at power plants. Some effort at using these data may be very productive for limited expenditure resources. A comparison of current practices as outlined in procedures and vulnerabilities due to vigilance deterioration could be undertaken. A comparison of current practices as outlined in procedures and vulnerabilities due to vigilance deterioration could be undertaken.

2.6.2.3. Extrapolation - A survey of the copious literature on boredom and vigilance, which has been produced in the past forty years, could be highly productive. An effort at drawing the conclusions from all this research for applicability at nuclear plants could be worthwhile. A qualified behavioral social scientist working with a security expert, both capable of understanding and elucidating similarities between the situation where existing data were developed and the power plant situation, would be required.

2.6.3. Practicality

2.6.3.1. Cost - An experimental program at a reactor would probably require more than 2 staff-years of effort, which merits a cost index of 1. The data analysis option would require an index of 3, since it would amount only to gathering and analyzing available data from operating plants. The extrapolation approach is estimated to demand about a staff-year's effort, and rates an index of 2.

2.6.3.2. Time - All proposed programs should require no more than 2 years; therefore all rate an index off 2 for time requirements.

2.6.3.3. Data Availability - The experimental approach will require taking data at one or two facilities. An index of 1 is judged appropriate for this. The data analysis and extrapolation approaches are simpler; in the former case, the data must be assembled so index of 2 is assigned and in the latter, the data are available in published form warranting an index of 3.

2.6.3.4. Equipment Availability - Equipment requirements are small in the first case yielding an index of 2 and negligible in the other two cases warranting an index of 3.

2.6.4. Usefulness

2.6.4.1. Regulatory Need - The regulatory need in this field is probably limited relative to other areas meriting an index of 1. Some useful information on guard force procedures could result but is not currently needed by NRC.

2.6.4.2. Risk Reduction - If procedures were to be developed as result of these efforts which could help mitigate inefficiencies due to boredom, a more effective and rapid response to alarm stimuli could be achieved meriting an index of 2.

2.6.5. Acceptance

2.6.5.1. Industry Interests - The intrusion upon industry is likely to be minimal if only procedures and manpower distribution are involved in suggested ameliorative actions. If with the need of a minimum of expense, the facility can significantly improve its response capability to alarms, one would anticipate a minimal resistance. This would rate an index of 2 for all avenues of research.

2.6.6. Summary of Values

Method	Experiment	Data Analysis	Extrapolation
Practicality			
Cost	1	3	2
Time	2	2	2
Data Availability	1	2	3
Equipment Availability	2	3	3
Usefulness			
Regulatory Needs	1	1	1
Risk Reduction	2	2	2
Acceptance			
Industry Interests	2	2	2

References for Section 2.6

1. One summary of a series of studies in this area is R. Mackie, "Six Years of Research on Human Factor Problems in ASW: A Summary," Technical Report 206-25, Human Factors Research, Inc., November, 1964.

2. P. Bierre, "Teaching Human and Artificial Intellegence for High Productivity Security Systems," in "The Human Element in Organizational Sensitivity," DNA-TR-82-13, November, 1982; Z. Kravets and D.L. Rockford," The Configuration, Development, and Interface of Nuclear Power Plant Security System," presented and Interface of a Nuclear Power Plant Security System," presented at the ANS workshop on Power Plant Security, April 25, 1983.

3. Mackie, Note 1.

2.7. Organizational Communication

2.7.1. Background

The typical compartmentalization of the licensee's organization has led to the development of relatively discrete organizational units such as health/physics, security, operations, maintenance and so on. These organizational units function in discrete contexts in which procedures have been separately developed, sometimes resulting in conflicts. For instance, health physics and safeguards access controls can limit operator access to manually operated valves. However, the organizational units are functionally defined by normal operations so that during normal conditions these conflicts will come to light infrequently. When an off-normal situation occurs the actions necessary to maintain plant safety may cut across the normal administrative boundaries of several organizational units necessitating a highly coordinated response. It has been shown that rotating personnel among the various organizational units can vastly improve communications[1] but that may not be practical for all units at a nuclear power plants. Some utilities currently rotate certain managers to improve communications. Communication during an off-normal situation is characterized in this study as Staff Coordination and is covered in Section 2.13 rather than have methodologically, both problems are related, but are treated separately in this section of the report.

It has been shown that conflicts occasionally arise among the procedures of various units. For instance, operators have been held up at access points by security procedures, but not during emergencies. The health/physics unit imposes rigid access restraints in various safety-related areas of the plant, but emergencies have not occurred in such a manner as to necessitate overexposure while dealing with a critical safety problem. As a result, these conflicts may not have surfaced in a manner which threatens the public health and safety. At one power plant, the D.C. Cook facility, the use of an integrated safeguards - health/physics computer system for tracking personnel exposures and vital area entry data has been successfully installed.[2] Some additional risk is imposed on the public if an emergency does raise these conflicts to dominant factors in a plant failure. This section, however, concerns only normal opeational communication problems between organizational units. It must be recognized that the separation between normal and off-normal procedural conflicts is some what artificial, but it is likely that an overall analysis of these conflicts would begin with normal situations and extend to the off-normal situation. In addition, organizational communication is highly related to attitudes covered in Section 2.9.

2.7.2. Method

2.7.2.1. Experimental - In order to remedy these normal operational conflicts they should be identified in a systematic manner. Drills involving performance of operational and security procedures have been shown to be a reliable way to identify any clear conflicts and point to potential methods for resolving those conflicts. Simulation of events using models developed from the procedures of the organizational units could also be used to identify potential conflicts for various normal operational situations. Simulation may include the use of logic trees or influence diagrams. Another approach would be to poll plant personnel in a systematic manner to reveal conflicts.

2.7.2.2. Data Analysis - Procedures could be selectively examined using postulated normal operational events as stimuli. Potential conflicts, once identified, could be subject to examination by a review of relevant personnel. The NRC's Regulatory Effectiveness Review Program already does this to some extent and has operated with very good results.

2.7.3. Practicality

2.7.3.1. Cost - An experimental approach to identifying potential conflicts between organizational units during normal situations could be costly. A full scale drill could cost a substantial amount to run and monitor so it is assigned a cost index of 1. If a simulation approach involving data analysis was used a large cost savings would result in a necessary effort of about one staff year so that a cost index of 2 is assigned.

2.7.3.2. Time - An experimental approach would require time to arrange, set-up, run and analyze. This could take from one to two years to complete and is assigned a time index of 2. If simulation involving data was used it would take less time but it would take a minimum of one year to receive valid results applicable to the industry as a whole. Therefore the time index for simulation is 3.

2.7.3.3. Data Availability - The data needed to set up an experimental research approach to the problem of procedural conflicts is available. These are procedures, postulated normal events and monitoring information. These data would have to be assembled so that a data availability index of 2 is assigned. Since a simulated approach and data analysis would require virtually the same data they are both assigned indexes of 2.

2.7.3.4. Equipment Availability - An experimental approach would require equipment to monitor and test the overall response to identify conflicts. This could involve procurement so that an equipment availability index of 2 is assigned. For simulated data analysis approaches all equipment needed is easily available so they are each assigned a index of 3.

2.7.4. Usefulness

2.7.4.1. Regulatory Need - There are currently investigations being conducted to examine the need for NRC action involving possible conflicts in procedures during normal situations indicating that while these conflicts have not been shown to be significantly dangerous their existence requires attention. However, a program aimed at analyzing normal conditions is not needed presently relative to the need to study off-normal events. As such a regulatory need index of 2 is assigned.

2.7.4.2. Risk Reduction - Studies have shown that a potential for organizational unit procedure conflicts playing a dominant role in safe reactor operation in some off-normal situations. The fact that such conflicts have also been shown to exist during normal operations leads to the conclusion that improved coordination could potentially reduce risk of normal situations becoming off-normal so it is assigned a risk reduction index of 3.

2.7.3. Acceptance

2.7.3.1. Industry Interests - An experimental approach imposed on licensees to identifying conflicts in procedures at a power reactor site would almost surely be opposed by industry so it is assigned an acceptance index of 1. A data analysis research approach would not be opposed if consultation and participation as in the case of D.C. Cook were used so that an index of 2 is assigned.

2.7.4. Summary of Values

Method	Experimental	Simulation and Data Analysis
Practicality		
Cost	1	2
Time Required	2	3
Data Availability	2	2
Equipment Availability	2	3
Usefulness		
Regulatory Need	2	2
Risk Reduction	3	3
Acceptance		
Industry Interests	1	2

References for Section 2.7

1. W.G. Ouchi, Theory Z, Addison-Wesley, Reading, MA, 1981.

2. G.M. Gurican, et al., "A Combined Security and RE&M System Operational Experience at the D.C. Cook Nuclear Plant," presented at ANS Workshop on Power Plant Security, April 25, 1983.

2.8. Rotation/Shiftwork/Manpower

2.8.1. Background

There are many industries in which shiftwork is common; in fact about one quarter of all U.S. workers are employed in shiftwork.[1] These industries involve use of equipment and buildings on a continuous basis either because of economies of scale or because the facility cannot be shut down overnight. In the nuclear energy industry, twenty-four hour-staffing is necessary for the latter reason. Accordingly, the issue of how shiftwork affects the performance of safeguards personnel at nuclear power plants must be focussed on whether shiftwork actually affects performance and, if so, how to remedy any adverse effects. It is not possible to eliminate shiftwork for these personnel.

NRC has issued regulatory guidance on shiftwork but it applies only to "the plant staff who perform safety-related functions (e.g., senior reactor operators, reactor operators, auxiliary operators, health physicists, and key maintenance personnel"). Safeguards personnel are not included.[1a]

There have been many studies of how shiftwork affects individuals in terms of physical health, social and solitary activities, productivity and satisfaction. There have also been studies attempting to focus on the causes for these effects by examining the relative frequency of these problems in communities adapted to shiftwork and those that are not. These studies are discussed below.

This is not a discussion of rotating among jobs within an organization which is a matter of organizational communication (Section 2.7) and attitude (Section 2.9).

2.8.1.1. Physical Health

Studies have shown that shiftworkers generally obtain fewer hours of sleep than day workers.[2] These problems have been attributed largely to noises in the home and community[3] and from deviations from normal social rhythms.[4] Increased appetite and digestive disturbances have been well documented for shiftworkers over day workers. These disturbances have been attributed to changes in rhythmic cycles for eating.[5] Research has shown that elimination rhythms are the most difficult to adapt to in a new work schedule.[6] Upper gastrointestinal disorders have been shown to be more associated with shiftworkers than day workers, however that effect has been primarily attributed to sleep disorders.[7]

The adjustment period for adapting to a new shift has been shown to vary greatly among individuals having a range of four days to two weeks. Research has shown that workers on a weekly rotating schedule have more health disorders than those of larger rotation duration.[8] It has also been demonstrated that some rhythm adjustment problems directly affect mental efficiency.[9] Accident rates are higher for nightshift workers than day workers.[10] These health effects have all been found to have roots in the social and physical environment as well as purely physical body adjustment.[11]

2.8.1.2. Social and Solitary Activities

Shiftworkers show a tendency toward less social contact with friends but show no effect on contacts with relatives.[12] They also participate less in social organizations presumably because their schedule usually precludes serious involvement. Shiftworkers also show an increased tendency toward solitary activities over social activities.[13] General family disturbances were more often found among shiftworkers than day workers[14] along with a higher incidence of sexual problems[15] and divorces[16].

2.8.1.3. Productivity

Nightwork has been shown to have a cumulative effect causing production levels to decrease.[17] Nightworkers are also more likely to make more mistakes than dayworkers.[18]

2.8.1.4. Satisfaction

The level of satisfaction shiftworkers find in their jobs appears to be directly related to how their social environment provides for them. In communities where there is a high shiftworker concentration, the level of satisfaction is very high, but in communities without many shiftworkers it is very low.[19]

2.8.1.5. Role of the Workers's Environment

Most communities are strongly oriented toward a normal day work schedule. It is well established that certain segments of the day have fixed social value that cannot be easily replaced.[20] The shiftworker does not typically have free time when most social activities are scheduled: when children are at home and awake, business and recreational facilities are open, organizational meetings occur, adult TV programs are broadcast, friends and relatives visit, the spouse is awake and not busy, and eating and drinking establishments are open.[21] Shiftworkers have been shown to feel like outsiders in their own communities due to their work schedules.[22] It has also been shown that physical adaptation to new shift schedules take longer for shiftworkers living with persons on non-similar schedules.[23] However, it has been demonstrated that shiftworkers have an easier time adapting in communities where the shiftworker population is relatively high and the community has so adjusted.[23]

2.8.2. Research Approach

2.8.2.1. Data Analysis

There has been considerable research on shiftwork and the data from these studies are generally available. The interest of NRC in safeguards personnel shiftwork practices is that performance may be degraded or alienation occur. The literature already contains many studies on performance and shiftwork so that application of those data may improve the system by which shiftwork is administered (e.g. weekly or monthly rotation). However, because community alienation may contribute to poor attitudes (and even "disgruntlement") measures aimed at minimizing potential alienation may be appropriate.

The issue to be examined is whether the established effects of shiftwork have a derogatory affect on the performance of safeguards personnel at power plants or contributes to any tendency toward malevolence (e.g. becoming disgruntled). If either of these effects were found to be present in safeguards personnel, NRC could consider extending the current shiftwork rules to cover them as well as those important to safety.

2.8.3. Practicality

2.8.3.1. Cost

A data analysis effort aimed first at establishing and assessing the effects of shiftwork on safeguards personnel could be undertaken with little difficulty. Such an approach may involve the use of a survey (i.e., experimental) and/or analysis of data (i.e. data analysis comparing shiftwork practice and performance indicators). This could be accomplished within ½-staff year so is assigned a cost index of 3.

2.8.3.2. Time

A study aimed at establishing and assessing the effects of shiftwork could be accomplished in less than one year so a time index of 3 is assigned.

2.8.3.3. Data Availability

All data needed to study and assess the effects of shiftwork are available so an index of 3 is assigned.

2.8.3.4. Equipment Availability

No equipment is necessary so an index of 3 is assigned.

2.8.4. Usefulness

2.8.4.1. Regulatory Need

NRC has addressed the practice of shiftwork for these positions it considers appropriate. As such NRC probably has less interest in the area of shiftwork than other areas. An index of 2 is assigned.

2.8.4.2. Risk Reduction

If it can be established that safeguards personnel are, in fact, negatively affected by shiftwork, a commensurate decrease in risk is possible. Because of the potential for risk reduction, an index of 2 is assigned.

2.8.5. Acceptability

2.8.5.1. Industry Interests

Licensees would not welcome regulation in this area beyond that already published. Industry may choose to actively oppose further regulation so it is assigned an index of 1.

2.8.6. Summary of Index Values

Data Analysis

Practicality	
Cost	3
Time	3
Data Availability	3
Equipment Availability	3
Usefulness	
Regulatory Need	2
Risk Reduction	2
Acceptability	
Industry Interests	1

References for Section 2.8

1. R.B. Dunham, "Shiftwork: A Review and Theoretical Analysis," Academy of Management Review, Oct. 1977, p. 624.

1a. "Clarification of TMI Action Plan Requirements" NUREG-0737, p. 3-10.

2. F.C. Mann and L.R. Hoffman, Automation and the Worker, Henry Holt and Co., N.Y. 1960; R. Marriot and S. Wyatt, "Night Work and Shift Changes," British Journal of Industrial Medicine, Vol. 10, 1953, p. 164; M. Smith et al., "Health and Safety Consequences of Shiftwork," Ergonomics Vol. 22, 1982, p. 133.

3. P.E. Mott, et al., Shiftwork, Univ. of Michigan Press, Ann Arbor, 1965.

4. N. Kleitman, Sleep and Wakefulness, Univ. of Chicago Press, Chicago, 1963.

5. G.M. Mather, et al., "Man, His Job and the Environment: A Review and Annotated Bibliography of Selected Research on Human Performance," NBS Special Publication No. 319, U.S. GPO, Oct. 1970

6. L. Teleky, "Problems of Nightwork: Influences on Health and Efficiency," Industrial Medicine, 1943, p. 758-779; E. Thiis-Evensen, "Shiftwork and Health" Industrial Medicine, 1958, p. 493; Kleitman, note 4.

7. B. Bjerner and A. Swenssen, "Shiftwork and Rhythm," Acta Medica Scandinavias, Supp. 278, 1953, p. 102.

8. Kleitman, note 4; W. Bloom, "Shiftwork and the Sleep-Wakefulness Cycle," Personnel, Vol. 38, 1961, p. 24.

9. W.P. Calquhour, "Circadian Rhythms, Mental Efficiency and Shiftwork," Ergonomics, Vol. 13, 1970, p. 558.

9b. Smith, note 2.

10. J.V. Chadwick James, "Shiftworking: Physiological Effects and Social Behavior" British Journal of Industrial Relations, Vol. 5, 1967, p. 237.

11. E. Blakelock, "A New Look at the New Leisure," Administrative Science Quarterly, Vol. 4, 1960, p. 446.

12. Mott, note 3.

13. Id.

14. Id.

15. S. Wyatt and R. Marriott, "Nightwork and Shift Changes," British Journal of Industrial Medicine, Vol. 10, 1953, p. 164.

16. Id.

17. Bjerwee, note 7.

18. Blakelock, note 11; A. Wedderburn "Social Factors in Satisfaction with Swiftly Rotating Shifts," Occupational Psychology, Vol. 41, 1967, p. 85.

19. N. Bell and E. Vogel (eds.), A Modern Introduction to the Family, Free Press, Glencoe, Ill. 1960; J. Bossard and E. Boll, Ritual in Family Living, Univ. of Penn. Press, Philadelphia, 1950.

20. Dunham, note 1.

21. Mann, note 2.

22. Calquhour, note 9.

23. Dunham, note 1.

2.9. Attitude

2.9.1 Background

At the initiation of this project a human factor suggested for study by NRC and various industry sources was "corporate attitude". After examination of the issue it became clear that the term "organizational attitude" more accurately reflects the issue of how attitudes affect the performance of safeguards personnel. It has been repeatedly asserted that safeguards must be considered important by the organization as a whole for security to be optimal. This is a salient aspect of safeguards quality.

It has been well established both that organizations differ significantly with regard to attitudes and that those differences manifest themselves in terms of the quality of personnel performance. Organizational attitudes have been successfully altered in many industrial contests resulting in significantly improved organizational performance.[1] Such methods may be of use in improving the performance of safeguards personnel. Some licensee have already attempted to use progressive management techniques for improving safeguards.[2] To now, NRC has not sought to regulate in areas in order to alter attitudes so an indepth discussion of the literature or attitudes is presented.

The organization operating a nuclear power plant, like any other organization, will develop and foster a set of general attitudes toward work. It has been well established that those attitudes contribute greatly to the level of performance of all personnel. It has been shown that an individual will perform optimally when "the goals of the organization and those of the individual became increasingly integrated or congruent."[3] Optimal attitude represents a state in which an individual identifies with a particular organization and its goals and wishes to maintain membership in order to facilitate these goals.[4]

Attitudes are a broader indication of general performance, differing in scope from that of job satisfaction. Attitude is a more global concept which reflects a general response to the organization as a whole emphasizing personal attachment to the organization. It has also been demonstrated that attitude is a more stable performance indicator over time than job satifaction.[5] Optimal attitude is attained when individuals feel 1) a strong belief in and acceptance of the organization's goals and values, 2) a willingness to exert considerable effort on behalf of the organization, and 3) a strong desire to maintain membership in the organization.[6]

For safeguards personnel optimal attitude is important in two different respects. First, performance margins which may exist will be better performed. For instance research has shown that guards sometimes tend to patrol least thoroughly during the last tour of their shift. This example of performance margins capable of being affected by attitudes. In addition, a general attitude among employees that security is important can greatly increase awareness (Section 2.5.1.4). Second, the threat posed by malevolence of a dissatisfied individual in the safeguards organization will be minimized if attitudes are optimal. As such risk may be substantially reduced by measures aimed at assuring optimal attitudes.

The general field of attitudes is usually described under the title of "organizational culture," which can be defined to be a set of beliefs and values which are widely held in an organization. Organizational culture has received considerable recent attention. Managers, researchers, and consultants have concluded that differences in culture can explain why some organizations perform better than others. Despite the current level of interest, however culture is not a new concept. Much work was done in the 1960's and early 1970's on the related topic of "organizational climate," but was discontinued until recently.

Much of the best-known recent work on organizational culture was inspired by the unquestionable success of Japanese companies, relative to their American counterparts, in slowly-growing, unattractive industries (e.g., steel, farm equipment, automobiles). Prompted by this difference in performance procedures initially studied a number of Japanese and American companies and found that they differed significantly on the following dimensions: duration of employment, are held accountable, and the degree to which organizations concern themselves with employees' well-being.[7] These are normally considered personnel practices, but they clearly reflect differences in beliefs about the way people and careers are to be managed in organizations. For instance, the concept of rotating employees among job in different organizational units has been shown to improve organizational communication. It was found that several very successful American corporations were operating in a manner which was consistent with many of the beliefs and values first observed only in Japanese companies. In effect, it was demonstrated in studies that differences in performance had more to do with organizational culture than with national culture.

Work that has been published since, echoes and elaborates this initial research. Other researchers have attempted to explain excellent organizational performance and, not suprisingly, have found that many factors are inolved.[8] Strategy, leadership, appropriate organizational structures, a bias for action, being close to the customer, encouraging entrepreneurship within a large organization, all play a significant role in dictating performance. However, both sets of authors assign culture an important role. More recent research has gone as far as expanding the definition of culture beyond the confines of personnel practices.[9] Many organizational cultures, in reality, are statements of beliefs about how to compete in the external environment. For example, Caterpillar Tractor's attitude can be paraphrased as "24-hour parts service anywhere in the world;" Sears Roebuck's can be stated as "Quality at a good price;" and IBM's and Delta Airline's cultures reflect an overrriding emphasis on customer service. In nuclear power plants an analogy can be made to commitment to safety and safeguards as a set of values and beliefs. While it is difficult to establish explicit linkage to safety (i.e. no significant events), there is overwhelming evidence that safety and safeguards could be improved where these factors are not optimized.

The above-discussed studies derive their conclusions from carefully-done case studies. As such, their results are subject to two criticisms. First, sample sizes are small. Second, the uncover a qualitative relationship between culture and organizational performance. Nevertheless, the evidence they provide is exceedingly convincing.

Organizational climate has been defined as the set of characteristics that describe an organization and that (a) distinguish the organization from other

organizations, (b) are relatively enduring over time, and (c) influence the behavior of people in the organization.[10] Four specific dimensions of climate were later identified. They are individual autonomy, degree of structured imposed on a position, reward orientation, and consideration, warmth and support. Measurement of these climate dimensions reveals something about what it is like to work in a particular organization. It is noteworthy that these climate dimensions are almost identical to the terms initially used to describe organizational culture.[12] Nevertheless, the newer cultural research has made very little use of the earlier work on climate.

Empirical research on climate is almost universally cross-sectional, large-sample, questionaire-based, rather than case-based.[13] As such, it has shown that differences in climate dimensions are definitely associated with differences in organizational and individual performance. However, because so many other variables are involved, the variance explained by cultural variables alone is generally small.

Anthropologists have always considered culture to be central to their discipline. They have pioneered and refined the longitudinal case method for studying culture. However, anthropologists' results are of limited use to managers and organizational researchers because their purpose has almost always been descriptive. They describe a culture and its evolution, but seldom if ever consider the relationship between culture and performance and the issue of purposeful cultural change.

A recent study has resulted in a reconceptualization which accommodates the newer work on culture and the earlier work on climate.[14] Organizational culture is defined to have two components, technical and social. Culture's technical component describes the beliefs widely-held in the organization, regarding which functions, policies, and practices are necessary for successful interaction with the external environment. Culture's social component describes the widely-held beliefs about personnel practices which are appropriate for managing employees. The concept of technical culture is consistent with the findings of the newer research, while social culture is virtually identical to the concept of climate.

2.9.2 Research Approach

2.9.2.1 Experimental. As mentioned above, most of the recent cultural studies are products of in-depth case research. The case method requires gathering background data from secondary sources, and extensive interviewing of large numbers of organization members and others familiar with the organization. It may also involve structured observation whereby the researcher observes the organization over time, but does so according to a structured plan.[15] Case research is generally conducted over an extended period of time.

Because the method is time consuming, the results of case method research are limited by typically small sample sizes (usually one particular firm). On the other hand, case research leads to an understanding of cause and effect relationships which other methods, specifically large-sample questionnaire studies, cannot provide. Also, a variant of this method, "action research," is useful if the objective is to change the organization under study.

In contrast, most climate studies are cross-sectional. That is, they look at climate variables and their relationship to performance at one particular point in time. Also, they use standardized questionnaires administered to a statistically large sample of organization members. Examples of standardized instruments abound.[16]

For example, a survey was recently conducted to measure the climate perceived by nurses at Beth Israel Hospital, a major teaching institution in Boston. A standardized instrument was administered to a very large percentage of the nursing staff. The instrument asked nurses to respond to questions in three areas; the nature of their jobs (in terms of job content, learning opportunities, skills utilized, perceived importance, pay and benefits, level of autonomy required, ambiguity regarding responsibilities, and work place aesthetics); the quality of their supervision (in terms of head nurse feedback, support, and improvement in decisions); and, individual performance (in terms of job satisfaction and stress).

Climate surveys of this kind produce associations that are statistically valid, however, they are short on explanation. The recipient of the survey results is often left to speculate about the nature of the cause and effect relationship between climate and performance. Thus, the recipient may discover that performance is not optimal and that climate may be associated with that level of performance. However, desirable changes may not be clear.

Optimally, a study of culture at a nuclear power plant would include elements of both the case-based and questionnaire-based methodologies. Interviews and observation would be employed to generate a set of hypotheses about the level of organizational and individual performance characterizing an organization. Similar hypotheses about the culture would also be generated. Then hypotheses which connect culture and performance in a case-and-effect way would be generated. A large-sample questionnaire survey, using readily available instruments, would then be conducted to support or disprove the hypotheses.

It is important to note that isolating a single organizational unit and studying its culture and climate separately from the overall organization is very difficult and inefficient. Such a study should be based on the organization as a whole. In this manner baselines are established which can then be applied to each organizational unit (i.e. safeguards).

2.9.2.2 Further Research Formulation

An important consideration is that of how NRC can exercise jurisdiction in this area. To a certain extent such exercises have already taken place.[17] However, efforts to date have stressed optimal static organizational structures and personnel qualifications. The issue of how to best utilize the considerable technical literature on organizational attitudes (i.e. culture and climate) through NRC regulation is not resolved. As a result, further research formulation may lend to a more coherent and rational means for NRC actions. For example, NRC may expand its assessment of organizational aspects of licensees, it may wish to conduct its own research at licensees which rate lower on licensee performance ratings compiled by NRC, it may use these methods in its Regulatory Effectiveness Review Program, and so on. Resolution of these issues

would assist greatly in more realistically recommending further research in a more effective and efficient manner.

2.9.3 Usefulness

2.9.3.1 Cost. An expermental approach could involve a small sample of utilities perhaps 2 or 3. This would involve substantial costs including procurement of relevant experts, travel, data collection, data analysis, and reporting findings. Therefore a cost index of 1 is assigned. Further research formulation would involve only research on these methods and how they could be used with regard to NRC's general regulating authority. This could be conducted using less effort justifying a cost index of 3.

2.9.3.2 Time. A full scale experimental approach would take one to two years so a time index of 2 is assigned. Further research formulation could be conducted in less than one year indicating an index of 3.

2.9.3.3 Data Availability. The data needed to design and manage an experimental approach or further research formulation are readily available meriting an index of 3.

2.9.3.4 Equipment Availability. No equipment is needed for either research approach so an index of 3 is assigned.

2.9.4 Usefulness

2.9.4.1 Regulatory Need. NRC has not formulated a general approach to assessing the organizational aspects of licensees. As a result, an experimental approach may be viewed as premature. This is especially true if only the safeguards organization is examined. However, an experimental approach may be a good point of departure especially if a pilot experiment aimed at assessing the impact of attitudes or performance were performed so an index of 2 is assigned. Further research formulation in this area could be of great use in preparing a regulatory position so an index of 3 is assigned.

2.9.4.2 Risk Reduction. It has been demostrated in NRC's ranking of licensees interms of performance that there are differing levels of organizational performance. It is important to note that these ranking are based primarily on how the organizations perform - not how hardware and equipment perform. As such, it can be assumed that a potential for risk reduction exists meriting an index of 3.

2.9.5. Acceptance.

2.9.5.1 Industry Interest - It is probable that licensees would strongly object to an experimental approach so an acceptance index of 1 is assigned. Further research formulation would face less objection so an index of 2 is assigned.

2.9.6 Summary of Index Values

Practicality	Experimental	Further Research Formulation
Cost	1	3
Time	2	3
Data Availability	3	3
Equipment Availability	3	3
Usefulness		
Regulatory Needs	2	3
Risk Reduction	3	3
Acceptability		
Industry Interests	1	2

References for Section 2.9

1. For recent examples see, L.E. Calonius, "In a Plant in Memphis, Japanese Firm shows how to Attain Quality," Wall Street Journal, April 29, 1983, p. 1; J. Main," Ford's Drive for Quality," Fortune, April 18, 1983, p. 62.

2. R.M. Tuttle, Jr.," Maximizing Motivational Techniques for the Security Force," Presented at the ANS Work Shop on Power Plant Security, April 25, 1983.

3. D.T. Hall, et al., "Personal Factors in Organizational Identification," Administrative Science Quarterly, Vol. 15, 1970, p. 176.

4. M.T. Monday, et al., "The Measurement of Organizational Commitment," Journal of Vocational Behavior, Vol. 14, 1979, p. 224.

5. L.W. Porter, et al., "Organizational Commitment, Job Satisfaction, and Turnover Among Psychiatric Technicians," Journal of Applied Psychology, Vol. 59, 19 1974, p. 603; P.C. Smith et al., The Measurement of Satisfaction in Work and Retirement, Rand-McNally, Chicago, 1969.

6. Monday, note 4.

7. Ouchi, W.G. Theory Z, Addison-Wesley Reading, MA, 1981.

8. Pascale, R.T., and Athos, A.G. The Art of Japanese Management. New York: Warner Books, 1981; I.J. Peters and R.H. Waterman, "In Search of Excellence," N.Y., 1982.

9. Deal, T.E., and Kennedy, A.A. Corporate Cultures: The Rits and Rituals of Corporate Life. Reading, MA; Addision-Wesley, 1982.

10. Forehand, G., and Gilmer B. "Environmental variation in studies of Organizational Behavior." Physchological Bulletin, 1964, 22, 361-382.

11. Campbell, J.P., Dunnette, M.D., Lawler, E.E. III, and Weick, K.E. Jr. Managerial Behavior, Performance and Effectiveness. New York: McGraw-Hill, 1970.

12. Ouchi, Note 7.

13. See for example: Johnston, H.R. "A New Conceptualization of Source of Organizational Climate." Administrative Science Quarterly, 1976, 21, 95-103; Lawler, E.E. Jr., Hall, D.T., and Oldham, G.R. "Organizational Climate: Relationship to organizational structure, process and performance." Organizational Behavior and Human Performance, 1974, 11, 139-155; Litwin, G, and Stringer, R. Motivation and Organizational Climate. Cambridge, MA: Harvard University Press, 1963; Schneider, B. "Organizational Climate: Individual preferences and organizational Realities." Journal of Applied Physchology, 1972, 56, 211-217.

14. Gupta, A.K., and Stengrevics, J.M. "Strategy, Culture and Climate: A Reconceptualization," to be presented to the Academy of Management, August 1983.

15. Mintzberg, H. The Nature of Managerial Work. New York: Harper and Row, 1973.

16. For example see, Pritchard, R.D., and Karasick, B.W. "The Effects of Organizational Climate on Managerial Performance and Job Satisfaction." Organizational Behavior and Human Performance, 1973, 9, 120-146; Lowler, Note 8; Johnson, Note 8; Schneider, Note 8.

17. Osborn, et al. "Organizational Analysis and Safety for Utilities with Nuclear Power Plants," NUREG/CR-3215, PNL-4655, July 1983.

2.10. Instruction and Training

2.10.1. Background

A principal question to resolve in this area is whether it would be advisable to promulgate more uniform standards for instruction, training, and selection of guard force personnel at nuclear power plants. At present, there are wide ranges of operational practice in all three domains. Training and instruction programs vary enormously from site to site.[1] NRC has published guidance on training programs[2] but this study has indicated that training still varies among licensees. Likewise, selection is left in large part to local discretion, in spite of a large number of highly specific qualifications required in 10 CFR 73.55, Appendix C. Some sites hire and train their own guard forces, others hire outside contractors to be responsible for hiring and training physical security forces.

It has been suggested that instruction be required to include specific training to gauge and improve guard force reactions to realistic safeguards situations by simulating possible safeguards events and having trainees respond. This kind of training closely overlaps with improved drills which will be covered in section 2.14 dealing with performance evaluation. Evaluations provide feedback to improve training programs. Further, there exists a considerable body of knowledge in training theory which should be of use in the case of safeguards personnel at power plants.

Future work should investigate the practicality and desirability of imposing more uniform standards on the nuclear industry, as well as the possibilities for improving selection criteria, guard training techniques using realistic emergency conditions, and devising new or additional instruction, training and selection criteria which are more closely task related than some of those currently in use. At a minimum specific and detailed criteria for assessing the adequacy of licensed training and qualifications plans should be developed.

In terms of selection preemployment, aptitute tests have proven to be of use. At Duke Power Company, the use of a scientifically designed test to select people who are primarily oriented toward security has lowered their attrition rate to 7-8% for employees and 10-12% for contractor personnel.[3] These attrition rates are well below normal for safeguards personnel nuclear power plants.

Research has shown that the important questions with regard to training and instruction are:

- Determining the scope of the training - Are all security personnel trained equally or just selected persons on all shifts?
- Securing appropriate, cost effective training materials - Are they easily available?
- The availability of training facilities and equipment - Live ammunition obviously cannot be used, but are there suitable alternatives?

- Overcoming any resistance from other plant orgnizational units to having security training taking place onsite.

- Creating realistic drills which will provide beneficial training experiences that rise above playing "cops and robbers".[3]

NRC currently receives for review a Training and Qualifications Plan for safeguards personnel which documents the licensee's training and instruction plan. The development of performance evaluation criteria based on determinants which have been demonstrated to be related to the quality of training programs could be of use to NRC as an alternative to specific training requirements. However, specific assessment criteria for reviewing licensee plans is still desirable.

2.10.2. Research Approach

2.10.2.1. Experimental

An experimental approach would involve drills aimed at performance evaluation to generate data related to the effectiveness of selection and training programs. This type of job performance is not necessarily restricted to nuclear power plant security so that alternative facilities could be used (e.g. Department of Defense or Department of Energy). The purpose of such an experiment would be to establish valid criteria for determining the adequacy of selection and training programs.

2.10.2.2. Data Analysis

An evaluation of data on power plant safeguards selection and training programs and indicators of performance could be undertaken. A method for classifying aspects of training programs and the outcome in terms of performance could be devised as appropriate measurement instruments are developed.

2.10.2.3. Further Research Formulation

The area of selection, instruction and training ties indirectly with several other areas in this study (i.e., performance evaluation (2.14), human reliability (2.5), use of force (2.12), staff coordination (2.13), etc.). There are many promising new techniques available for training involving drills (MILES and SSORA, Section 2.14). Options for attaining improved selection and training through regulation or further guidance could be explored along with the potential of using new techniques.

2.10.3. Practicality

2.10.3.1. Cost

A well-defined, comprehensive effort in this area could be quite costly. To adequately assess drills as an experimental approach would involve in excess of two staff-years warranting a cost index of 1. If data analysis were pursued, similar costs may be encountered. Further research formulation could probably be accomplished for less than two staff-years of resources therefore receiving a cost index of 2.

2.10.3.2. Time

An experimental project and/or data analysis could possibly be finished in one to two years receiving at time index of 2. Further research formulation could be accomplished in less than one year warranting a time index of 3.

2.10.3.3. Data Availability

The data needed for any of the research approaches considered are available but would have to be collected warranting a data availability index of 2.

2.10.3.4. Equipment Availability

For an experimental approach equipment capable of recording data from drills must be used. Since it can be obtained through normal procurement an index of 2 is assigned. For data analysis and further research formulation no equipment is needed so an index of 3 is assigned.

2.10.4. Usefulness

2.10.4.1. Regulatory Needs

NRC currently evaluates the adequacy of Training and Qualification Plans submitted by the licensees. No detailed, comprehensive set of assessment criteria are presently used in this determination. Because of the highly divergent nature of individual programs, it can be assumed NRC would find criteria of substantial use so that an index of 3 is assigned.

2.10.4.2. Risk Reduction

The assurance of safeguards personnel effectiveness which could result from a valid set training program assessment criteria could be substantial. As such an index of 3 is assigned.

2.10.5. Acceptability

2.10.5.1 Industry Interests

While industry may not actively object to better assessment criteria they probably would oppose a set of uniform requirements. Assuming the objective will be to develop assessment criteria on acceptability index of 2 is assigned. Comprehensive training requirements would probably be highly resisted.

2.10.6. Summary of Index Values

	Experimental	Data Analysis	Further Research Formulation
Practicality			
Cost	1	1	2
Time	2	2	3
Data Availability	2	2	2
Equipment Availability	2	3	3
Usefulness			
Regulatory Need	3	3	3
Risk Reduction	3	3	3
Acceptability			
Industry Interests	2	2	2

References for Section 2.10

1. R. Kindilien and R.K. Harper, "Practical Implementation of Security at Nuclear Power Plants - Impact on Cost, Operations and Safety," presented at ANS Workshop on Power Plant Security, April 25, 1983.

2. "Site Security Personnel Training Manual," NUREG-0464; "Vehicle Access and Search Training Manual," NUREG/CR-0485; "Nuclear Power Reactor Security Personnel Training and Qualification Criteria," NUREG-0576; "Security Personnel Training and Qualification Criteria," NUREG/CR-1327.

3. Private Correspondence, Atomic Industrial Forum, May 2, 1983.

4. Kindilien, note 1.

2.11. Format and Wording of Contingency Plans

2.11.1. Background

This topic deals both with procedures for selecting appropriate guard responses and with the format for displaying those responses. The guard force is assumed to follow contingency plans given a series of alarms indicating either a safeguards-related event or a false alarm. Much research and study has already been accomplished regarding the appropriate tactical response of a guard force in case of defined contingency events involving design basis threats.[1] NRC has published guidance on acceptable security plans.[2] Practical exercises to test the effectiveness of the tactics developed have also been widely used. However, the usefulness of contingency plans as a procedures document has been widely questioned. Contingency planning documents may function more as a statement of procedural security policy than anything else since expeditious reference to them during an event is hampered by their format. For more complex threats in which there is time available for consultation NRC, has formed an Information Assessment Team which is on-call to assist in assessing the seriousness of threats involving licensed facilities.[3] Problems outstanding include: methods of improving the assessment accuracy of alarms in the minimum reasonable time; means of making available to the CAS/SAS the correct procedures to follow in the event of possible combinations of alarms; doing the latter in the most efficient way possible which minimizes the possibility of human error; developing means of testing the effectiveness of the previously developed tactics and human-machine interface systems. A substantial amount of work in this area has already been completed.[4]

2.11.2. Research Approach

2.11.2.1. Experiment - Use could be made of evaluative methodologies of format presentation aimed at testing the effectiveness of systems for communicating rapidly to the guard force the correct procedures to follow in the event of a contingency. In addition, practical exercises could be developed which test the ability of the guard force to follow procedures correctly. Apart from the efficient display of the correct procedures to the CAS/SAS, the question of whether the guard force can and will perform the correct procedures even when available can also be addressed.

2.11.2.2. Data Analysis - There is a need to review the tactics to be used by guard forces in light of previous analyses and the results of the several drill-type exercise techniques such as MILES and SSORA (section 2.14). However, the data are easily available and it would be useful to correlate them to develop modifications for optimal responses. Data analysis could be aimed at prior safety related display technologies (e.g. Safety Parameter Display System).

2.11.2.3. Further Research Formulation - This research approach involves the study of new methods for aiding the CAS/SAS to correctly assess any alarm or set of alarms as quickly as possible, in a correct manner, and accurately distinguishing real from false alarms. A rapid and correct response is most vital in reducing plant vulnerability to an external assault and providing increased deterrence to potential events. Many new studies have been conducted and can be comprehensively reviewed in the context of this issue. For instance,

it has been suggested that selective use of the two-man rule may improve response capabilities.

2.11.3. Practicality

2.11.3.1. Cost

For the experimental program, at least two staff years of effort are needed to accomplish the required tasks warranting an index of 1. For the data analysis approach, the work to be done requires a few months of staff effort meriting an index of 3. For work under further research formulation, between one and two staff-year's worth of effort is anticipated yielding an index of 2.

2.11.3.2. Time - The experimental tests may require several year's worth of effort, indicating an index 1. The data analysis approach would be substantially more rapid, giving an index level 2. Further research formulation would, like the experimental program may take time to formulate better research meriting an index of 2.

2.11.3.3. Data Availability - For the experimental methodology, data needed for experimental design and management should be obtainable. Since appropriate data would have to be collected an index of 2 is assigned. For the data analysis of this topic, the availability of data is high and an index of 3 is justified. Further formulations in this area probably require much work in devising experiments and in data reduction. An index of 1 is assigned.

2.11.3.4. Equipment Availability - For the tests of developed methodologies, some procurement of equipment would be necessary. Developing practical exercises and measuring guard responses might also necessitate the designing of equipment. All this argues for an assignment of an index 1. For data analysis, equipment requirements are minimal warranting an index of 3. Finally, future research formulation may entail procurement of specialized equipment and is assigned an index of 2.

2.11.4. Usefulness

2.11.4.1. Regulatory Needs - Regarding the development of tactical responses or testing the effectiveness of newly-developed alarm display and assessment techniques, the need is perceived as reasonably great. If there are deficiencies in either of these areas, they should be understood and remedied as soon as possible. New software and procedures are currently being introduced[3] so an index of 3 is justified. As far as efforts toward further research formulations are concerned they less directly affect the needs of NRC so an index of 2 is assigned.

2.11.4.2. Risk Reduction - Similarly to the preceding section, the results from experimental evaluations and data analysis of current techniques have a great effect on risk reduction warranting an index of 3. The longer term further research formulation effort would again probably have a lower effect on risk rating an index of 2 until measures are implemented.

2.11.5. Acceptance

2.11.5.1. Industry Interests - For experimental and data analysis approaches to improving guard force response reliability, particularly if methods are developed at nominal cost using current equipment, industry acceptance is likely to be high warranting an index of 3. For the further research formulation approach, there is probably going to be some resistance in expectation of more "ratcheting" in the area, unless clearly improved performance is certain to result so an index of 2 is assigned.

2.11.6. Summary of Values

	Experimental	Data Analysis	Further Formulation
Practicality			
Cost	1	3	2
Time	1	2	2
Data Availability	2	3	1
Equipment Availability	1	3	2
Usefulness			
Regulatory Needs	3	3	2
Risk Reduction	3	3	2
Acceptance			
Industry Interests	3	3	2

References for Section 2.11

1. See for example R.A. Al-Ayat, et al. "Analyzing Safeguards Alarms and Response Decisions," NUREG/CR-2404, January 1982; D.G. Baehr, et al. "Tactical Improvement Package," NUREG/CR-2400, July 1982; D. Engi and C.P. Harlan, "A Study of Fixed Site Neutralization Model (FSNM); NUREG/CR-0787, November 1979; S. Rountree, "Security Officer Response Strategies (SECURORS)," NUREG/CR-2588, March 1982.

2. "Acceptance Criteria for the Evaluation of Nuclear Power Reactor Security Plans," NUREG-0908, August 1982.

3. G.W. McCorkle, "The NRC Threat Assessment Program," presented at ANS Workshop on Power Plant Security, April 25, 1983.

4. S. Weissman, "A Microcomputer Based System for Intrusion Detection Display and Assessment," IEE Transactions on Nuclear Science, Vol. NS-29, February 1982. Some other related developments can be found in Z. Kravets and D. Rockford, "The Configuration, Development, and Interface of a Nuclear Power Plant Security System, American Nuclear Society Power Plant Security Workshop, Savannah, Georgia, April 25, 1983; G.M. Gurican, et al., "A Combined Security and RE&M System Operational Experience at the D.C. Cook Nuclear Plant," presented at ANS Workshop on Power Plant Security, April 25, 1983; P. Bierre," Teaming Human and Artificial Intellegence for High Productivity Security Systems," in "The Human Element in Organizational Sensitivity," DNA-TR-82-13, November, 1982.

2.12. Use of Force

This human factor was originally named "the use of deadly force and self-preservation." During the course of this study it was recognized that the "use of force" included all aspects of police power including arrest, search, seizure and deadly force, and is, therefore, more appropriate. The impact of this human factor has been argued to be both significant and meaningless so resolution of this issue is desireable.

2.12.1. Background

A guard may have to use force against an individual in order to stop an act against the facility. The guard's willingness to use force and the justifications for such use are important to the quality of site security. Legal problems have been asserted to exist, however these problems may not affect the quality of a safeguard.

Historically, nuclear power plants have been primarily regulated by the federal government with state involvement limited to matters such as zoning and land use permits. Early Atomic Energy Commission facilities were heavily guarded with strict paramilitary security requirements. Early commercial nuclear power plants, however, provided only industrial level security until the NRC (AEC's successor) began to implement increasingly stringent regulations requiring additional security at licensed facilities. These increased security requirements, which have been imposed for the most part in the last ten years were in response to the NRC's growing awareness of the potential risk from the possibility that a nuclear facility could be sabotaged causing radioactive materials to be released.[1]

Regulation of radiological hazards is a sphere of authority specifically granted to NRC by the Atomic Energy Agency Act[2] and confirmed in many court cases.[3] Using the Atomic Energy Act as authority, the NRC has required utilities to provide physical barriers and an armed guard force to protect licensed reactor sites.

The states and localities have always been free to regulate most aspects of electrical generation including price rates, siting, non-radioactive effluents, air pollution, location of power lines and so on. As a result, states and localities have had control over most regulatory aspects of fossil fuel and hydroelectric generating stations. This is not the case for nuclear stations. The traditional regulatory relationship utilities have had with states on fossil or hydro plants has changed in the case of nuclear stations because they pose a very serious public health and safety threat if sabotaged. Because of the threat of radiological sabotage the level of security required by NRC for nuclear sites is far higher than the normal industrial security measures employed at fossil or hydro sites.

Industrial security is regulated by the states under an exercise of their constitutional police power. As a result, it has always been clear that security guards and activities at fossil and hydro sites are subject to state legal jurisdiction and are, therefore, state regulated.[4] Security guards at any industrial site, unless specifically deputized (i.e., designated as a public peace officer or police officer), possess no more legal authority to arrest or use force

than any private person. They are, in fact, considered "private persons" in any legal proceeding.

The security practices at nuclear power plants are extremely rigorous relative to industrial security generally. However, the state and local laws which have traditionally governed security practices still control security activity undertaken to conform with federally mandated security requirements. In this interface between state and federal requirements some commentators have alleged that federal and state requirements may conflict. However, no conflict has been revealed by examination.

The legal exercise of force is an evolving subject which, although heavily litigated and studied, varies from state to state. Because the jurisdictional issues of state-versus-federal, involved in nuclear power plant security, are relatively new, there are some unresolved practical issues concerning the use of force by nuclear power plant safeguards personnel. It is important to note, however, that these unresolved issues can only be realistically resolved by the courts or legislation. NRC administrative decisions or opinions in this area are not helpful because the subject involves fundamental constitutional questions[5] such as equal protection, substantive due process, eighth amendment cruel and unusual punishment, procedural due process, right to trial and fourth amendment excessive use of force tort questions. Hence, further legal research in the area is not likely to be helpful to the further resolution of any existing conflicts. In addition, NRC policy has been repeatedly stated that all plant security practices and particularly those involving the use of force, must conform to state and local law.[6]

What is at issue, however, is how safeguards personnel performance may be affected by any legal or policy ambiguities in these areas. For example, it cannot be made completely clear in advance under the law whether the use of deadly force is justifiable in all circumstances. Hence, a security guard using deadly force in a marginal situation may be subject to prosecution under the state laws which have traditionally governed such conduct. However, no amount of NRC research can resolve these conflicts except where they are obvious. The best approach is to assure that the safeguards personnel understand the law and its constraints so that an informed decision can be reliably made when the occasion arises.

Safeguards personnel who are now standing on the cutting edge of this legal issue must be properly trained or they may use overly conservative judgements in conducting their job related responsibilities. The use of conservative security at a site may degrade the level of protection sought to be provided.

2.2.2. Research Approach

2.12.2.1. Experimental - It may be reasonable to conduct an experimental data gathering exercise aimed at assessing the impact in terms of personnel performance of ambiguities involved in authority to use force. This could be accomplished using standardized measurement instruments and interviews. If it can be shown that safeguards personnel do perceive a potential for degraded performance stemming from these legal ambiguities then a mitigating strategy can be developed. However, it is important to first establish whether there is a potential performance problem involving legal ambiguities.

2.12.2.2. Further Research Formulation - If a problem can be identified which links potential performance deficiencies with ambiguity concerning the use of force then a mitigation strategy must be developed. This would probably require an extensive examination of training and drills in this context.

2.12.3. Practicality

2.12.3.1. Cost - An experimental approach can be used to determine the existence of a problem such as this. The cost would be minimal (under one staff-year) so a cost index of 3 is assigned. Further research formulation could be done for a similar cost and is assigned an index of 3.

2.12.3.2. Time - Neither experimentation or further research formulation would take more than one year so that a time index of 3 is assigned.

2.12.3.3. Availability of Data - The data needed to set up an experimental approach to this problem are easily available. They are principally related to methodological issues so an index of 3 is assigned. For further research formulation data are available but must be collected so an index of 2 is assigned.

2.12.3.4. Availability of Equipment - No equipment is needed for either approach so an index of 3 is assigned.

2.12.4. Usefulness

2.12.4.1. Regulatory Need - There persists a question of whether there is a problem in nuclear power plant safeguards due to these legal ambiguities. The real nature of the legal ambiguities can even be questioned since, for most postulated situations, safeguards personnel can reliably decide whether force is justified using the general rules of law. The issue is whether safeguards personnel understand the general law and can work comfortably with it. As a result, a reliable data collection exercise aimed at measuring the real nature of the problem if it exists would be very useful. Therefore, a regulatory need index of 3 is assigned. For further research formulation little of real practical use could result so an index of 1 is assigned.

2.12.4.2. Risk Reduction - If real life threatening safeguards contingencies involving threats to the reactor arise, then an increase in risk to the public may exist at that time. It would be in these situations, specifically, where both higher risk and increased performance demands are simultaneously at work. It has been shown that guards respond better when made aware of the difficulties they may face in advance. If a problem does exist, then any improvement in personnel performance during the time in which they are most needed could greatly reduce risk. As a result, development of a mitigation strategy could potentially reduce risk. A risk reduction index of 3 is assigned.

2.12.5. Acceptability

2.12.5.1. Industry Interests - It is certainly in the interests of a power plant owner to have the laws concerning the use of force correctly followed by their guard force. A strategy that identifies the problem and in-

volves a mitigation strategy would be of great use. However an experiment alone could only serve to focus attention on it so industry may chose to oppose a survey of guards. It is doubtful however that active opposition would arise to an acceptability value of 2 is assigned. Further research formulation may be more acceptable than experimentation however it is also assigned a value of 2.

2.12.6. Summary of Factor Values

	Experimental	Further Research Formulation
Practicality		
Cost	3	3
Time Required	3	3
Data Availability	3	2
Equipment Availability	3	3
Usefulness		
Regulatory Needs	3	1
Risk Reduction	3	3
Acceptability		
Industry Interests	2	2

References for Section 2.12

1. 10 CFR 73.55.

2. Atomic Energy Act of 1954, as amended.

3. Northern States Power Co. v. State of Minnesota, 447 F2d 1143 (CA 8th, 1971), affd., 405 US 1035, 31 L Ed 2d 576, 92 S Ct 1307 (1972).

4. Kakalik and Wildhorn, Private Police in the United States: Findings and Recommendations, 1971.

5. "Deadly Force to Arrest: Triggering Constitutional Review," 19 Harvard Civil Rights - Civil Liberties Law Review, p. 1976, p. 361.

6. See Lester B. Orfield, Criminal Procedure Under the Federal Rules, Vol. I 4.6, 140.

7. "Deadly Force to Arrest," Note 5, p. 384.

2.13. Staff Coordination

2.13.1. Background

The Three Mile Island incident, among others, suggested that security forces at nuclear reactors could respond more effectively during safety-related emergencies. In addition, concern has surfaced over the possibility of operational personnel not being sufficiently aware of security procedures to cooperate in neutralizing a security threat.

Regulatory requirements for emergencies at power plants are set forth in Title 10 of the Code of Federal Regulations Parts 50 and 73 (10 CFR 50, 73). The required emergency plan outlined in Appendix E to 10 CFR 50 is intended principally to be advanced planning for handling radiological consequences of accidents at licensed plants. 10 CFR 50.34(c) requires a physical security plan in accordance with criteria in 10 CFR 73.55, and 10 CFR 50.34(d) requires that a safeguards contingency plan be developed as set forth in 10 CFR 73, Appendix C. Little is said in regulatory guidance concerning the actions of security guards during safety-related emergenices or visa versa. In a recent paper, the author points out:

> It is noteworthy that minimal mention is made in applicable regulations and guidance materials regarding security actions during an emergency. Appendix E to 10 CFR Part 50 indicates that security personnel must be trained to perform their duties during (a safety-related event) and NUREG-0654/FEMA-REP-1 in Table B-1 indicates that security personnel should perform site access control and personnel accountability "per the security plan." Regulatory Guide 1.101 infers that security personnel may be involved in events triggering the declaration of an emergency action level and that an emergency action level may be initiated by sabotage. The regulatory guide also indicates that security is a functional area that must be addressed in the emergency response plan for purposes of shift assignments. Other than this, the actions of security personnel, and the interface between emergency planning and security planning are not addressed in detail in appropriate regulatory materials.
>
> In terms of safeguards contingency planning, licensees are required to develop a series of actions to respond to events involving progressively more serious threats to the security of the plant, to define the objectives of the response to each event, to identify the information required and the necessary decisions to support the response, and to indicate the conditions under which response to an initiating event should be upgraded. In addition to the information in the safeguards contingency plan, a set of procedures must be developed which details the actions to be taken and decisions to be made by each position or entry assigned responsibilities in the safeguards contingency plan. Depending on the guidance used, approximately 22 events must be covered by the safeguards contingency plan.[1]

When examining the procedures for operational and safeguards personnel to follow during site emergenices it becomes clear that procedures tend to segregate security responses to safeguards threat situations from security response to operational emergencies. Planning has not generally considered an operational emergency intertwined with a security threat. The resulting gap in proce-

dures must be addressed in an ad hoc fashion during an event and coordination problems could occur. Studies have shown that the following aspects of safeguards contingency and emergency response should be addressed:

(1) identification and description of any special security for functions, reorganization, or responsibilities required during a safety related event.

(2) the likelihood of sabotage or threat of sabotage occurring during a safety-related event,

(3) special equipment and training required by security,

(4) implementing procedures that cover all functions required of security during a safety related event including necessary deviations from approved security plans, and

(5) provisions for drills and training to develop the necessary practical abilities to accomplish the planning goals.[2]

Issues which arise from these considerations include organizational (i.e., how the security organization functions within the overall emergency response organization), training (e.g., the use of radiation protection equipment), and manpower (i.e. the need for reserve personnel).

It has also been suggested that a glossary of terms be developed to allow safeguards and operational personnel to communicate more effectively. This would allow nontechnical personnel (safeguards) and technical personnel (operational) to communicate and understand plant status and determine security priorities during an emergency.[3]

Work has been done to analyze the operational impact of access control systems. A methodological approach using personnel transit times into and out of vital areas was developed as part of the International Training Course on the Physical Protection of Nuclear Facilities and Materials. While more work is needed on that particular method to make it useful, it points out potentially fruitful research.[4]

NRC currently conducts the Regulatory Effectiveness Review Program which has several objectives. These are 1) to evaluate the overall effectiveness of physical protection systems as implemented on a site basis, 2) to identify generic issues and validate the regulatory basis, 3) to assist licensees in cost effective application of security assets, and 4) to identify safety problems resulting from safegurds procedures.[5]

The forth objective directly and the others indirectly address the issue of staff coordination during emergencies. This program has been found to be effective in improving staff coordination.

NRC has also released a study which investigates the impact of security on plant safety.[6]

2.13.2. Research Approach

2.13.2.1. Experimental

Collection of primary data could be accomplished through drills that are designed to reveal when and how staff coordination can become difficult. Research has shown that drills are necessary to develop the "practical abilities to accomplish planning goals."[7] The information necessary to design and manage drills such as job task analyses for safeguards personnel during emergencies is available. The cost of conducting drills has been shown to be reasonable[8] and data collection could be done systematically. The objective of such an experiment would be to verify the existence of coordination problems and identify the scope and nature of these problems.

2.13.2.2. Data Analysis

Analysis of existing procedures to reveal potential coordination problems is ongoing internally at some power plants. In addition, a large part of NRC's Regulatory Effectiveness Review Program is aimed at such data analysis. The review team examines the licensee's final safety diagrams and a vital area analysis to identify routes toward radiological sabotage. Then a set of site specific data sheets are developed for documenting relevant features of site safeguards hardware and procedures. To collect sufficient information to perform meaningful data analysis on safety and safeguards procedures, schedules, practices, and so on would be useful in identifying such problems.

2.13.2. Practicality

2.13.2.1. Cost

Assuming that some type of drill program is in place at a facility, an experiment designed specifically to identify staff coordination problems could be accomplished at a relatively low cost. The problem with this research is that results will be relatively site-specific necessitating such an approach at each reactor site. It will be assumed here that NRC would simply want to verify an experimental drill method that can be demonstrated to identify problems in and improve staff coordination. As such only two or three trials would be necessary. This could be accomplished for less than $50,000[9] and is assigned a value of 3. Data analysis would have similar site specific disadvantages, however, both NRC's Regulatory Effectiveness Review Program and industry's internal efforts have been aimed at data analysis, so a project to verify the usefulness of data analysis in identifying problems in and improve staff coordination could be done without great difficulty. Therefore a cost value of 3 is assigned.

2.13.2.2. Time

Using either technique a project aimed at verifying the use of either experimental (drills) or data analysis (procedures) to develop improved staff coordination could be done in under one year. As a result a time value of 3 is assigned.

2.13.2.3. Data Availability

The data and information needed to design and manage a drill experiment aimed at revealing problems in staff cooperation is available so a data availability value of 3 is assigned. This will be especially true if organizational communication is previously addressed (Sec. 2.7).

2.13.2.4. Equipment Availability

To conduct a drill procurement is necessary for simulated weapons and equipment used to record the event for later analysis. Equipment availability for an experimental approach is 2. For a data analysis approach no additional equipment is needed so a value of 3 is assigned.

2.13.3. Usefulness

2.13.3.1. Regulatory Need

It has been recognized that the functional organizational structure at nuclear power plants does not fully account for procedures and related events during off-normal situations. NRC may opt to perform a Regulatory Effectiveness Review at all facilities which is an activity which would encompass a data analysis project although the depth of that review may not be as great as is warranted. In that case, the review team could simply increase the scope and rigor of their data analysis. As a result, a project aimed solely at data analysis techniques would be of possible use to NRC they are assigned a regulatory need value of 2.

For an experimental approach regulatory guidance may be more appropriate. As noted in Section 2.14, there is limited existing guidance on designing and managing drills. As a result, a regulatory need of 3 is assigned to developing an experimental drill approach to identifying and improving staff coordination problems.

2.13.3.2. Risk Reduction

Since risk is at its highest during a site emergency, whether it is a safeguards contingency or safety related event, considerable risk reduction may potentially result from improved staff coordination during emergencies. As a result a risk reduction value of 3 is assigned.

2.13.4. Acceptability

2.13.4.1. Industry Interests

Licensees are generally willing to pursue research in this area on their own when evidence of a problem actually exists. Different licensees may have different views as to the existence of a problem. It is not likely that industry would oppose guidance in these areas if that guidance were aimed at assistance and voluntary corrective activities as in the Regulatory Effectiveness Review Program. Therefore an acceptability value of 2 is assigned.

2.13.5. Summary of Feasibility Factors

	Experimental	Data Analysis
Practicality		
Cost	3	3
Time	3	3
Data Availability	3	3
Equipment Availability	2	3
Usefulness		
Regulatory Need	3	2
Risk Reduction	3	3
Acceptability		
Industry Interests	2	2

References for Section 2.13

1. D.A. Moul, "Security During Safety-Related Emergencies at Nuclear Power Plants," presented at ANS Workshop on Power Plant Security, April 25, 1983.

2. Id., "The Role of Security During Safety Related Emergencies at Nuclear Power Plants," NUREG/CR-3251, forthcoming.

3. V.M. Callaghan, "Safety Functions: Role in Security and Safety Interfacing" presented at ANS Workshop on Power Plant Security, April 25, 1983.

4. T.J. Leahy, "Assessing the Impact of Access Control Systems on Plant Operations," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

5. G.W. McCorkle, "The NRC Regulatory Effectiveness Review Program," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

6. "Report of the Committee to Review Safeguards Requirements at Power Reactors," NUREG-0992, May 1983.

7. Moul, note 1.

8. C.E. Higgins, "Cost Effective Plant Security," presented at the ANS Power Plant Security Workshop, April 25, 1983.

9. Id.

2.14. Performance Evaluation

2.14.1 Background

There are two types of performance evaluation techniques which can be used to evaluate safeguards personnel at nuclear power plants. These are 1) evaluations drawn from drills and exercises meant to stimulate actual safeguards events and 2) evaluations made by superiors of individual performance based on organizational practices. These are two discrete activities which can be used in combination or separately. These techniques provide feedback in terms of training program design and selection criteria.

Presently NRC requires physical, mental, training, and weapons requalification annually.[1] Requalification activities are aimed at assuring adequate performance if a safeguards event should occur. NRC Regulatory Guide 1.17[2] stipulates that ANSI/ANS 18.17[3] be used as a reference for satisfying federal requirements. The ANSI/ANS standard calls for "appropriate training with particular emphasis on those matters for which the person has responsibility. This training shall be conducted by or under the direction of the owner organization...and retraining shall be conducted annually."[4] No where in the regulations or related guidance does any particular means evaluation of performance directly appear as a requirement. However, under the regulations there is a general requirement that safeguards personnel:

> "demonstrate mental alertness and the capability to exercise good judgement, implement instructions, assimilate assigned security tasks and possess the acuity of senses and ability of expression sufficient to permit accurate communication by written, spoken, audible, visible, or other signals required by assigned job duties."[5]

The ANSI/ANS standard does not address this generalized requirement for a performance evaluation program.

In addition, regulations require requalification of general and weapons training abilities.[6] The original version of the ANSI/ANS standard published in 1973[7] did contain a section on drills and tests:

> 4.8 Drills and Tests. Periodic drills and tests shall be conducted to provide reasonable assurance of the effectiveness of security measures, to assess the adequacy of performance of employees and security force personnel and to demonstrate operability of equipment. Full participation of off-site support groups need not be a part of drills; however, communications with such groups should be verified during such drills.[8]

However this language was deleted from the upgraded ANSI standard released in 1982.[9] As such, there is no current guidance on whether licensees should conduct drills except as contained in each licensee's approved Training and Qualifications Plan which varies from site to site. In addition, drills are generally conducted more as a practice and training exercise than as a performance evaluation tool so that formal evaluations may not be practical.

The two types of performance evaluation methods are discussed below.

2.14.1.1. Task Based Performance Evaluation

A reliable indicator of how an individual will perform a job task is to observe the individual performing the task itself. For safeguards personnel, that is not a viable practice because real events do not occur with any type of frequency. Indeed, safeguards activities are designed to minimize the possibility of such events through deterrence. Exercises which simulate safeguards events must, therefore, be used to observe the actual performance of safeguards personnel.

While standard drills can be used, they are not direct surrogates for real situations. Drills are normally aimed at practice and training rather than evaluations. Systems which increase the evaluative nature of drills have been developed. For example, the Multiple Integrated Laser Engagement Simulation (MILES)[10] was developed to simulate actual armed intrusions by using laser rifles and laser sensitive vests worn by intruders and security personnel. It has been used by DOE and DOD to simulate security events. Another system developed to simulate intrusions and record security personnel response is the Security System Operational Recording and Analysis (SSORA) system. It is connected to record all site security systems (e.g. alarms, communications equipment, etc.) for approximately ten days and video tapes guard force responses to stimuli from the SSORA team. All recorded information is then analyzed.[11]

Both of the systems described above have been used to evaluate site security with good results. Improvements in security can be measurably demonstrated. For instance, the SSORA system has been used at five military installations in the U.S. and Europe in over 140 simulated intrusions. Follow-up SSORA exercises have shown dramatic changes in search behavior, in attention paid to equipment calibration and alignment, and in a better understanding of environmental factors.[12]

These and other systems may be employed to evaluate the performance of safeguards personnel with a high degree of confidence in the results including pinpointing areas needing improvement.

2.14.1.2. Organizational Practice Performance Evaluation

While the real measure of performance is how individuals perform at their specific tasks (i.e. responses for safeguards personnel) the unavailability of real events makes that type of measurement impractical for safeguards. However, every licensee has some system for evaluating individual employees with regard to performance in order to reasonably decide on promotions, raises and other standard incentives for better performance.

Performance evaluations are an inextricable part of any organization's mode of operation. They range from informal modes (such as that of a sole proprietor evaluating his single employee by intuition and observation) to very formal mechanisms (such as those rendered in large organizations which include specific criteria and written rating statements).

In the organizational literature there is a research concept called "performance appraisal criteria"[13] which is aimed at developing optimal methods for conducting performance evaluations. The literature draws some basic conclusions which may be applicable to performance evaluations at nuclear power plants.

2.14.1.2.1. Purposes of Organizational Practice Performance Appraisal

There are two major purposes in conducting performance appraisals in organizations. These are organizational control and individual development.[14] Organizational control is aimed at obtaining information needed for making administrative decisions and to promote organizational efficiency and goal attainment. Individual development is aimed at assisting the employee in identifying areas for improvement and growth. The basic function of an effective organizational control system is the specification of appropriate behaviors and explicitly linking those behaviors to the reward system.[15] Other researchers have concluded that optimal organizational effectiveness cannot be attained without such an arrangement.[16]

The assertion that an explicit linkage between behavior and rewards is necessary is supported by studies in the application of motivational theory in organizational behavior. Motivation theory, which has developed theoretical and practical models of organizational behavior, has been shown to be a meaningful factor in successfully run organizations.[17]

The second goal, that of individual development, is beneficial to the organization as a whole, in addition to the individual. Recognition of individual employee strengths and weaknesses as related to performance and provision for employee participation in determining the exact form and content of the appraisal are necessary components of an optimal system.[18]

2.14.1.2.2. Research on Performance Appraisal Systems

Research on actual operating organizations has shown that three factors can cause serious deficiencies in appraisal systems. First, supervisors are often unaware of the actual reward-behavior relationships reflected in their appraisal of subordinates.[19] Second, supervisors often combine performance information inconsistently when making overall ratings.[20] Third, subordinates are often unable to perceive clear relationships between job behavior and subsequent performance ratings.[21]

There have been many studies aimed at systematically determining and establishing the relationship between behaviors and rewards in particular types of organizations. Usually a scientific methodology such as "policy capturing" is used[22]. This particular method is characterized by using an organization's appraisal raters and (1) presenting them with a series of profiles consisting of scores on job dimensions, (2) instructions to review each profile then assign each an overall evaluation, and (3) multiple regression analysis to calculate statistics from responses.

Profile determinants (i.e., job dimensions) can be developed from (1) reviews of current evaluation policies, (2) interviews with managers and key ad-

ministrators and (3) interviews with subordinates subject to evaluations. Definitions of behaviors for performance are then developed for below average, average, and above average performance. The resulting matrix (three performance categories and n determinants) is then issued to supervisors who normally do performance appraisals. Each supervisor is asked to come up with an overall performance rating for each of approximately 100 systematically generated behavior profiles. Statistical analysis of results is conducted by using a squared multiple-correlation coefficient to measure the raters' consistency. A systematic evaluation of each determinant's importance is conducted (e.g., Hoffman's (1960) Formula for Relative Weights)[23]. Relative weights indicate the percentage of total predictable variance accounted for by each single determinant. Hierarchial clustering[24] can be used to attempt combining determinants into a smaller number of composite clusters. Clusters can then be prioritized using regression analysis validated by a multivariate analysis of variance (MANOVA) test[25].

The main advantage of this particular method of formalizing performance appraisal criteria is that it appears to address all three major problems cited earlier. First, the lack of supervisor awareness of actual reward-behavior ratings reflected in appraisals can be remedied by providing each supervisor with a statistical description of their rating behavior which can then be used as a benchmark for future appraisals. Second, a standard combinational system can be given to each rater to assist in providing consistency to the process of determining an overall appraisal. Third, inaccurate subordinate perceptions can be corrected by providing subordinates with the supervisors' captured statistical policy.[26]

Performance evaluation systems developed using the method described above have shown measurable improvements in organizational performance. The use of these technologies for organizational analysis and assessment may provide a good start for improving performance evaluation of safeguards personnel at nuclear power plants.

2.14.2. Research Approach

All four methods of research could be used to study performance evaluation for safeguards personnel at nuclear power plants.

2.14.2.1. Experimental

An experimental approach to studying performance evaluation would involve generation of new data to be analyzed in such a way as to reveal deficiencies in site security. Methods of realistic simulation such as SSORA and MILES could be examined as an experimental means of generating and collecting data on performance.

2.14.2.2. Data Analysis

Performance evaluation could be examined by analyzing existing data on performance contained in event reports, licensee files, and inspection and enforcement records. This could be done with the aim of determining how licensee's evaluate their own personnel and developing criteria for assessing licensee programs.

2.14.2.3. Extrapolation

In the field of management science many researchers have studied the optimal means of designing performance evaluation mechanisms which will best improve performance. These studies, described in the first part of this section, could be examined and recommendations for personnel evaluation methods made.

2.14.2.4. Further Research Formulation

A plan to attempt combining the methods above into a more comprehensive study could be developed. This would involve available data, extrapolation from related fields and experimentation. This would lead to a larger study.

2.14.3. Practicality

2.14.3.1. Cost and Time

To run an experiment using the SSORA system would involve approximately two staff-years and about $40,000 to 80,000 worth of equipment. It would involve two sites (minimum) in order to assure applicability to nuclear power plant sites generally. If the experiment proved to significantly improve performance evaluation it could be made available to licensees or used by NRC directly. The overall cost of an experimental approach is estimated to be $200,000-300,000 and is assigned index value of 1.

An analysis of existing data would center on gathering event reports, inspection and enforcement records and licensee files to analyze their relationship and ascertain the current state-of-affairs in performance evaluation. This would take between one-half and one staff year and is assigned a cost index of 3.

An overall review of existing technologies for performance evaluation and extrapolation could be conducted in order to recommend optimal methods for licensee use. This would require one-half to one staff-year and is assigned a cost index of 3.

A project could be initiated to formulate a comprehensive approach to research in performance evaluation combining the three previous methods. The cost of developing such a plan would require approximately one-half staff-year and is assigned a cost index of 3.

2.14.3.2. Time

The experimental research approach suggested would take less than two years to accomplish so a time index of 2 is assigned. For data analysis, extrapolation and further research formulation, a shorter time frame is reasonable so a time index of 3 is assigned.

2.14.3.3. Data Availability

Data needed for a analysis is available through public records and those that the licensees are required to keep under NRC regulations. Therefore, the data availability index is 3.

The relevant data for extrapolation from other fields is available through open literature as well as from management consulting agencies handling similar problems. The data availability index is, then, 3.

Data needed for future research formulation are available so that a data availability value of 3 is assigned.

The data needed to set up such a system is freely available through other agencies sponsoring such research (i.e. DNA and DOE). Therefore the data availability value is 3.

2.14.3.4. Equipment Availability

Both DOE and DOD presently have significant available for experimental testing of performance under realistically simulated conditions. If this equipment could be borrowed, for instance DNA's SSORA system, it would cut costs but it cannot be assumed that such interagency agreements could be easily reached. If appropriate equipment cannot be borrowed then it can be purchased through normal channels. Therefore, equipment availability value of 2 is assigned. Equipment is not specifically needed for data analysis, extrapolation or further research formulation so an equipment availability index of 3 is assigned to each.

2.14.4. Usefulness

2.14.4.1. Regulatory Need

NRC has been moving into the area of monitoring licensee performance to an increasing degree. A preference for performance based, rather than standards-based, requirements has also surfaced. In addition, the issue of safeguards adequacy can be directly addressed using the results from experimental methods, data analysis, or extrapolation. Regulatory need indexes are 3 for each of these methods. Further research formulation is not as clearly needed so that an index of 2 is assigned.

2.14.4.2. Risk Reduction

There is a consensus that better performance evaluation techniques will improve safeguards in general and some methods have been shown to do so in similar contexts. Therefore, data analysis and extrapolation methods are judged to potentially decrease risk. Experimental methods have been demonstrated to probably reduce risk. Further research formulation would, in itself, negligibly affect risk. Therefore, experimental techniques are assigned a risk reduction index of 3, data analysis and extrapolation an index of 2 and further research formulation an index of 1.

2.14.5. Acceptability

2.14.5.1. Industry Interests

The industry probably would not welcome experimental approaches to site security and may object strongly. The experimental approach is assigned an acceptance index of 1. Data analysis would most likely not face strong oppositon and is assigned an index of 2. Extrapolation of data from other

fields would probably be welcomed by industry and is assigned an index of 3. Further research formulation would not meet with opposition and is assigned an index of 2.

2.14.6. Summary of Index Values

	Experimental	Data Analysis	Extrapolation	Further Research Formulation
Practicality				
Cost	1	3	3	3
Time	2	3	3	3
Data Availability	3	3	3	3
Equipment Avail.	2	3	3	3
Usefulness				
Regulatory Need	3	3	3	2
Risk Reduction	3	2	2	1
Acceptability				
Industry Interests	1	2	3	2

References for Section 2.14

1. 10 CFR 73, App. B, I.E., II.E, IV.D.

2. U.S. NRC Reg. Guide, 1.17, "Protection of Nuclear Power Plants Against Industrial Sabotage."

3. "Security for Nuclear Power Plants," ANSI/ANS 3.3-1982, formerly ANSIN18.17-1973.

4. Id. p. 11.

5. 10 CFR 73, App. B, I.B.2.

6. Id. II.E., IV.D.

7. ANSI-N 18.17-1973.

8. Id. p. 8.

9. ANSI/ANS-3.3-1982.

10. "Physical Standards Validation Study: Final Report," DOE Contract No. DE-ACOI-80-DP-30226 (8-8-80); L.D. Chapman, et al., "Tactical Improvement and Security Force Evaluation Program," presented at the ANS Workshop on Power Plant Security, April 25, 1983.

11. R. Mackie and R. Hall, "Security System Operational Recording and Analysis," Presented to 7th Annual Symposium on the Role of Behaviorial Science in Physical Security, Oct. 1, 1982, sponsored by the Defense Nuclear Agency.

12. Id. p. 7.

13. C.J. Hobson, et al, "Cl rifying Performance Appraisal Criteria," Organizational Behavior and Human Performance, Vol. 28, 1981, p. 164.

14. L. Cummings and D. Schwab, Performance in Organizations, Foresman, Glenview, Ill. 1973.

15. E.E. Lawler, "Control Systems in Organizations" in M.D. Dunnette (ed.), Handbook of Industrial and Organizational Psychology, Rand McNally, Chicago, 1976.

16. D. McGregor, The Human Side of Enterprise, McGraw-Hall, NY, 1960.

17. R.M. Tuttle, "Maximizing Motivational Techniques for the Security Force," presented at the ANS Work Shop on Power Plant Security, April 25, 1983.

18. J.C. Naylor and R.J. Wherry, "Feasibility of Distinguishing Supervisor's Policies in Evaluations of Subordinates Using Ratings of Simulated Job Incumbents" Lackland USAF Base, Personnel Research Laboratory, Aerospace Medical Division, PRL-TR-64-25, 1964.

19. R.L. Taylor and W.D. Wilsted, "Capturing Judgement Policies: A Field Study of Performance Appraisal," Academy of Management Journal, Vol. 17, 1974, p. 440; S. Zedeck and D. Kafry, "Capturing Rater Policies for Processing Evaluation Data," Organizational Behavior and Human Performance, Vol. 18, 1977, p. 269.

20. R.M. Daves, "A Case Study of Graduate Admissions: Application of Three Principles of Human Decision Making," American Psychologist, Vol. 26, 1971, p. 180; L.R. Goldberg, "Man versus Model of Man: A Rationale, Plus Some Evidence For a Method of Improving on Clinical Inferences," Psychological Bulletin, Vol. 73, 1970, p. 422; J.S. Wiggins, Personality and Prediction: Principles of Personality Assessment, Addison-Wesley, MA, 1973.

21. D.R. Ilgen, et al, "Consequences of Individual Feedback on Behavior in Organizations" Journal of Applied Psychology, Vol. 64, 1979, p. 349.

22. P. Slovic, et al, "Behavioral Decision Theory," Annual Review of Psychology, Vol. 28, 1977, p. 1; Naylor, Note 17; Taylor, Note 18, Zedeck, Note 18.

23. P.J. Hoffman, "The Paramorphic Representation of Clinical Judgement," Psychological Bulletin, Vol. 57, 1960, p. 116.

24. Hobson, note 13.

25. Id.

26. Id.

2.15. Central Alarm Station/Secondary Alarm Station (CAS/SAS) Design

2.15.1. Background

Since the Three Mile Island accident, considerable effort has been put into improving the man-machine interface at nuclear power plants, particularly regarding the reactor control room, because obvious serious deficiencies in operator interaction with instrumentation and controls occurred. A similar problem, largely in the domain of the field of ergonomics, exists in the presentation and disposition of information to the CAS/SAS operator. Every reactor is required to have two hardened protected alarm stations in which all alarms and communications are monitored and the guard force is directed. The man-machine interface in alarm stations contains the most straight-forward parallel between similar problems which exist in operational safety.[1] NRC has already performed significant safeguards studies on this matter[1] and further work has continued.[2]

Specific areas which need to be addressed in future research include: 1) the integration of all the physical security systems and controls into one coherent and easily operable system, 2) the optimal arrangement and formats of dials and CRT terminals, 3) the optimal display of alarms in the system to ensure the best and most timely response, and 4) proper control in CAS/SAS of alarms, sensors[3] and CCTV in real time to ensure maximum effectiveness of the detection system.

2.15.2. Research Approach

2.15.2.1. Extrapolation

Some data analysis of current system should be included in this work, but a great wealth of ergonomic data has been produced by the study of reactor control rooms and can be of use. Great care must be taken to accurately transfer results between the systems already studied in detail (i.e. control rooms) and the ones to which the studied methods are meant to be applied (i.e. alarm stations). There are many close parallels which can be drawn between those systems already analyzed and the CAS/SAS of nuclear power plants.

2.15.3. Practicality

2.15.3.1. Cost - The cost for such a detailed survey of past data and work is likely to be one staff-year or more. An index of 2 is assigned, although a complete and detailed survey could possibly rate an index of 1.

2.15.3.2. Time - The time necessary should be about one year, rating an index of 3. This would include a study of the literature, together with derived recommendations by behavioral scientists.

2.15.3.3. Data Availability - The data for this study are readily available, although some small portion of them may be classified information. An index of 3 is meritied.

2.15.3.4. Equipment Availability - Virtually no equipment will be needed for this study, beyond possible use of a small computer. The results could eventually be tested at a site or simulator. This step, if considered

part of tasking under this effort, could require the procurement of equipment. Overall, an index of 3 is felt to be most appropriate.

2.15.4. Usefulness

2.15.4.1. Regulatory Needs

It is not of high priority to provide mandated changes in the details of CAS/SAS equipment disposition at this time, but eventually information from this effort could be useful in determining future additions to equipment requirements and criteria for assessment of adequacy. In addition, review of training programs could include consideration of critical man-machine interface problems. As a result an index of 2 is assigned.

2.15.4.2. Risk Reduction - The importance of this topic in reducing vulnerability to sabotage is substantial, but less than in other areas. The present designs have proven adequate to the point is that there is little reason to think that response could still be significantly improved solely by changes in the CAS/SAS design.

An index of 2 is assigned.

2.15.5. Acceptance

2.15.5.1. Industry Interests - New regulations in this field would result in some costs to the industry and would encounter resistance. However, in general, the cost-effectiveness of any suggested changes is most likely to be very positive. An index of 2 is assigned.

2.15.6. Summary of Values

Method	Extrapolation
Practicality	
Cost	2
Time	3
Data Availability	3
Equipment Availability	3
Usefulness	
Regulatory Needs	2
Risk Reduction	2
Acceptance	
Industry Interests	2

References for Section 2.15

1. H. Wait and H. Manning, "Design Concepts for Independent Control Alarm Station and Secondary Alarm Station Intrusion Detection Systems," NUREG/CR-1468, November, 1980; "Basic Considerations for Assembling a Closed-Circuit Television System," NUREG-0178; "Interior Intrusion Alarm Systems," NUREG-0320; "Security Communications for Nuclear Fixed-Site Facilities," NUREG-0508; "Central Alarm Station and Secondary Alarm Station Planning Document," NUREG/CR-0543.

2. Z. Kravets and D. Rockford, "The Configuration, Development, and Interface of a Nuclear Power Plant Security System," presented at the ANS Workshop on Power Plant Security, April 25, 1983; A.E. Windblad, "An Integrated Sabotage Protection System Concept," SAND-82-2963C, April 1983; C.E. Higgins," Cost Effective Security", presented at the ANS Workshop on Power Plant Security, April 25, 1983.

3. D. Stedinak, "Software Enhancements to Security System Computers," American Nuclear Society Power Plant Security Workshop, Savannah, Georgia, April, 1983.

2.16. Maintenance

2.16.1. Background

As the Three Mile Island accident focussed attention on the man-machine interface, the Salem malfunction drew direct attention to the human element in the field of maintenance of equipment. Analogously, just as vital safety related equipment can be compromised by inadequate maintenance, so could safeguards-related equipment, such as sensors, alarms, CCTV, and so on. Proper maintenance can lower false alarm rates which have been shown to have a detrimental effect on security.

It is suggested that as well as examining the sensitivity of safeguards equipment to maintenance failures, it would be useful to require more stringent upkeep of maintenance records and possibly to require more specific standards for equipment maintenance than is now the case.

2.16.2. Methods

2.16.2.1. Data Analysis

Current failure rates for commercial alarms, sensors, cameras, and other safeguards-related equipment should be studied for correlation with failures in proper maintenance. In particular, past instances of failure should be examined for the possibility that poor maintenance, and not normal wear and tear or manufacturing defects were responsible. A reasonable subsample of such equipment would be adequate for the purposes of such a study, since a rigorously exhaustive work would be an unmanageably large effort. These data may be available from vendors and testing labs.

2.16.2.2. Future Formulation - Possible techniques or regulatory requirements for assuring the proper standards of maintenance for important safeguards-related equipment should be proposed and examined for effectiveness in providing reasonable certainty that no equipment failure caused by maintenance errors will significantly increase vulnerabilities at a licensee site.

2.16.3. Practicality

2.16.3.1. Cost - For the data analysis work, an estimate of a staff year appears appropriate and for the future formulation, probably ½ staff year would be adequate indicating indexes of 3.

2.16.3.2. Time - About a year would be necessary for the data analysis work and somewhat less time for the examination of possible changes in requirements indicating indexes of 3.

2.16.3.3. Data Availability - A significant amount of data would have to be amassed and understood in order to determine with confidence the effects on vulnerability of improper maintenance. An index of 2 is assigned.

2.16.3.4. Equipment Availability - For both cases, minimum equipment is needed to do the proposed research, and an index of 3 is given.

2.16.4. Usefulness

2.16.4.1. Regulatory Needs - At this point, the best estimate is, that both avenues of research would lead to filling some needs for equipment maintenance. It is difficult to estimate the level of need for such work but it appears reasonable that the data analysis studies could lead to satisfying needs so an index of 2 is assigned and the future formulation could satisfy to a higher level than that, meriting index of 3.

2.16.4.2. Risk Reduction - Moderate risk reduction could be anticipated in both cases if improvements in regulatory requirements are found necessary. It is anticipated that this will be the case. An index of 2 is assigned.

2.16.5. Acceptance

2.16.5.1. Industry Interests - Moderate resistance to future regulatory suggestions on maintenance should be expected because of additional costs. An index of 2 is considered reasonable.

2.16.5. Summary of Values

Methods	Data Analysis	Future Formultion
Practicality		
Cost	3	3
Time	3	3
Data Availability	2	2
Equipment Availability	3	3
Usefulness		
Regulatory Needs	2	3
Risk Reduction	2	2
Acceptance		
Industry Interest	2	2

2.17. Communications Equipment

2.17.1. Background

In addition to providing improvements in morale, performance, and attitude, communications equipment is vital in giving the guard force the capability of an effective, rapid response in a coordinated fashion to a safeguards-related incident. There is also the element in increased safety for the force if one considers the duress alarm option in protecting the individual guard.[1] (This is a part of the communications system which is sometimes overlooked in addressing the subject.) NRC has committed research and put forth guidance on safeguards communications systems.[2]

It remains to determine whether current requirements for communications systems and backups in the case of emergencies are adequate in a rigorous fashion. A review of the current requirements, together with a study of a representative, state-of-the-art systems should be sufficient to determine whether current equipment is adequate.

2.17.2. Method

2.17.2.1. Data Analysis - The study of the current system only need involve data analysis, including system characteristics and the data from past safeguards-related events which may have involved failures or inadequacies in the communications system. In addition, the possible uses and improvements in duress systems should be studied, using past tests and in-field experience.

2.17.3. Practicality

2.17.3.1. Cost - Such a review of data on communication systems performance and capabilities at power plants should require no more than one half a staff-year and therefore would rate an index of 3.

2.17.3.2. Time - Likewise, the time needed for such a review would be small, less than a year, warranting an index of 3.

2.17.3.3. Data Availability - Data to study currently used communications systems are readily available and open indicating an index of 3.

2.17.3.4. Equipment Availability - Study of the equipment may require visiting one or two sites, where the current communications system would be already installed, or to vendors or laboratories, where new equipment may be in the process of development. An index of 3 is assigned, because no significant procurement is necessary.

2.17.4. Usefulness

2.17.4.1. Regulatory Needs - There are already fairly comprehensive specifications for required communications systems, and changes are not of the highest priority. However, particularly in regards to duress monitoring systems, there are some areas where modifications may be advisable. An index 2 appears appropriate.

2.17.4.2. Risk Reduction - Similarly, while current communications systems have redundancies and are significant improvements over practices of several years ago, some risk reduction could be accomplished in some areas, depending on the results of the suggested study. An index of 2 is assigned.

2.17.5. Acceptance

2.17.5.1. Industry Interests - It is suggested that modifications are likely to be minimal in cost and could add substantially to the morale and capability of the guard force. Therefore, an index of 3 is assigned.

2.17.6. Summary of Index Values

Method	Data Analysis
Practicality	
Cost	3
Time	3
Data Availability	3
Equipment Availability	3
Usefulness	
Regulatory Needs	2
Risk Reduction	2
Acceptance	
Industry Interests	3

Reference for 2.17

1. A. Fainberg "Stress and Duress Monitoring at NRC-Licensed Facilities," NUREG/CR-1031, 1979.

2. "Security Communication Systems for Nuclear Fixed-Site Facilities," NUREG-0508.

2.18. Environmental Influences

2.18.1. Background

To a great extent those areas which are to be maintained in a secure fashion are environmentally altered. For instance, trees and foliage surrounding the site perimeter are usually cut down to allow an unimpeded view. However, environmental influences such as weather cannot be controlled and must be otherwise accommodated. Terrain and physical obstructions can sometimes be a problem as well. Even physical movement can be made difficult if all-weather walking surfaces are not used in secure areas. (The ANSI/ANS 3.3 standard recommends all-weather walkways.) Environmental influences can affect personnel viewing closed circuit TV monitors as well. Presently DNA and the National Bureau of Standards are sponsoring research on a system which is aimed at digitizing video data to provide better performance of surveillance.

Environmental influences are influences on performance and reliability. Realistic drills have been shown to reveal security deficiencies due to environmental influences. For instance, DNA's SSORA system (section 2.14) has revealed environmental influences which affect security such as grass at the fence which is too high and insufficient illumination.

The Regulatory Effectiveness Review Program reviews the environmental physical aspects of the sites visited by examining site maps and drawings. A research program could be designed to reveal the optimal methods for assessing the impact of environmental influences during reviews.

2.18.2. Research Approach

2.18.2.1. Experimental

Environmental influences are usually site specific in terms of impact. For instance grass which is too long at one site may not be at another depending on surveillance capabilities. As a result it may be better to identify environmental influences in the context of drills designed and managed to reveal these influences. The subject of drills conducted for analysis has been covered in section 2.14.

2.18.3. Practicality

2.18.3.1. Cost

The cost of developing standards for design and management of drills in terms of environmental influence would not be much in the context of conducting drills for other purposes. As a result, a cost index of 3 is assigned. This does not consider the cost of the drills which are presumed to be conducted for other related reasons (e.g. training and performance evaluation).

2.18.3.2. Time

A standard, as described above, could be developed within a year so that a time index of 3 is assigned.

2.18.3.3. Data Availability

There are sufficient data already available to design pilot experiments aimed at identifying impacts of environmental influences on safeguards. As a result a data availability index of 3 is assigned.

2.18.3.4. Equipment Availability

The equipment necessary for an experimental approach would involve video and audio recording equipment to record data for later analysis. This equipment availability index of 2 is assigned.

2.18.4. Usefulness

2.18.4.1. Regulatory Needs

NRC has requirements for dealing with environmental influences (e.g. required isolation zones, minimum illumination requirements, etc.) The Regulatory Effectiveness Review Program already examines environmental influences on security as does the licensing process itself. As a result a regulatory need index of 2 is assigned.

2.18.4.2. Risk Reduction

NRC licensed sites have already been examined for obvious environmental influences which would degrade security. It is possible that drills specifically designed and managed to identify and rectify significant environmental influences could reduce risk so a risk reduction index of 2 is assigned.

2.18.5. Acceptability

2.18.5.1. Industry Interests

Licensees may view additional requirements for dealing with environmental influences as unreasonable. However, guidance aimed at the design and management of such drills would probably not be opposed. As such, an acceptability index of 2 is assigned.

2.18.6. Summary of Index Values.

	Experimental
Practicality	
Cost	3
Time	3
Data Availability	3
Equipment Availability	2
Usefulness	
Regulatory Need	2
Risk Reduction	2

2.19. Nuisance and False Alarms

2.19.1. Background

The efficiency of guard force response to alarms is greatly affected by the rates of alarms caused, not by intruders or other safeguards-related events, but by sensor malfunction, winds, animals, and so on. There is, in fact an overlap between this topic and the previous section's subject of environmental factors and that an vigilance (section 2.6). Under normal circumstances, the incidence of actual intrusions is extremely low so that even in the absence of false alarms, there are problems in maintaining guard vigilance and effectiveness. This difficulty is aggravated when the only alarms are false ones, and is aggravated further when the incidence of such false alarms is high. Research as how best to lower false alarm rates by using advanced techniques such as artificial intelligence is currently being conducted.[1]

It would be useful to study current false alarm levels in typical plant security systems with a view to determining: obvious needs for improvement in particular sensors or other related instrumentation; state-of-the-art developments which could reduce false alarms systems improvements (taking advantage of redundancies, artificial intellegence or signal processing techniques) which would reduce alarms which would have to be dealt with by the guard force.

2.19.2. Methods

2.19.2.1. Data Analysis - A first step would be to analyze rates and sources of false alarms in currently used systems. The results could provide information on where, or for which types of sensors, improvements are most appropriate. Also, a study of recent developments in the field of sensors, including either the development of new devices with inherently lower false alarm rates or improvements in existing devices, would appear advisable.

2.19.2.2. Further Research Formulation - A study of potential modifications in integrated alarms would be useful. Physical security systems which could be used to reduce nuisance and false signal processing techniques could be cost effective in reducing unwanted alarms. This could provide suggestions on the regulatory guide level which would aid licensees in dealing with the problem.

2.19.3. Practicality

2.19.3.1. Cost - Both studies could be accomplished within the limit of one-half staff-year of work. This justifies an index of 3.

2.19.3.2. Time - Both studies would be able to be accomplished within a calendar year, yielding an index of 3.

2.19.3.3. Data Availability - For the data analysis approach, all data are readily available but will have to be assembled for analysis. The amount of such data could be substantial. An index of 2 is appropriate. A similar observation applies to the further formulation study.

2.19.3.4. Equipment Availability - For these approaches, the equipment needed to be examined would be present and available either at licensee facilities or, in the case of state-of-the-art equipment at vendors' laboratories. An index of 3 is justified.

2.19.4. Usefulness

2.19.4.1. Regulatory Needs - Some assistance in terms of suggested approaches in reducing false alarms could be provided by the results of such studies. This would more likely apply to regulatory guides than to mandates contained in potential regulations. An index of 2 is appropriate.

2.19.4.2. Risk Reduction - Some potential reduction on in risk, because of improved guard force response, could be obtained by reducing nuisance alarms. However, it is felt that the reduction of risk is less significant here than in most other areas discussed. An index of 1 is assigned.

2.19.5. Acceptance

2.19.5.1. Industry Interests - The data analysis study could result in the suggestion that licensees purchase more equipment with only a marginal or, at least, not so obvious a benefit. The study itself would not, of course, interfere with any facility to any important degree. A level of 2 is given. Regarding the future formulation study, it could produce result which would not require expensive modifications but would improve guard force (although only to a degree). Since the industry could attain some benefits for little effort or cost, an index of 3 is assigned.

2.19.6. Summary of Values

Method	Data Analysis	Future Formualtion
Practicality		
Cost	3	3
Time	3	3
Data Availability	2	2
Equipment Availability	3	3
Usefulness		
Regulatory Needs	2	2
Risk Reduction	1	1
Acceptance		
Industry Interests	2	3

Reference for Section 19

1. P. Bierre, "Teaming Human and Artificial Intelligence for High Productivity Security Systems," presented at the ANS Workshop on Power Plant Security, April 25, 1983; "Nuclear Power Plant Perimeter Intrusion Alarm Systems," E-Systems, Inc., EPRI-NR-2355, April 1982.

Table 3. Summary Matrix

Project	Cost	Time	Data	Equip.	Need	Risk	Accept
2.1.2.1	2	3	2	3	1	2	1
2.2.2.1	1	2	2	3	3	3	1
2.3.2.1	2	2	1	3	1	2	2
2.3.2.2	2	3	2	3	1	2	2
2.3.2.3	3	3	3	3	3	2	3
2.4.2.1	2	2	2	2	2	3	3
2.5.2.1	2	2	3	2	2	3	2
2.5.2.2	2	1	3	2	2	3	2
2.5.2.3	2	1	3	3	2	3	2
2.6.2.1	1	2	1	2	1	2	2
2.6.2.2	3	2	2	3	1	2	2
2.6.2.3	2	2	3	3	1	2	2
2.7.2.1	1	2	2	2	2	3	1
2.7.2.2	2	3	2	3	2	3	2
2.8.2.1	3	3	3	3	2	2	1
2.9.2.1	1	2	3	3	2	3	1
2.9.2.2	3	3	3	3	3	3	2
2.10.2.1	1	2	2	2	3	3	2
2.10.2.2	1	2	2	3	3	3	2
2.10.2.3	2	3	2	3	3	3	2
2.11.2.1	1	1	2	1	3	3	3
2.11.2.2	3	2	3	3	3	3	3
2.11.2.3	2	2	1	2	2	2	2
2.12.2.1	3	3	3	3	3	3	2
2.12.2.2	3	3	2	3	1	3	2
2.13.2.1	3	3	3	2	3	3	2
2.13.2.2	3	3	3	3	2	3	2
2.14.2.1	1	2	3	2	3	3	1
2.14.2.2	3	3	3	3	3	2	2
2.14.2.3	3	3	3	3	3	2	3
2.14.2.4	3	3	3	3	2	1	2
2.15.2.1	2	3	3	3	2	2	2
2.16.2.1	3	3	2	3	2	2	2
2.16.2.2	3	3	2	3	3	2	2
2.17.2.1	3	3	3	3	2	2	3
2.18.2.1	3	3	3	2	2	2	2
2.19.2.1	3	3	2	3	2	1	2
2.19.2.2	3	3	2	3	2	1	3

Table 4. Unweighted Feasibility Rankings

	Sum
Trustworthiness - Further Research Formulation	20
Attitude - Further Research Formulation	20
Format and Wording of Contingency Plans - Data Analysis	20
Use of Force - Experimental	20
Performance Evaluation - Extrapolation	20
Staff Coordination - Experimental	19
Staff Coordination - Data Analysis	19
Performance Evaluation - Data Analysis	19
Communications Equipment - Data Analysis	19
Training - Further Research Formulation	18
Maintenance - Further Research Formulation	18
Human Reliability - Data Analysis	17
Organizational Communication - Data Analysis with Simulation	17
Shiftwork - Data Analysis	17
Use of Force - Further Research Formulation	17
Performance Evaluation - Further Research Formulation	17
CAS/SAS Design - Extrapolation	17
Maintenance - Data Analysis	17
Environmental Influences - Experimental	17
Nuisance and False Alarms - Further Research Formulation	17
Fitness for Duty - Data Analysis	16
Human Reliability - Data Analysis and Equipment	16
Human Reliability - Extrapolation	16
Training - Data Analysis	16
Nuisance and False Alarms - Data Analysis	16
Behavioral Observation Programs - Data Analysis and Experiment	15
Trustworthiness - Extrapolation	15
Vigilance - Data Analysis	15
Vigilance Extrapolation	15
Attitude - Experimental	15
Training - Experimental	15
Performance Evaluation - Experimental	15
Two-man Rule-Experimental and Data Analysis	14
Format and Wading of Contingency Plans - Experimental	14
Trustworthiness - Data Extrapolation	13
Organizational Communication - Experimental	13
Format and Wording of Contingency Plans - Further Research Formulation	13
Vigilance - Experimental	11

2.20 Conclusions

Table 3 contains all index values and Table 4 is an unweighted ranking of human factors research in terms of research feasibility. These data were also analyzed using hierarchical aggregative clustering and no strong associations emerged.

The ranking which results should be thought of as approximate and not as a rigid means for prioritization. An important result of the analysis is that none of these issues were found to "unresearchable". However, some are clearly more amenable to practical and meaningful research than others. This analysis will be used to design the final research plan.

3.0. Development of Research Groups

In Section 2 each human factor was examined separately in terms of research approach and feasibility. Many human factors have been shown to be related and can be studied using common research approaches and results. Grouping research involves putting together research approaches and similar human factors to minimize resource requirements. In this section human factors will be grouped into program elements according to 1) common research approaches, 2) similar human factors impacts, 3) importance of human factors to safeguards, and 4) feasibility of research.

3.1. How Reseach is Grouped

Research in human factors associated with nuclear power plant safeguards must be oriented toward behavioral sciences as well as the traditional areas of nuclear power plant human factors such as control room ergonomics and cognitive decision making. This is due to the great breadth and complexity of human actions required to be taken by safeguards personnel in being able to perform their job-related duties. Psychology, sociology, and management sciences all bear strongly on the various aspects of security which are affected by safeguards personnel. Each of these fields has a long history of methodological development and numerous subdisciplines which can contribute to a better understanding of plant security and opportunities for improvement if deficiencies are found to exist.

In order to structure a research plan which takes advantage of these disciplines and their associated methodologies, research projects can be "grouped." This process can start by developing conceptual models which more clearly reflect a behavioral science oriented methodological view of these human factors. Once conceptual models are developed then specific methodological groupings are made. Three such models are described below. These models will be used to structure the final research plan.

The groups which are described below are meant to suggest a means for clustering research to take advantage of similarities in human factors and the methods available for studying them. Since there are various methodological approaches to measurement and analysis three groupings are described. Not suprisingly these three approaches yield very similar groupings. These groupings are the results of extensive discussions with safeguards professionals, behavioral scientists, and traditional human factors experts. Various groupings are possible depending on the number of methodological perspectives considered. However, three presented appear to best address the variety of human factors under examination in this project. The results of the ranking from section 2.0, Chapter 2, and the following groups will be used to develop priorities for a long-term research plan.

3.2. Organizational Approaches

An organizational view of the human factors found to affect safeguards at nuclear power plants treats the organization and its activities as the central frame of reference on the overall question of how security may be affected and how to improve it. Three somewhat distinct groups of organizational activities can be identified in power plant safeguards which include all of the human fac-

tors considered in this project. These are 1) individual entry, 2) normal organizational operation and 3) off-normal organizational operation. The grouping for an organizational approach is summarized in Table 5. Each is described in the following sections.

3.2.1. Individual Entry

The organization which operates a nuclear power plant is made up of a large group of individuals acting in concert to safely operate the plant. The safeguards organization is either proprietary (utility personnel) or contract (outside personnel). In either case the licensee (utility) is ultimately responsible for the action of each individual in the safeguards organization as it affects the safety of the plant. As such, there is typically a screening process which attempts to assure that each individual will act correctly and in the best interests of the licensee.

Individual entry involves the means for filling personnel positions so that each individual is assessed for reliability and trustworthiness before being hired. For safeguards personnel this screening process involves a prior employment check and minimum qualification requirements to assure reliability and a psychological test and background investigation to assure trustworthiness. Once an individual is subject to the entry screening process and found acceptable, means for further assuring reliability and trustworthiness are based mainly on the individual's organizational practices rather than prior history. As a result, initial screening is a different process. Organizational practices are assessed by behavioral observation, performance evaluations, and requalification. In terms of individual entry the applicant is viewed and appraised on the basis of factors developed entirely from outside the licensee's organization and after that by developed from factors within the organization. As such, activities aimed at individual entry entail some fundamental differences from normal organizational practices, but mainly the need to rely on determinants developed outside of the licensee context.

3.2.2. Normal Organizational Operation

Once individuals are employed by the licensee organization it is the actions of each individual that both affects safety and provides input for performance evaluations. Effects on safety can occur in three major modes. These are 1) errors, 2) procedural conflicts, and 3) purposeful malevolence. In terms of errors, human reliability, vigilance deterioration, fitness for duty, attitudes, inadequate training, over reliance on shiftwork, and environmental influences are all important. Procedural conflicts can occur because of inadequate consideration of one organizational unit's interrelated responsibilities with another's and inadequate attention to maintenance and required compensatory measures. Purposefully malevolent acts can be countered with behavioral observation, multiple-man rules and requalification programs. Performance evaluation for personnel must generally take place in the context of normal or simulated situations. Measures taken to appraise a performance include both assessment of an individual's organizational practices and performance of duties (i.e. drills) subject to data collection and analysis.

3.2.3. Off-Normal Organizational Response

When an off-normal situation occurs appropriate procedures are to be expected. For many off-normal situations, procedures contained mainly in contingency plans cover actions to be taken by CAS/SAS operators and the guard force. As a result, the format and wording of contingency plans can become very important. Contingency plans, in addition to specifying particular responses for certain situations, often include general instructions for dealing with unanticipated situations. Therefore, there are cases when ad hoc planning must take place involving staff coordination, command and control, communications equipment, and consideration of the use of force.

3.2.4. Application of An Organizational Approach to Human Factors Affecting Safeguards

3.2.4.1. Measurement of Effectiveness

When assessing the effectiveness of changes implemented to improve performance of any kind, a reliable means of measuring improvement is necessary. There have been various attempts to develop personnel performance measures both in and out of the nuclear power plant context. However, the measurement techniques necessary to study particular changes in safeguards may vary substantially from case to case. For this reason a generic performance measurement technique for nuclear power plant safeguards personnel has not emerged. Instead, either organizational performance or analysis of drills have served as general indicators of the quality of site security from an organizational perspective (see section 2.14). In the nuclear power industry there are few uniform practices for measuring general or specific improvements in site security. In fact, there is no singular, concrete notion of what distinguishes a very good safeguards organization from others.

The measurment technique used for each of the three groups of organizational safeguards activities described above (i.e. individual entry, normal organizational operation, and off-normal organizational response) can be specifically developed for each group. In this way measurement of several activities (i.e. a group) can be examined using a consistent set of data collected for each group. Measurement issues are described below.

3.2.4.2. Individual Entry

Criteria for determining whether an individual is suitable for employment are used by all licensees. For safeguards personnel reliability and trustworthiness are assessed. The result of a good program can be characterized organizationally. Individuals have success by remaining in the organization by performing well within its structure and mission. To adequately assess whether certain criteria are more effective than others, some reliable measure of success must be established. Studies of screening results have been done so data do exist. The success measure must be amenable to data which can be collected or otherwise obtained. Once suitable success measures are established for individual entry criteria then, the desirability and accuracy of those criteria can be evaluated. As a result, grouping of research having to do with individual entry criteria appears to be appropriate from an organizational viewpoint in order to take advantage of common data sources (i.e., terminations performance,

Table 5

Organizational Approach Grouping

Individual Entry

- Trustworthiness (A.3)
  - Psychological testing
  - Background Investigation
- Reliability (A.5)
  - Prior Employment
  - Qualifications

Normal Organizational Operation

- Errors in Performance
  - Human Reliability (A.5)
  - Vigilance Deterioration (B.1)
  - Fitness for Duty (A.4)
  - Attitudes (B.4)
  - Inadequate Training (B.5)
  - Overreliance on Shiftwork (B.3)
  - Environmental Influences (D.4)
  - False and Nuisance Alarms (D.5)
- Procedural Conflicts (B.2)
  - Interrelated Responsibilities
  - Compensatory Measures
  - Inadequate Maintenance (D.2)
- Malevolence
  - Multiple-Man Rules (A.1)
  - Behavioral Observation (A.2)
  - Requalification
- Performance Evaluation (C.4)
  - Organizational Performance Appraisals
  - Drills, Data Collection and Analysis

Off-Normal Organizational Response

- Procedural Response
  - CAS/SAS Design (D.1)
  - Format and Wording of Contingency Plans (C.1)

Table 5 (cont)

Ad Hoc Response

Staff Coordination (C.3)
Command and Control
Communications Equipment (D.3)
Use of Force (C.2)

etc.). An organizational perspective also includes considerations of the needs of administrators in screening personnel successfully such as access to specific form of evidence.

3.2.4.3. Normal Organization Operation

3.1.5.3.1. Personnel Errors

As an issue, human reliability in terms of error has received a great deal of attention in the context of operational personnel actions. The techniques used in probabilistic risk assessment have recently involved the use of human error probabilities derived from extensive analysis of relevant human factors. Human reliability impacts for safeguards personnel have undergone no similar analysis. In order to measure the impact of human reliability on physical security some type of task analysis as it relates to safety must be carried out for each position in the security organization. This could be done in such a way as to identify in a sensitivity analysis those types of human reliability problems that are most important to safety; this has been done to a limited extent. The type of human reliability deficiencies which can be considered are vigilance deterioration, fitness for duty, attitudes, inadequate training, overreliance on shift work, and environmental influences. By comparing the relative impact on safety of various positions in the security organization and those human reliability deficiencies associated with each position the relative importance of each human factor could be established. As a result, it is reasonable to group human reliability issues together to rationally address and determine the relative importance of these factors in terms of safety as a basis for common analysis. This importance ranking would be based on an analysis of plant safety as opposed to that developed in Chapter 2.

3.2.4.3.2. Procedural Conflicts

Analysis of procedural conflicts among organizational units can be grouped together. Relevant data (i.e., normal operational procedures) can be analyzed using various techniques for determining where procedural conflicts exist. Clear lines of authority and responsibility must be established to minimize ambiguities capable of causing deficiencies in safety and/or security. Appropriate compensatory measures can be established which maintain security while easing difficulties posed during normal operation. Analysis of this group will also provide input for studying ad hoc responses (section 3.2.4.2.) and to design and manage drills.

3.2.4.3.3. Malevolent Behavior

The potential for malevolent behavior by an employee who is disgruntled or otherwise prone to malevolence has been cited as a major factor in risk due to radiological sabotage. While there has been no instance of successful radiological sabotage by a knowledgeable insider, the high consequences of such an event should it occur require that continual attention be paid to its potential occurrance. This is done to maintain a deterrence and prevention function. Activities aimed at dealing with malevolence are multiple-man rules, requalification, and behavioral observation. The impact of these activities on the potential for radiological sabotage are difficult to establish, however some measures of risk reduction can be made. By considering both the various tech-

niques available to perform each of these activities and their relative contribution to reduction in risk due to potential sabotage an optimal set of procedures can be developed. As such, it appears reasonable to group together research for behavioral observation, requalification and multiple-man rules.

3.2.4.3.4. Performance Evaluation

Tecnniques for conducting performance evaluation in organizations have been shown to be strong influences improving performance when designed correctly (see Section 2.14.). The use of organizational practice indicators and analysis of data derived from drills can be studied together to take advantage of their mutual similarities. Both techniques, if properly designed, are aimed at providing personnel with positive feedback, clear goals and visible means for attaining them. As a result, organizational performance evaluation and evaluations of drills can be grouped together for study.

3.2.4.4. Off-Normal Organizational Response

3.2.4.4.1. Procedural Response

For many situations the apporpriate response to a security event or site emergency is contained in the contingency plans. In those cases responses are required to be carried out according to the means specified in the contingency plans. The CAS/SAS design and the format and wording of contingency plans come into play during procedural off-normal responses. The indicators of quality relative to a response will be associated with both of these factors and therefore, can be grouped together for study.

3.2.4.4.2. Ad Hoc Response

When an event occurs which is not specifically covered in the contingency plans the policy set forth in the contingency plans for unanticipated events must be used. The quality of the response will involve staff coordination, command and control, and communications equipment, and consideration of the use of force. Information developed from procedural conflicts (section 3.3.3.2.) can be used as input to the grouped study of these human factors from a behavioral scientific standpoint.

3.3 Evaluative Approaches

Another behavioral scientific approach can reflect different methodological considerations which center around the concept of performance evaluation. This concept yields three relatively distinct evaluation activities which are not primarily organizational functions, but which address human factors affecting nuclear power plant safeguards. These are 1) individual personnel performance evaluation, 2) organizational performance evaluation, and 3) response to threat performance evaluation. The evaluative approach is summarized in Table 6.

3.3.1 Individual Personnel Evaluation

In order to assess the performance of individuals in nuclear power plant safeguards several considerations arise. These are trustworthiness, behavioral

observation, fitness for duty, selection, and performance evaluation. Each of these activities is aimed at individuals and they are, thus, related. No distinction is made with regard to entry versus continued tenure. Instead this approach focusses on how to best assure an individual's performance is adequate while performing job related duties.

3.3.2. Organizational Performance Evaluation

As a concept the performance of an organization depends not only on individual performance but also on how individuals act in concert. In order to evaluate organizational performance several considerations can be grouped. These are training, vigilance, organizational communication, multiple-man rules, human reliability, attitude, maintenance, nusiance and false alarms, and shiftwork. All of these considerations can be viewed as more dependent an organizational performance than individual performance.

3.3.3. Response to Threat Performance Evaluation

When a stimulus triggers a response several considerations concerning performance arise. These are the format and wording of contingency plane, use of force, staff coordination, CAS/SAS design, communications equipment, and performance evaluation. These considerations all center an the performance of response activities by both individuals and the organization.

Table 6

Evaluative Approach Grouping

Individual Personnel Evaluation
- Trust worthiness (A.3)
- Behavioral Observation (A.2)
- Fitness for Duty (A.4)
- Selection (B.5)
- Performance Evaluation (C.4)

Organizational Performance Evaluation
- Traning (B.5)
- Human Reliability (A.5)
- Boredome and Vigilance (B.1)
- Organizational Communication (B.2)
- Multiple-Man Rules (A.1)
- Attitude (B.4)
- Maintenance (D.2)
- Nusiance and False Alarms (D.5)
- Shiftwork (B.3)

Response to Threat Performance Evaluation
- Format and Wording Contingency Plans (C.1)
- Use of Force (C.2)
- Staff Coordination (C.3)
- CAS/SAS Design (D.1)
- Communications Equipment (D.3)
- Performance Evaluation (C.4)
- Environmental Influences (D.4)

3.3.4. Application of An Evaluative Approach to Human Factors Affecting Nuclear Power Plant Safeguards

3.3.4.1 Measurement of Effectiveness

As discussed previously (Section 3.1.5.1.) in order to judge the effectiveness of changes made in safeguards to improve site security a means of measurement must be developed. In a performance evaluation approach various human factors can be viewed as to how they affect performance and can be specifically measured for that purpose.

3.3.4.2. Individual Personnel Performance

Individual personnel performance differs from individual entry (Section 3.2.4.2.) in that the data used to indicate success include all data applicable to individuals regardless of the source. This approach combines analysis of all safeguards programs and activities aimed at assessing individuals. Because of the similarity of data used for performance evaluation all of the measures aimed at individuals then can be grouped for research.

3.3.4.3. Organizational Performance Evaluation

Organizational performance evaluation includes all human factors that effect the concerted efforts of the organization aside from those related solely to each individual. Measurements made are of organizational performance with respect to the human factors in this group. The effect of change in each human factor is then related to an improvement in organizational performance. In most regards organizational performance evaluation is the same as normal organizational operation (section 3.2.4.3)

3.3.4.4. Response to Threat Performance Evaluation

This group is again very similar to off-normal response (section 3.1.5.4) and can be described similarly.

3.4. Functional Approaches

A functional approach combines the organizational and evaluative approach by viewing the actual functions of a safeguards organization, rather than organizational or evaluative activities, and using research methods from the previous approaches to address the resulting research issues. Four final groups emerged. These are 1) training and performance evaluation, 2) organizational factors, 3) man-machine interface, and 4) trustworthiness and reliability. The functional approach is summarized in Table 7.

3.4.1 Training and Performance Evaluation

All safeguards organizations perform the function of selecting, training, and evaluating personnel. Selection is a function which is in the trustworthiness and reliability group (Section 3.4.4). Training was identified as a critically important factor in nuclear power plant safeguards in Chapter 2. Because of the lack of real safeguards events, guard forces and individuals are generally evaluated in simulated situations (i.e., drills) and by their organizational practices (i.e., work habits, absenteeism). As a result, these forms of performance evaluation constitute the primary means of obtaining feedback on training program design and administration. As such they are tied together in this group. In addition, a properly designed performance evaluation program (i.e., including well designed drills) would reveal environmental influences which adversely affect security.

Table 7

Functional Approach Grouping

Training and Performance Evaluation

- Training (B.5)
- Performance (C.4)
- Environmental Influences (D.4)

Organizational Factors

- Attitude (B.4)
- Staff Coordination (C.3)
- Organizational Communication (B.2)
- Shiftwork (B.3)
- Use of Force (C.2)

Man-Machine Interface

- Format and Working of Contingency Plans (C.1)
- Communications Equipment (D.3)
- CAS/SAS Design (D.1)
- Vigilance (B.1)
- Maintenance (D.2)
- Nuisance and False Alarms (D.5)

Trustworthiness and Reliability

- Trustworthiness (A.3)
- Human Reliability (A.5)
- Behavioral Observation Programs (A.2)
- Fitness for Duty (A.4)
- Multiple Man Rules (A.1)

3.4.2. Organizational Factors

The organization which operates a nuclear power plant is divided into departments which handle separate functions. For example, the operations department is responsible for adjusting plant functions to operate safely, the health physics department is responsible for minimizing and recording personnel exposures to radiation. The instrumentation and control department is responsible for assuring that measurement instruments in the plant are correctly calibrated, and the security department is responsible for the integrity of the site against adversarial action. The functions of these departments can become a problem if their responsibilities come into conflict. In addition, when the functions of these departments becomes sufficiently fragmented the overall sense of responsibility for the safe operation of the plant can become diluted. For example, maintenance personnel must hold the attitude that security is important if the adequacy of security is to be assured. As a result, the organizational factors which affect the quality of security can be clustered into a single group.

3.4.3 Man-Machine Interface

In order for safeguards personnel to effectively function, they must competently use systems and equipment designed for site security. Security systems are becoming highly sophisticated due to the demonstrated advantages, in terms of both cost and effectiveness, of automation. Systems which interpret and simplify signals to the alarm station can degrade security if personnel are not fully aware of the system's functions and limitations. Likewise, equipment failures can compromise site security.

The man-machine interface involves any situation where personnel must use a device to assist in a safeguards action. That includes automatic access controls, communications equipment, alarm systems, surveillance systems, firearms, and systems for selecting and presenting appropriate events and responses. The training and performance evaluation group contains the concept of designing optimal training for the man-machine interface, but research should be done to examine the rapidly advancing state-of-the-art in security systems. That information could be effectively used as input for training programs and as a technical basis for regulatory action concerning the security aspects of the man-machine interface.

3.4.4. Trustworthiness and Reliability

As a function of plant management new applicants are screened for trustworthiness and reliability before being hired and current employees are observed to assure their continued reliability (and trustworthiness). This group is similar to that presented in the evaluative approach (Section 3.3.1 and 3.3.4.2) and reader is referred to those sections.

4.0. Conclusions

This document has presented an examination of the feasibility of conducting research on human factors in nuclear power plant safeguards. The aspects of practicality, usefulness and acceptability were studied for each human factor identified in the previous chapter. Then human factors were grouped according to research approaches and other common characteristics. The information contained in this chapter will be used to formulate an integrated, long-term research plan.

CHAPTER 4

A REVIEW OF RESEARCH DESIGNS FOR EXAMINING HUMAN FACTORS AFFECTING NUCLEAR POWER PLANT SAFEGUARDS

Allan Mazur, Sidney Arenson,
Jeff Katzer, and Barbara Settel

CONTENTS

CHAPTER 4

1. INTRODUCTION

1.1 Purpose

Chapter 2 identified and ranked human factors issues which affect safeguards and Chapter 3 assessed the feasibility of research on those same human factors issues. This chapter develops a general review of the open literature for research which could be brought to bear on the human factors issues identified in the second chapter as important to safeguards and recommends research designs for optimally studying them.

The research designs which are recommended are based entirely on scientific methodological considerations. Problems of acceptability and practicality associated with research on nuclear power plant personnel are addressed in Chapter 3 and not here. As such, the research designs which are suggested in chapter 4 are not being recommended solely as NRC projects, but rather as research designs which could also be used or modified for use by the industry itself or other related organizations interested in these issues. Some of these research designs may not be appropriate or practical for NRC-sponsored research.

1.2 Scope of Inquiry

Since the accident at Three Mile Island, there has been increased concern with "human factors" as a determinant of safe or unsafe operation of nuclear power plants (Cordes, 1983). Here we discuss human factors related to the guard forces that are employed at all nuclear power plants to prevent breeches of security, whether sabotage by knowledgeable insiders (Edelhertz and Walsh, 1978) or assault from the outside. The underlying assumption of this work is that nuclear power plant safeguards can be improved by a better understanding of security forces. Naturally, before extensive new research is begun, it is worthwhile reviewing the existing literature for promising leads and to avoid dead ends already taken by others. We have searched security industry journals and the literature in social science and psychology (but no government or industry reports which are reviewed in Chaper 3) to locate research results that are relevant to conducting specific research on security forces. After assessing what has been done, we suggest research on the behavior of security forces.

This chapter does not attend to sensitive nuclear materials diversion and theft or to the behavior of potential adversaries, both of which have been defined as outside the scope of this inquiry, but instead with the response of the plant security force to such threats. While this chapter focuses on security personnel, some findings are relevant to other members of the nuclear power plant work force as well.

2. CLUSTERING ISSUES

Chapter 2 identified 19 human factors issues of particular concern in nuclear power plant safeguards. While these issues have been useful in setting our research priorities, they are not convenient topics for an efficient search of the literature. Some are so broad (e.g., Instruction, Training, and Selection) that they would produce long lists of research titles which are mostly

irrelevant to our purposes; others are so specialized (e.g., Two-man Rule) that they cannot be used as key words in a bibliographic data base.

Fortunately, the issues cluster into three clear-cut groupings which formed the basis of our literature search. We have named the first of these groupings "Personnel Evaluation" because its topics are primarily concerned with the question: How do you select new employees for the security force and once selected, how do you evaluate the efficiency of their performance? Issues in the second cluster, "Organizational Evaluation," are all concerned with the question: How do you keep your security force attentive, with good morale, during the ordinary (and sometimes boring) routine of security operation? The third cluster, "Response-to-Threat Evaluation," is concerned with the rare occasion when a real threat emerges, asking: How do you assure that the guard force operates properly in an actual threat situation? Table 2.1 shows the division of the issues identified in Chapter 2 into these three clusters.

Single articles located in our search often address two (or more) issues within a cluster, but the same article rarely addresses issues in different clusters attesting to the coherence of the groupings as we have defined them. Moreover, as we began to develop new research strategies, we found that the several issues within a cluster could be researched in a similar way, whereas the different clusters require different research design strategies.

In summary, the use of these clusters greatly simplified both the task of reviewing the literature and that of suggesting new research, for each cluster corresponds to a basic problem of evaluation, first of personnel, then of the organization's routine operation, and finally of the organization's response to threats.

Table 2.1 The Human Factor Issues Divided into Three Clusters.

Personnel Evaluation:
- Trustworthiness (A.3)
- Behavorial Observation (A.2)
- Fitness for Duty (A.4)
- Selection (B.5)
- (Individual) Performance Evaluation (C.4)

Organizational Evaluation:
- Instruction and Training (B.5)
- Human Reliability (A.5)
- Boredom and Vigilance (B.1)
- Organizational Communication (B.2)
- Corporate Attitude (B.4)
- Maintenance (D.2)
- Communications Equipment (D.3)
- Nuisance and False Alarms (D.5)
- Rotation/Manpower/Shiftwork (B.3)
- Two-Man Rule (A.1)

Response-to-Threat Evaluation:
(Security Force) Performance Evaluation (C.4)
Format and Wording of Contingency Plans (C.1)
Self Preservation and Deadly Force (C.2)
Coordination Between Staffs (C.3)
CAS/SAS Design (D.1)

3. LITERATURE SEARCH

We have searched the professional literature in the behavioral sciences (and adjacent fields) for research that is directly relevant to nuclear power plant safeguards. While pertinent material exists in government and industry reports, these were defined outside of our scope and are instead reviewed in Chapters 2 and 3.

3.1 Method

It was necessary at the onset to form an efficient search strategy, since the literature is voluminous and our resources limited. A computer search was chosen over a manual search for more exhaustive coverage across disciplines and subjects, and for its great time saving. We chose three computer databases, which together encompass most of the recent behavioral science literature. These are Psychology Abstracts, covering the psychology literature back to 1967; Sociological Abstracts, covering sociology and organizational behavior back to 1963; and ABI/Inform, covering business, management, and human resources back to 1971. We excluded dissertations and foreign language works from the search because of the cost of obtaining readable copies.

During a search, a subject or "keyword" is entered into the computer, which then generates a list of relevant titles with abstracts. Important tradeoffs must be considered in chosing subjects for the search. If a subject is too general, a lengthy list of titles will be produced, most having little bearing on the problem at hand and the efficiency of computer searching is lost. If one is too specific, it is easy to miss relevant articles. We attempted a mid-course, retriving what was important without overwhelming ourselves with irrelevant abstracts. Subjects were approached on three levels:

1. Literature directly related to nuclear power plants - security, threats, human factors.

2. Literature on the security guard profession - industrial security, personnel selection, training, motivation, job attitudes.

3. Related literature on military and police organizations.

Over 400 abstracts were generated in this manner. Each was read by everyone in our group and if it was thought that an article looked worthwhile, a hard copy was obtained. The bibliographies of these articles were further searched for relevant pieces that had been missed by the computer. We also compiled names of researchers in the field (including those who had authored relevant government and industry reports) and searched for their publications.

Finally, we drew on our own expertise in psychology, sociology, organizational behavior, and information studies to add articles which appear to be relevant.

3.2 Results

Overall, we did not find a well developed literature that is directly relevant to nuclear power plant safeguards. Of nearly 60 articles located in the search, many are anecdotal or programmatic in nature; relatively few are methodologically strong studies. Our conclusion is that human factors related to guard forces, whether at nuclear power plants or comparable industrial facilities, have been little researched--at least, such research does not appear in the published, open literature.

At this point, our strategy became not only to review what studies are available, but more important, to draw on our own background in the behavioral sciences in order to suggest research designs which optimally address these topics.

4. SUGGESTIONS FOR RESEARCH

In the remainder of this report, we take up each of the three clusters, review the pertinent literature, and suggest optimal research designs.

4.1 Personnel Evaluation

Personnel screening at the entry level is aimed at identifying all applicants who have a high probability of manifesting unreliable or untrustworthy behavior as members of a security guard force at a nuclear power plant. Background information and psychological assessment are the major sources of information for screening.

With respect to background information, the search of the literature indicates that major security firms collect medical, residential, and employment histories (Kmet, 1979). The Department of Defense has applicants for security clearance interviewed by a psychiatrist for indicators of vocational instability and psychopathology (Linn, 1973). Specific indicators, such as tendency to act out abnormal behavior patterns and history of alcohol abuse have been associated with rejection of security clearance. We found only one study that related background factors with job performance. A study of Air Force Security Police investigated the correlation between pre-training biographic factors and supervisors' performance evaluation (McFarlane, Kantor, and Guinn, 1980). The significant correlates of job performance were not those usually found in a background information investigation, but instead were the self-reported attitudes of the trainees, such as attitudes toward parents and former teachers. It has been suggested that applicants for security force positions undergo the same type of background investigation used in screening people for access to classified military information (Menkys, 1979). Such suggestions may be premature since the research supporting this sytem which was located is mainly limited to stating what the criteria for rejection are, or have been, and offers little evidence for the validity of such criteria.

4.1.1 Psychological Assessment

It is not clear what type of psychological assessment to use in evaluating the trustworthiness and reliability of prospective employees, both operational and security. We found that psychological assessment focuses mainly on personality characteristics with assessment of attitudes, values, and motives as subsidiary concerns.

Literature on personality characteristics of security force applicants was mainly descriptive, usually showing and discussing frequency distributions from various tests used in the security industry and the nuclear power industry.

The Minnesota Multiphasic Personality Inventory (MMPI) is the most popular instrument among professionals serving the nuclear power industry (Baird and Hammond, 1982). Bernstein (1981) found that the Psychopathic Deviancy Scale of the MMPI consistently identified applicants for security force positions who had committed criminal acts. Kmet (1979) reports that 12% of applicants for security force positions who showed elevation on one of six particular MMPI scales were judged to be high risk. Bernstein (1980) provides normative data on MMPI profiles for a sample of 4,500 actual security guards. Bernstein (1981) also reports that elevated scores on the Pd (Psychological Deviancy) and the Ma (Excitability) scales of the MMPI are often related to problems in the security force industry, including high employee turnover.

Other personality assessment instruments that have been used are the Myer-Briggs test (Hanewicz, 1978), Gough and Heilbrun's Adjective Check Test (Murrell, Lester, and Arcuri, 1978), Eysenck Personality Inventory (Hester and Brown, 1981), and Cattell's 16 Personality Factors Questionnaire (Baird, 1981; Krug, 1981).

The literature on the uses of these instruments does not offer much guidance on how to select a security force that will be trustworthy, reliable, and competent. The cutoff scores on these instruments, which are used to define high risk individuals, are usually arbitrary. There are no comparisons between the profiles of security force samples and adults in the general population. In addition, an appropriate comparison group is difficult to specify since the pool of applicants for security force positions may come from a relatively disadvantaged segment of society.

4.1.2 Assessment of Attitudes, Motives, and Role Expectations

Although hard data on turnover of security personnel in the nuclear power industry were not located, it is known that the turnover in private security agencies is very high (Parry, 1976). Employee dissatisfaction in both contract and proprietary security agencies is high. Clark (1982) reports that major areas of employee dissatisfaction in such agencies are: (1) inadequate pay and benefits, (2) boredom on the job, (3) feeling that other employees regard security personnel as inferior, (4) no room for personal growth, (5) fear of mistakes, (6) personal problems, and (7) inadequate or poor supervision. Many of these sources of dissatisfaction are organizational problems discussed in Section 4.2. However, it appears that these problems may be mitigated by careful screening of the attitudes, motives, and role expectations of applicants.

There is evidence that frustration of motives and violation of role expectations can lead employees to participate in anti-social behavior. In a study of white collar crime, Dellheim (1979) found these crimes associated with such job frustration factors as: (1) not being allowed to make decisions and express preferences, (2) lack of variety in the job, and (3) no room for personal growth. Goldsmith (1979) includes lack of pride in work, wage disputes, and personal problems as characteristic of the employee thief profile. Clark and Hollinger (1980), in a questionnaire study, found that employees most concerned with improving themselves and meeting career goals were involved in employees theft at an above average rate.

From this, it seems that unrealistic attitudes, inappropriate motives, and inflated role expectations can contribute significantly to employee dissatisfaction which is associated with high turnover, employee theft, incompetent execution of duties, tardiness, absenteeism, violation of rules and other behavior counter-productive to safeguards objectives. A study of Air Force Security Police (McFarlane, Kantor, and Guinn, 1980) found four such job experience-attitudinal factors related to job performance ratings.

4.1.3 Establishing Criteria for Psychological Assessments

The major problem in using psychological assessments appears to be the establishment of some validity criteria for the assessment techniques. An example of such an effort has been reported by Guinn, Wilbourne, and Kantor (1977). They administered a battery of measurement instruments to 4,502 basic airmen, prior to their entering technical training for Air Force Security Police, and then checked to see if the original scores predicted who would complete the training successfully.

An optimal research design would involve the use of such instruments for the collection of existing data on the personality characteristics of actual guards from two licensees. These data can then be used to discriminate between two groups of guards identified as demonstrating different degrees of performance on the basis of such criteria as supervisor's evaluations, history of absenteeism, interpersonal difficulties on the job, reports of alcohol and drug problems, and other performance criteria found to be relevant. Stepwise Discriminant Analysis (Jennrick and Sampan, 1981) is a convenient statistical technique leading to the elimination of those personality variables that do not contribute to the discriminant function. We estimate that the collection and analyses of such existing data would require the time of one person for six months.

A next step would be to validate the findings of this analysis at other sites. This would entail predicting the performance evaluations of guards from the data on their personality characteristics. We estimate this would also require one person part-time for two years. If it is not possible to use actual licensee sites, other industrial sites or DOE facilities might be used with proper cautions on extrapolation biases.

4.1.4 Identifying Appropriate Attitudes, Motives, and Role Expectations for Prospective Security Guards

Research found during this literature review has suggested that attitudes, motives, and role expectations have a strong relationship with the guard's performance and satisfaction with the job. Therefore, it seems useful to investigate how attitudes, motives, and role expectations actually affect criteria of performance such as turnover in security forces. The interview method is appropriate for this inquiry.

Exit interviews (Lapides, 1979) could be conducted with both those who leave the security force voluntarily and those who are terminated. Interviews with presently employees guards would be conducted to determine their perceptions of the position and restrictive aspects of the job as has been done with prison guards (Jacobs, 1978; Piretti and Hooker, 1976). As an example, Jocobs (1978) found that prison guards regard job security as one of the main advantages of their jobs. Having such a motive may, in some manner, determine whether or not an applicant will become a satisfied employee in a security force. At one reactor site, the use of an attitudes and motives screening process resulted in a very low turnover rate (see Vol. 2, Chapter 3, Section 2.10).

Elicitation of such perceptions would contribute information concerning which attitudes, motives, and role expectations are congruent with the job and can be used in screening for applicants who possess them. This information would be derived from content analyses of the interviews. The results would be used to construct an interview schedule that would identify inappropriate attitudes, motives, and role expectations. We estimate this would require two people for one year.

A final step would be to implement the use of the interview schedule at a few sites while using others as controls. The success of the additional screening provided by the interview schedule could be evaluated against the criterion of job turnover. We estimate that it would take two years to collect sufficient data for such an evaluation, but the actual work effort associated with the analysis of the data would require only one person for three months.

4.2 Organizational Evaluation

The behavioral literature on security organizations is remarkably scant, most of it simply personal accounts of particular safeguards programs. A theme which occurs frequently in these accounts is the problem of low morale and consequently poor performance among guards in security forces (e.g., Higgins, 1980; Hoffman, 1980).

These published accounts strongly suggest that a major cause of poor morale is the general alienation (or "apartness") of the security force, reinforced by the low status and salaries of guards. Langer (1982) reports an average security guard's salary as only $15,000 in 1981, and security supervisors do not make much more unless employed by a large company having many subordinates. The common perception of the security guard is one of low occupational status, low education, and low income (Grant, 1980). This view often affects relations within the company, so security managers seem particularly concerned with

enhancing their image as professionals and avoiding the tag of "company cop" (Evans, 1978). Such image improvement may be difficult in a corporate setting where the function of the security force is not always well understood or appreciated (Kmet, 1979). In any case, one attempt to raise the professional image of prison guards did not have a very beneficial effect on attitudes (Regoli, et al., 1981), though it would be invalid to generalize from the hostile prison setting to the friendlier climate at a nuclear power plant. Nonetheless, the very function of the guard carries the potential for adversarial relations with others on the site, as when it is necessary to control personnel access or search employees. These actions sometimes promote antagonism between guards and other personnel (Hoffman, 1980). Even local police, who have many commonalities with security guards (Chang and Jenekesla, 1977), hold guards in lower esteem than they do other policemen (Hallcrest, 1981).

Several researchers have asserted that the solution to this problem is to integrate the guard force into the body of the corporation, or to raise its status, or both. Thus, proprietary security forces are often seen as preferable to contract forces because they are an integral part of the company and, therefore, presumably have higher status and morale (Cohen, 1979). We have located no firm evidence that this is the case. While there are assertions about the superiority of proprietary forces (e.g., Bitter, 1982), others claim that contract guards are fully satisfactory when properly trained (Cumbow, 1979).

It is clear that a guard force has the same dynamics as other small work groups (Ridgeway, 1983), though the particular setting of the guards in their work place, and their special organizational problems, seem virtually unstudied. At this point, it is not possible to identify the factors which make one guard force work well and another poorly, except for assertions about the kinds of proprietary/contract differences discussed above. Occasional claims that "corporate attitude" makes the difference may be empty because corporate attitude has never been measured independently of the behavior of the guard force. Instead, when a poorly appearing guard force is encountered, it is often assumed to be an indicator of poor corporate attitude. Thus, the reasoning here appears to be circular.

An optimal research design to study these factors would involve a three-step research strategy aimed at improving the routine operation of guard forces. In the first step, case studies would be prepared of three sites where guard forces are widely acknowledged to work exceptionally well in routine operation, and also of three other less knowledges sites. A comparison of these cases would allow for the generation of hypotheses to account for the difference in efficacy among working security forces. This method has been routinely applied to other kinds of projects to discern possible causes of weak and strong performances, and is an effective means of generating hypotheses for improvement (Mazur and Boyko, 1981). Such a study would require about two persons for one year.

Once such hypotheses are formed, the second stage of research would test them using correlational data from a survey of about 30 sites. The guard force at each site would be rated on its efficacy of routine performance, perhaps by reputational means supplemented with inspection and reporting data. (Reliable

performance evaluation techniques must be developed.) All other factors hypothesized to affect guard performance would also be measured at each site, including contract vs. proprietary status, salary levels of the guards, type and duration of training programs, corporate attitude (properly measured), and whatever other factors appeared from the case studies to distinguish good from weak security organizations. This data from approximately 30 sites would allow statistical correlation of security force performance (the dependent variable) with each of the hypothesized causes (the independent variables) in order to discern which ones are in fact related to performance according to statistical analysis. Such a survey could be completed in one year with the work of two to four persons, depending upon the scope of the survey.

In the survey of plant sites in step two, factors that correlate with guard performance, and therefore show promise of improving performance (if they are implemented) are identified. However, correlation does not imply causation. Therefore, the third step in the research is experimental, actually implementing some of these changes on a trial basis in order to see if they do in fact improve the operation of the security force. It is not possible to specify the time or manpower needed for this stage until the desired experimental designs are known in some detail.

4.3 Response-to-Threat Evaluation

A central task of human factors research is to develop means to assess and improve the security force's response to a threat. In order to do this, there must be some reliable way to evaluate the guards' response efficacy; otherwise there is no way to know if there is an improvement or not. This task would be simple if threats occurred frequently because it would be possible to judge the security force's response in precisely those situations that it was trained to meet. However, serious threats are rare in actual experience, so there is little opportunity to reliably appraise the security forces' response to true crises.

In current practice, indirect means are used to evaluate guard force preparedness, these usually being formal inspections by the NRC or the nuclear industry (Perry, 1981; Bush, 1981; Bailey, 1981). NRC inspectors do not normally watch the guards in operational drills or simulations, instead basing their evaluations on the adequacy of written procedures the completeness of record keeping, equipment maintenance, appearance of the guards, and the like. Implicit here is an assumption that guards who follow procedures and have the correct appearance will perform adequately in a crisis.

To test this hypothesis, in one pilot study, safeguards inspection results for the period 1978-80 were collated for nuclear plants included in NRC's Region I computer data-base (Mazur, 1981). These plants were then ranked from "high" to "low" on their success in passing inspections. During 1979-80, there were nine intrusion events recorded at these plants (in the Safeguards Summary Event List, NUREG-0525), none major threats but rather instances such as an unauthorized person or contraband on the site. The security forces were then judged to have responded properly in three of these events and improperly in six. These judgments allow plants to be scored on their adequacy of response to real (if minor) threats to security. When the two variables were crosstabulated, there was little correlation. According to this, guard forces

that inspect well do not necessarily respond any better to an actual breech of security than forces that inspect poorly. While this result should be regarded as tentative until it is replicated on a larger number of sites and more comprehensive data (requiring about one person-month of effort), it provisionally suggests that formal inspections, as presently done, may not be entirely inadequate for evaluating guard force preparedness.

In view of this potential inadequacy, a three-step strategy is recommended for research on security forces' response to threat, the first step being to develop reliable indicators of the efficacy of security force response. Until that is done, NRC will not be a good position to reliably evaluate potential improvement in security force behavior. Once indicators of adequate threat response are available, the second research step would be a survey, covering a large number of plants, to identify the correlates of effective response. Factors which promote effective response, identified in this second step, will be further evaluated in a third (experimental) step, to determine if their implementation would indeed enhance guard response to threat. The logical flow from one step to another will be clearer as we describe each in more detail.

4.3.1 Developing Indicators of Response-to-Threat

This literature review has indicated that several kinds of indicators should be considered as potential criteria for evaluating response-to-threat efficacy, including:

1. Tests taken by individual guards. While each guard's knowledge of relevant information does not by itself assure that he/she, much less, the whole guard force, will respond properly in a crisis, nonetheless, command of relevant information is a minimum requirement for proper response.

2. Performance of the guard force during simulated events. While the nuclear industry uses simulations for training purposes (Kriessman, 1981; Hollnagel, et al., 1981), they are not generally used to measure safeguards efficacy, through experience in other security settings suggests their desirability for this purpose (Otway and Misenta, 1980; Sloan et al., 1978; Shirar, 1978). Since guards are aware of the simulated nature of these exercises, they lack the stress and urgency of real situations, however, such drills should allow evaluation of important features of the response, particularly those requiring coordination among team members and with other plant and law enforcement personnel, and problems posed by environmental factors.

3. Response to real intrusions. We have already referred to NRC's routine tabulation of real (though usually minor) intrusions which occasionally occur at plant sites (SSEL-NUREG-0515). An indicator of response efficacy, based on guards' proper or improper reactions to such intrusions, has the advantage of realism, though at a low level of degraded security.

4. Inspections. Although the result described above casts doubt on the validity of cursory inspections as an indicator or response efficancy,

a more thorough study might show otherwise. Also, other forms of inspection than those currently used by NRC may have better validity.

5. Covert attempts to breach security. While it is not reasonable to suggest full scale "black hat" assaults on a nuclear site for the purpose of testing the security force, more innocuous attempts to breach security may be acceptable, including ostensibly unauthorized approaches to fences or limited access areas, or attempts to bring contraband on site (Bean and Prell, 1978; Rose, 1980). Such actions have occasionally been taken by NRC inspectors, and they may allow the most realistic evaluation of guard force response, short of a true threat.

It could simply be assumed that each of these indicators measures response-to-threat efficacy, however, we will be on firmer ground if we actually test the assumption. Consideration ought to be given to applying all of these indicators to security forces at several sites, and then examining the intercorrelation among indicators. If all indicators do indeed measure response-to-threat efficacy, then security forces that score high on one should score high on the others as well, so the intercorrelations would be generally high. However, if we find that one indicator (e.g., inspections) does not intercorrelate with the others, then we would conclude that it fails to measure response efficacy. By this method of "convergent validity" (Cook and Campbell, 1979), we identify that subset of indicators which "hang together," as common measures of response efficacy.

The resources needed to develop response-to-threat indicators will depend on how extensive a research project is planned. Data on intrusions are available in NUREG-0525, while NRC inspection results are stored in each region's data computer, so these are easily obtainable. More time and labor is required to design guard tests, simulations, and covert security breeches, if these were included in the study. One calendar year should suffice for this design, assuming one or two persons working. Once indicators are developed, they should be applied to a sample of 30 or more sites in order to provide clear correlation results, a task that could take one or two years, and one or two persons (not counting site personnel), depending on the scope of the study. In total, the development of response-to-threat indicators should take one or two persons from one to three years, depending upon the scope of the work.

4.3.2 Correlates of Response Efficacy

Once trustworthy indicators of response-to-threat efficacy have been developed, we are in a position to identify potential improvements in guard response, which is the purpose of step two in the three-step research strategy.

Some of the factors which might contribute to response efficacy have already been discussed in Section 4.2. Good training and positive corporate attitude should not only improve the routine operation of a security force, but its response during a crisis as well. Additional factors not discussed in Section 4.2 seem particularly pertinent to crisis management. An obvious example is consideration of the use of deadly force. Less discussed, though perhaps more important, are the format and wording of contingency plans which guards must expeditiously consult during an emergency. As security forces

increasingly move toward computer displays to call up this information regard must be paid to the generalization from human factors research in operational safety that people should not have to reply on unfamiliar equipment as part of their response to a stressful event. Unless guards are trained to the point where computer displays become "second nature," these are as likely to inhibit as facilitate their response to a threat. Similar problems arise in the coordination of central and secondary alarm stations (Natali, et al., 1975), so that what appears, at first blush, to be an improvement sometimes turns out to produce unforeseen difficulties in practice.

The purpose of step two is to see which of the many factors that might conceivable influence the quality of threat response do in fact correlate with it. Do guard forces which use computer displays respond better to threats than those which do not? To answer such questions, we use the same sample of approximately 30 sites that is utilized in step one. At the same time that the various criteria of response efficacy are being measured at each site (for step one), we also obtain measures of all those factors which are hypothesized to influence the quality of the threat response. These would include type and duration of training, format and wording of contingency plans, use of sidearms or not, whether the guard force is contract or proprietary, and the like. Once these measures are obtained, they can be crosstabulated against the criteria of response efficacy in order to see which ones are, in fact, associated with quality of response, and which are not.

The efforts required here are, first, specification of the factors to be measured at the sites, then collection of data (during the same site visits used for step one), and finally the correlation analysis. These tasks are easily merged with step-one chores and should require no additional time or manpower.

4.3.3 Experimental Test of Promising Factors

As we have already discussed in Section 4.2, correlation does not imply causation. Before changes in regulations or procedures are instituted, experimental testing of these factors to assure that they do indeed bring about the desired changes is recommended. Frequently policies which are implemented on theoretical, anecdotal, or correlational grounds turn out, in practice, to fail in their intended efforts. Experimental tests give firmer ground on which to proceed. Experiments have shown, for example, that police especially trained in crisis intervention techniques are no better at handling real crises than those who are untrained (Mulvey and Dickson, 1981), thus raising doubts about the cost-effectiveness of such training programs. On the other hand, instruction in self defense has been effective in making unarmed guards feel more confident and secure (Goldberg, 1980), thus verifying the wisdom of that policy.

It is difficult to project the cost of experimental tests since their scope depends on the factor being tested, the effects that are expected, and the number and type of sites used for testing. An experimental evaluation of two different forms of contingency plans, to see which gave the clearest information to guards, might require only a few person-months of effort at one or two sites. On the other hand, an elaborate comparison of two different alarm station arrangements, to see which produced better guard response during simulated threats, may require a more ambitious experiment, probably involving several sites and much equipment.

5. SUMMARY AND CONCLUSION

Chapter 2 identified 19 human factors issues of particular concern to nuclear safeguards experts. It is likely that behavioral research on some of these issues will lead directly to recommendations for regulatory policy, so we have taken preliminary steps in planning a cost-effective research program.

The 19 human factors issues of concern fall into three natural clusters, each focused on one broad research question. The first cluster pertains to Personal Evaluation and asks, "How do you select new employees for the guard force, and once selected, how do you evaluate the efficacy of their performance?" The second cluster pertains to Organizational Evaluation and asks, "How do you keep your guards prepared, with good morale, during the ordinary routine of security operations?" The third cluster pertains to Response-to-Threat Evaluation, asking "How do you assure that the guard force operates properly in an actual threat situation?"

We have searched the behavior science journals (but not government or industry reports) for research that is directly relevant to these questions. While there are vast literatures on the topics of "personnel" or "organizations," most of it has little direct bearing on our present concerns, so we have focused in on security-like situations.

Overall, we found little by way of a developed body of behavioral research in the security and safeguards area. It is likely that in the future, as very specific research questions become articulated, more specialized behavioral-science literature will provide useful sources. At present, however, human factors related safeguards research is in its infancy.

We have suggested research strategies to be pursued in each of the separate clusters on personnel, organization, and response to threat. To coordinate these, and economize on overlapping efforts, we bring these three research agendas together here, into a unified program, as shown in Figure 5.1.

Easy, inexpensive, preliminary studies were suggested for each cluster, none requiring more than one calendar year of more than one or two people. For personnel evaluation, we recommend validation studies on existing data by relating personal characteristics of people who have been hired as guards (e.g., prior work experience, personality test results) with criteria of success as guards (e.g., supervisor ratings, longevity on the job); we also suggest interviews of good and poor functioning guards to discern differences between them which might be used in screening. For organizational evaluation, we recommend case studies of three sites noted for very good routine performance of guards, and three sites noted for less good performance, comparing these for systematic differences that may explain performance levels. For response-to-threat evaluation, we recommend the design of several alternate indicators which might measure the response efficacy of a guard force. All of these studies are precursors to follow-up work, and therefore in an optimal research design all should be done during the first year of the research program.

If the results of the first year's work on personnel evaluation appear useful, we propose that they be implemented on a trail basis at one or two

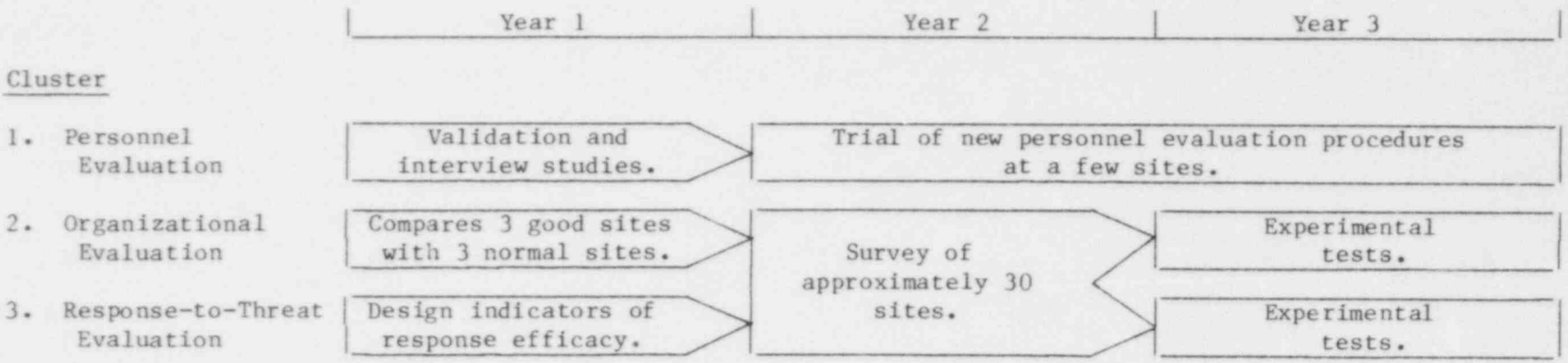


Figure 5.1 Suggestions for a unified research program.

sites, and that the sites be monitored over the next two years in order to determine if these new evaluation practices produce satisfactory results.

The first year's work on organizations and response-to-threat leads, in both cases, to a second step (during Year 2) in which approximately 30 sites are surveyed. For economy's sake, these surveys should be merged, since both can be done simultaneously for nearly the price of one (which we judge to be 2-4 person-years, depending on scope).

With correlation results from the Year 2 survey in hand, we will be ready to do experimental tests on the specific policy options identified in this work. It is difficult to estimate the cost of these experiments without further specification of the policies to be tested; they may range from modest to elaborate efforts, and the larger ones would presumably be justified on an ad hoc basis.

By the end of Year 3, firm experimental findings ought to be available which translate directly into recommendations for regulatory policy, and a long-term behavioral-research program on safeguards will be well underway.

BIBLIOGAPHY

For Chapter 4

Bailey, D. "Nuclear security: A Systematic Approach," Security Mangement, 25 (June): 44-54, 1981.

Baird, J., Jr. "Reliability of the 16 PF Questionnaire for Security Guard Applicants," Journal of Personality Assessment, 45: 545-546, 1981.

Baird, J., and Rammond G. "Nuclear power: Using Psychology to Protect It," Security Management, 26: 77-79, 1982.

Bean, C. and Prell, J. "Personnel Access Control--Criteria and Testing," Security Management, 22 (June): 6-8, 45-47, 1979.

Bernstein, I. "Security Guards' MMPI Profiles: Some Normative Data," Journal of Personality Assessment, 44: 377-380, 1980.

Bernstein, I. "One Way to Screen Guards," Security Management, 25: 35-38, 1981.

Bitter, R. "The Changing of the Guards," Security Management (May) 26: 30-35, 1982.

Bush, Jr., L. "A Joint Responsibility," Security Management, 25 (June): 36-43, 1981.

Chang, D. and Janeksela, C. "The Subjective Factor in the Perception of Social Problems," Journal of Offender Therapy and Comparative Criminology, 21: 66-78, 1977.

Clark, J. and Hollinger, R. "Theft by Employees," Security Management, 24: 106-110, 1980.

Clark, R. "Stop the Revolving Door," Security Management, 36: 55-59, 1982.

Cohne, J. "Choosing Contract or Proprietary Security," Security Management, 24 (October): 26-30, 1979.

Cook, T. and Campbell D. Quasi-Experimentation, Chicago: Rand-McNally, 1979.

Cordes, C. "Human Factors and Nuclear Safety: Grudging Respect for a Growing Field," APA Monitor (14): 1, 13-14, 1983.

Cumbow, T. "Getting Off on the Right Foot with a Contract Guard Service," Security Management, 22 (November): 14-17, 1978.

Dellheim, S. "It's Owed to Me," Security Management, 23: 26-27, 1979.

Edelhertz, H. and Walsh, M. The White Collar Challenge to Nuclear Safeguards, Lexington, MA, 1978.

Evans, C. "Don't Get Tagged as the 'Company Cop'," Security Management, 22 (August): 58-60, 1978.

Goldberg, M. "To Arm or Not To Arm," Security Management, 24 (May): 8487, 1980.

Goldsmith, R. "Recognizing the Employee Thief," Security Management, 24: 53-54, 1979.

Grant, N. "College Students' Perceptions of Security," Security Management, 24 (June): 86-90, 1980.

Guinn, N., Wilburn, J. and Kantor, J. "Preliminary Development and Validation of a Screening Technique for Entry into the Security Police Career Field," JSAS Catalog of Selected Documents in Psychology, 7: 122, 1977.

Hallcrest Systems. "The Security-Police Relationship," Security Management, 25 (November): 35-41, 1981.

Hanewicz, W. "Police Personality: A Jungian Perspective, "Crime and Deliquency, 24: 152-172, 1978.

Held, B., Levine, D., Swartz, V. "Interpersonal Aspects of Dangerousness," Criminal Justice and Behavior, 6: 49-58, 1979.

Hester, R., and Brown, W. "Eysenck Personality Inventory: A Normative Study on an Adult Industrial Population," Journal of Clinical Psychology, 36: 937-939, 1980.

Higgins, C. "The Security Director as Trainer," Security Management, 24 (May): 77-81, 1980.

Hoffman, G. "Good Morale from a Sense of Purpose," Security Management, 24 (June): 19-25, 1980.

Hollnagel, E., Pedersen, O., and Rasmussen, J. "Notes on Human Performance Analysis," Roskilde, Denmark: Riso National Laboratory, 1981.

Jacobs, J. "What Prison Guards Think: A Profile of the Illinois Force," Crime and Delinquency, 24: 185-196, 1978.

Jennrich, R., and Sampson P. "Stepwise Discriminant Analysis," In Dixon, W. (Ed.), BMPD Statistical Software, Berkeley: Univer. of Calif. Press, 1981.

Kmet, M. "What is a Security Management," Security Management, 23 (May): 6-11, 43, 1979.

Kmet, M. "Placing Employees for Best Results," Security Management, 23: 6-14, 1979.

Kriessman, C. "A Spectrum of Simulators for Power Plant Training," Training and Development Journal, 35 (September): 37-39, 1981.

Krug, S. "Development of a Formal Measurement Model for Security Screening in the Nuclear Power Plant Environment," Multivariate Experimental Clinical Research, 5: 104-123, 1981.

Langer, S. "Salary Survey 82," Security Management, 26 (May): 15-17, 1982.

Lapides, G. "Exit Interviews as a Loss Protection Techniques," Security Management, 23: 36-37, 1979.

Linn, L. "Psychiatric Factors in Security Screening," American Journal of Psychiatry, 130: 643-652, 1973.

Mazur, A. Boyko, G. "Large-Scale Ocean Research Projects: What Makes Them Succeed or Fail?" Social Studies of Science, 11: 425-49, 1981.

McFarlane, T., Kantor, J. and Guinn, N. "Correlates of Successful On-the-Job Performance in the Security Police Career Field," JSAS Catalog of Selected Documents in Psychology, 10: 95, 1980.

Menkus, S. "Hardware Alone Won't Prevent Theft: Basic Security Principal Paramount," Business Insurance, 13: 30-61, 1979.

Milvey, E. and Reppucci, N. "Police Crisis Intervention Training: An Empirical Investigation," American Journal of Criminal Psychology, 9: 527-48, 1981.

Murrill, J., Lester, D., and Arcuri, A. "Is the Police Personality Unique to Police Officers?" Psychologoical Reports, 43: 298, 1978.

Naatali, J., Seedman, A., and Taback, S. "How Effective are Central Security Stations?" Chain Store Age (June); E22-E23, 1973.

Otway, H. and Misenta, R. "Some Human Performance Paradoxes of Nuclear Operations," Futures, 12: 340-57, 1980.

Parry, J. "Make Sure You Have the Right Security Guards," Guardian Business, (March): 73-75, 1976.

Perry, T. "INPO: Utilities Create Their Own Policeman," IEEE Spectrum (March): 58-61, 1981.

Piretti, P., and Hooker, M. "Social Role Self-Perceptions of State Prison Guards," Criminal Justice and Behavior, 3: 187-196, 1976.

Robert, J., Singer, L. and Watson, F. "Hostage Survival," Security Management, 22 (August): 46-50, 1978.

Regoli, R., Poole, E., and Lotz, R. "An Empirical Assessment of the Effect of Professionalism on Cynicism Among Prison Guards," Sociological Spectrum, 1: 53-65, 1981.

Ridgeway, C. The Dynamics of Small Groups, New York: St. Martins Press, 1983.

Rose, R. "Arkansas Nuclear One," Security Management, 24 (July): 52-56, 1980.

Sauer, D., Campbell, W., Potter, N., and Askren, W. "Human Resource Factors and Performance Relationships in Nuclear Missile Handling Tasks," Brooks Air Force Base, Texas: Air Force Human Resources Laboratory, 1977.

Shirar, G. "You Can Motivate your Nighttime Guards," Security Management, 22 (December): 32-35, 1978.

Sloan, S., Kearney, R., and Wise, C. "Learning about Terrorism: Analysis, Simulations, and Future Directions," Terrorism, 1: 315-29, 1978.

Appendix A

Description of Nuclear Power Plant Safeguards, Regulatory Requirements and Industry Standards

1.0 NRC Regulation of Safeguards at Nuclear Power Plants

Safeguards at nuclear power plants evolved from early concerns that nuclear materials could be diverted from peaceful purposes and put to malevolent uses. As a result, early nuclear safeguards were aimed almost entirely at strict accounting for and control of sensitive nuclear materials in terms of its potential for construction of nuclear explosives. At that time nuclear material held by the government and industry was considered sufficiently valuable that appropriate physical security measures would be instituted to protect it on an economic basis. During the early 1970s events lead to increased concern about the security of nuclear materials. At the same time sabotage of a nuclear power plant became increasingly recognized as a potential danger. Safeguards began to receive greater attention; research and development efforts began to seek more sophisticated material control and accounting (MCA) technologies along with increased regulatory intervention into plant security practices.

In 1973 NRC (then the Atomic Energy Commission) published Regulatory Guide 1.17 titled "Protection of Nuclear Power Plants Against Industrial Sabotage" which outlined methods for satisfying physical security regulations. It contains a direct endorsement of American National Standards Institute (ANSI) N18.17 titled "Industrial Security for Nuclear Power Plants" as an adequate basis for physical security planning. This standard was developed by the Standards Committee of the American Nuclear Society.

In 1977 NRC promulgated extensive physical security regulations aimed specifically at nuclear power plants. These regulations, contained in the federal regulations (10 CFR 73.55), then became the law and ANSI-N18.17 became somewhat outmoded. The American Nuclear Society's Standards Committee began work on a new, upgraded standard which was finalized and published in 1982. The new standard, "Security for Nuclear Power Plants" ANSI/ANS 3.3, is specifically meant to supercede ANSI-N18.17. The NRC Regulatory Guide 1.17 is still in place so that ANSI/ANS-3.3 has become, at least tacitly, the endorsed reference for adequate physical security as the successor to ANSI-N18.17.

The following sections outline the requirements of the regulations, NRC Regulatory Guide 1.17, and ANSI/ANS-3.3.

1.1 Regulations

The Code of Federal Regulations contains requirements for safeguarding nuclear power plants. Regulatory Guide 5.4.3, "Plant Security Force Duties" essentially repeats these regulations. The physical protection in place at power plants is designed to protect against the design basis threat of radiological sabotage as described in 10 CFR 73.1(a) which states:

> (1) Radiological sabotage. (i) A determined violent external assault, attack by stealth, or deceptive actions, of several

persons with the following attributes, assistance and equipment: (A) Well-trained (including military training and skills) and dedicated individuals, (B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both, (C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy, (D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and (ii) An internal threat of an insider, including an employee (in any position).

The definitions of the term used in this requirement are given in 10 CFR 73.2, and should be referred to if any are unfamiliar.

The standard of administrative review for determining adequacy of safeguards is similar to that used for safety determinations; namely that the licensee "provide high assurance that activities involving special nuclear materials are not inimical to the common defense and security, and do not constitute an unreasonable risk to the public health and safety."

The regulations require licensees to establish a "security organization" which may be a contract organization. However, the licensee is always ultimately responsible for site security, all records and reports must be available to NRC, and the security organization must demonstrate its ability to carry out the provisions of the licensee's security plans. At least one full-time member of the security organization with authority to direct security activities must be on site at all times. A licensee management system is required "to provide for the development, revision, implementation, and enforcement of security procedures." Security procedures, which are required for an operating license, document the structure of the security organization and detail the duties of guards (security officers), watchmen, and other responsible individuals.

The licensee is not permitted to hire individuals for its security force unless they are qualified under the "general criteria for security personnel" in 10 CFR 73, Appendix B. These criteria include employment suitability and qualification (education, criminal records, age, prior experience, physical fitness, vision, hearing, diseases, addictions, mental alertness, emotional stability, behavioral observation, and requalification), general training (security knowledge including tactics, knowledge of facility and plans, and over ninety other categories of knowledge) and weapons training and qualification. Two current regulatory activities have direct bearing on these requirements. A new rule on "fitness for duty" has been proposed and a rule on "trustworthiness" is currently under internal review by the NRC staff and not presently available for comment. Each licensee security employee must be requalified every 12 months under current regulations.

The licensee is required to establish physical barriers and defensible spaces around vital equipment. These take the form of a "vital area" within a

"protected area" surrounded by an "isolation zone." Vital equipment is defined as:

> "any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to protect public health and safety following such failure, destruction or release are also considered to be vital."

Vital equipment, which is so designated according to a specific method, is to be located only in a vital area which in turn is within a protected area. (The issue of what constitutes vital equipment may not be in step with the current trend in operational safety to reclassify "non-safety" equipment as "important to safety" when it has been shown to impact risk.) Since physical barriers surround vital and protected areas, access to vital equipment requires passage through at least two barriers. An isolation zone must be maintained around the perimeter of any protected area such that the activities of people on either side of the perimeter can be observed in the event of an intrusion. In addition, the reactor control room must be subject to positive access control and completely bullet resistant.

The licensee is required to control all points of access into any protected area. Entrants are to be searched for firearms, explosives, and incendiary devices. The security officer ultimately in charge of controlling access through any access control point must be isolated within a locked, bullet-resisting structure. All packages and vehicles entering a protected area must also be searched. This search can be done by remote means (e.g., magnetometer) or physical means (e.g., pat-down search). Licensee vehicles are to be limited in their use and are to remain in the protected area except for operational, maintenance, repair, security, and emergency purposes.

NRC has proposed rules which would require the mandatory use of remote search equipment for employee searches and pat-down searches of all visitors (45 Fed. Reg. 79492, Dec. 1, 1980). Regular employees would not need to be subject to routine pat-down searches.

A numbered picture-badge system is required for all individuals authorized for unescorted access to protected areas. For all others, an escort must be used and a badge indicating the need for an escort must be worn by the unauthorized individual at all times.

Access to vital areas is required to be highly restricted. For instance, access for the purpose of general familiarization and other non-work related activities cannot be authorized. All unoccupied vital areas must be locked and equipped with intrusion alarms. Access hatches and doors to the reactor containment are to be alarmed and equipped with locks of "substantial construction to offer penetration resistance and impede both surreptitious and forced entry." All keys, locks, combinations, and related equipment are to be controlled and changed whenever there is any evidence of compromise or termination of an employee under adverse circumstances.

NRC has proposed rules (45 Fed. Reg. 15937, March 12, 1980) which would require that access to vital areas be allowed to authorized personnel only for a specific task to be undertaken. If any authorized individual does not need to enter a vital area, then access would not be allowed. Current licensee practice is to grant blanket access authorizations to individuals with limited control on specific need for access.

The licensee is required to maintain a "continuously manned central alarm station (CAS) located within the protected area and... at least one other continuously manned (secondary alarm) station (SAS)." The interior of the CAS cannot be visible from the perimeter of the protected area and is not to be used for any operational activities which could potentially interfere with alarm response functions. All alarms must be self-checking and indicate the type and location of any break or malfunction. The CAS is, itself, considered a vital area.

Each security officer is required to carry communications equipment capable of continuous communication with the CAS and SAS which, in turn, are required to be capable of telephone and radio communication with other personnel and local law enforcement agencies. All communications equipment must be operable from independent power sources.

The licensee is required to establish test and maintenance procedures for all security related equipment. For example, each intrusion alarm must be tested a minimum of once every seven days and all communications equipment tested at the beginning of every shift. Redundancy in security equipment is required:

> "The licensee shall develop and employ compensatory measures including equipment, additional security personnel and specific procedures to assure that the effectiveness of the security system is not reduced by failure or other contingencies affecting the operation of the security related equipment or structures."

In addition, it is required that all alarms be maintained in operable conditions at all times. While this is not possible, it indicates that all maintenance procedures be of high integrity and repair activities carried out immediately.

An annual internal review of all security procedures, testing and maintenance programs, local law enforcement response plans, and the effectiveness of the physical protection system is required. The individuals conducting the review must be independent of both management and security supervision. The review itself must be documented and delivered to licensee management at least one level higher than that having day-to-day responsibility for plant operations. These reviews are to be kept available for NRC inspection for a minimum of five years.

The licensee is required to be capable of a minimum response capability as outlined in the regulations. "Safeguards contingency plans" are required and the necessary contents are outlined in 10 CFR 73, Appendix C. The licensee must also establish and fully document liaison with local law enforcement agencies. At least ten armed, trained personnel must be onsite at all times including at

least five uniformed security officers. Some licensees have trained and armed non-security (operational) personnel for the purpose of meeting this requirement while minimizing the number of uniformed security officers needed.

If an intrusion does occur the licensee is required to determine the existence of the threat, assess its extent, and neutralize it if necessary. Security officers are required to "interpose themselves between vital areas and... any adversary attempting entry for the purpose of radiological sabotage..." and simultaneously inform the local law enforcement agencies of the threat and request assistance. The level of force authorized by NRC to prevent radiological sabotage is:

> "force sufficient to counter the force directed at him (the responding officer) including the use of deadly force when the guard or other armed response person has a reasonable belief it is necessary in self-defense or in the defense of others.

The CAS is required to have remote means of detection and assessment of threats, such as closed circuit (CC) TV, in order to minimize security personnel exposure to dangerous threats.

1.2 NRC Regulatory Guide 1.17 - "Protection of Nuclear Power Plants Against Industrial Sabotage" - 1973

Regulatory Guides are published by the Government to describe and make available to the public methods acceptable to NRC in implementing parts of the Commission's regulations and to provide general guidance to licensees. Methods and solutions different from those set out in Regulatory Guides are acceptable if they provide an equivalent level of protection.

Regulatory Guide 1.17, published in June 1973, has 3 major sections including an introduction, discussion, and regulatory position. The introduction describes the need for a physical security plan and states that the Advisory Committee on Reactor Safeguards has concurrred in the regulatory position outlined. The discussion is principally on the ANSI standard which is described in the next section. The discussion specifically endorses the ANSI standard as a means for satisfying NRC requirements.

The regulatory position section presents supplements to the ANSI standard recommendations necessary to assure regulatory compliance. Security forces are required to be on-site to protect facilities, and all security alarms are required to annunciate in a continuously manned alarm station. All security equipment except communications equipment must be tested weekly. Communications equipment is checked every shift. The regulatory position also stresses the need to protect vital areas in such a way as to reveal unintentional acts as well as intentional acts. It also stipulates that details of physical security plans for specific sites will be withheld from the public.

1.3 ANSI/ANS 3.3

As discussed above, the ANSI standard issued in 1973 was outmoded by the promulgation of 10 CFR 73.55 in 1977. The Standards Committee of the American

Nuclear Society developed the new standard which was issued in 1982 to comply with the 1977 regulations.

This document outlines appropriate security plans, plant design, and facility requirements. The introduction states the philosophy that security plans must be designed very site-specifically so that recommendations must be balanced against the unique needs of each plant. It goes on to state that same threat as the regulations (10 CFR 73.1(a)).

The security program must be tailored closely to the unique characteristics of each site. The standard uses the same requirements as the regulations in terms of what should be in the contingency plans but further defines the management system which is more generally required in the regulations. It states that the plant manager (or designee) should have full authority over ant security in the case of an emergency. Day-to-day security is to be handl by "security specialists" who must be responsible for:

(1) formulation of hiring policy for security force personnel (by contract or as employees of the owner organization);

(2) formulation of general owner organization policy for the security force;

(3) liaison with appropriate law enforcement agencies;

(4) formulation of the required security personnel training and qualification program;

(5) establishment of a recordskeeping system;

(6) establishment of reporting requirements;

(7) investigation of security violations;

(8) establishment of a sensitive security document control system.

The plant design section emphasizes that design planning should begin at the outset of construction in order to take advantage of design changes which could be considered at that stage. The standard recommends that a particular individual be designated as responsible for security design reviews throughout construction. It recommends that vital areas be clustered where possible inside the same protected area, that isolation zones be 20 feet or both sides of the barrier and that all weather roads and walkways be used. Vital areas should be designed with security in mind but other considerations are recognized (i.e. environmental hazards, ease of maintenance, minimization of piping and wiring interconnections, and functional requirements such as pump submergence.) When considerations other than security dictate design security measures must be taken in addition to those recommended in the standard. The standard goes on to recommend that all non-safety related activities be, to as great as extent as possible, adjacent to, rather than in vital areas. Entrances to vital areas should be minimized to those necessary for safe evacuation. Lastly, plant design for security purposes should not be disseminated and, further, withheld from public disclosure in most cases.

The facility requirement in this standard are divided into four sections. Those are personnel, plant layout and physical structures, physical equipment and hardware, and procedures.

1.3.1. Personnel

This section states that the owner organization (licensee) is responsible for confirming the acceptability of selection, training and equipping the security force. Armed response personnel are required but personnel manning alarm stations are not to be considered response personnel. Guidelines for staffing state that there should always be nominally ten armed response personnel available at any time of which 5 must be uniformed guards. Consideration which can be used to lower this number from 10 are:

(1) site considerations which enhance physical protection;

(2) location and reliability of intrusion detection devices;

(3) local law enforcement response capabilities;

(4) vital area hardening;

(5) protected area barrier design and construction;

(6) other demonstrated capability.

Qualification requirements should be designed to comply with 10 CFR 73.55 Appendix B "General Criteria for Security Personnel" and screened according to a process set forth in the procedures section (below). A "Training and Qualification Plan" is required (as in the regulations, 10 CFR 73.55(b)(4)) and requalification every 12 months is to be included in the plan.

1.3.2. Plant Layout and Physical Structures

The size of openings in barriers other than doors is layed out (not to exceed 96 square inches.) The standard goes on to define "owner-controlled area," "protected areas" and "vital areas." These definitions are in line with those of the regulations.

1.3.3. Security Equipment

Detection aids and alarms are required for all protected and vital areas all capable of detecting a penetration when it occurs and annunciating in a central alarm station (CAS) and secondary alarm station (SAS). The CAS and SAS operator must acknowledge and reset any alarm. The entire alarm system must be self-checking and tamper indicating. Exterior illumination and surveillance system requirements are the same as those in the regulations.

Access control equipment is required including search equipment (metal and explosive detectors), package inspection systems, various lock types (key, combination, electric, card-key, etc.). Emergency egress is allowed with panic

hardware and emergency access allowed with a mechanical lock and key override of automated access controls.

Communications equipment must be two-way voice with at least two-channel transmission. All antennas are to be located in the protected area. Hardwire communication between the CAS and local law enforcement agencies must be mentioned. The central room and both alarm stations must all have redundant inter-communication modes.

Weapons, uniforms, and badges are required as in the regulations. Back up electrical sources are required for communications systems and intrusion alarms which are capable of supplying sufficient electricity for 24 hours of off-site loss of power.

1.3.4. Procedures

The part of this standard on procedures is lengthy and comprehensive. Since human factors play a dominant role in human performance of and adherence to procedures this section is reviewed in some depth.

1.3.4.1. Protected and Vital Area Access Controls

Unescorted access to these areas is to be granted only to authorized individuals and vehicles. If an access control point is manned and is the last control point before access the station must be bullet-resistant. All personnel must display badges inside these areas.

All locks and combinations must be controlled and changed upon either, evidence of compromise or termination of an authorized individual under adverse circumstances. As stated in the regulations, access to vital areas must be allowed only to perform specific duties -- not for familiarization.

During special operations (i.e. refuelling, maintenance) a guard or watchman must be assigned to all access points.

Personnel searches are required as in the regulations. If appropriate remote sensors are not available, pat-down searches and disrobing are recommended. Individuals authorized to have regular access are to be searched only by metal detectors. Individuals authorized for a specific access are to be searched for explosives as well.

All packages and materials entering these areas must be checked for proper identification and authorization. If entering vital areas search must be prior to entry. Unpackaged bulk deliveries (i.e. concrete, oil, etc.) must be off loaded in the presence of a guard or watchman.

All vehicles, except emergency vehicles, must be fully searched for items suitable for sabotage. All emergency vehicles must be escorted. During special operations a special security plan must be developed and approved.

1.3.4.2. Communications

All guards and watchmen must be capable of continuous communication with the CAS and SAS. Procedures for communication with local law enforcement agencies must be maintained. Procedures must also be established for inter-force communication between a plant under construction and the operating plant on the same site.

1.3.4.3. Contingencies and Response

A contingency plan, as outlined in the regulations, is required. Upon detection of an intrusion the security organization must

(1) determine whether or not a threat exists;

(2) assess the extent of the threat, if any;

(3) require guards to interpose themselves between vital areas and any adversary attempting entry to prevent or delay an act or radiological sabotage by applying a sufficient degree of force to counter that degree of force directed at them;

(4) inform the plant management;

(5) inform the local law enforcement agencies of the threat and request assistance, as necessary.

The liaison agreement with local law enforcement agencies must be documented and updated as appropriate, must designate the responsible individuals, and state the levels of support these agencies can provide in what time frame. Tours of the site and meetings are recommended for off-site agency personnel.

The use of force must be addressed in the contingency plan and policies established consistent with state and local use of force laws. Procedures for testing and maintenance of security equipment must be documented and implemented. These procedures must include a minimum of weekly testing of all intrusion sensors and alarms. Special purpose detectors, such as metal detectors, must be tested at the beginning of every shift and calibrated according to manufacturer standards. Communications systems must be tested every shift and off-site communications tested daily. Compensatory measures must be outlined in these procedures for dealing with equipment which is not operable.

1.3.4.4. Access Authorization

Each licensee must establish a screening program for employees of the security organization. An applicant must be apprised of the scope and purpose of the investigation prior to its initiation. The background check is to include investigation of prior employment, education, criminal record, and references. These sources must establish that the individual has a reputation in terms of reliability and trustworthiness which is acceptable for determining whether to grant access authorization. The discovery of will omission or false statements, use of nonprescribed drugs or alcohol abuse, criminal conviction,

history of mental illness, existence of coercion which may be applied to the applicant, or other derogatory information can lead to a negative determination. The determination will initially be made by the plant manager or designee on the recommendationfrom responsible plant management personnel.

Psychological evaluation before granting access authorization and continued observation after granting access is also required. The psychological evaluation must be indicated by the results of a "reliable and valid written personality test or other professionally accepted clinical assessment procedure administered by a licensed psychologist or psychiatrist cognizant of this standard." A program for continued observation of authorized individuals must be established by the licensee. Supervisory personnel are instructed to recognize unusual behavior are required to observe performance, attendance and attitudes of employees and report to plant management if unusual behavior is observed.

Each authorized individual is required to have a tamper-resistant picture badge or an automatic device reading fingerprints or hand geometry must be used to allow access. All persons with unescorted access must be trained, and annually retrained, on those matters for which the individual has responsibility.

1.3.4.5. Security Force Duties

The generic duties of the security force are:

(1) control access to the protected and vital areas;

(2) escort individuals not authorized for unescorted access and nondesignated vehicles within the protected and vital areas;

(3) patrol exterior areas within the protected area via random routes at irregular intervals, but at a frequency of at least once every four hours;

(4) operate the central alarm station;

(5) respond to threats.

The ability of safeguards personnel to execute these tasks must be demonstrated in a manner set forth in the Training and Qualification Plan. Inquiries directed to NRC staff responsible for reviewing these plans have shown that these plans rarely contain a comprehensive description, but rather a generic assessment of critical tasks and the conditions and standards under which they will be tested. Actual details of drills on performance evaluation techniques are not usually provided to NRC for review.

Written procedures must include:
bomb or other overt threats;
civil disturbances;
communications;
employee security training;
security force duties and responsibilities;
incoming package and material control;

intrusion alarm response;
lock and key control;
patrol;
personnel identification;
access control;
vehicle traffic and parking control;
surveillance requirements;
testing and maintenance of security systems;
reporting requirements;
security during opeational emergencies;
support from and orientation of law enforcement agencies;
security during construction, maintenance and refueling outages.

The security force must provide individuals as escorts who are familiar with escort responsibilities whenever unscreened individuals are allowed in to the protected or vital areas.

Audits and Reviews

Each licensee must establish and maintain an audit system to review the site security program at least annually. It must compare security effectiveness being attained by personnel, hardware, and equipment in comparison to that specified in the security plan. These audits must be of sufficient depth to ensure compliance.

Records of security equipment must be maintained for the life of the equipment, for individuals whose access authorization is termined for one year, for maintenance, testing, training and personnel testing for five years, and all other records for one year. The record system must include:

(1) documenting maintenance actions performed on physical barriers, intrusion alarms, communication equipment and other security-related equipment;

(2) documenting security tours and inspections;

(3) documenting all tests or inspections performed on physical barriers, intrusion alarms, communications equipment and other security-related equipment;

(4) recording each alarm, alarm check and tamper indication identifying type of alarm, location, date and time;

(5) recording details of the response by facility guards, watchmen and, if applicable, armed response individuals to each alarm, intrusion or other security incident;

(6) recording of persons who have been authorized unescorted access to a protected area;

(7) recording of persons authorized access to vital areas;

(8) recording of name, badge number, time of entry, and time of exit from normally unoccupied vital areas;

(9) recording of visitors, vendors and other individuals who have been granted access with escort to the protected area, including name, address, date, time, purpose of visit, employment affiliation, citizenship, and name of individual to be visited;

(10) recording of access to keys, combinations and other related equipment;

(11) recording of personnel screening.

NRC FORM 335 (6 83) U S NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1 REPORT NUMBER (Assigned by TIDC and Vol No if any)
NUREG/CR-3520
BNL-NUREG-51718
Vol. II

2 Leave blank

3 TITLE AND SUBTITLE
Long-Term Research Plan for Human Factors Affecting Safeguards at Nuclear Power Plants, Volume II: Development of Detailed Analyses

4 RECIPIENT'S ACCESSION NUMBER

5 DATE REPORT COMPLETED
MONTH: February YEAR: 1984

6 AUTHOR(S)
John N. O'Brien and Anthony Fainberg

7 DATE REPORT ISSUED
MONTH: April YEAR: 1984

8 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Department of Nuclear Energy
Brookhaven National Laboratory
Upton, NY 11973

9 PROJECT/TASK/WORK UNIT NUMBER

10 FIN NUMBER
A-3260

11 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Human Factors and Safeguards Branch
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

12a TYPE OF REPORT
Formal

12b PERIOD COVERED (Inclusive dates)

13 SUPPLEMENTARY NOTES

14 ABSTRACT (200 words or less)

The first task was to identify and rank human factors affecting the quality of nuclear power plant safeguards in terms of their importance. The opinions of over 85 experts were solicited and 28 responses were received. These responses were rigorously analyzed to ascertain what human factors could be considered important to power plant safeguards. In addition, the Safeguards Summary List (NUREG-0525) was systematically analyzed for human factors influences. Also, relevant government and industry literature was reviewed. These data sources were ther aggregated and an overall importance ranking of human factors issues was developed. This part of the research effort is fully documented and described in Chapter 2 of Volume II.

The second part of this effort involved determining the feasibility of conducting research in the areas found to be important to power plant safeguards. A determination of research feasibility was based on the practicality, usefulness, and acceptability of conducting research and using the results in a regulatory context. This part of the effort is fully documented in Chapter 3 of Volume II.

Research efforts addressing human factors in safeguards were then developed and prioritized according to the importance of human factors areas derived in the first part of the study and the feasibility of research determined in the second part. Research was also grouped to take advantage of common research approaches and data sources where appropriate. Chapter 4 of Volume II details the development of methodological groupings for optimizing resource use.

15a KEY WORDS AND DOCUMENT ANALYSIS
Safeguards, Security, Human Factors
Training Evaluation, Organization,
Man-Machine Interface, Trustworthiness
Human Reliability

15b DESCRIPTORS

16 AVAILABILITY STATEMENT
Unlimited

17 SECURITY CLASSIFICATION (This report)
Unclassified

18 NUMBER OF PAGES

19 SECURITY CLASSIFICATION (This page)
Unclassified

20 PRICE
$